

AUTOMATION 2023

VOLUME 2

Cybersecurity & Connectivity

- ▶ Moving Process Data Across Segmented Networks
- ▶ Emerging Technology Solutions in Industrial Cybersecurity
- ▶ Finding a Faster Fieldbus
- ▶ Integrating Safety and Security
- ▶ Securing Critical Infrastructure with Zero Trust
- ▶ Industrial Security Case Studies



Introduction

AUTOMATION 2023 VOLUME 2

Getting Granular with Cybersecurity & Connectivity

Welcome to the March edition of AUTOMATION 2023 focused on cybersecurity and connectivity. For this month's issue, we're featuring articles that delve into the specifics of connecting and securing industrial operations in various use cases. From segmenting networks so process data is safeguarded to securing critical infrastructure with zero trust, you'll find plenty of useful information to ponder as we all strive to protect our information and equipment from... well, everything. To that end, you'll also get valuable insight into meeting NIST SP 800-82 guidelines and the NIS 2 Directive, as well as understanding the IEC 61158 standard with an up-close look at the EtherCAT fieldbus.

If you have a moment, let us know what you thought of this issue. We are always striving to bring our readers more of what they want to see in upcoming AUTOMATION ebooks.

Lynn DeRocco
Automation.com Managing Editor
lderocco@automation.com

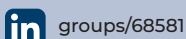
SPONSORS



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.



groups/68581



company/internationalsocietyofautomation



automationdotcom



InternationalSocietyOfAutomation



@automation_com



@ISA_Interchange

Renee Bassett, Chief Editor
rbassett@automation.com

Chris Nelson, Advertising Sales Rep
chris@automation.com

Richard T. Simpson, Advertising Sales Rep
rsimpson@automation.com

Gina DiFrancesco, Advertising Sales Rep
GDIFrancesco@automation.com





OT CYBERSECURITY SUMMIT

**PROTECT YOUR
FORTRESS**

31 May – 1 June 2023 | Ardoe House Hotel & Spa, Aberdeen, Scotland

This brand new event will focus on how you can protect your fortress with the ISA 62443 series of standards and related training courses. Cybersecurity is a hot topic as supply chain risk emerges as a top concern in the energy sector. A cyber breach at any level in a supply chain has the potential to take down the whole operation.

Regulators in the North Sea are asking contractors detailed questions about OT Cybersecurity, especially on operations classified as critical infrastructure. This increased scrutiny has resulted in more detailed contractual requirements. Insurance companies are also looking for specific details before writing a cybersecurity policy.'

ISA has established a series of industrial cybersecurity standards that serve as your roadmap to improve security and protect your operations with strategies such as zero-trust architecture and OPC/protocols. Join us to learn more—register now!

Keynote Speakers



Megan Samford
VP, Chief Product
Security Officer –
Energy Management,
Schneider Electric



Cheri Caddy
Deputy Assistant
National Cyber
Director at ONCD/
the White House

TRAINING OPPORTUNITIES*

29 May

CyberSensors: Advancements in
Automation CyberPhysical Security
(IC87C)

29–30 May:

Using the ISA/IEC 62443 Standards to
Secure Your Control Systems (IC32)

30 May

Cybersecurity Awareness Training for
Industry Professionals (IC31C)

Cyber Incident Response (ICS4ICS)
Workshop — *FREE with conference
registration!*

WHO SHOULD ATTEND?

- Automation Engineers
- Process Control Engineers
- Security Engineers
- QA Engineers
- Plant Engineers
- Manufacturing Engineers
- ICS Cybersecurity Engineers
- Digital Transformation Managers
- Engineering Manager
- Security Operations Center (SOC) Managers
- Compliance and Risk Managers
- Chief Information Officers (CIOs)
- Chief Information Security Officers (CISOs)

INTERESTED IN SPONSORING?

View the prospectus at
isa.org/sponsor or contact:

Kim Belinsky: +1 919-990-9404
or kbelinsky@isa.org

Morgan Foor: +1 919-990-9267
or mfoor@isa.org

Register Now

Table of Contents

AUTOMATION 2023 VOLUME 2
CYBERSECURITY & CONNECTIVITY

Page 7

Moving Process Data Across Segmented Networks

By Xavier Mesrobian, Skkynet

Meet NIST SP 800-82 guidelines and the NIS 2 Directive with a system that incorporates demilitarized zones.

Page 16

Emerging Technology Solutions in Industrial Cybersecurity

By Philip Marshall, Hilscher

Protocol stacks built to cybersecurity standards improve safety for device communication.

Page 23

Finding a Faster Fieldbus

By Jack Smith, Automation.com

When it comes to fieldbus options, EtherCAT is a robust contender for its speed, flexibility, and simplicity.

Page 33

Integrating Safety and Security Strengthens Cybersecurity

By Nick Creath, Rockwell Automation

Closing security gaps and strengthening security make organizations more resistant to future threats.

Page 40

Securing Critical Infrastructure with Zero Trust

By Anand Oswal, Palo Alto Networks

Being operationally resilient requires a multitude of safeguards that should take both OT and IT into consideration.

Page 47

Cyber Safeguarding Industrial Operational Support

By Steve Mustard, National Automation

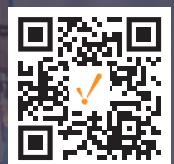
Read an excerpt from the new OT cybersecurity book *Industrial Cybersecurity Case Studies and Best Practices*.

The Plant Floor in Your Pocket

Get an overview of your process at a glance.
Control your SCADA with a swipe.



See the live demo now.
Scan this QR code with your phone
or visit demo.ia.io/tech



Tunnel/Mirror
simply better
networking



DataHub®

For data protocols that are difficult to connect, the DataHub Tunnel/Mirror provides easy-to-configure, secure and robust networking. Eliminate the hassles of DCOM, detect network breaks quickly and recover from them smoothly. Access your remote data, not your plant systems. Connect and share data among locations with no DCOM or Windows security issues.

The DataHub Tunnel/Mirror goes beyond the basics, letting you integrate your data without exposing your network. Simply better networking.

Learn more about
DataHub®

Moving Process Data Across Segmented Networks

Meet NIST SP 800-82 guidelines and the NIS 2 Directive with a system that incorporates demilitarized zones.

It is vital to keep our industrial processes secure. Governments at the highest level are weighing in on this as they recognize the link between industrial data security and national security. A recent White House memo to corporate executives and business leaders across the USA urges them to protect their companies against unwelcome intruders. One of the key action items is to segment networks, to isolate OT (operations technology) from IT.

By Xavier Mesrobian,
Skkynet



The memo says, “It’s critically important that your corporate business functions and manufacturing/production operations are separated, and that you carefully filter and limit internet access to operational networks, identify links between these networks, and develop workarounds or manual controls to ensure that ICS networks can be isolated and continue operating if your corporate network is compromised.”

In Europe, the EU has gone further in its NIS 2 Directive, which will become mandatory in October 2024. This document specifies a number of basic security practices, including standards for networking data between the production and corporate levels of a company. Again, its recommended approach is to segment networks. This is spelled out in NIST document SP-800-82, which says: “The most secure, manageable, and scalable control network and corporate network segregation architectures are typically based on a system with at least three zones, incorporating one or more DMZs.”

However, digital transformation, Industrial IoT, and Industry 4.0 all underscore the need to use OT data outside the plant. Clearly there must be a secure way to get to it.

What happened to VPNs?

Until recently, many companies have used virtual private networks (VPNs) to access data on their OT networks. But this is what the recommendations to segment networks advise *against* doing. Rather than segmenting networks, VPNs join them. A VPN extends the IT security perimeter into the plant network, effectively connecting the two networks. Anyone hacking the IT network and accessing the VPN can use it to reach every other connected node, including those on a linked OT network.

Rather than using VPNs, and to eliminate the risks they pose, the OT and IT networks must be segmented with a demilitarized zone (DMZ) between them to allow the secure transmission of data (Figure 2).

Connecting through a DMZ

To segment networks, NIST SP-800-82 recommends a system of three zones: the control zone (OT), the corporate zone (IT), and the DMZ. Using a DMZ ensures that there is no direct link between corporate networks and control networks, and that only known and authenticated actors can enter the system at all. The NIST document describes the value and use of firewalls to separate these zones, and to ensure that only the correct data passes from one to the other.

● ● ● ● ● **Digital transformation, Industrial IoT, and Industry 4.0** all underscore the need to use OT data outside the plant. Clearly there must be a secure way to get to it.

However, implementing a DMZ in an Industrial IoT environment is problematic for the two most commonly used IoT protocols: OPC UA and MQTT. Getting data out of a plant through a DMZ typically requires two or more servers, chained together one after the other. The OPC UA protocol is simply too complex to reproduce well in a daisy chain like this. Information will be lost in the first hop. The synchronous multi-hop interactions needed to pass data across a DMZ would be fragile on all but the most reliable networks and would result in high latencies. And there would be no access to the data at each node in the chain. MQTT, on the other hand, can be chained, but it requires each node in the chain to be aware that it is part of the chain and to be individually configured. The Quality of Service (QoS) guarantees in MQTT cannot propagate through the chain, making data at the ends of the chain unreliable.

Since neither OPC UA nor MQTT is well suited to passing data through a DMZ, another approach is needed—one that integrates well with both of these protocols. Secure tunnel/mirroring middleware can do this and pass the data along daisy-chained connections, securely crossing a DMZ. The middleware connects to either MQTT or OPC UA at

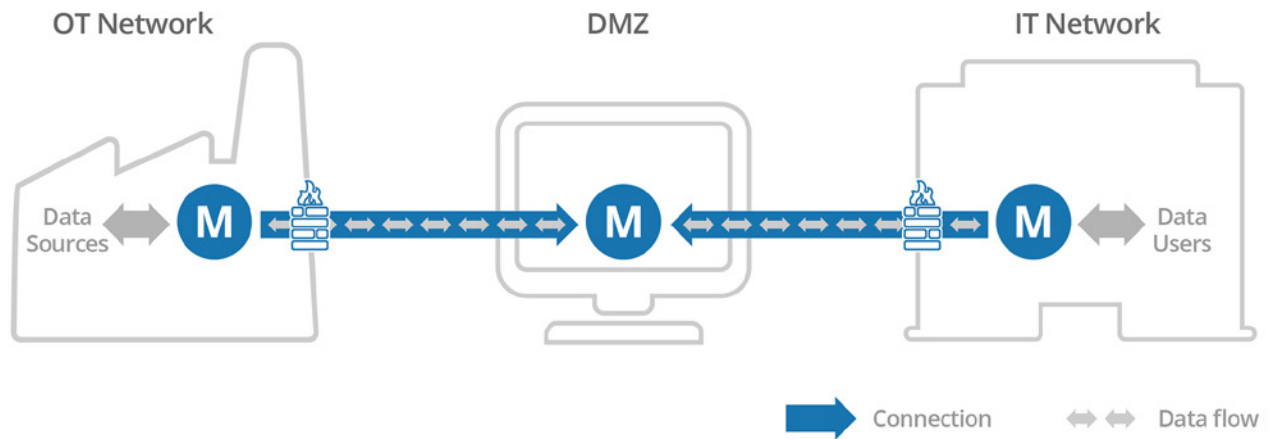


Figure 1. OT and IT networks must be segmented with a demilitarized zone (DMZ) between them to allow the secure transmission of data.

each end of the tunnel and mirrors the full data set through each server in the chain. It provides access to the data to registered, qualified clients at each node, as well as at the final destination. The mirroring capability of the tunnel/mirroring middleware guarantees consistency so that any client or intermediate point in the chain remains consistent with the original data source.

Securing open firewall ports

To provide the highest level of cybersecurity, data connections to the DMZ must not open any inbound firewall ports on either OT or IT. This is something that most industrial protocols were not designed to do. For example, OPC DA and OPC UA both use a client/server architecture, in which the client initiates a connection and the server accepts it. The server must listen for the connection on a TCP port, and that port must be open for incoming connections on the server's firewall, and on any other upstream firewalls between the client and the server. To provide access to the data via OPC means opening at least one port on each of those firewalls, a significant risk.

Any open incoming firewall port constitutes a security exposure. Network attacks are not made on a port, nor are they made on a

protocol—they are made on an application. The risk is that the listening application has an exploitable flaw that may or may not be due to the protocol implementation.

For example, an application may perfectly implement the OPC UA protocol yet be vulnerable to flaws in OpenSSL. The application may have no exploitable flaws in OPC UA or SSL but still have a buffer overrun in a string processing function executed on incoming data. No application is free of bugs. Every open incoming port is an opportunity for an attacker to probe an application for exploitable flaws and can give instant access to a network if one is discovered.

The best security practice is to not open any incoming ports at all in the secure network's firewall. Properly designed tunnel/mirroring middleware can meet this requirement. As long as it can make an outbound TCP connection from the server side to the client side, then there is no need to open any inbound firewall ports. This eliminates the attack surface altogether.

Securing the tunnel/mirror connection

In addition to using a DMZ and keeping all inbound firewall ports closed, security best practices should be implemented in the tunnel/mirror connection itself. For example:

- ▶ SSL encryption is essential, preferably with support for the most recent versions, such as TLS 1.2 and TLS 1.3. The system should use and enforce server certificates.
- ▶ User authentication is best applied on a per-connection basis. Each client program should be required to transmit a username and password, an access token, or a client certificate to authenticate.
- ▶ Any potential connection over plain-text transports should be avoided because unencrypted data, possibly including passwords, could be retrieved with a network packet capture program.

MQTT: advantages and drawbacks

MQTT is a lightweight messaging protocol originally developed for the oil and gas industry. Devices and programs called “clients” connect to a server called a “broker” and publish their data to it and/or receive data from it. The MQTT broker does not examine the data payload itself, but simply passes it along as a message from each publishing client to all subscribing clients.

One of the benefits of using MQTT is its ability to connect outbound through a firewall. This “push” architecture avoids the client-server architecture problem of OPC, allowing devices to make outbound connections without opening any inbound firewall ports. And, by using a central broker, it is possible to establish many-to-many connections, allowing multiple publishers to connect to multiple subscribers. MQTT thus solves some communication and security problems.

Despite these architectural advantages, MQTT has drawbacks that must be addressed if it is to be truly useful for OT/IT and Industrial IoT communication scenarios.

- ▶ MQTT is a transport protocol. It does not specify a payload format, which poses interoperability problems among applications from different vendors. Sparkplug has been created to address this issue and is starting to gain traction among vendors and users.
- ▶ An MQTT broker does not preserve time order among data values on different topics. This means that events in the physical system that occur in the order A then B then C could be delivered to an application as C then B then A, or any other ordering, which is an error in many industrial-control use cases and could lead to serious consequences.
- ▶ MQTT brokers do not have a way to indicate that a data source is disconnected. The consuming application cannot tell the difference between an old value from a sensor that has failed or a current value that has simply not changed recently. The “last will” mechanism in MQTT designed to deal with this requires

unreasonable levels of coupling between the producers and consumers of data, resulting in duplicate configuration and increased integration and maintenance costs.

- ▶ MQTT quality of service (QoS) levels are not adequate for use across a DMZ, as they only apply to single connections. Since connecting through a DMZ requires multiple hops, the data producer will never know whether an MQTT message has reached a user, regardless of the QoS it selects. What is needed is guaranteed eventual consistency, so that each value transmitted by a producer will either reach the user or be superseded by a more recent value.
- ▶ MQTT brokers do not handle overload situations well. If data is arriving faster than a consumer can process it, it is likely that data consistency and time order between data producer and consumer will be lost.

To put it briefly, MQTT keeps inbound firewall ports closed, making it useful for some Industrial IoT applications, particularly “first mile” data collection from embedded devices. But its inability to guarantee consistency of data between producer and consumer, particularly through a DMZ, does not make it an ideal candidate for OT/IT connections. Connecting MQTT to tunnel/mirroring middleware can significantly expand its flexibility and value.

Meeting the needs of the times

Connecting OT and IT offers enormous benefits for those able to make it happen. But above all, these connections must be secure. Business leaders and policy makers worldwide see that their process, manufacturing, and critical infrastructure is under attack as never before. Even as they acknowledge the value of accessing industrial data, they are issuing calls for urgent action to raise the levels of industrial system security. Without it, millions of dollars will continue to be lost or wasted in ransomware attacks and other exploits.

Most industrial cyberattacks are directed towards corporate IT systems that present a broad attack surface. OT systems need not share

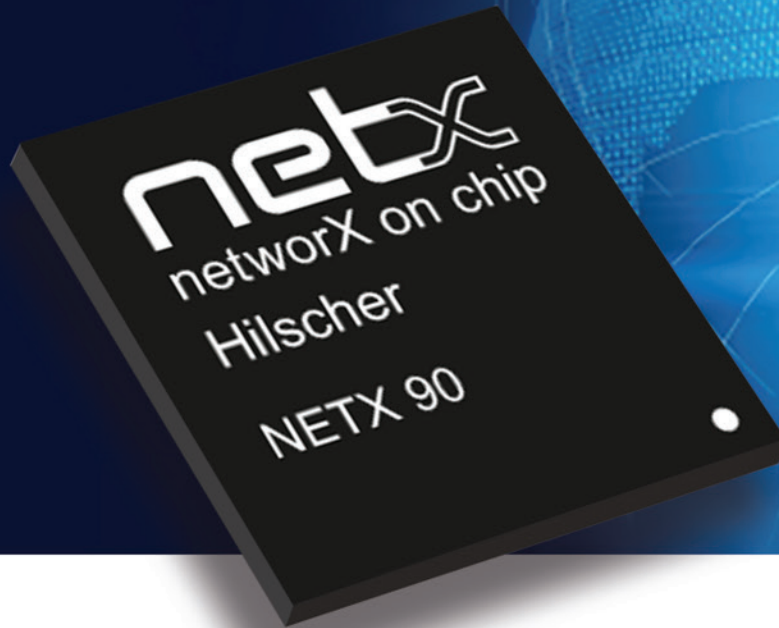
that risk. OT networks can have zero attack surface. There is no need to expose an OT system to the internet, or to join OT and IT networks, either directly or through a VPN. The NIST and NIS 2 guidelines are clear—segmenting networks and sharing data through a DMZ is far more secure. The technology is here, available now. Tunnel/mirroring middleware can be deployed to link to existing protocols and pass data securely and consistently from OT to IT across a DMZ.

ABOUT THE AUTHOR



Xavier Mesrobian is the vice president, sales and marketing, at [Skynet Cloud Systems](#), which allows companies to securely acquire, monitor, control, visualize, and consolidate live process data in-plant or over insecure networks with no VPNs or changes to IT policy required.

Secure Your Industrial Ethernet With netX 90



Built-in Security:

- **Secure boot and cryptography**
Encryption via SSL/TLS for HTTPS, OPC UA, MQTT, VPN
- **IEC 62443 compatible**
Enables layered security for Defense-in-Depth design
- **Built-in diagnostics**
Monitor operating conditions for predictive analysis
- **Multiple processors**
Logical separation of communication and application tasks
- **Partitioned design**
Restricts software access to on-chip peripherals on either side
- **Minimum ten-year availability**

Single Pair Ethernet Ready:

- **IEEE 802.3cg standard**
10 Mbit speeds and intrinsically safe with Ex equipment
- **Internal xMAC processors**
Enable protocol specific switching between two channels
- **Supports SPE**
Connect external PHY devices via MII interface
- **IO-Link sensor networks**
Connect two 10 Mbit channels with SPE port up to 1,000 meters
- **Real-time Ethernet connections**
Pair existing 100 Mbit RTE with 10 Mbit SPE
- **Switch Capabilities**
Use netX 90 as a switched device between 100 Mbit RTE and 10 Mbit SPE



Learn more from Hilscher:

call 1.630.505.5301
email: info@hilscher.us or
visit www.hilscher.com,
www.netIOT.com



The Growing Need for Emerging Technology Solutions in Industrial Cybersecurity

Historically, industrial cybersecurity in automation systems has concentrated on controller-to-controller communications and using dedicated IT/OT gateways, with systems segmented into interconnected zones. Today, integrators are primarily applying cybersecurity to the interfaces of these zones. These segments typically include operations technology (OT) industrial networks, and their device intercommunications are generally unprotected. Integrators are installing firewalls and strict on-premises access control to increase security in this space.

By Philip Marshall, Hilscher

Protocol stacks built to cybersecurity standards make device communication safer.

A good strategy to prevent incidents from spreading and reduce risks is segmentation. However, segmentation alone isn't enough to resolve every issue. User groups, standardization bodies, and technology providers are working on extensions to secure OT-level communications. These extensions include field devices, servo drives, IO-devices, and small sensors, to name a few, and they are equipped with security capabilities (Figure 1).

With new heightened security functionalities, network nodes will be able to authenticate each other and data can be protected against tampering to ensure that only trusted devices can communicate. Data encryption is another viable method of confidential information protection.

Hilscher has already implemented such cybersecurity standards into its communication protocol stacks. Devices based on the multiprotocol netX chips that feature security-enabled hardware and firmware make use of these advantages.

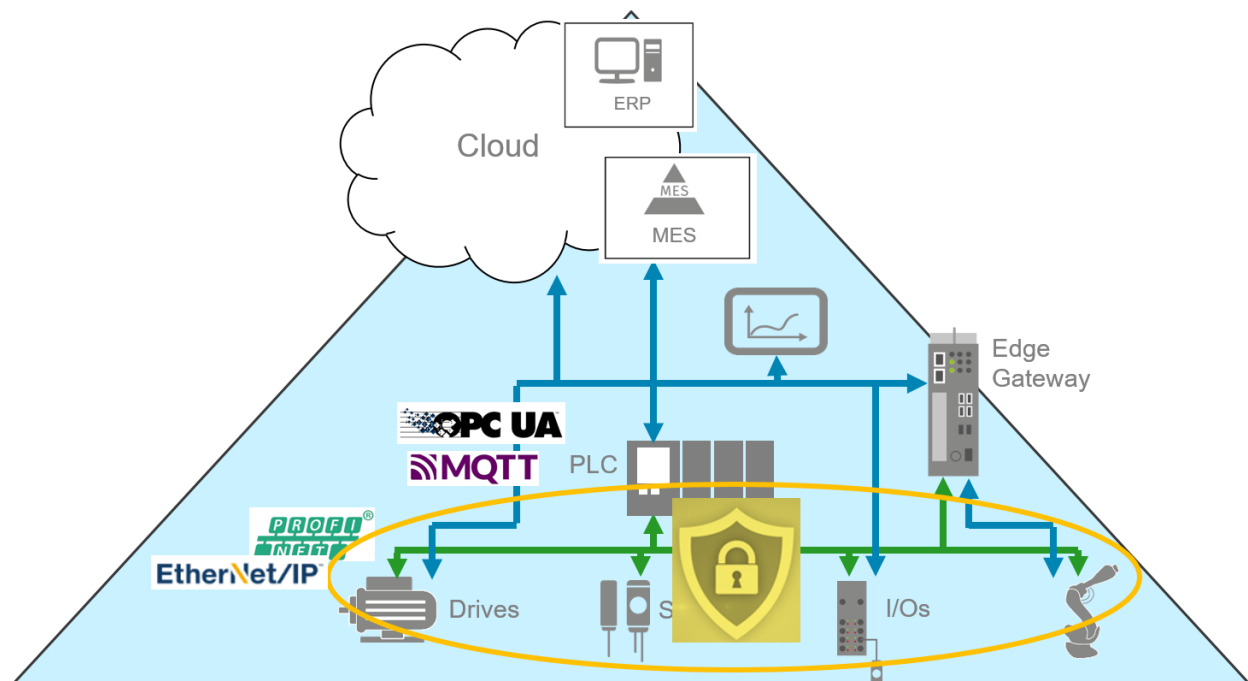


Figure 1. OT-level communications.

Advantages of field-level security

Field-level security is required to further open industrial networks toward enterprise networks and the internet. Access to field-level data increases production process transparency and visibility, enabling new technologies to increase productivity.

One simple application is asset management, while device condition monitoring, remote diagnostics, and predictive maintenance are other potential applications that enable system operators to save time and money.

New business models are possible when applications in the cloud can directly access the field level. Machine builders can release their products and charge customers by production quantities rather than selling a machine. This will lead to more flexibility in production processes — factories could offer individualized products down to a lot size of one.

Controlling physical access to industrial facilities is difficult, expensive, and sometimes impossible when systems are distributed over large areas like chemical process automation systems. However, cybersecurity-protected networks could make physical access restrictions obsolete because a communication channel that prevents infiltration allows a system to be exposed to the public without risks. Going forward, it is expected that authorities worldwide will increase mandatory requirements related to cybersecurity functions for industrial automation equipment.

Device makers must follow these upcoming requirements and can benefit from Hilscher solutions since cybersecurity functions are transparently integrated into the protocol stacks. This alleviates a lot of development-engineering responsibilities—an API interface can be used for security certificate handling.

Applying new technologies to industrial environments

It isn't necessary to reinvent the wheel in order to provide security functions to field devices. OT can borrow well-established security methods and standards from the IT world. One example is EtherNet/

IP CIP Security, which makes use of proven SSL/TLS technology and its underlying methods, to secure IP-based real-time Ethernet communication. It uses the same cryptographic algorithms like Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), or Diffie-Hellmann Elliptic Curve Cryptography (ECC), which are all already established in IT systems. This is similar to Profinet security and other industrial Ethernet-based communication standards.

However, technologies must be adapted to the unique requirements of OT networks such as determinism, guaranteed timing behavior and long maintenance intervals. But this adaptation is a difficult task, as OT devices typically have limited resources in terms of CPU performance, memory, and available space.

For this reason, Hilscher includes dedicated security hardware support to its netX 90 multiprotocol communication controller. Security-enabled firmware makes use of a hardware accelerator for encryption functions to unburden the CPU and guarantee deterministic real-time behavior (Figure 2).

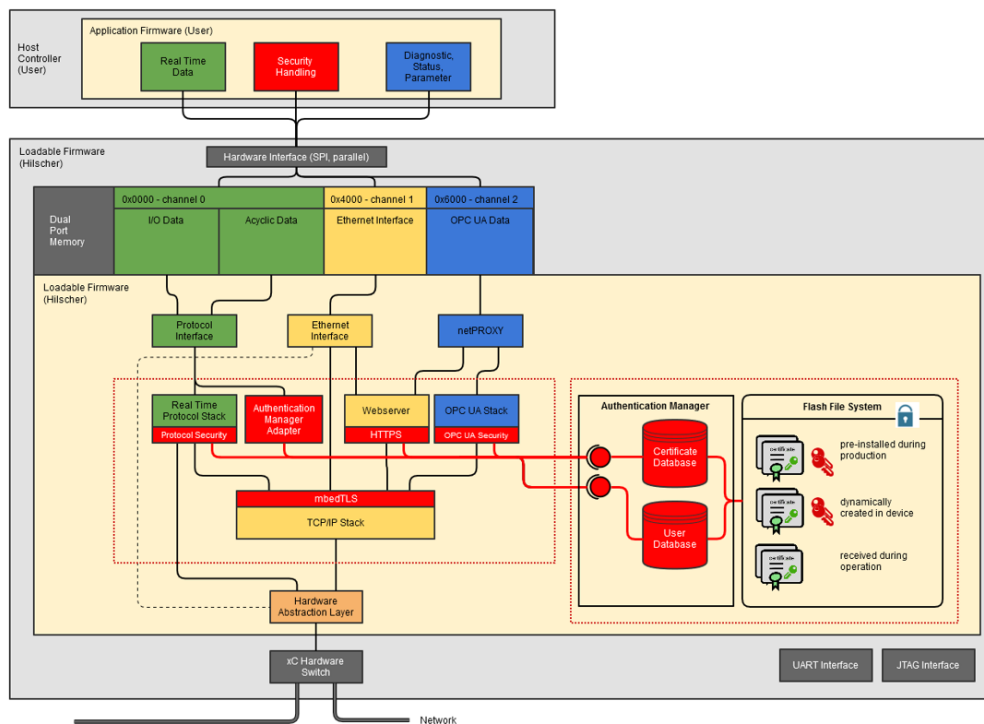


Figure 2. Security at the OT level.

Hilscher provides the protocol firmware as a monolithic binary, running independently on a dedicated CPU on the netX communication controller. Users won't have to hassle with library integration, enabling fast time to market.

Where to direct cybersecurity efforts

Field-level cybersecurity is important for all sectors of the industrial automation market. As discussed earlier, every system operator who wants to benefit from IT/OT convergence must consider field-level cybersecurity. Automation system operators must reduce the high-cost risks caused by cyberattacks.

Authorities will define systems rules, beginning with critical infrastructure, and certain security levels will be mandatory in such systems. This shows there is a market demand for all kinds of security-enabled automation equipment such as servo drives, sensors, valves, and IO-systems. These components, and others like them, will have to meet IEC 62443 requirements. Hilscher's solution is ideal for device makers, as it provides a ready-to-use protocol firmware with integrated security functionality that helps them equip their devices quickly at a low cost.

Cybersecurity solves industrial automation challenges

Real-time Ethernet protocols are common and widespread in automation systems. But implementing them requires constant maintenance since the compliance test specifications are continually adjusting and expanding. Security extensions add another level of complexity, because even if device integrators are familiar with the protocol specifications, the latest cybersecurity extensions require a lot of time to build knowledge, train, and implement. The Hilscher netX 90 with security protocol firmware is a solution for this problem.

Handling security certificates poses another challenge. Each device in a secure network requires certificates that must be initially

deployed (transferred to and stored on the device), then updated in regular intervals. Typically, this task is the operator's responsibility, and it should occur during normal system operation. But there are different approaches to address this issue.

Operators may want full control over certificates and keys because they are using a public key infrastructure (PKI) or they might want to leave key generation and certificate signing to the device maker. Therefore, component manufacturers must provide flexible solutions for their products.

The security-enabled protocol firmware from Hilscher provides a flexible certificate manager that supports a variety of different uses and enables the freedom to adapt to individual requirements and use cases.

ABOUT THE AUTHOR



Philip Marshall is the CEO of [Hilscher North America](#) and is responsible for overseeing all development and sales activities for the U.S. and Canada. Marshall has been active in industrial communications since 1985. He holds a BS in operations management and information systems from Bradley University.

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.



Finding a Faster Fieldbus

Speed, flexibility, and simplicity make EtherCAT a robust fieldbus contender.

By Jack Smith,
Automation.com

Ethernet-based fieldbuses have their challenges, but speed, flexibility, and simplicity make EtherCAT a robust contender in industrial automation environments. The EtherCAT (Ethernet for control automation technology) fieldbus system was invented by Beckhoff Automation to apply Ethernet to automation applications requiring short data update times (cycle times) of less than 100 microseconds with low communication jitter of less than 1 microsecond. The protocol is standardized in IEC 61158 and is suitable for both hard and soft real-time computing requirements in automation technology.

Why fieldbuses are important

While the controller is obviously important to the controlled architecture, the bus system is the core. “The bus system defines

system performance much more than the controller,” said Martin Rostan, executive director of [EtherCAT Technology Group](#). “It’s the bus system that defines the choice of suppliers, especially if [users] pick a bus system that is supported on the controller side by only one supplier. Therefore, it’s also the bus system that defines the cost. It’s a bus system that defines if [users] have the choice, if [they] can go with centralized controls—closed, fast control loops—over the bus system or not.”

People used to think decentralized controls was a solution for difficult situations because neither their “centralized” controllers nor their bus systems had the performance to close fast-acting loops on a centralized CPU. They had to live with many programming languages and/or controllers to close those fast control loops in a decentralized way. However, with EtherCAT, users can do both. “Users can do either centralized or decentralized,” Rostan said.

●●●●● **Three main challenges** associated with Ethernet and fieldbus control performance are bandwidth utilization, stack delay issues, and switch delays.

“The control- and the bus-cycle times have a big impact on the reaction time,” Rostan explained. “It has an even bigger impact, not on the control cycle time, but whether you can make use of the control cycle time. We see people who use PC-based controls, which can execute PLC [programmable logic controller] code quickly and do cycle times in the sub-millisecond range, combine that with a legacy bus technology, or with one of our competitor’s bus technologies, which is more in the several millisecond range. Then, they’re disappointed by the performance of the overall architecture.”

Tackling the challenges of Ethernet fieldbuses

Three main challenges associated with Ethernet and fieldbus control performance are bandwidth utilization, stack delay issues, and switch delays.

Bandwidth utilization. The Ethernet frame is a minimum of 84 bytes (Figure 1). There is no smaller Ethernet frame than that. The inter-packet gap is considered since it must be considered in a bandwidth-count situation. “If such a large container is used to transport a few bits or bytes, there will be a poor application data ratio,” Rostan said. “With four bytes of process data, for example, in such a frame, there would be less than 5 percent application data ratio—the rest is just air. It’s not the most efficient usage of bus bandwidth.”

Stack delays. Most people neglect stack delays based on the assumption that by the time the frame has arrived in the node, it’s available. “On the contrary, it must go through the local stack, with 1 MB of code or more if EtherNet/IP or Profinet is used,” Rostan said. “This takes time because these industrial Ethernet protocol stacks are big and time consuming to get through all those intermediate layers and get through to the application. In a simple case, the application is the output, or it’s the control algorithm of your device.”

Measurements show that EtherNet/IP takes up to 3 milliseconds to get through the protocol stack. According to Rostan, EtherCAT is lean in contrast. The EtherCAT stack is about 70 kB of code. “With digital input/output (I/O) and EtherCAT, the stack delay time is zero because the EtherCAT chips have I/O onboard. In the hardware, there’s no software interaction whatsoever.”

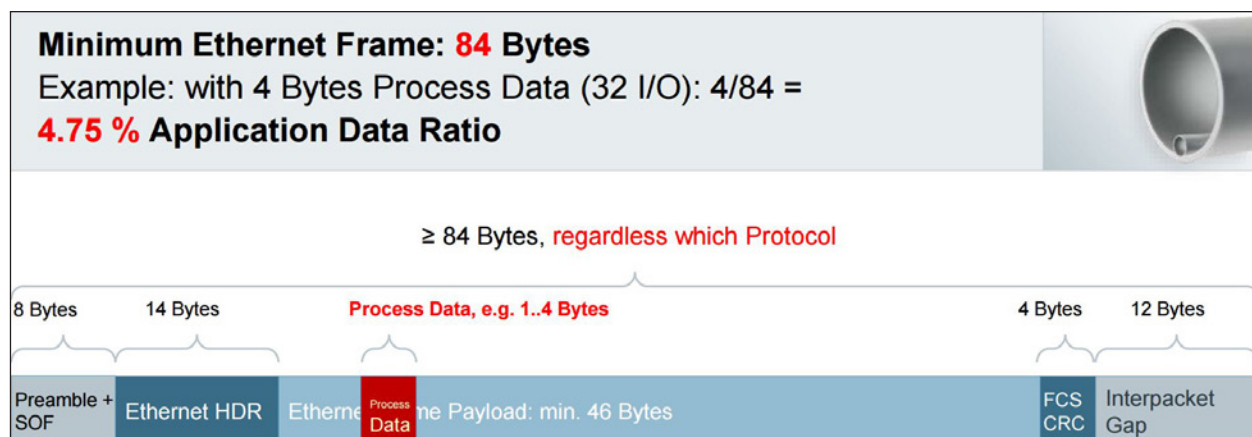


Figure 1. The Ethernet frame is a minimum of 84 bytes.

Switch delays. Switches are unpredictable by nature. “We don’t know in what sequence the frames arrive in the switch, so we don’t really know in what sequence they will leave that buffer again,” Rostan said. “Also, the buffer is in between; that’s the big issue with switches. Even if there is no other traffic, switches operate in so-called “store and forward mode,” which means when they receive the frame, first, switches check for the frame check sequence or the cyclic redundancy check (CRC) in the end of the frame. Only if the frame is healthy, switches will copy it to the send buffer. This is the only recognized method by IEEE because that’s what information technology (IT) personnel prefers. They don’t want corrupted frames floating around in their network.”

In switches, the store and forward methodology takes time to receive the frame and look at the CRC at the end of the frame. For 20 nodes and a large frame, it takes 2.5 milliseconds just to get through those cascaded switches. A device may not look like a switch; it may look like a drive. But, if it’s a switch-based technology such as Ethernet/IP or Profinet, there’s a switch chip inside, so it is a switch from a network point of view.

According to Rostan, EtherCAT does not have that issue; the frame goes through the devices right away. Those three reasons combined are the reasons why most industrial Ethernet technologies are not faster than the previous generation fieldbus they are supposed to replace.

High performance Ethernet on the fly

Rostan claims that EtherCAT is the fastest industrial Ethernet technology. Speed claims include:

- ▶ 1,000 distributed digital I/O in 30 microseconds
- ▶ 100 servo axis updates every 100 microseconds
- ▶ EtherCAT goes directly to the I/O slice, no sub-bus
- ▶ Optimal usage of the standard Ethernet port in the controls with no extra hardware

This performance is attributed to the EtherCAT functional principle: Ethernet on the fly (Figure 2). Characteristics include:

- ▶ Efficient: typically, only one Ethernet frame per cycle
- ▶ Ideal bandwidth utilization for maximum performance
- ▶ Resolves the three main performance problems (bandwidth utilization, stack delay issues, and switch delays)
- ▶ Operates in real time and can reach down to the I/O level
- ▶ No underlying subsystems, thus no delays in bus coupler gateways
- ▶ Connects everything in one system: I/O, sensors, actuators, drives, and displays

Rostan explains Ethernet on the fly further. “Instead of sending one frame to each node in each cycle in each direction, EtherCAT sends one frame through the node, and each device extracts data from that frame

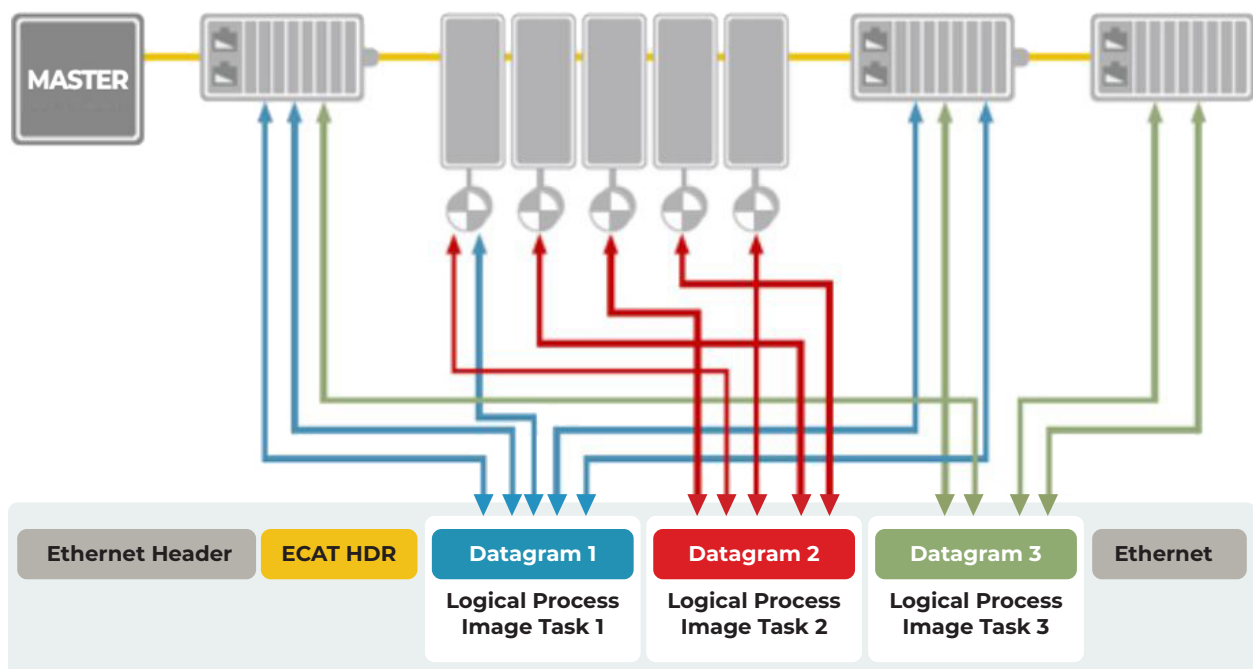


Figure 2. Inserting process data on the fly.

and inserts its data into the very same frame. In doing so, all sub-devices share one frame, and the bandwidth is even doubled—in ideal cases—because EtherCAT uses the same frame for input and for output data, so we get 200 megabits up front if we have a symmetrical process image.”

EtherCAT configuration/operation

The EtherCAT master sends an Ethernet frame that passes through each node. Each EtherCAT sub-device reads the data addressed to it “on the fly” and inserts its data in the frame as the frame is moving downstream. The frame is delayed only by hardware propagation delay times. The last node in a segment (or drop line) detects an open port and sends the message back to the master using Ethernet technology’s full duplex feature.

The frame’s maximum effective data rate increases to more than 90 percent, and due to the utilization of the full duplex feature, the theoretical effective data rate is even higher than 100 Mbit/s (greater than 90 percent of two x 100 Mbit/s).

●●●●● **Instead of sending one frame** to each node in each cycle in each direction, EtherCAT sends one frame through the nodes, and each device extracts data from that frame and inserts its data into the very same frame.

The EtherCAT master is the only node within a segment allowed to actively send an EtherCAT frame. All other nodes merely forward frames downstream. This concept prevents collisions as well as unpredictable delays and guarantees real-time capabilities.

The master uses a standard Ethernet media access controller (MAC) without an additional communication processor. This allows a master to be implemented on any hardware platform with an available Ethernet port, regardless of which real-time operating system or application software is used. EtherCAT sub-devices use an EtherCAT sub-device controller (ESC) to process frames on the fly and entirely in

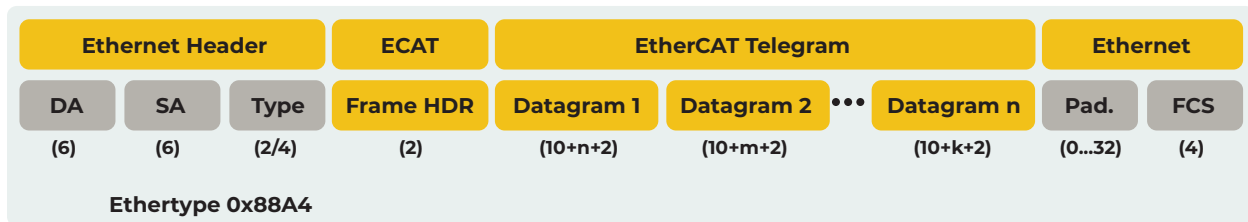


Figure 3. EtherCAT in a standard Ethernet frame (according to IEEE 802.3).

hardware, making network performance predictable and independent of the individual sub-device implementation.

EtherCAT protocol. EtherCAT embeds its payload in a standard Ethernet frame (Figure 3). The frame is identified with the Identifier (0x88A4) in the EtherType field. Since the EtherCAT protocol is optimized for short cyclic process data, the use of protocol stacks such as TCP/IP or UDP/IP for process data communication can be eliminated.

During startup, the master device configures and maps the process data on the sub-devices. Different amounts of data can be exchanged with each sub-device, from one bit to a few bytes, or even up to kilobytes of data.

The EtherCAT frame contains one or more datagrams. The datagram header indicates what type of access the master device would like to execute:

- ▶ Read, write, or read-write
- ▶ Access to a specific sub-device through direct addressing, or access to multiple sub-devices through logical addressing (implicit addressing)

Logical addressing is used for the cyclical exchange of process data. Each datagram addresses a specific part of the process image in the EtherCAT segment, for which 4 GB of address space is available. During network startup, each sub-device is assigned one or more addresses in this global address space. If multiple sub-devices are assigned addresses in the same area, they all can be addressed with a single datagram.

Since the datagrams completely contain all the data access-related information, the master device can decide when and which data to access. For example, the master device can use short cycle times to

refresh data on the drives, while using a longer cycle time to sample the I/O. A topology-related fixed process data structure is not necessary. This also relieves the master device in comparison to conventional fieldbus systems in which the data from each node had to be read individually, sorted with the help of the process controller, and copied into memory.

With EtherCAT, the master device only needs to fill a single EtherCAT frame with new output data and send the frame via automatic direct memory access (DMA) to the MAC controller. When a frame with new input data is received via the MAC controller, the master device can copy the frame again via DMA into the computer's memory—all without the CPU having to actively copy any data. In addition to cyclical data, further datagrams can be used for asynchronous or event-driven communication.

Flexible topology. EtherCAT supports all topologies—line, tree, star, or any combination of these (Figure 4). EtherCAT makes a pure bus or line topology with hundreds of nodes possible without the limitations that normally arise from cascading switches or hubs.

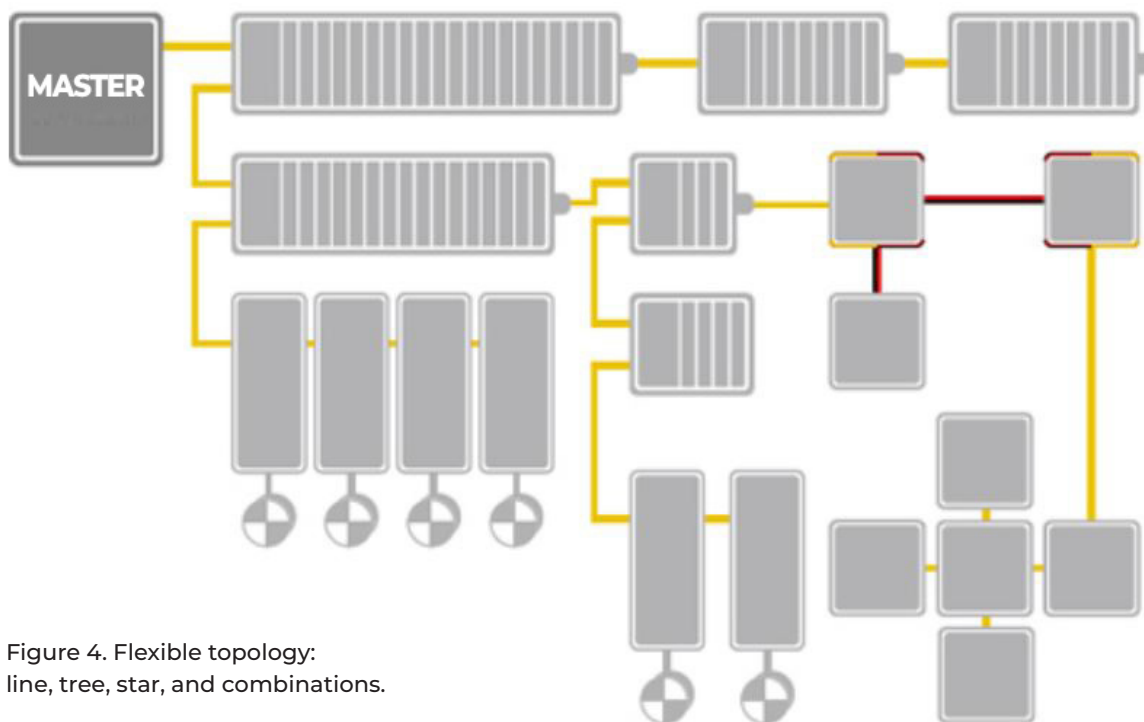


Figure 4. Flexible topology: line, tree, star, and combinations.

When wiring the system, the combination of lines with drop lines is beneficial. The ports necessary to create drop lines are directly integrated in many I/O modules, so no additional switches or active infrastructure components are required. The star topology—the Ethernet classic—can also be used.

EtherCAT offers flexibility regarding cable types, so each connection can use the exact type of cable that best meets its needs. Inexpensive industrial Ethernet cable can be used between two nodes up to 100 meters apart in 100BASE-TX mode. The protocol extension EtherCAT P enables the transmission of data and power via one cable. This option enables the connection of devices such as sensors with a single line. Fiber optics (such as 100BASE-FX) can also be used, for example, for a node distance greater than 100 meters. The complete range of Ethernet wiring is also available for EtherCAT.

Final thoughts

Up to 65,535 nodes can be connected to one EtherCAT segment, so network expansion is virtually unlimited. Because of the practically unlimited number of nodes, modular devices such as “sliced” I/O stations can be designed in such a way that each module is an EtherCAT node of its own. Therefore, the local extension bus is eliminated. The performance of EtherCAT reaches each module directly and without any delays since there is no gateway in the bus coupler or head station.

ABOUT THE AUTHOR



Jack Smith (jsmith@automation.com) is a senior contributing editor for Automation.com and ISA's *InTech* magazine. He spent more than 20 years working in industry—from electrical power generation to instrumentation and control, to automation, and from electronic communications to computers—and has been a trade journalist for 22 years.



✓ Protected

✓ Protected

✓ Protected

Industrial Cybersecurity. **Simplified.**



Keep the Operation Running



Integrating Safety and Security Strengthens Cybersecurity

By Nick Creath, Rockwell Automation

Most conversations about the Industrial Internet of Things (IIoT), safety, and security revolve around two separate topics: “smart” machinery or process safety to protect people and equipment, or industrial control system (ICS) security.

These conversations are important and valid. However, too many industrial companies are not focused on the inherent safety implications of common security risks. For example:

- ▶ When an oil pipeline was hacked in Turkey causing an explosion and 30,000 barrels of spilled oil, the cyber attackers negated the existing safety system to shut down alarms, cut off communications, and super-pressurize crude oil in the line.

Closing security gaps and strengthening security make organizations more resilient to future threats.

- ▶ A regional water supplier experienced a cybersecurity breach that not only compromised customer data but caused unexplained valve and duct movements, including manipulation of programmable logic controllers (PLCs) that managed water treatment and public safety.

These attacks highlight how safety and security programs are inextricably linked in industrial production.

Many manufacturers are tapping into IIoT technology to remotely access production machinery, allow wireless access to pumping stations, or connect plant-floor equipment to the information technology (IT) infrastructure. This is the future. This is how manufacturers can realize improved asset utilization, faster time to market, and lower total cost of ownership. However, greater connectivity can increase security risks that will impact safety. This is where better enterprise risk management is important.

●●●●● **The concept of digital transformation** is bringing production intelligence to manufacturers for measuring and improving nearly every aspect of their operations.

Integrating safety and security efforts

Safety and security have traditionally been viewed as separate entities, but there is a commonality between them in the approaches used to analyze and mitigate risks. For example, the concept of “access control” is common between safety and security. In both cases, policies and procedures are built based on business practices, risk management approaches, application requirements, and industry standards.

Manufacturers and industrial operators who want to reduce the likelihood of security-based safety incidents must rethink safety. Specifically, start thinking of safety and security in relation to each other. This relationship can have the biggest impact in three key areas:

- 1. Behavior:** In addition to helping protect intellectual property, processes, and physical assets, security personnel must make protecting safety systems a core value in everything they do. Greater collaboration between environmental, health, and safety (EHS); operations; and IT teams is more important than ever. All three teams should work together to develop co-managed objectives for safety and security and identify critical safety-data requirements from plant-floor systems. Because a strong safety culture involves every employee, a companywide understanding of the relationship between security and safety is needed.
- 2. Procedure:** Compliance efforts should meet the security requirements in safety standards, such as [IEC 61508](#) and [IEC 61511](#). Conversely, security efforts should follow an in-depth defense approach and address safety-related security risks at all levels of an organization. Defense in depth is recommended in the [IEC 62443](#) (“Security for Industrial Automation and Control Systems”) standard series (formerly ISA99) and elsewhere.
- 3. Technology:** All safety technologies should have built-in security features. They should also use security technologies that help protect against safety-system breaches and enable speedy recoveries should a breach occur.

Risk mitigation

The list of potential security threats that could have safety implications is quite vast. So, any mitigation of a company’s security-based safety risk must start with understanding where it is most vulnerable. This should be done by conducting separate safety and security risk assessments, then comparing reports to examine where security most impacts safety. This will allow users to best address their unique set of risks.

The concept of digital transformation is bringing production intelligence to manufacturers for measuring and improving nearly every aspect of their operations. It’s also providing instantaneous information sharing and seamless collaboration across organizations.

For these opportunities, more connection points can create more entrance points for security threats. Users must account for and address how these threats impact the safety of their people, their infrastructure, and the environment around their operations. The IIoT is bringing opportunity, risk, and the ability to holistically integrate safety and security programs to optimize operations.

A proactive approach to ICS security

Industrial organizations must prioritize safety and reliability to protect against cyberattacks—and quickly. With risks and reporting mandates growing, a paradigm shift must occur. Five key focus areas, or steps, can help assess and improve cybersecurity hygiene and a converged IT and operational technology (OT) security strategy. These factors are based on guidance from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

●●●●● **Industrial organizations** must prioritize safety and reliability to protect against cyberattacks—and quickly.

Step No. 1: Identify. One of the biggest roadblocks to building a great cybersecurity program is that many production environments are poorly inventoried. If users don't know what's connected to their network, whether it's part of the ICS or a new type of productivity software used by an employee, they can't secure that environment properly.

First, identify, map, and verify everything that's connected to the network. Users can do this themselves or work with a partner that offers installed base asset identification tools and services. Determining vulnerabilities and initial risk posture is the first step.

Another helpful technique in understanding exactly what to protect is reviewing operations through a zero-trust lens, using a protect surface approach that prioritizes business-critical data, assets, applications, and services (DAAS) in priority order. Apply the best protect controls available as close as possible to what's being protected.

Step No. 2: Protect. Once users have taken inventory of their assets and understand what must be protected, it's time to apply the right safeguards against the ever-changing landscape of cyber threats.

There are many protective measures that can be implemented. Choose the types of controls that are in alignment with any compliance standards or security frameworks, such as the NIST CSF. That includes multi-factor authentication, access control, data security, perimeter network deployment, and micro segmentation. Protective measures also include the common industrial protocol (CIP) product security, perimeter hardening, firewall deployment, and patch management. These countermeasure controls help manage risk proactively and protect the data that's essential to your operations.

Step No. 3: Detect. Protecting industrial networks against cyber threats requires constant vigilance. Knowledge of all endpoints on the organization's network from plant-floor assets to laptops, mobile devices, even security cameras, or USB ports, is critical. Users also need real-time visibility into how, when, and where others are accessing or manipulating assets.

●●●●● **Threat detection services** can help users monitor and detect these increasingly complex threats.

Threat detection services can help users monitor and detect these increasingly complex threats. These services provide visibility across all levels of IT and OT environments, meaning they not only look for malicious activities, but offer real-time monitoring and deep network inspection across all assets.

Managed threat detection is a powerful cybersecurity defense, especially in critical infrastructure, industrial manufacturing, and other OT environments. An OT security operations center (SOC) staffed with experienced security veterans provides a unique pooling of talent,

technology, and first-hand experience. This cybersecurity protection expertise is difficult to duplicate for the same cost by individual organizations. With the convergence of security operation tools in IT—such as security information and event management (SIEM) and security orchestration, automation, and response (SOAR)—these security tools will soon hit production environments, driving the need for automated response and triage, disaster recovery, and response planning.

Step No. 4: Respond. If a security incident occurs, it's critical to respond immediately and address the threat before it spreads and causes greater damage. That's why having threat detection services in place beforehand is essential to effective risk management. Similarly, having a mature incident response plan or disaster recovery plan will achieve minimized downtime to restore production operations.

Step No. 5: Recover. The top priority after a security-related downtime event is to get production up and running as quickly as possible. For this step, it's important to use backup and recovery services to keep near real-time records of production and application data. Having these resources in place will allow users to resume normal operations after an incident, shortening the recovery cycle.

Once operations are running smoothly again, investigate and analyze the incident and fully identify the root cause. This analysis will illuminate ways to close security gaps and improve security posture. It will also make the organization more resilient to related threats down the line.

ABOUT THE AUTHOR



Nick Creath is a senior product manager at Rockwell Automation. He has more than 15 years of experience in the automation industry. In his current role, he is responsible for bringing new cybersecurity services to market that will enable Rockwell Automation customers to increase the security posture of their industrial control environments. Nick can be reached at nncreath@rockwellautomation.com.

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

Get Engaged!

[Follow our blog](#)

[Download our white papers and guides](#)

[Join the End User Council](#)



Securing Critical Infrastructure with **ZERO TRUST**



SECURITY



WIFI



CLOUD SERVICE

MUTUAL
AUTHENTICATION

CHECK



NETWORK



ACCESS

Being operationally resilient requires a multitude of safeguards that span OT and IT.

By Anand Oswal,
Palo Alto Networks

Critical infrastructure forms the fabric of our society, providing power for our homes and businesses, fuel for our vehicles, and medical services that preserve human health. With the acceleration of digital transformation spurred by the pandemic, larger and larger volumes of critical infrastructure and services have become increasingly connected. Operational technology (OT) serves a critical role as sensors in power plants, water treatment facilities, and a broad range of industrial environments.

Digital transformation has also led to a growing convergence between OT and information technology (IT). All of this connection brings accessibility benefits, but it also introduces a host of potential security risks.

Cyberattacks on critical infrastructure threaten many aspects of our lives

It's a hard fact that there isn't an aspect of life today free from cyberthreat. [Ransomware](#) and [phishing attacks](#) continue to proliferate, and in recent years, we've also seen an increasing number of attacks against critical infrastructure targets. Even in environments where OT and IT have been traditionally segmented or even air-gapped, these environments have largely converged, presenting attackers with the ability to find an initial foothold and then escalate their activities to more serious pursuits, such as disrupting operations.

Examples are all around us. Among the most far-reaching attacks against critical infrastructure in recent years was the Colonial Pipeline incident, which triggered resource supply fears across the United States as the pipeline was temporarily shut down. Automobile manufacturer Toyota was forced to shut down briefly after a critical supplier was hit by a cyberattack. Meat processing vendor JBS USA Holding experienced a ransomware cyberattack that impacted the food supply chain. The Oldsmar water treatment plant in Florida was the victim of a cyberattack that could have potentially poisoned the water supply. Hospitals have suffered cyberattacks and ransomware that threaten patients' lives, with the FBI warning that North Korea is actively targeting the U.S. healthcare sector. The list goes on and on.

Global instability complicates this situation further as attacks against critical infrastructure around the world spiked following Russia's invasion of Ukraine, with the deployment of Industroyer2 malware that is specifically designed to target and cripple critical industrial infrastructure.

Today's challenges place an increasing focus on operational resiliency

With all of these significant challenges to critical infrastructure environments, it's not surprising that there is a growing focus on operational resiliency within the sector. Simply put, failure is not an option. You can't have your water or your power go down or have food



supplies disrupted because an outage of critical infrastructure has a direct impact on human health and safety. So, the stakes are very high, and there is almost zero tolerance for something going the wrong way.

Being operationally resilient in an era of increasing threats and changing work habits is an ongoing challenge for many organizations. This is doubly true for the organizations, agencies, and companies that comprise our critical infrastructure.

●●●●● **Even where OT and IT have been segmented** or air-gapped, these environments have largely converged, presenting attackers with the ability to find a foothold and then escalate their activities.

Digital transformation is fundamentally changing the way this sector must approach its cybersecurity. With the emerging [hybrid workforce](#) and accelerating [cloud migration](#), applications and users are now everywhere, with users expecting access from any location on any device. The implied trust of years past, where being physically present in an office provided some measure of user authenticity simply no longer exists. This level of complexity requires a higher level of security, applied consistently across all environments and interactions.

Overcoming cybersecurity challenges in critical infrastructure

To get to a state of resiliency, there are a number of common challenges in critical infrastructure environments that need to be overcome because they negatively impact security outcomes. These include:

Legacy systems. Critical infrastructure often uses legacy systems far beyond their reasonable lifespan from a security standpoint. This means many systems are running older, unsupported operating systems, which often cannot be easily patched or upgraded due to operational, compliance, or warranty concerns.



IT/OT convergence. As IT and OT systems converge, OT systems that were previously isolated are now accessible, making them more available and, inherently, more at risk of being attacked.

A lack of skilled resources. In general, there is a lack of dedicated security personnel and security skills in this sector. There has also been [a shift](#) in recent years toward remote operations, which has put further pressure on resources.

Regulatory compliance. There are rules and regulations across many critical infrastructure verticals that create complexity concerning what is or isn't allowed.

Getting insights from data. With a growing number of devices, it's often a challenge for organizations to get insights and analytics from usage data that can help to steer business and operational outcomes.

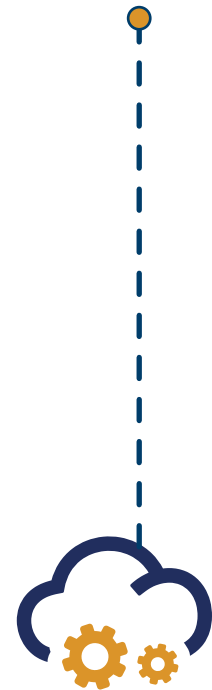
The importance of Zero Trust in critical infrastructure

A Zero Trust approach can help to remediate a number of the security challenges that face critical infrastructure environments and also provide the level of cyber resilience that critical infrastructure needs now.

How come? The concept of Zero Trust, at its most basic level, is all about eliminating implied trust. Every user needs to be authenticated, every access request needs to be validated, and all activities continuously monitored. With Zero Trust authentication, access is a continuous process that helps to limit risk.

Zero Trust isn't just about locking things down; it's also about providing consistent security and a common experience for users, wherever they are. So, whether a user is at home or in the office, they get treated the same from a security and risk perspective. Just because a user walked into an office doesn't mean they should automatically be granted access privileges.

And it isn't only about users: the same principles apply to cloud workloads and infrastructure components like OT devices or network nodes. There is still a need to authenticate devices and access to



authorize what the device is trying to do and provide control, and that's what the Zero Trust Model can provide.

All of these aspects of Zero Trust enable the heightened security posture that critical infrastructure demands.

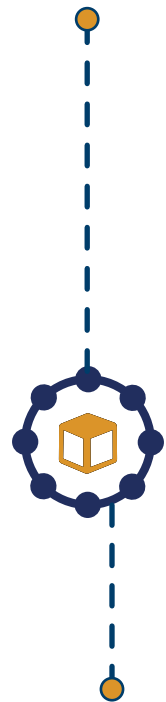
Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of implicit trust from an organization's network architecture. The most important objectives in CI cybersecurity are about preventing damaging cyber physical effects to assets, loss of critical services, and preserving human health and safety. Critical infrastructure's purpose-built nature and correspondingly predictable network traffic and challenges with patching make it an ideal environment for Zero Trust.

Applying a Zero Trust approach that fits critical infrastructure

It's important to realize that Zero Trust is not a single product; it's a journey that organizations will need to take.

Going from a traditional network architecture to Zero Trust, especially in critical infrastructure, is not going to be a "one-and-done" effort that can be achieved with the flip of a switch. Rather, the approach we recommend is a phased model that can be broken down into several key steps:

- 1. Identifying the crown jewels.** A foundational step is to first identify what critical infrastructure IT and OT assets are in place.
- 2. Visibility and risk assessment of all assets.** You can't secure what you can't see. Broad visibility that includes behavioral and transaction flow understanding is an important step in order to not only evaluate risk but also to inform the creation of Zero Trust policies.
- 3. OT-IT network segmentation.** It is imperative to separate IT from OT networks to limit risk and minimize the attack surface.



4. **Application of Zero Trust policies.** This includes:

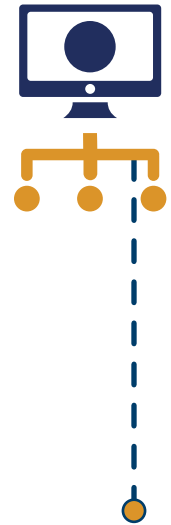
- ▶ Least-privileged access and continuous trust verification, which is a key security control that greatly limits the impact of a security incident
- ▶ Continuous security inspection that ensures the transactions are safe by stopping threats—both known and unknown, including zero-day threats—without affecting user productivity

By definition, critical infrastructure is vital. It needs to be operationally resilient, be able to reduce the potential attack surface, and minimize the new or expanding risks created by digital transformation. When applied correctly, a Zero Trust approach to security within critical infrastructure can play a central role in all of this—ensuring resilience and the availability of services that society depends on every day.

Built for comprehensive security

We have designed Zero Trust OT Security to enable both best-in-class security and superb operational up-time by focusing on three pillars:

1. **Start with comprehensive visibility:** As they say, you can't secure what you can't see. And, OT assets are among the hardest devices to discover. The Palo Alto Networks Zero Trust OT Security solution starts with our already best-in-class visibility and adds deep and broad OT device coverage with our new Industrial OT Security offering. With Zero Trust OT Security, you can see everything, and that's the foundation.
2. **Cover every environment with Zero Trust:** Customers tell me they struggle trying to cover the wide variety of environments they run into. They have OT and IT devices converging on their networks. They have employees, partners and vendors remote-accessing their facilities. And, they have increasingly complex architectures with new technologies, like 5G networks expanding everywhere. Zero Trust OT Security makes it easy to secure each of these environments with the industry's best Zero Trust security. From least



privilege access control, to continuous trust verification and security inspection, Zero Trust OT Security has you covered, everywhere.

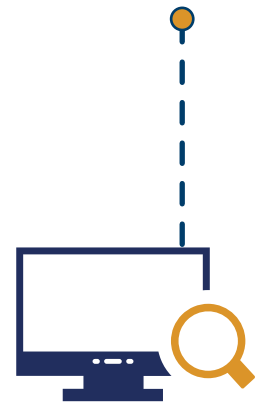
- 3. Make it simple to operate:** Perhaps my favorite customers to talk to are the ones who have cobbled together siloed solutions, who try to chip away at their visibility challenges, and who plug security holes in every unique environment they have. These customers tell me that the complexity of multiple solutions is leaving security gaps, breaking their teams and breaking their bank. They need something that is consistent, easy to use and affordable in this increasingly volatile economy. Zero Trust OT security is designed to provide consistent security from a single trusted partner, freeing you and your teams to spend time on security, not on setup and silos.

By sticking to these three principles our solution delivers exactly what OT leaders need – Zero Trust security that keeps operations up 24/7, not CISOs.

More on Zero Trust and industrial ot security

Visit our [solutions page](#) for more resources and case studies on Zero Trust OT Security.


Learn more about how [Industrial OT Security](#) helps customers achieve a return on investment (ROI) of 351% with up to 95% lower complexity than alternative OT security solutions.



ABOUT THE AUTHOR



Anand Oswal is the senior vice president and general manager at Palo Alto Networks, where he leads the company's Firewall as a Platform efforts. Prior to this he was senior vice president of engineering for Cisco's Intent-Based Networking Group. In this role, he was responsible for building the entire set of platforms, from switching, wireless and routing to IoT and cloud services, that make up Cisco's extensive enterprise networking portfolio. Anand holds more than 60 U.S. patents and holds a bachelor's degree in telecommunications and a master's in computer networking. He is a frequent speaker on technology, innovation, management, diversity, and the importance of family.

A photograph of industrial machinery, featuring large green cylindrical tanks and a complex network of pipes and valves. The scene is lit with a cool, blue-green light, creating a technical and industrial atmosphere. The machinery is the central focus, with various pipes, valves, and tanks visible, suggesting a complex industrial process.

Cyber Safeguarding Industrial Operational Support

By Steve Mustard, National Automation

Excerpt from new OT cybersecurity book, *Industrial Cybersecurity Case Studies and Best Practices*.

One of the distinguishing features of operational technology (OT) is the operational life of the equipment. Information technology (IT) is refreshed every 18 months to 3 years to keep pace with the demands of users and their applications. Conversely, OT equipment is designed for a specific, limited set of functions. Once deployed, there is little desire to change it.

Safety is a major concern in industrial environments, yet cybersecurity, despite being a potential initiating cause in these hazards, is not respected in the same way as safety is. Many organizations begin meetings or presentations with the refrain that safety is the number one concern. But in those same meetings, there may be comments to the effect that “We have more important priorities than cybersecurity.” Clearly, there is still much to do before cybersecurity receives the attention it requires in operational environments.

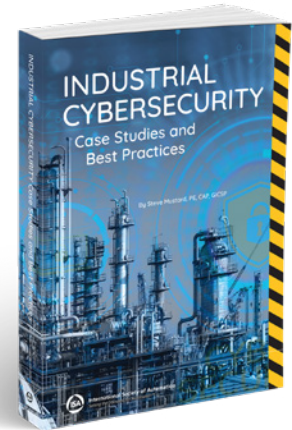
Some important operational considerations are:

- ▶ Monitoring the effectiveness of cybersecurity controls
- ▶ People management
- ▶ Inventory management
- ▶ Incident response
- ▶ Suppliers, vendors, and subcontractors
- ▶ Insurance

Monitoring the effectiveness of cybersecurity controls

Barrier model analysis is widely used in process industries to help analyze and visualize the status of the layers of protection required to maintain a safe operation.

Organizations may use different means to visualize their layers of protection. One approach is to use bowtie diagrams. Another is to use the Swiss cheese model, shown in Figure 1. The methodology in either case is simple: identify a set of barriers to prevent and mitigate an incident or accident. A failure of one of the barriers may not be sufficient to cause an accident: however, should a series of failures occur across several barriers, there is the potential for an incident to occur. The bowtie or Swiss cheese model is used in organizations to answer the question *are we still safe to operate?* by interrogating data related to each barrier.



Industrial cybersecurity expert and former International Society of Automation president Steve Mustard has written multiple books on industrial automation topics. This latest, [*Industrial Cybersecurity Case Studies and Best Practices*](#), is available now in print, ePub, and Kindle formats from [ISA Books](#). Learn more about it in his own words in his October 2022 appearance on [NasdaqTV](#).

Integrating cybersecurity into such a reporting tool helps to make cybersecurity a key factor. Now the barrier representation being reviewed clearly shows the status of cybersecurity at the facility. The question *are we still safe to operate?* now includes the status of cybersecurity.

People management

Employers need a means of overseeing their employees to quickly identify any issues that may lead to a cybersecurity incident, particularly from disgruntled persons.

- ▶ **Background checks:** The depth of the background check should be appropriate to the role being filled. Background checks must be conducted in accordance with relevant employment laws. Some form of ongoing or continuous screening may be required, along with strict oversight.
- ▶ **Separation of duties:** This involves ensuring that more than one person is required to complete a particular task where safety or security might be at risk. This approach reduces the risk of fraud, theft, and human error. Typical separation of duties may involve the following: Separate electronic authorization for actions such as to change set points in a control system; The use of multiple security keys (physical or electronic) held by separate personnel.

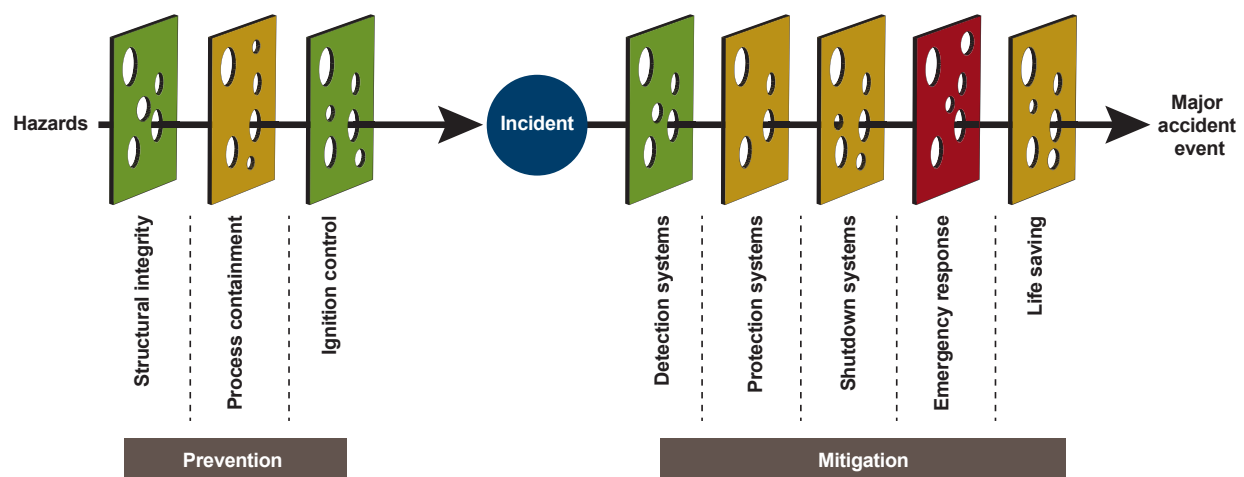


Figure 1. Barrier representation of cybersecurity controls.

- ▶ **Joiners, movers, and leavers:** User roles should be at a sufficiently granular level that no person has access to data or functions they do not need to do their job. Once someone is in a role, a periodic review process will ensure access is still required. Changes should be made with immediate effect. Most importantly, an individual leaving an organization should trigger prompt action to remove all physical and electronic access.

Inventory management

When a product vulnerability is announced, the first question to answer is: Does this affect my organization, and if so, where, and how much? It is impossible to answer this question without an accurate and up-to-date equipment inventory. An equipment inventory can be as simple as an Excel spreadsheet or can be a purpose-made relational database and application. IT and OT security vendors offer inventory management systems.

Consider the following points when creating an OT device inventory:

- ▶ The range of device types is much larger and includes many firmware and software solutions that are not designed to interact with asset management solutions (Figure 2).

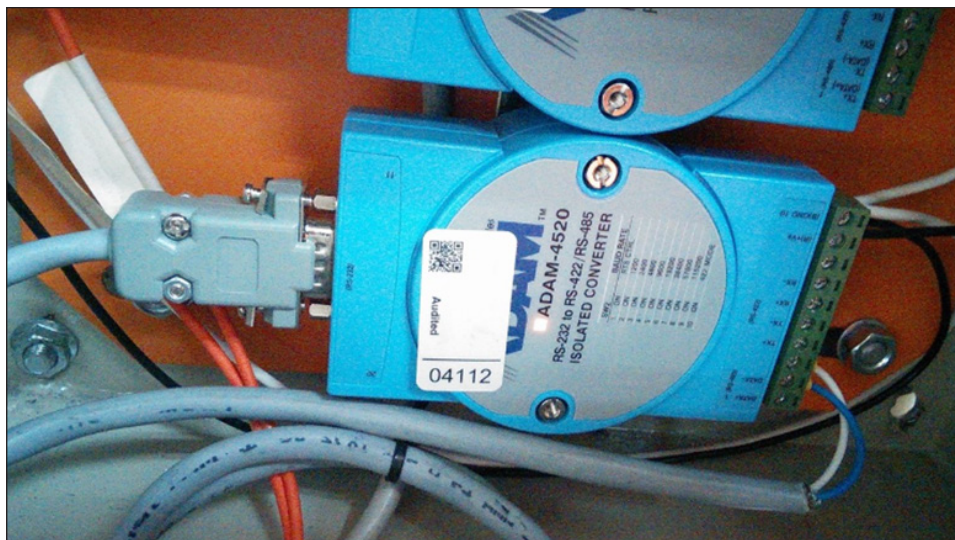


Figure 2. Legacy devices can be hard to identify in inventory systems.

- ▶ Many devices that are networked may only respond to the most basic industrial protocol commands. Rarely do these commands support the return of configuration information.
- ▶ There is no guarantee that devices are accessible on a common communications network. Many installations will contain serially connected (RS-232, RS-485, RS-422) devices that only respond to basic industrial protocol commands.
- ▶ In more modern OT networks, there may be industrial firewalls or data diodes that isolate devices from the wider network. This design limits communications to very few industrial protocol commands.

●●●●● **Cybersecurity**, despite being a potential initiating cause of hazards, is not respected in the same way safety is.

Incident response

Incident response planning is not just about preparing for the inevitable incident. Considering plausible scenarios facilitates a review of business risk and the identification of additional mitigations to reduce this risk.

Consider the Oldsmar example. In early February 2021, an operator at a water treatment plant in Oldsmar, Florida, noticed someone remotely accessing an HMI at the plant. Later that day the operator noticed a second remote access session on the HMI. This time, the remote user navigated through various screens and eventually modified the set point for sodium hydroxide (lye) to a level that would be toxic to humans. The remote user logged off, and the operator immediately reset the sodium hydroxide level to normal.

Although it resulted in a near miss, the Oldsmar incident highlighted gaps in process and people elements:

- ▶ The operator should have known who was initially accessing the HMI, and whether they were authorized to do so. Unauthorized access should have triggered an immediate incident response.

- ▶ The company that developed the SCADA system used in the facility exhibited poor information security behavior. They maintained a page on its website displaying a screen from the HMI, providing details of plant processes. It was easy to see the button that would enable navigation to the sodium hydroxide page. Such a screenshot is extremely valuable in terms of planning a potential attack.
- ▶ There appeared to be no assessment of the remote access requirement, or the cybersecurity risks associated with it. Was remote access necessary, or was it *nice to have*? If remote access was required for viewing process state, why was *read-only* access enforced in the remote access scenario.
- ▶ The functionality of the SCADA system should have prevented a user from setting dangerous levels in any part of the treatment process. This should have been risk assessed and mitigated during the design stage. Addressing the remote access risk does not remove the risk of unauthorized physical access to the same system.

Suppliers, vendors, and subcontractors

In many cases, the personnel from third party organizations are in place so long that they become indistinguishable from asset-owner personnel. Few asset owners properly manage the cybersecurity risks arising from these arrangements:

- ▶ Third-party computers may not have the necessary security controls, yet they may be connected to business-critical systems or networks.
- ▶ Vendors may not have sufficient controls in place to manage user credentials for their clients' systems.
- ▶ Vendors may not have procedures in place to manage system backups.
- ▶ Suppliers, vendors, and subcontractors may not have adequate security management systems in place in their organization.
- ▶ Suppliers, vendors, and subcontractors may not provide adequate security awareness training to their personnel.

A key step to establishing control is contract management. Contracts should be tailored to specific arrangements. Contract clauses should reflect the controls required to manage cybersecurity risks.

Insurance

There is an established cyber insurance market focused on IT cybersecurity risks, and insurers and brokers are now developing policies to cover threats to OT infrastructure. Insurers and brokers are still learning what risks an asset owner is exposed to from an OT cybersecurity incident. Tom Finan of Willis Towers Watson, a global insurance broking company, points out that “having a cyber insurance policy does not make a company safer. Instead, an enhanced cybersecurity posture results from going through the cyber insurance application and underwriting process.”

Final thoughts

Although OT environments have a different operational support culture from IT environments, several factors can give OT cybersecurity the management attention it requires.

- ▶ The safety culture that is ingrained in all OT environments can incorporate cybersecurity, treating it as another initiating cause of high-impact incidents that can occur.
- ▶ The use of management monitoring tools, such as the barrier representation, can ensure that cybersecurity is considered at the same level as other protective layers.

Technology is not the only element of the cybersecurity challenge. People and process are critical weak points. Much of what happens in operational environments revolves around people. Cybersecurity relies on training and awareness, and the adherence to strict processes and procedures. Gaps in training and awareness or in processes and procedures create vulnerabilities that can be as severe as any technical issue.

Incident response is one of the most importance plans to have in place. With the growth in high-profile cybersecurity incidents and the knowledge of the costs of dealing with them, it is harder for organizations to ignore the need for good preparation.

There is still work to be done to educate asset owners that good incident response planning does not begin and end in their own organization. The use of suppliers, vendors, and subcontractors means that cybersecurity risks, and their remediation, rely on the cooperation of all parties.

One key control that asset owners can use is contract management. A set of model clauses that represent good cybersecurity management should be included in all third-party contracts. Although insurance can be a useful tool for an asset owner, it cannot replace effective identification and proactive management of risk. As with all other aspects of cybersecurity management, there is still much to do in operational support, but the elements are in place to improve the cybersecurity posture of all organizations.

ABOUT THE AUTHOR



Steve Mustard, P.E., B.Eng,C.Eng,CAP, GICSP, is an independent automation consultant and a subject matter expert of the International Society of Automation (ISA). Backed by more than 30 years of engineering experience, Mustard specializes in the development and management of real-time embedded equipment and automation systems. He serves as president of National Automation, Inc., and served as the 2021 president of ISA. Mustard is a licensed Professional Engineer in Texas and Kansas, a UK registered Chartered Engineer, a European registered Eur Ing, an ISA Certified Automation Professional (CAP), a certified Global Industrial Cybersecurity Professional (GICSP), and a Certified Mission Critical Professional. He also is a Fellow in the Institution of Engineering and Technology (IET), a Senior Member of ISA, a member of the Safety and Security Committee of the Water Environment Federation (WEF), a board member of the Mission Critical Global Alliance (MCGA), and a member of the American Water Works Association (AWWA).