APRIL 2025

Automation.com MONTHLY

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

InTech IS NOW Automation.com Monthly!

How to Create a Sustainable Industrial Security Program

- A Cybersecurity Framework for OT
- How to Secure Network Traffic
- Security for IIoT and Remote Operations
- Solutions for SCADA Access Control
- OPC for Secure Alarm Integration
- Threat-Hunting in OT Infrastructure

A MESSAGE FROM ISA

The International Society of Automation (ISA) is a non-profit professional association whose vision is to create a better world through automation by driving the advancement of individual careers and the overall profession. ISA owns Automation.com, a leading online publisher of automation-related content.

This digital magazine, *Automation.com Monthly*, is one way ISA fulfills its mission of empowering the global automation community through standards and knowledge sharing. The magazine is published nine times per year. ISA members receive the magazine as part of their annual membership and get access to archived magazine issues, including *InTech* and *AUTOMATION 202X*. Qualified non-members can subscribe to the magazine and other publications.

ISA helps its members and the global automation community advance technical competence by delivering standards-based technical resources to engineers, technicians, and management engaged in industrial automation. ISA develops widely used global standards; certifies professionals; provides education and training; hosts conferences and exhibits; publishes technical articles and other resources; and provides networking and career development programs.

ISA created the ISA Global Cybersecurity Alliance (isagca.org) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. Through a wholly-owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (isasecure.org) and the ISA Wireless Compliance Institute (isa100wci.org).

Mimo: A Large-Language Model Educated on ISA Content
Ask Mimo your questions about industrial automation at https://www.isa.org/mimo

ISA Connect https://connect.isa.org/home

company/internationalsocietyofautomation

InternationalSocietyOfAutomation

Editorial and advertising offices are located at 3252 S. Miami Boulevard, Suite 102, Durham, NC 27703 USA. Phone: 919-549-8411 Email: info@isa.org

ISA | Automation.com MONTHLY

InTech IS NOW Automation.com Monthly!

APRIL 2025 | VOL 1, ISSUE 3

Automation.com MONTHLY
APRIL 2025

A MESSAGE ABOUT OUR SPONSORS

ISA's mission and *Automation.com Monthly* digital magazine are supported by advertisers and sponsors. They contribute technical articles, case histories and other technical resources designed to educate, inform and inspire automation professionals and advance their careers. Articles from advertisers are identified with a "Sponsored" tag.

To obtain further information from any of the advertisers in this issue, contact them directly using the information found in their ad or author bio.

For news and product information from suppliers, visit Automation.com. The online directory of Featured Suppliers lists automation product vendors, machine manufacturers and systems integrators. You can also subscribe to topical newsletters and alerts that will deliver news, new product and technical resources via email.

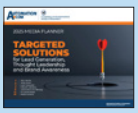
A Note to Potential Advertisers

With decades of experience crafting high-quality periodicals, the International Society of Automation (ISA) and its media brand Automation.com have helped thousands of automation and control professionals do their jobs and enhance their careers. We can help you inform these professionals about your solutions through our publications, events and sponsorship opportunities.

ADVERTISING & SPONSORSHIP

Rick Zabel, PUBLISHER - rzabel@isa.org
Ed Manns, SALES MANAGER - emanns@isa.org
Chris Nelson, MANAGER, ADVERTISING SALES & SPONSORSHIP - chris@isa.org
Gina DiFrancesco, ACCOUNT EXECUTIVE - gina@isa.org

Send press releases to **Press@automation.com**
Send ad materials to **Materials@automation.com**



2025 Media Planner

To order reprints of digital articles, contact reprints@mossbergco.com or 800-428-3340.

Advertisers Index

AXIOMTEK

Level Up Your

OT Security

Bring network security to the next level with
Axiomtek's certified industrial OT systems

iNA200

ICO & iNA Series

C1D2 · EN 50121-4 · Ex ZONE2 · EN50121-4

The ideal solutions for OT field site cybersecurity and secured edge applications.

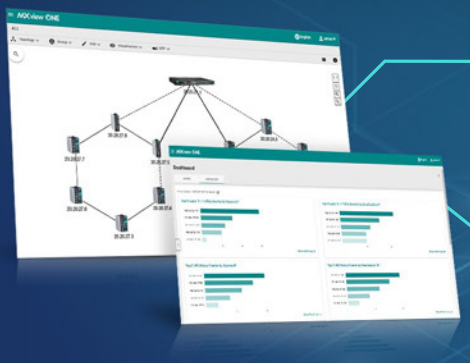
Featuring the iNA200 DIN-Rail Cybersecurity Gateway
with Intel Atom® x6212RE/x6414RE Processor and up to 6 LAN.

intel ATOM

us.axiomtek.com info@axiomtek.com **Axiomtek Co., Ltd.**

Visualize Industrial Network Security with Moxa

Click or Scan to Learn More



MXview One Series

Industrial Network Management Software

MXview Security

MXview One Add-on for Industrial Network Security Management

Moxa's secure networking solutions deliver industrial-grade protection with IEC 62443-certified devices and centralized security management. Build a resilient foundation for IT/OT convergence with layered defense and full network visibility.

Connect with us

+1-888-MOXA-USA
+1-714-528-6777
info.us@moxa.com
www.moxa.com

MOXA®

How to Build a Sustainable Industrial Security Program

Follow all seven steps to ensure your automation and control system is secure.

By Chris McLaughlin

Many organizations struggle to get their industrial security programs started or have programs that really aren't working well. An industrial security program takes time and requires the organization's full attention. Because information technology (IT) and operational technology (OT) teams often have different skills and perspectives, industrial security programs can fail. I believe that there are ways to address this issue and get a program back on track.

Here are seven steps that I believe every organization should take to establish an Industrial security program. I often see companies focusing on one or two of these steps, but potentially overlooking others, which can negatively impact progress.

1 Step 1: Admit that you have a problem

Admitting that an organization has a problem is the first step to solving it. Many security programs skip this step, assuming that cybersecurity risks are obvious to everyone. The problem is that most people link cyber risks to high-profile public breaches of corporate systems. Business email compromises (BEC) or ransomware attacks are in the news every day, however, industrial system attacks are rarely disclosed.

Tabletop exercises that simulate real cyber incidents have become standard practice for most IT security programs. However, these exercises typically concentrate on corporate-level events such as a breach of HR systems or a ransomware attack. Conduct tabletop exercises that focus on industrial assets such as manufacturing lines to effectively engage leadership and enhance awareness regarding operational technology risks.

To fully understand the company's risks, I recommend that organizations engage operations leaders, plant managers and engineering teams in at least one industrial security tabletop exercise. The exercise should focus on a critical industrial asset. Begin the discussion using an example of a significant, but plausible, cyber event affecting an industrial asset.

A typical industrial tabletop might look like this:

- An engineering integrator has connected a laptop to a critical production line, introducing malware. Even if the company believes it has controls in place to prevent this, this scenario is realistic and can happen.
- Malware then spreads to all Windows-based computers within the asset, including industrial HMIs, servers and workstations, causing them to become unrecoverable.

At this point, it's important to keep things simple. Here are some key questions that should be discussed:

- What impact would this event have on the business?
- Could the asset be restored from backups? How reliable are the backup systems? What would happen if the backups were sabotaged?
- If all Windows computers get infected, can the industrial process safely implement a shutdown?
- Could this event impact safety?

Use this tabletop to engage key leaders and gain their support for the program. Keep discussions at a high level and limit tabletops to one or two hours. Ensure the conversation stays focused and postpone follow-up discussions for later.

Conduct tabletop exercises that focus on industrial assets such as manufacturing lines to effectively engage leadership and enhance awareness regarding operational technology risks.

2 Step 2: Hire a translator

Tension between OT and IT in organizations can hinder industrial security programs. This is often because each field has specialized skills and a lack of mutual understanding, leading to communication breakdowns. Many organizations have stories about how actions by one side caused issues for the other, fostering and spreading mistrust.

Engineers will usually have stories about IT disrupting systems that negatively affected production, feeling that IT did not understand the environment. Conversely, IT professionals will have examples where industrial failures occurred due to an engineer's lack of networking or server knowledge, calling in IT for last-minute fixes.

To establish a meaningful dialogue between IT and OT, the industrial security program needs to get an OT translator. OT security programs are often led by IT security teams, but few IT professionals really understand OT. Including someone from OT can add credibility to the program and facilitate better communication.

There are a few tactics that I have seen work for organizations.

- **Recruit internally:** If there is a strong engineer in the organization who can be brought into the program, this may be the best choice. The OT translator doesn't need to be a security person, but should have a good foundation in IT and a passion for learning.
- **Hire:** Hire an engineer from outside the organization who can bring in new ideas and the necessary skills. Look for someone with strong communication skills and experience in industrial security. Resources with a strong mix of industrial controls, IT and security are rare, so the organization may need to make concessions.
- **Borrow:** In many cases, it may be helpful to use a consulting group that has experience in industrial security. This experience will help build the foundation for the program while the team develops its own internal OT/IT capabilities.

3 Step 3: Understand critical business and OT processes

Once the business has demonstrated support for the effort and an OT translator is in place, the next step is to understand the organization's industrial processes. If multiple processes exist, begin with an industrial process that is perceived to have a large impact on the organization.

To gain a better understanding, it is helpful to see the process firsthand. Take a plant tour that focuses on the overall manufacturing process and the role that the control system plays in that process. It is not necessary to know every detail of the process, however, the team should focus on essential components and systems. Here are some crucial questions to cover on the tour.

- What is the goal of the manufacturing process?

- How is the system controlled to prevent safety issues?
- What are the most critical systems in the process?
- What happens if this system fails?
- Are there other critical control systems that are required for regulatory requirements?
- Who has access to these systems and how are they accessed? Do employees or third parties access this system remotely for implementation, maintenance or support?

With this information in hand, the industrial security program can start to prioritize the next steps.

4 Step 4: Understand your OT assets

Some IT security experts suggest an asset inventory should be the first step in a program, however, I have placed this as the fourth. While inventory is important, completing the first three steps can help the team better understand the inventory and the impact systems have on the process.

Organizations sometimes purchase tools to help them identify assets and vulnerabilities before they understand the context of the process and technology supporting it. This can cause programs to focus on the wrong assets and the wrong priorities.

Open-source tools, which are often free, can be sufficient for many organizations while establishing the first high level inventory. Purchased tools, however, can significantly reduce the effort required to create an inventory. They may often do it with greater precision. These automated tools can be used after the inventory process has been completed and can help the organization monitor changes to the environment.

The OT translator may be able to help the team safely connect inventory tools to OT networks and should be able to help interpret scan results. Some purchased tools are passive and can only view network traffic. These systems may be a lower risk as they are unlikely to negatively interact with production systems. Others are active and may require software on industrial system computers or may generate network traffic that could be disruptive. Whichever approach is taken, it is crucial to exercise extreme caution to ensure that any asset management tool keeps operations safe.

The OT translator may be able to help the team safely connect inventory tools to OT networks and should be able to help interpret scan results.

The ISA/IEC 62443 series of standards is a great resource for organizations during this phase and is the de facto standard for industrial security. This series of standards provides guidance on evaluating industrial system risk. One of the key deliverables for this step will be to diagram the current system in terms of zones and conduits. The

ISA/IEC 62443 series provides guidance on these concepts and helpful information for conducting the initial risk assessment.

The purpose of this step is to prioritize your efforts and identify critical assets that should be included in your program.

Step 5: Add value

Security programs usually focus on reducing risks, but it is important to show OT teams value beyond cyber risk reduction. If OT teams see additional value from the industrial security team's initiatives, then they are much more likely to fully engage. Here are a few areas where an industrial security program can provide value to OT Teams.

System backup and failover review. Conduct a thorough review of critical systems to ensure that system backups are being performed and failover mechanisms are operating correctly. It is common for system integrators to implement a backup system or redundant server solutions during initial installations; however, these may not be properly maintained over time. Identifying and addressing these issues promptly can help the plant avoid costly outages.

Virtualization. System implementations have used virtualization technology like VMware frequently. There is a great deal of value to these systems, however, many integrators lack experience in deploying these environments, and OT staff usually have little experience managing them. The team should review these environments for performance, reliability, or security enhancements. Ensure compliance with industrial system manufacturer requirements before making recommendations and rigorously test any changes.

Investment support. The inventory can highlight risky assets that the OT team has been unable to get funding for. The program team may have more experience in describing the risks of old IT systems to management.

Once the industrial security program starts to add value to the OT team, greater collaboration will follow.

Step 6: Implement an OT governance program

Security frameworks are an essential foundation for any security program. Fundamentally, most IT organizations adhere to a security framework with the most common being ISO 27001 or NIST 800-53. Each of these frameworks provides a consistent approach to address security. For industrial security, the gold standard is the ISA/IEC 62443 series. The 62443 industrial security standards can either complement an existing security framework or be implemented independently if no IT security framework is in place.

For anyone interested in learning about 62443, start with ISA-62443 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models. This standard offers a good overview of the framework, and the ISA provides online training to help gain a deeper understanding.

Next, review Part 2-1: Security program requirements for IACS asset owners. This standard includes essential program-level requirements that are essential to a program. For those familiar with the ISO 27000 series of standards, this standard is similar to ISO 27002 in that it defines specific requirements and guidance, but for industrial security.

Some requirements of 62443 2-1 overlap with traditional cybersecurity frameworks, but many are unique to industrial security. ISA 62243 2-1 also includes mappings to traditional frameworks such as ISO and NIST, so there won't be duplicate efforts.

7 Step 7: Keep it real

Now that the security program is in place and the OT-IT partnership is established, it's crucial to engage all industrial employees, including operators, maintenance firms and contractors, into the program.

Companies with industrial systems likely prioritize safety as a fundamental company value. Industrial security programs should include the message of security and safety to strengthen their message. Like safety, take time to talk to employees about security and the impact that it can have on them.

Security threats will continue to evolve, so employees must understand how their decisions can help maintain a safe and secure environment. To effectively engage employees, awareness training should ensure employees understand not only what steps to take but also why they are taking those steps. Real examples can help employees understand negative consequences and how their actions could avoid them.

The relationship between IT and OT is a critical foundation that any industrial program should nourish. When IT and OT work together and appreciate each other's strengths, they can create a solid security framework that tackles the unique challenges of industrial environments.

ABOUT THE AUTHOR

Chris McLaughlin is a frequent speaker on OT cybersecurity topics and the ISA/IEC 62443 standard. McLaughlin is the chief information security officer at Johns Manville, a Berkshire Hathaway Company, in Denver, Colorado. He welcomes reader feedback and questions. McLaughlin will be speaking at ISA's OT Cybersecurity Summit in Brussels, Belgium 18-21 June 2025. Find out more and register at https://otcs.isa.org/

MOORE INDUSTRIES
WORLDWIDE
Demand Moore Reliability

Need a Hand with Protecting Your Process?

Keep Your Process and Plant Safe With FS Functional Safety Series Instruments From Moore Industries

Designed and built from the ground up to meet IEC 61508 standards, Moore Industries FS Functional Safety Series instruments help bring the confidence you need to your SIS implementation. Our FS Series now includes the easily programmable, SIL 3 capable SLA Multiloop Safety Logic Solver and Alarm, with voting and powerful built-in math & logic capability.

Keep it Safe by Learning Moore about our FS Series Solutions
Call 800-999-2900 or visit www.miinet.com/fs-automation

Production processes, above all, must be safe, reliable and efficient. With our level and pressure measurement technology, you get exactly that. Durable sensors and accurate measured values make your work smarter, easier and more sustainable.

Everything is possible. With VEGA.

vega.com

VEGA HOME OF VALUES

A Cybersecurity Framework for Operational Technology

By Ariel Lee

A resilient, proactive framework can protect critical industrial infrastructure.

Industrial operations are becoming increasingly interconnected, bridging once-isolated operational technology (OT) and information technology (IT) systems to deliver unprecedented levels of efficiency, real-time data access and granular control across a wide range of sectors such as oil and gas, energy, manufacturing, transportation and smart city technology. While these advances exponentially improve operational efficiency, they also introduce additional vulnerabilities into critical infrastructure, where a single breach can halt production, disrupt supply chains and even threaten public safety.

As both the modern industrial landscape and security threats evolve, it is no surprise that the OT security market is forecast to grow at a 16.30 percent CAGR from 2024 to 2030. Organizations must adopt a comprehensive OT cybersecurity framework that is both

resilient and proactive, integrating robust hardware, intelligent software and industry-specific best practices. Such an approach anticipates emerging threats while prioritizing risk management, allowing businesses to reinforce their growing operations and protect vital infrastructure. Building such a framework will present both challenges and opportunities.

A successful OT cybersecurity strategy must address stringent requirements that vary across diverse industries. Sectors such as oil and gas, energy, power utilities and railways often require rugged, reliable equipment that meets specific safety and durability standards. Within these industries are several core challenges. These include certifications, redundancy and recovery.

Certifications for safety and stability. Safety and trusted platforms are of paramount concern, requiring resilient designs that can endure conditions such as extreme temperatures and explosive risks. For instance, oil and gas operators must secure anti-explosion compliance through standards like ATEX/C1D2, and electric vehicle charging stations must adhere to Underwriters Laboratories (UL) and National Electrical Code (NEC) safety standards.

Power utility operators often rely on IEC61850-3 and IEEE 1613 certifications to ensure that systems can withstand electromagnetic interference and other harmful conditions, while railway organizations maintain EN 50121-4 compliance to ensure stability and reduce the risk of wayside signal disruption.

Stability in target application fields is equally essential, as operational continuity depends on robust structures that withstand wide operating temperature ranges and electrical fluctuations. Surge protection and isolated power elements are necessary to prevent downtime in remote or outdoor installations where equipment can be exposed to volatile conditions.

The newest hardware and software advances enable the integration of artificial intelligence directly into cybersecurity architecture and OT devices in the field, supporting real-time threat detection, behavioral monitoring and vulnerability management.

Redundancy. Another challenge is ensuring redundancy in OT environments to safeguard against the consequences of unplanned outages. Dual power inputs and LAN bypass capabilities serve as insurance against unexpected failures, allowing redundant systems to seamlessly take over if a primary system malfunctions, and thereby reducing disruption.

Recovery. Reliable recovery processes are likewise indispensable in the case of failure due to malicious activity or simple human error. Automated remediation for BIOS,

firmware, and operating systems minimizes interruption and the associated economic or safety consequences by allowing systems to rebound swiftly.

Amid these challenges, edge AI solutions present valuable opportunities throughout OT security. The newest hardware and software advances enable the integration of artificial intelligence directly into cybersecurity architecture and OT devices in the field, supporting real-time threat detection, behavioral monitoring and vulnerability management. These techniques can identify even subtle deviations from normal patterns, which is essential in identifying malicious intrusions or anomalies before they escalate.

Platforms optimized for AI workloads allow operators to conduct large-scale data processing and analysis at the edge, rather than offloading everything to a central data center. This distributed approach accelerates the response to threats and lowers latency.

As AI grows more sophisticated, it helps optimize security software to run efficiently and accurately with hardware processors and NPUs, complementing existing certifications and redundancy features.

By deploying certified products and using a proactive cybersecurity defense model that evolves alongside emerging threats, organizations can significantly lower the likelihood of unsafe conditions, physical damage and catastrophic incidents arising from failures or targeted attacks.

How to integrate IoT devices securely

When integrating IoT devices into OT environments, it is crucial to consider a holistic, layered approach that weaves cybersecurity principles into both hardware and software in concert. This integrated method ensures that organizations can manage countless endpoints ranging from sensors and controllers to gateways and servers while maintaining consistent security.

As digital transformation increasingly extends into the operational landscape, a mismatch between IoT device security and overarching OT requirements can introduce or exacerbate vulnerabilities and weaken an organization's overall resilience.

One essential consideration is endpoint security. A zero-trust approach in which every device and user must continuously verify identity, and authorization helps impede the spread of threats across interconnected systems. In a similar vein, identity and access management (IAM) restricts access to critical systems based on the level of privileges a user holds, lowering the possibility of inadvertent or intentional misuse.

Another equally significant element of endpoint security is maintaining asset visibility through continuous monitoring. By knowing every device on the network, operators can promptly detect unauthorized additions or suspicious activity that might indicate tampering.

A comprehensive disaster recovery and business continuity plan should also be in

place. Even a brief disruption in OT can trigger cascading operational and financial impacts, so swift restoration of normal operations is vital. To bolster prevention, advanced methods like deep packet inspection (DPI) provide insights into the content of network traffic, supporting early detection of malicious payloads. Meanwhile, next-generation firewalls (NGFWs) assist in monitoring and regulating data flow, applying dynamic rules that adapt to evolving threats and protect against intrusions.

Once these foundational requirements are established, organizations can further protect their field sites by enabling secure boot through the BIOS/UEFI and employing OS verification to confirm the integrity of each device during startup and ensure only authorized firmware and software are loaded.

Ongoing oversight of network traffic, device status and device behavior help detect deviations in real-time, while efficient reporting mechanisms escalate any irregularities and issue alerts for rapid human intervention or automated remediation. If a device's firmware or operating system becomes corrupted or crashes, rapid recovery methods help bring critical systems back online with minimal downtime. This tight interplay between proactive and reactive measures keeps operations running, protects sensitive assets and diminishes the overall risk profile.

Wrapping up

By blending certified hardware, advanced software and rigorous industry standards, organizations can develop OT cybersecurity frameworks that are robust enough for today's challenges while remaining adaptable to tomorrow's innovations. Adopting AI-driven detection, ensuring multi-layered security and developing resilient system designs connected by DIN-rail security gateways and certified devices can collectively provide the visibility and flexibility needed in complex operational settings. With the promise of ongoing technological progress, the ability to integrate these diverse elements securely underlines a commitment to both safety and long-term sustainability in industrial domains.

ABOUT THE AUTHOR

Ariel Lee is a marketing manager for Axiomtek USA, a provider of industrial PCs committed to advancing OT/IT infrastructure and emerging AI technologies. The company's U.S.-based design engineering and integration services, alongside its comprehensive ecosystem partners, empower the gateway and embedded system to bridge operational technology (OT) and information technology (IT), and ensure secure, high-performance computing for industrial automation, smart manufacturing, and edge AI applications.

ENGINEERED FOR PERFORMANCE.

DESIGNED FOR PROTECTION.

In high-risk environments, early flame detection is critical. Our advanced flame detectors are built to withstand extreme conditions while providing fast, reliable detection to help you safeguard people, assets, and operations. Designed with precision and tested for durability, our solutions support your safety strategy when every second counts.

Explore our flame detection solutions: msasafety.com/flame-detectors

MSA
The Safety Company

Software toolbox®

PROVEN SOLUTIONS | PLAN AHEAD | GET AHEAD | STAY AHEAD

Data Analytics Industry 4.0 UNS DataHub OPC UA

Sparkplug-B OPC Router MQTT IT/OT/ET Convergence

Productivity Tools SAP CUSTOM PROTOCOLS OmniServer

CONNECT EVERYTHING

Cyber Security Device Connectivity IoT & IIoT Industrial DataOps

Digital Transformation OPC Data Logger Decision Support Systems

TOP Server Tunneling Enterprise Connectivity

EDGE TO CLOUD

Flow Software

SCAN ME

SOFTWARETOOLBOX.COM

How to Secure Otherwise Insecure Network Traffic

SPAN port evolution and protocol interoperability enable OT continuous monitoring.

By Moreno Carullo

When the developers of Modbus began enabling communications from heterogeneous devices leveraging the RS-485 standard in 1979, it was off to the races for fieldbus communications interoperability. RS-485 defines the electrical characteristics of drivers and receivers used in serial communications systems to connect a wide range of controllers, sensors, instrumentation, PID controllers, motor drives and more. DeviceNet, Profibus, SERCOS, ASi, Foundation Fieldbus and HART followed suit—all of which remain unencrypted.

OPC UA (IEC 62541), a unifying technology that bridges industrial automation and modern computing technologies, serves as the background for the interoperability spawned by vendors and suppliers, industrial and enterprise software and, yes, cloud service technologies. OPC UA standards allow sensors to communicate with many types of controllers and devices to coordinate sensor data within a historian. This functionality allows enterprise layers to correlate process data with business functions without redundant software for translation. But how can all of this connectivity and data be networked and managed?

Hubs, switches and modern networking

Before network switches, hubs were the main way to interconnect Ethernet-based networks. A hub is a quite simple device that physically copies each packet from its source port to each destination port and connects them to a single hub in a multicast manner.

While cheap and simple, this technology does not scale well because even a small network with a low number of clients has many packets transferring between computers, causing too much traffic and potential spamming and jamming on the hub. For example, if a client behind port 1 was exchanging packets with a client behind port 10, in principle, only these two ports should have seen those packets.

The solution for this predicament was the introduction of Ethernet switches. A switch is more sophisticated than a hub, as its hardware can better understand and route packets on a local network. It can read the Ethernet layer (the first 14 bytes, 6x2 for the MAC addresses and 2 for the EtherType, stating the protocol of the next layer; e.g., IP), and some upper layers like ARP, and understand which MAC addresses are connected to each single port. With that, it builds what is called an ARP table and uses that to forward packets only to the right port(s), similar to the old switchboard used for telephone communications.

Broadcast packets, sent to all clients on a network, still require forwarding to all ports, but the switch remains a huge improvement compared to the all-speak-to-all situation that is a reality with early hub technology.

Modern network switches have adopted increased capabilities to deal with complex network design complexities like VLANs and QoS and can even do router-like jobs if defined as “Layer 3 switches,” where packets are routed to their default MAC address gateways. Layer 3 switches support virtual router redundancy protocol (VRRP) and open shortest path first (OSPF). VRRP provides automatic assignment. When a master router fails to connect, the backup router is automatically switched to the new master

router. OSPF is often used in large network-like substations; it can calculate the shortest route for data transmission and make the process more efficient.

All of the functions described above are designed to work at high speeds: originally at speeds of 10 Mbits, then 100 Mbits or 1,000 Mbits. Today, certain switches can operate at tens of gigabits. To achieve that, an ASIC (application specific integrated circuit) is usually employed. This hardware circuit is dedicated solely to the purposes of a switch, and while less flexible (it cannot be reprogrammed or used as a generic processing unit), it can transmit data at wire speed, where full gigabit traffic can be transmitted without packet loss and collision. Another CPU (Central Processing Unit) remains to orchestrate other functions, configuration, setup, etc.

SPAN ports enter the chat

SPAN (switched port analyzer) ports, also known as mirror ports, were originally introduced by Cisco to allow network engineers to troubleshoot network issues around switches. With hub technology, it was quite easy to understand what was going on in a network. All you needed to do was connect to a free port, and all packets flowing in that network were visible for inspection. But with switches, that is no longer possible.

A SPAN port is basically a configuration of one (or more) ports so that they can receive a copy of the traffic transferred on the switch, or in a specific VLAN, or on a set of ports. Nowadays, configurations are certainly more complex than in the beginning.

The beauty of SPAN port technology is that this capability is included in the ASIC unit discussed above; therefore, it does not affect network performance by eating into other tasks and services. For example, SPAN configurations will not cause the switch to drop packets on the other ports or introduce latency.

While there are no major concerns about performance when it comes to setting up SPAN ports, certain limitations can apply. Some older models may omit some packets to the SPAN port under certain situations, but the main and core functionalities of the switch won't introduce delays in its wire speed.

No impact on performance is observed when SPAN or mirror ports are used.

Enabling monitoring for OT/ICS networks

When my company began as one of the earliest companies dedicated to industrial cybersecurity network monitoring, an early milestone was to produce a third-party certified review of SPAN port technology. The report confirmed that no impact on performance is observed when SPAN or mirror ports are used.

In that test, different kinds of switches of different brands and prices were tested to show customers that it was not essential to upgrade to the latest and greatest brand and model to enable network monitoring capabilities and introduce cybersecurity tools and controls.

Industrial control system (ICS) environments, comprised largely of heterogeneous components with custom operating systems and network protocols, historically have had fewer cybersecurity tools designed to interrogate customized protocols and behaviors. This is especially true for areas of cyber-physical systems architecture closest to the field and input/output (I/O) devices. Customized sensors, installed at a SPAN or TAP port within the customer network, passively monitor raw network data in real time without disrupting business operations, which provides real-time visibility into all network activity and the ability to alert on vulnerabilities, potential attacks in progress and emerging anomalies.

Modern networking, SPAN port evolution and protocol interoperability paved the way for operational technology (OT) and ICS network monitoring and cybersecurity. Today, security solution providers have expanded their software capabilities to interrogate the analyzed traffic to include:

- complete database matching of known vulnerabilities and indicators of compromise
- deep packet inspection to analyze packet traffic, commands and connectivity
- threat intelligence feeds and
- machine learning engines to define baseline network traffic and alert on anomalies in communications and process variables.

Such third-party security offerings offer holistic security awareness where vendor-specific options cannot cover heterogeneous systems across an environment. They enable continuous monitoring of multi-vendor OT systems and help secure otherwise insecure network traffic.

ABOUT THE AUTHOR

Moreno Carullo is the technology expert behind Nozomi Networks industry-leading cybersecurity solution for industrial control networks. Armed with a Ph.D. in artificial intelligence, and an extensive background in systems engineering and software development, he has led the way in redefining the ICS cybersecurity product category.

Ensuring Cybersecurity for Remote Operations

Effective cybersecurity for remote industrial operations combines several complementary technologies and practices.

By Jack Smith

Remote access to plant floor machines saves manufacturers time and money. Instead of costly downtime waiting for engineers to arrive, remote access can resolve issues without needing an onsite engineer.

Remote monitoring is a necessity for today's global manufacturing operations, said Nick Shaw, vice president of product at Dragos. "There are numerous scenarios from remote diagnostics and maintenance to condition monitoring that enable predictive maintenance, acting as an enabler for large-scale distributed operations. Remote monitoring can also assist post-incident recovery to ensure that control is restored safely to operations," he said.

"Manufacturing plants with distributed facilities need centralized visibility into production metrics and equipment performance," said James Winebrenner, CEO at Elisity. "Critical infrastructure like power generation, water treatment and oil and gas pipelines demand 24/7 monitoring regardless of physical location. During unplanned events or emergencies, experts must quickly access systems without physical presence.

Predictive maintenance programs require continuous data collection from industrial equipment, while contract manufacturers and supply chain partners often need secure visibility into production processes. The COVID-19 pandemic accelerated this trend, establishing remote operations as a standard business continuity requirement rather than an exception."

The expertise to be able to troubleshoot issues and understand what's happening is not always onsite. "To me, the biggest use case is to be able to leverage offsite expertise within their own company from the other sites that may have experience to help drive issues," said Travis Cox, chief technology evangelist at Inductive Automation. "Users being able to see the data and understand what they're doing helps play a big role in that. Integrators are crucial to many projects for remote access."

Oil and gas pipelines also have remote infrastructure like compressor stations or pumping stations. "For gas, it's a compressor station, and for liquid, it's a pumping station. Water/wastewater facilities have similar assets. They are geographically distributed and need to connect remotely," said Gurvie Waraich, director of sales and marketing at Skkynet.

Remote operation risks

Remote operation can pose risks as it exposes the network to unauthorized individuals. It introduces several significant security risks to operational technology (OT) environments. "When you do remote access, you're opening [the network] to contractors and other third parties that can get access to your tools and link to data, disrupt processes and affect safety," said Cox. "There are many systems that use legacy protocols that weren't designed with security in mind."

Only the paranoid can survive. You must be paranoid about your information. You must be super hypervigilant about your privacy and data ownership because things are getting connected to the cloud.

Shaw often speaks about viewing risks through the lens of safety, productivity and quality. "Some of the biggest risks include exploitation of remote connections to gain control over critical systems, and once in an OT environment, an attacker could potentially pivot toward impact, such as causing physical damage or operational disruption of a process."

"Expanded network connectivity creates additional attack surfaces and potential entry points for threat actors," explained Winebrenner. "Legacy OT systems, often designed without built-in security controls, become exposed to modern cyber threats when connected to external networks. Authentication vulnerabilities may allow unauthorized access, but increased IT/OT

integration can enable lateral movement if segmentation is inadequate. The introduction of remote access tools can introduce unpatched vulnerabilities, and remote monitoring often requires privileged access credentials that become high-value targets. Many industrial protocols also lack encryption, which potentially exposes sensitive operational data during transit across networks."

Pros and cons of VPNs

"VPN [virtual private network] creates a tunnel from one server to the other side," said Waraich. "Your service provider keeps logs of the information. [But] only the paranoid can survive. You must be paranoid about your information. You must be super hypervigilant about your privacy and data ownership because things are getting connected to the cloud. Companies were told to send data to the cloud. So, who owns that data?"

Cox said that one of the biggest risks is out-of-date VPNs because they have vulnerabilities that lead to cyberattacks. "VPNs are important, but they're also a risk that cyber attackers can exploit. If they know the endpoint—the URL for that VPN—they could do harm," he said. "Many OT people deploy VPNs but they don't change them, they don't update them, they're not managing them properly and that becomes a bigger risk over time. IT [information technology] can be very successful in deploying VPNs, securing them and keeping them going. I think [deploying] the traditional VPN into the OT network directly is the wrong approach. But VPNs are a necessary evil because these systems are on-premises."

Scott Dowell, senior vice president and general manager at Wesco, wrote an Automation.com article, *The Cybersecurity Threat Lurking in Your Operational Efficiency Efforts: Remote Access Vulnerabilities*. In it, he said, "VPNs in particular can represent a significant risk to OT networks due to their potential to grant extensive access to critical systems. When implemented without appropriate security measures, VPNs can open the door for unauthorized access, allowing malicious actors to infiltrate the entire network, including sensitive OT infrastructure.

"This vulnerability exists primarily because attackers can exploit weaknesses within the VPN itself or obtain user credentials, providing them with a gateway to industrial processes that are crucial for daily operations," Dowell continued. "Given that many OT systems [use] older protocols that are inherently more susceptible to cyber threats, unauthorized access can lead to severe consequences, including operational disruptions and physical damage to equipment. Without stringent security controls and vigilant monitoring, organizations risk compromising their entire operational framework."

Instead of VPNs, use a cybersecurity platform designed for OT networks that allows remote access to a controlled environment, urges Dowell. "Consider a solution that includes a virtual server environment that has both the resources and tools that an engineer may need to access the network—without having to dial in to a VPN. A virtual network enables the engineer to safely

connect without allowing access from an outside, untrusted network. Plus, they help consolidate hardware infrastructure, leading to cost savings; improve flexibility and scalability by allowing for the easy creation and migration of virtual machines (VMs); and management is simplified through centralized tools."

Winebrenner added, "VPNs typically grant broad network access rather than limiting connections to specific required resources, which violates the principle of least privilege. VPN vulnerabilities are regularly discovered and exploited by threat actors, as seen in recent high-profile attacks targeting industrial organizations. Additionally, VPNs often lack OT-specific security controls and monitoring capabilities, and their authentication methods may not provide sufficient protection for critical industrial systems. The persistent connections VPNs establish can also serve as long-term attack vectors into sensitive OT networks, especially when over-privileged accounts are compromised."

Effective cybersecurity solutions

Data diodes, network segmentation and multifactor authentication are among the cybersecurity solutions that apply to remote operations and monitoring. However, according to Winebrenner, the most effective cybersecurity approach for remote industrial operations combines several complementary technologies and practices.

"For IT environments, identity-based access controls provide precision in managing user access. For OT and IoT [Internet of Things] environments, network-based microsegmentation enables OT security experts to define and enforce clear boundaries based on operational requirements and risk profiles—without changing the underlying infrastructure," Winebrenner said.

Elisity's platform and others support this approach by respecting the unique needs of both IT and OT environments while providing a unified management plane. "Network monitoring solutions with OT protocol awareness provide visibility into industrial network traffic. For unidirectional data flow requirements, software-defined microsegmentation can enforce one-way traffic patterns without dedicated hardware appliances," he said.

Waraich said that Skyynet's Cogent DataHub has security features that include multifactor authentication, the ability to white-label IP addresses and protocols, the creation of custom roles, data diode mode, data isolation, tunneling and DMZ.

"It's important to consider the Zero Trust methodology," Cox explained. "Turn everything off and be very selective about who's getting access to what and make sure the proper firewalls are in place. If we want to open up access to somebody, there must be some process and awareness around the authorization to allow that kind of access.

"There should be no direct access whatsoever to programmable logic controllers [PLCs], devices and/or these legacy protocol type systems," Cox continued. "It's advantageous

for integrators to be able to access the PLC program and potentially change things. There might be scenarios where you want to allow it, but ultimately, they should be onsite for something like that because there are safety implications to changing control programs. Companies must figure out what remote access means to them. Segmented networks and having layers of security are important. Zero Trust methodology is important. To me, transport layer security [TLS] authentication or encryption, two-factor authentication and strong passwords are big and a lot more approachable."

Cox added that it's important to make sure the system is up to date, patched regularly, there are audit trails set up, and employees and contractors are trained on how to operate and manage security effectively.

Shaw said starting with a purpose-built remote access solution for ICS [industrial control system] environments, look for features such as multifactor authentication, session recording, encrypted communications and granular access control. "Network segmentation features and OT-protocol specific features further reduce risk. Outside of the core secure remote access solution, ICS network visibility and monitoring are a must to audit access and detect threats."

Data diodes. Winebrenner said that hardware-based data diodes are not ideal for every remote access scenario, despite their security benefits for one-way data transfers. Their inflexibility makes them ill-suited for dynamic environments requiring frequent configuration changes, and their hardware implementation limits deployment locations and increases costs. "Many industrial use cases require bidirectional communication for control functions, making unidirectional diodes impractical," he said.

Data diodes (Figure 1) can be overkill in some cases. Waraich explained that if you're reading a temperature from a remote well site, you are monitoring only a temperature measuring device. There is no control

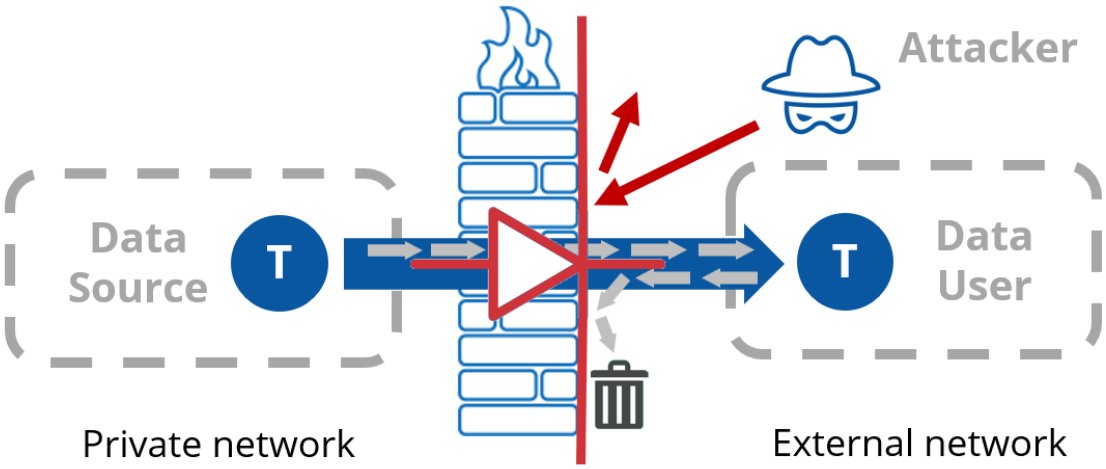


Figure 1. Tunnel/mirror in Data diode mode. *Courtesy: Skkynet*

element connected to it. "A data diode could be overkill in that scenario. But if it's connected to a control valve, then it might make sense," he said.

"Data diodes allow data to flow in only one direction," said Cox. "If there were a completely air-gapped secure network, we could use a data diode to get data out. They are very useful for getting data out for historical purposes, but there's no communication back. We would have to get data out by storing it through a database or using OPC UA or MQTT. To do that, the data diode vendor must support that protocol, which is likely to be designed to support stateless connections in a data diode scenario where there is no direct connection."

"I think for those cases where [users] just care about storing the data, it can work as a step," Cox continued. "They can be expensive too. If you look at setting up the right DMZ and the right firewalls and use the right protocols, you can achieve the same effect with a lot less cost and complexity. But today, there's more that users need to do than just get historical data. They need to have live information; they need to be able to do control in some respects or acknowledge alarms or various things that must happen remotely."

Network segmentation. Gregory Hale, editor and founder of *Industrial Safety and Security Source*, *ISSSource*, wrote in his article, *While Cyberattacks Are Inevitable, Resilience Is Vital*, that network segmentation helps implement secure remote access programs. With network segmentation, companies can restrict vendors to specific assets and prevent remote access OT devices from interacting with other parts of the network."

Modern software-defined microsegmentation solutions offer a more versatile alternative than data diodes by providing logical unidirectional enforcement where needed while supporting secure bidirectional communication when required, explained Winebrenner. "This approach leverages existing network infrastructure, scales more efficiently and provides greater operational flexibility while maintaining strong security controls—all based on policies defined by OT security specialists rather than imposing IT-centric models on operational environments," he said.

Pursuing integration and resilience

Effective OT/IT convergence is crucial for remote monitoring security, but it must respect the fundamental differences between these environments. Winebrenner explained that while traditional approaches kept these domains strictly separated, "modern digital transformation requires secure integration with appropriate boundaries. Unified security governance between IT and OT teams enables consistent policy enforcement, streamlined incident response and comprehensive visibility across both domains."

Solutions that bridge this gap must honor OT security principles while providing the controls that OT security teams design based on operational requirements and risk

assessments. “Organizations should pursue what Gartner calls ‘controlled convergence’—strategic integration with appropriate security controls rather than complete unification or continued strict separation,” Winebrenner added.

As industrial organizations embrace remote monitoring capabilities, it’s critical to adopt security solutions that enhance operational resilience rather than impede it. Traditional security approaches often force difficult tradeoffs between security, operational needs and cost. Winebrenner said that modern microsegmentation platforms provide an alternative by enforcing network-based security policies without requiring network reconfiguration, new hardware or agents.

“By leveraging the organization’s existing network infrastructure as the enforcement fabric, [an effective] solution enables industrial organizations to implement secure remote monitoring solutions in days rather than months,” Winebrenner explained. “This approach respects the distinct requirements of OT environments while allowing OT security teams to define and enforce appropriate control boundaries based on their expert understanding of industrial processes and risk profiles. Most importantly, it reduces the attack surface and minimizes lateral movement risk, addressing the primary threat vector exploited in most industrial cybersecurity incidents.”

“Companies need to take digital transformation seriously,” added Cox. “That means becoming more digital, having remote operations, being able to get data to the cloud and having OT and IT work together. That is a leadership culture change exhibited by the ones who are successful. They’re getting everybody in the organization trained, they’re communicating well together, they’re working together to solve these challenges and they can accomplish those goals in a more secure way that mitigates more risks.”

ABOUT THE AUTHOR

Jack Smith is senior contributing editor for Automation.com and *Automation.com Monthly* digital magazine, publications of ISA, the International Society of Automation. Jack is a senior member of ISA, as well as a member of IEEE. He has an AAS in Electrical/Electronic Engineering and experience in instrumentation, closed-loop control, PLCs, complex automated test systems and test system design. Jack also has more than 20 years of experience as a journalist covering process, discrete and hybrid technologies.

Solutions for SCADA Access Control Challenges

Successful programs must address technical, operational and organizational obstacles.

By Ashraf Sainudeen

Implementing access control in supervisory control and data acquisition (SCADA) systems is challenging and often considered impractical due to the unique nature of industrial environments and operational technology (OT) systems. Here are some of the key reasons why it can be difficult, followed by solutions that address these challenges.

SCADA systems are often built on legacy technologies that were not designed with modern cybersecurity in mind. Integrating modern access control mechanisms with legacy SCADA systems can be difficult. Compatibility issues may arise, leading to system instability or performance degradation.

OT systems often control critical infrastructure, such as power grids, water treatment facilities and ports and terminals. Any disruption caused by the implementation of access controls can lead to significant operational risks and downtime concerns for configuration and testing.

Industrial organizations, particularly those with a long history of operation, may be resistant to changes in how access is managed, especially if it impacts productivity. IT teams may be familiar with implementing access controls, but OT teams may prioritize operational efficiency and safety, leading to conflicting priorities.

SCADA systems often involve a wide variety of devices, such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), sensors and communication protocols. Different vendors may have their own access control mechanisms for these devices, and implementing a unified access control policy across such a diverse environment is complex.

Industrial control system (ICS) environments are often managed by engineers who specialize in process control and other OT systems. The lack of specialized cybersecurity expertise can make it difficult to design and implement effective access control strategies.

Implementing access controls, particularly those that involve authentication and authorization processes, can introduce latency, potentially impacting real-time operating system performance. Access control mechanisms like role-based access control (RBAC) might involve complex authorization logic that can slow down the system's responsiveness, which is critical in time-sensitive industrial processes.

The lack of specialized cybersecurity expertise can make it difficult to design and implement effective access control strategies.

Resolving SCADA access control challenges

Overcoming the challenges of implementing access control in SCADA systems requires a multifaceted approach that addresses technical, operational and organizational barriers. Here are strategies to tackle these challenges.

Gradual modernization of legacy systems. Instead of a complete overhaul, gradually upgrade legacy components with modern systems that support advanced access control features. Implement secure interface layers or gateways between legacy systems and modern access control solutions. This minimizes downtime and allows for a smoother transition.

Standardization and centralization. Develop a standardized access control framework that can be applied across all systems and devices, regardless of vendor. This reduces complexity and ensures consistency. Use a centralized access control management

Start with pilot projects in less critical parts of the SCADA environment to test and refine access control implementations before rolling them out more broadly.

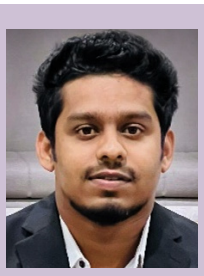
system to enforce policies across the entire SCADA environment. This helps simplify the administration and auditing of access controls.

Incremental implementation. Start with pilot projects in less critical parts of the SCADA environment to test and refine access control implementations before rolling them out more broadly. Treat access control as an ongoing process, with continuous monitoring, feedback and improvement.

Redundant systems and fail-safe mechanisms. Design access control systems with redundancy in mind. Use high-availability configurations that ensure that access control enforcement does not disrupt operational continuity. Implement fail-safe mechanisms that maintain basic operational functionality in the event of an access control system failure, ensuring that critical processes are not interrupted.

Contextual and adaptive authentication. While RBAC and multi-factor authentication (MFA) are great, using contextual information (such as location, time or device) to dynamically adjust authentication requirements can reduce the burden on users while maintaining security.

Collaboration with vendors. Work closely with SCADA vendors to ensure that their products support the required access control features. Encourage vendors to develop and maintain secure products.



ABOUT THE AUTHOR

Ashraf Sainudeen is a system specialist at DP World. An ISA/IEC 62443 certified professional with experience in industrial automation and control systems (IACS), he is dedicated to delivering exceptional service to clients with a strong passion for learning and exploring state-of-the-art technology in Industry 4.0, ICS/IT networks and OT cybersecurity trends.

Using OPC for Secure Alarm Integration: A Case Study

Create unified data sets for alarm and event data regardless of system age or location.

By John Weber

Alarm and event data is critical to industrial operations to notify operators of problems or potential future problems, convey status of process sequences, support the optimization of operations, predict maintenance needs and more. Many times, this data is only found on human-machine interfaces (HMIs), supervisory control and data acquisition (SCADA) and notifications systems in the operations side of the business and historically is often isolated to just those systems.

During the pandemic, companies realized where they had blind spots to managing operations with fewer onsite staff and that data of all types needed secure, convenient and reliable access, including beyond operations and into information technology (IT) and central offices.

For alarm and event data, the problem historically has been more challenging than just getting real-time data. Alarm and event data is typically a structure of multiple data points related to a single occurrence of a process value out of normal range, indicating when it went out of range, current value, limit and more. In the original OPC standards, the

OPC Alarm and Events specification, or OPC A&E, was designed to provide a standardized interface and data structure for accessing alarm and event data from systems that used to be closed systems or systems only offering proprietary interfaces.

In the OPC UA standards, this functionality has evolved into the OPC UA Alarms and Conditions, or OPC UA A&C standard, benefitting from the transport independence, security and other integrated features of OPC UA. With OPC UA, a process point can offer real-time values, alarm and event data and even historical data from that same node.

To get the most from these OPC standards, tools are needed to provide secure alarm networking using modern technologies; aggregation, centralization, redundancy and conversion from OPC A&E to OPC UA A&C; and logging. Consider these alarm integration application examples, the benefits to users and how they achieved the results.

Fuel-terminal automation with OPC A&E and OPC UA A&C

In this application, the user had multiple fuel terminals with variations in the programmable logic controllers (PLCs) used in the control systems at each location. They were seeking to generate new alarms and events from those PLCs but also from Varec Fuels Manager, a key application used at each site. To deal with the varying PLC types, they used the TOP Server OPC UA server to create a common tag definition regardless of PLC type. The Varec application was an OPC DA server, which they also pulled into TOP Server using its OPC DA client capabilities, which makes real-time data available via OPC UA. They then defined their alarms in the TOP Server A&E plug-in, which made them available as OPC Alarms and Events (Figure 1).

To implement a local and corporate-wide information roll-up using Emerson PlantWeb/inmation, they needed to

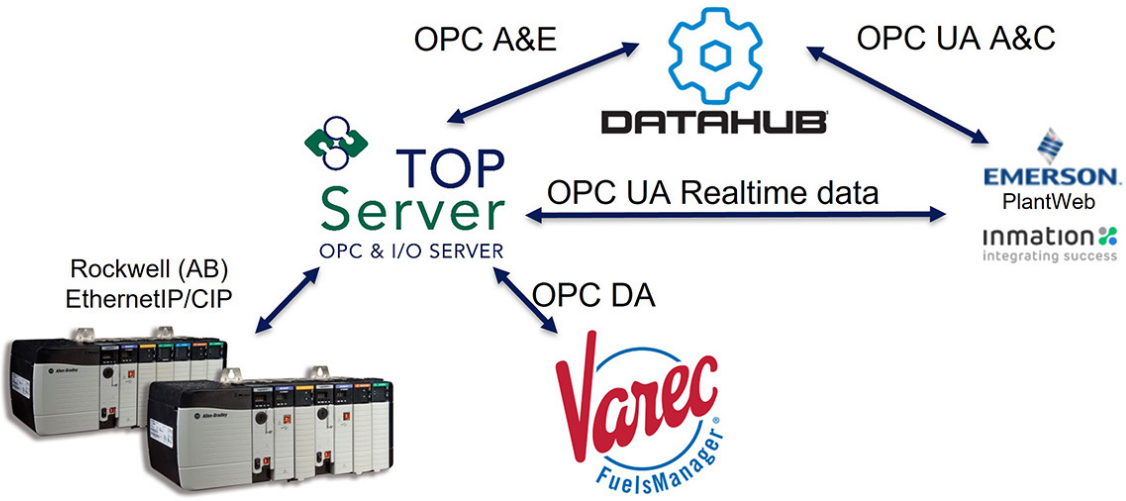


Figure 1. Omron and other PLC protocols varied by location and/or region.

have all the data available via OPC UA—both real-time and alarms and events data. They chose the DataHub to handle the OPC Alarms and Events (A&E) to OPC UA Alarms and Conditions (A&C) conversion.

DataHub aggregates OPC A&E alarm data from multiple sources, and with a few clicks, exposes that data as OPC UA Alarms and Conditions data for clients supporting the most modern OPC UA standard. It can also automatically break out the individual tags within a single alarm or event structure and make them available as single tags via OPC UA real-time data interfaces. That data can also be aggregated with OPC DA or UA real-time data from other systems, as well as many other DataHub interfaces. This is helpful for integrating alarm and event data with HMI, SCADA and other systems that do not support OPC UA Alarms and Conditions or, as in the case of this story, integrating existing systems using OPC classic standards with systems using OPC UA.

By integrating with OPC UA real-time and A&C to roll up data locally and corporate wide, the customer has experienced improved visibility of key operating metrics, which allows them to identify new opportunities for optimization (Figure 2).

Alarm and event networking advanced applications

All industrial data must be kept secure. Alarm and event data is even more critical. When aggregating and transporting that data over a network, it must be encrypted, and the sender and receiver should be authenticated. The OPC UA standard common infrastructure provides this capability automatically, but what about existing OPC

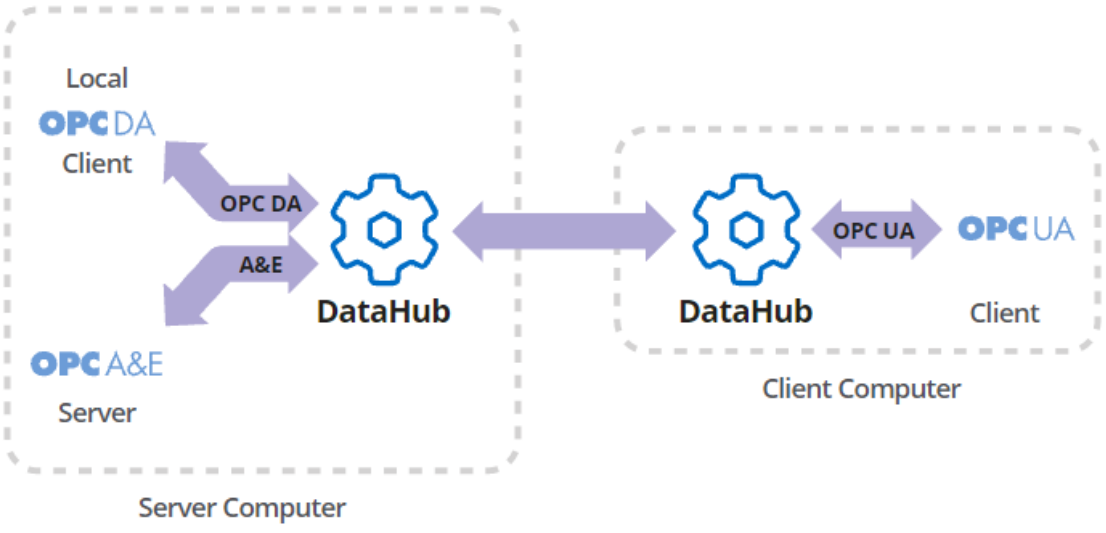


Figure 2. The user has experienced improved visibility of key operating metrics, which allows it to identify new opportunities for optimization.

A&E applications that have not yet migrated to OPC UA A&C? They need to be able to move that alarm data without losing the fidelity of the alarm information structures while meeting security requirements. With DataHub V10, one option would be to use the conversion of OPC A&E to UA A&C functionality and tunnel OPC UA A&C across the network.

There are some applications though that have intermittent network connections and need store-and-forward capability. These same applications typically involve reduced bandwidth data transmission over cellular, radio or satellite networks and are found in applications such as pipelines, water/wastewater, wind energy and oil/gas. Some of these same applications require redundant systems and networks, which the DataHub also supports. There are also use cases where the user—for their own security reasons—wants to not move OPC calls across network boundaries. The next application story involves exactly this type of situation where OPC needed to be augmented by store-and-forward capabilities, giving the customer the best of OPC with the added resilience it needed.

DataHub provides a solution for applications that need network isolation, reduced bandwidth and redundancy with its included secure data tunneling functionality that keeps the OPC A&E structures intact, moving them in an encrypted, authenticated network connection between instances of the DataHub. Only data changes are moved, which provides lightweight bandwidth utilization. In the previous diagram, this tunneling capability is used between the server and client machines. Store-and-forward capabilities ensure that data gets through when connections drop and resume.

Another scenario involves corporate cybersecurity policies that require the use of proxies and DMZs and even requiring that there be no inbound firewall ports on the IT or OT side of the connection. DataHub's tunneling functionality is designed to work in this advanced secure networking configuration moving OPC UA real-time, A&C, OPC DA & OPC A&E data securely and reliably (Figure 3).

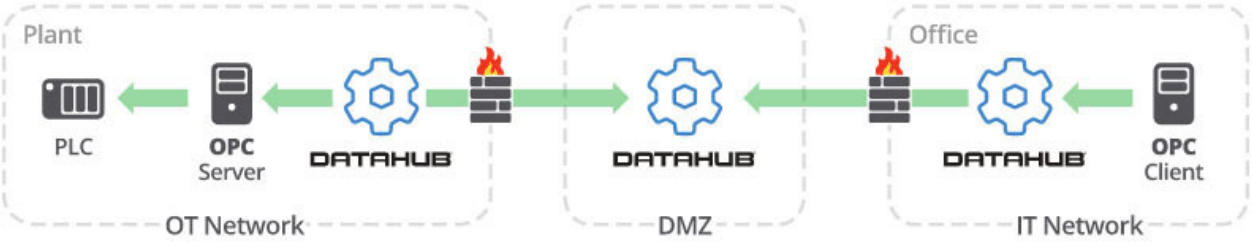


Figure 3. The tunneling functionality is designed to work in advanced secure networking configurations to move OPC UA real-time, A&C, OPC DA & OPC A&E data securely and reliably.

Secure tunneling of alarm and events data in pipeline automation

ABB used DataHub middleware to support highly redundant, secure networking of OPC A&E and real-time data on the Trans-Anatolian Natural Gas Pipeline (TANAP) project in Turkey (Figure 4). Reliable data communication is critical to the secure operation of the pipeline. This application story, provided by our partner Skkynet, shows how the advanced OPC integration features of DataHub are put to work on a large scale. Although at the time this system was implemented, integration with OPC UA A&C was not an option, the same concepts apply to the use of OPC UA real time and A&C data. Also, this customer now has the option to add OPC UA integration into its data aggregation and networking infrastructure within the same application instead of having to add other software.

Every aspect of operation from equipment functioning to leak detection is monitored, controlled, stored and transmitted between the remote stations and the control center.

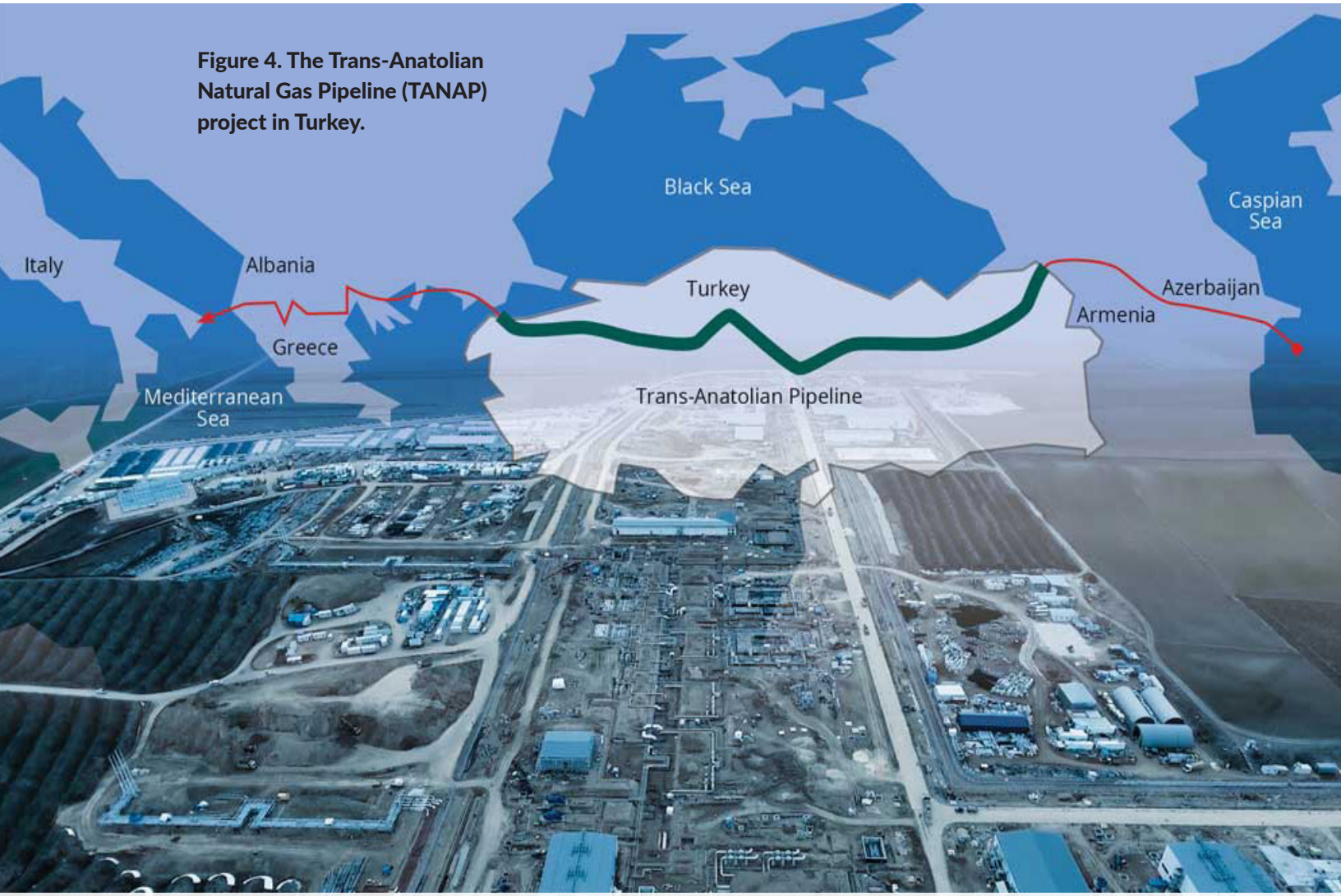


Figure 4. The Trans-Anatolian Natural Gas Pipeline (TANAP) project in Turkey.

Hundreds of thousands of OPC DA and OPC A&E data values are tunneled by the DataHub across redundant, state-of-the-art fiber optic networks with VSAT satellite backup, and are seamlessly integrated with SCADA systems for monitoring and supervisory control.

Because it isolates the OPC connection from the networked tunnel connection, the DataHub can just as easily transmit OPC A&E alarm data across the tunnel as OPC DA real-time data. And since it supports OPC server-to-server bridging, it can connect OPC servers at the control center with OPC servers in the field. Perhaps most important, the DataHub's built-in redundancy support has allowed the ABB team to configure a highly reliable system with multiple layers of redundancy.

Final thoughts

Modern success requires unified data sets regardless of the varying age of systems and secure solutions that can connect from the field operations to the enterprise and on to the cloud. Alarm and event data is a subset of that data that is critical to industrial operations to notify operators of problems or potential future problems, convey status of process sequences, support the optimization of operations, predict maintenance needs and more.

ABOUT THE AUTHOR

John Weber is president and founder of Software Toolbox. Weber has worked in automation software for 35 years and since 1996 has led the Software Toolbox team that's focused on delivering complete product experiences that combine innovative open software solutions, expert knowledge of how to apply the software to solve problems and support that 97 percent of users say is "awesome" or "excellent."

Threat-Hunting in OT Infrastructure: A Case Study

A public utility used a cybersecurity platform to identify and counteract a persistent breach.

By John Burns

The Littleton Electric Light and Water Departments (LELWD) needed a cybersecurity platform. As a small public utility established in 1912, LELWD grappled with limited resources and expertise, making it vulnerable to cyber threats targeting its operational technology (OT). The situation escalated when the sophisticated threat group

VOLTZITE compromised their networks, underscoring the urgent need for enhanced security measures.

David Ketchen, assistant general manager of LELWD, received a phone call from the FBI on a Friday afternoon alerting the utility of a suspected compromise. The gravity of the situation became evident when FBI agents, accompanied by representatives from the Critical Infrastructure Security Agency (CISA), arrived at LELWD's offices the following Monday.

To LELWD's credit, the utility had already taken steps to bolster its cybersecurity posture. It was implementing the Dragos cybersecurity platform to gain visibility of its OT assets, secure IT-OT network traffic and monitor communications between OT devices and systems. Additionally, the utility had initiated the engagement of OT Watch's threat hunting-as-a-service.

Now prompted to deploy quickly and bypass the planned onboarding timeline, OT Watch gained access to the customer's platform and identified VOLTZITE actions close to the utility's OT. Specifically, the Dragos platform confirmed server-message-block traversal maneuvers and remote desktop protocol lateral movement involving LELWD's Geographic Information System (GIS) server.

OT Watch provided these findings to LELWD, empowering responders to eradicate the adversary and secure the network against additional threats. Further investigation determined that the compromised information did not include any customer-sensitive data, and the utility was able to change its network architecture to remove any advantages for the adversary.

With OT Watch proving its value, LELWD started using the platform for several other cybersecurity activities:

- **Asset visibility and inventory.** The platform uses passive network monitoring and deep packet inspection to automatically discover and classify OT assets, providing a comprehensive inventory without disrupting operations.
- **Threat detection and response.** Littleton leverages the platform's advanced analytics and threat intelligence to identify malicious activities, alerting security teams and providing actionable insights for rapid response.
- **Vulnerability management.** The platform combines asset information with threat intelligence to prioritize vulnerabilities based on actual risk to the OT environment, enabling focused remediation efforts for LELWD's small staff.
- **Network segmentation analysis.** The platform analyzes network traffic patterns to identify potential segmentation issues and recommend improvements.
- **Incident response guidance.** LELWD can see detailed forensic data, threat intelligence and expert playbooks within the platform to support efficient and effective incident investigation and remediation

Help from the American Public Power Association

LELWD's decision to partner with a cybersecurity company was driven by the need for specialized OT security expertise and a desire to work with someone with a strong industry reputation. The utility also sought a partner to who could align its goals with those of the American Public Power Association (APPA).

APPA leverages funding to support OT cybersecurity deployments at public power utilities. Through cooperative agreements, APPA members have access to a host of programs and resources, including deployments of monitoring technology like the Dragos Platform. Through its cybersecurity programs to date, APPA has awarded more than $14 million to 32 utilities, funding 78 cybersecurity projects.

The partnership aimed not only to address immediate threats but also to establish a

OT Watch identified VOLTZITE actions close to the utility's OT. Specifically, the cybersecurity platform confirmed server-message-block traversal maneuvers and remote desktop protocol lateral movement.

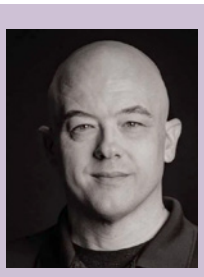
proactive security framework capable of adapting to evolving cyber risks.

According to Josh DeTerra, LELWD supervising engineer, "The improved visibility we gained through [the platform] has been a game-changer for our day-to-day operations. Just being able to see all the IP addresses that we know should or shouldn't be talking to each other—it's huge. This level of insight allows us to quickly identify and investigate any unusual network communications, potentially catching security breaches or operational issues before they escalate."

"It's not just about cybersecurity, but also operational efficiency," said DeTerra. "We can now optimize our network configurations, troubleshoot issues faster and ensure that our critical systems are communicating as intended. This visibility has empowered our team to make data-driven decisions, improve our incident response times and maintain a reliable and secure infrastructure for our community," he said.

Just being able to see all the IP addresses that we know should or shouldn't be talking to each other—it's huge. This level of insight allows us to quickly identify and investigate any unusual network communications.

LELWD has transformed its approach to cybersecurity, "shifting our mindset to see it as an ongoing process requiring constant adaptation," said DeTerra. Working with Dragos "has empowered us to take ownership of OT security, equipping us to protect critical infrastructure and foster a culture of security awareness throughout our operations."



ABOUT THE AUTHOR

John Burns is director of OT Threat Hunting at Dragos Inc. The company has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure. It is a privately held company based in the Washington, D.C. area with a regional presence around the world. The Dragos Platform is designed to monitor, manage and respond to cyber threats to industrial control systems. The company also provides urgent incident response services, threat intelligence and a variety of tools to protect critical OT assets.

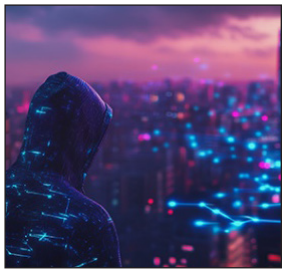
More from Automation.com

Automation.com offers daily news in the form of press releases, features, white papers, product postings and more. Don't miss out! Sign up to receive our general interest and topical newsletters or follow us on LinkedIn, Facebook and X. —*Melissa Landon, Senior Content Editor*

Industrial Cybersecurity & Safety

How Will Quantum Computing Impact Industrial Cybersecurity?: Quantum computing is a quickly evolving field that applies physics principles to solve complex problems using quantum bits rather than classical computer bits. Although these new technologies are exciting, they bring potential cybersecurity risks.

Why 2025's Cybersecurity Landscape Demands a Complete Overhaul of Your IT Infrastructure:



The convergence of sophisticated attack methods with aging IT infrastructure has created a perfect storm for cybercriminals. In 2025, organizations must confront an uncomfortable truth: Their legacy systems may be their greatest vulnerability.

Enterprise Architecture and Networks

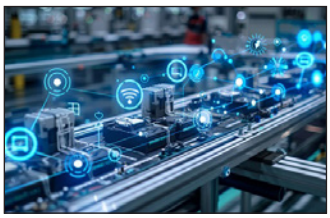
Report: Cybersecurity, IT/OT Collaboration and AI Efficiency Driving Decision-making for Industrial Networks: Cisco's 2024 State of Industrial Networking Report for Manufacturing provides insights from 739 industry professionals.

Report: Wireless Networks Unprotected as Threats to Critical Infrastructure Escalate:

In the second half of last year, critical infrastructure organizations in the United States saw the highest number of attacks, according to the Nozomi Networks Labs OT & IoT Security Report. The analysis of more than 500,000 wireless networks worldwide found that only 6% are adequately protected against wireless deauthentication attacks.

IIoT & Digital Transformation

Edge Computing Adoption in IIoT: A Rockwell Automation software project engineering leader delves into the transformative impact of edge computing on industrial automation, touching on its advantages, challenges and future growth opportunities.



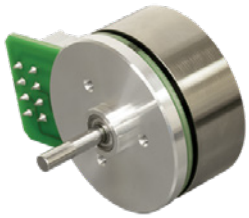
Will AI Take My Job in Manufacturing?:

AI has advanced to the point that people across various sectors are worried AI will take their jobs. However, robots aren't new to manufacturing and there are ways to make oneself "AI-proof" to secure employment.

Factory Automation & Control

Growth Forecast for Global Manufacturing in 2025, But Challenges Remain: The outlook for the global manufacturing industry looks uncertain in 2025, with political and economic events hampering growth. These include an escalating tariff war between the U.S. and other territories, deindustrialization in some large European economies and the AI arms race.

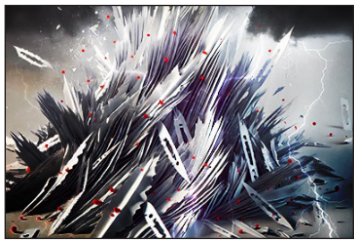
Enhancing Motor Performance Through Innovative Rotor Designs: Brushless direct current (BLDC) motors are widely used across medical, aerospace and industrial automation applications. Their specific design plays a significant role in the motor's performance, with optimizing the motor's design for specific applications ensuring that OEMs achieve optimum performance and reliability. Research and development efforts also play a vital role in refining these design options.



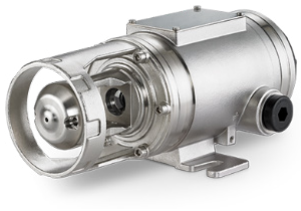
Process Automation & Control

Asia-Pacific Leads Fragmented Global Battery Recycling Equipment Market: The market may see the integration of different metallurgical techniques, leading to more efficient and environmentally friendly battery recycling solutions, according to Interact Analysis.

Death by a Thousand Papercuts: Why You Need to Prioritize Surge Protection: You already know surge protection is important. But what you may not realize is how close your surge protection—and the equipment it's supposed to safeguard—is to failing. Most surge protection technology is slow, inconsistent and degrading.



Product Updates



Emerson's Fixed Point Gas Detector Provides Fast and Reliable Detection without False Alarms: The Rosemount 625IR Fixed Gas Detector is designed to provide reliable and fast gas detection in all plant environments using advanced optical absorption detection technology.

Siemens Expands Industrial Copilot with Generative AI-powered Maintenance Offering: The Siemens Industrial Copilot enables customers to leverage generative AI across the entire value chain—from design and planning to engineering, operations and services.

A MESSAGE FROM THE EDITOR

ISA Enhances Automation Knowledge Sharing and Discussion

Have you ever found yourself with a technical question and didn't know who to ask for help? The International Society of Automation has created a place where members can crowdsource answers and discuss details. Connect Forums represent a new avenue for ISA members to grow their professional networks and find answers.

Consider these queries:

- A member presented a dynamic process simulation with specific attributes and asked, "Is this a digital twin?" That question led to a lively discussion on terminology, which then evolved into an example of how digital twins are used for gas pipeline leak detection. Expanding even further on the topic was a new question about whether the same technology can be used for water pipe leak detection.
- "Our company is starting work on updating our grounding guidelines for designing and installing automation systems in the field. I am looking for some good reference material. Has ISA published anything related to grounding PLC/instrumentation systems?"
- "I recently got a project request from a customer that has kind of stumped me. Situation: The client is an OEM machine manufacturer that builds systems (collection of components). If they want their product to be ISA/IEC 62443 compliant and achieve an SL3, do they have to look to the SL requirements according to Part 3-3 or the Component requirements from Parts 4-1 and 4-2?"

Connect Forums are hosted on ISA Connect, ISA's members-only community. There, ISA members engage with other automation professionals across industry sectors, dive deep into cutting-edge automation challenges and get real-world answers to their toughest questions on a wide range of technical topics.

ISA's new Connect Forums reflect and serve the needs and interests of the society's growing member base around the world. Professionals from Hong Kong to Houston can directly connect across industry sectors to share experience and find new solutions. All can also grow as professionals for the duration of their careers by interacting with peers.

"Post new questions and answer questions from other members, share your knowledge and learn," said Carlos Mandolesi, ISA's Technical Assembly Chair and 2022 President. "We can create a better world through automation together."

Renee Bassett Chief Editor,
Automation.com Monthly

International Society of Automation
Setting the Standard for Automation™

2025 Executive Board

The International Society of Automation is pleased to introduce the 2025 Executive Board.

President
Scott Reynolds
Johns Manville, A Berkshire Hathaway Company

President-elect
Secretary
Ashley Weckwerth
P.E.
Burns and McDonnell

Past President
Prabhu Soundarrajan
Kingston Capital

Treasurer
Ardis Bartle
Apex Measurement and Controls

CEO and Executive Director
Claire Fallon
International Society of Automation

Dr. Soloman Almadi
Saudi Aramco

Marco Ayala
MITRE

Alan Bryant
P.E., PMP
Occidental

Alexa Burr
NEMA

Francisco Diaz-Andreu
Repsol

Nick Erickson
AWC, Inc.

Colleen Goldsborough
CPSC
United Electric Supply

Sherry LaBonne
Rockwell Automation

David Lee
C.Eng, FIChemE
User Centered Design Services

Robert E. Lee
Dragos

Edward Naranjo

Mary Riedel
Martin Control Systems, Inc.

Megan Samford
Schneider Electric

Sujata Tilak
Ascent Intellimation

Jeff Winter
Critical Manufacturing

2025