



industrial ethernet book

Industrial Ethernet Automation Networking & IIoT

Special Report

IT-OT Convergence Tech Trends

Page 36

Industrial Cybersecurity Experts Weigh In

6

Building futureproof
industrial security

17

IEC 62443 standards:
targeting cyberattacks

19

Industrial Ethernet Book
Corporate Profiles

43

Using Industrial PoE
switches

60

groov EPIC

Your Digital Transformation-ready Edge Platform



groov RIO

- Industrial design
- Enterprise-grade security
- Programming choices
- Web & mobile visualization
- Cloud connectivity
- Secure remote access

All the tools you need, included.



Learn more today at www.opto22.com.



Made and supported in the U.S.A.
Call us toll-free at 800-321-6786 or visit www.opto22.com.
All registered names and trademarks copyright their respective owners.

50
Anniversary

OPTO 22
Your Edge in Automation.™

Cybersecurity trends in focus

Earlier this year, Antaira Technologies highlighted cybersecurity trends that should be in focus for industrial network managers. According to the Cybersecurity and Infrastructure Security Agency (CISA), cyberattacks cost the US economy \$242 billion annually. But fortunately, just as cybercriminals are evolving with new techniques and strategies, so are the security and information technology professionals responsible for stopping them.

Here are the key trends Antaira noted:

Machine Learning-Powered Malware Detection: Network security professionals are turning to Machine Learning (ML) to improve the detection and classification of malware. ML programs can learn behavioral patterns shared by different malware types by analyzing millions of representative malware samples, combined with input from humans, or the program's own queries.

Quantum-resistant Encryption Algorithms: Data scientists fear that a powerful quantum computer may soon be able to breach the encryption algorithms that protect and authenticate digital information. Data today is kept private thanks to cryptographic techniques managed by the National Institute of Standards and Technology (NIST). This year, the NIST is on schedule to standardize four quantum-resistant encryption algorithms, a process that will involve the NIST creating guidelines to ensure the new algorithms are used correctly.

Spikes in Ransomware Attacks: Financially motivated ransomware attacks were up 95 percent in 2023, year over year. In 2024 there is an expectation to see a similar spike in both the frequency and the sophistication of ransomware attacks on industrial networks.

Focus on IIoT Device Security: Industrial device security is coming to the forefront, especially with industrial switches and sensors. Industrial networks contain sensitive data that make them a target for hackers seeking proprietary intellectual property.

Zero Trust Framework Adoption: Zero Trust (ZT) architecture assumes that no user, device, computer system, or service inside or outside the organization should be trusted to gain unauthorized access until verified.

Regulatory Changes: Cybersecurity regulations are continually evolving to keep pace with the shifting threat landscape.

Antaira noted that, as the digital landscape continues to evolve, so do the tactics and strategies employed by cybercriminals and malicious actors. It's crucial for those involved with industrial networks to stay informed about the latest cybersecurity trends to protect their data and assets effectively.

Al Presher



2024 Corporate Profiles: 43



New Products: 62

Contents

Industry news	4
Industrial cybersecurity experts look to the future	6
Building futureproof industrial network security	17
IEC 62443 standards: defending against infrastructure cyberattack	19
Effective strategies for keeping IoT environments secure	24
Automatic CIP Security via Pull Policy	26
Cybersecurity basics: industrial security fundamentals	31
IT-OT convergence leverages advanced technology solutions	36
2024 Industrial Ethernet Book Corporate Profiles	43
Digital tool life monitoring: making machine data transparent	55
Heat treatment OEM chooses flexibility and scalability	57
Maximizing automation efficiency with Industrial PoE switches	60
New Products	62

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **November/December 2024**.
Deadline for editorial: December 13, 2024 **Advertising deadline:** December 13, 2024

Editor: Al Presher, editor@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +1 585-598-6627

Free Subscription: iebmedia.com/subscribe

Published by IEB Media Corp., 1247 Anthony Beach Rd., Penn Yan, NY, 14527 USA ISSN 1470-5745

Emerson latest to join Margo interoperability at the edge

Industrial automation leaders drive digital transformation through seamless edge interoperability with new open standard.

EMERSON IS THE LATEST AUTOMATION supplier to join the Linux Foundation's Margo, the new open-standard initiative designed to make edge applications, devices and orchestration software work together seamlessly across multi-vendor industrial automation environments.

According to an Emerson press release, as process and discrete manufacturers implement enhanced digitalization, they encounter challenges at the edge due to multi-vendor and multi-technology devices, apps and orchestration environments that do not easily integrate. The Margo initiative addresses these challenges through the creation of practical reference implementation, open standards and testing toolkits.

This approach will help remove obstacles and simplify the process of building, deploying, scaling and operating complex, multi-vendor industrial edge environments, helping manufacturers of all sizes build new and better digital operations or modernize existing ones.

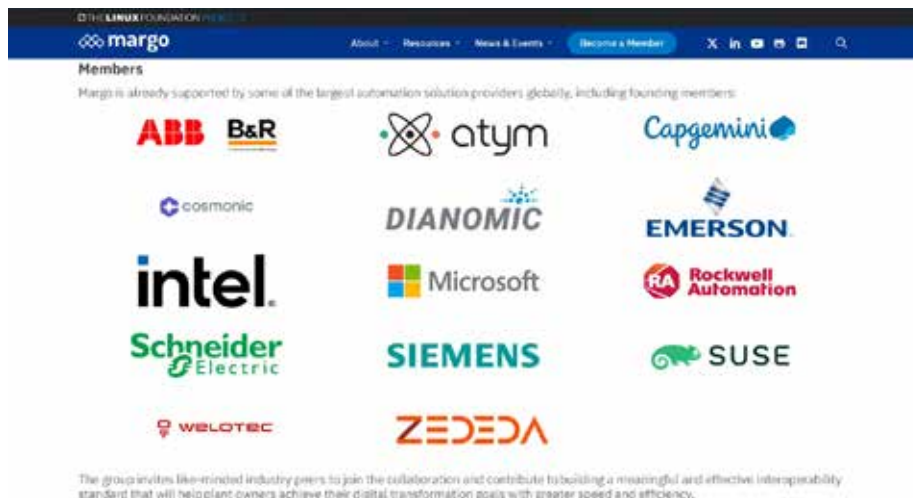
"The modern OT edge is the backbone of our next-generation automation architecture, enabling the availability of data and computing closest to where it is needed," said Peter Zornio, Emerson's chief technology officer. "Successful implementation will require open edge standards that will enable scalable, simplified and seamless interoperability among applications, edge devices and orchestration software – no matter the vendor technology.

Launch of Margo

Earlier this year, the Linux Foundation announced the launch of Margo, (www.margo.org), a new open standard initiative for interoperability at the edge of industrial automation ecosystems. Drawing its name from the Latin word for edge, Margo defines the mechanisms for interoperability between edge applications, edge devices, and edge orchestration software. The open standard promises to bring much needed flexibility, simplicity, and scalability – unlocking barriers to innovation in complex, multi-vendor environments and accelerating digital transformation for organizations of all sizes.

Joint Development Foundation

Hosted by the Joint Development Foundation, a part of the Linux Foundation family, the initiative is supported by some of the largest automation ecosystem providers globally, including founding members ABB (including



Margo is supported by some of the largest global automation solution providers worldwide.

B&R), Capgemini, Microsoft, Rockwell Automation, Schneider Electric (including AVEVA) and Siemens. The group invites like-minded industry peers to join the collaboration and contribute to building a meaningful and effective interoperability standard that will help customers achieve their digital transformation goals with greater speed and efficiency.

"At the core of Margo development is a commitment to delivering interoperability in a modern and agile way," said Bart Nieuwborg, Chair of the Margo Initiative and Senior Program Manager, Rockwell Automation. "A comprehensive open-source reference implementation aims to facilitate the adoption, and the associated compliance test toolkit will ensure the trust in Margo's interoperability promise, paving the way for the industry to tap the full potential of, for example, data and AI at the edge."

"The idea that users should be free to create the best solution for their needs without unnecessary constraints, costs, or delays embodies the spirit of open-source collaboration," said Jim Zemlin, Executive Director of the Linux Foundation. "Open interoperability among a wide selection of apps and devices will reduce the need for specialized resources and streamline the deployment, scaling and operation of multi-vendor ecosystems."

Industry Support

"Mastering efficiency, flexibility and quality faster than competitors is key to success

in today's industrial world. Digitalization can help deliver on these benefits, but digital ecosystems require a robust, secure and interoperable framework at the edge, connecting operations and information technologies. For ABB, a long-standing advocate of open automation systems, driving a forward-thinking collaborative initiative like Margo is key to achieving this goal." – *Bernhard Eschermann Chief Technology Officer, ABB Process Automation.*

"Interoperability is the key to digital transformation at scale – empowering manufacturers to unlock the potential of the Industrial IoT at full speed without large teams of IT specialists." – *Florian Schneeberger, Chief Technology Officer, B&R.*

"Microsoft is thrilled to be supporting Margo and continuing our efforts to help industrial customers accelerate their digital transformation journey. Our customers tell us every day about the challenges to scale and operate their industrial solutions due to a lack of interoperability at the edge. They want help to reduce the complexity, cost, and time to value. Microsoft is committed to align our adaptive cloud strategy architecture, such as Azure Arc and Azure IoT Operations, with the Margo initiative to help our customers build, deploy, and scale their applications faster, and run them both on the edge or in the cloud". – *Christoph Berlin, General Manager, Microsoft Azure.*

News report by Emerson and Margo.

Compact, powerful, predictive: The Beckhoff power supplies with EtherCAT



- 24/48 V DC power supplies with EtherCAT interface
- increase plant availability with predictive diagnostics
- reliable current and voltage monitoring
- prewarning thresholds individually adjustable
- detection of input transients
- monitoring of internal device temperature
- output switchable via EtherCAT



Scan to discover
more about the
full range of
power supplies

New Automation Technology **BECKHOFF**

Industrial cybersecurity experts weigh in on the future

Cybersecurity has become the number one issue for factory networks. Experts predict that artificial intelligence and machine learning will make an impact, the IT and OT worlds will grow closer together and that resilient network infrastructure and structured frameworks will strengthen industrial cybersecurity solutions.



SOURCE: ITTECH INDUSTRIAL

"Key technology trends in industrial cybersecurity include the adoption of enhanced OT visibility, software-based segmentation, zero-trust remote access, and unified IT/OT security platform. Vendors are addressing these concerns with innovative solutions designed to protect industrial environments effectively."
 Fabien Maisl, Marketing Lead, Industrial Security, Cisco.

THE FUTURE OF INDUSTRIAL CYBERSECURITY is dependent on the development of new technologies that will make the next generation of industrial networks more intelligent and more secure than ever before.

For this special report on Industrial Cybersecurity, IEB reached out to a series of industry experts to get their perspective on the technologies that are shaping present and future industrial cybersecurity solutions.

Seven leading companies have responded with their take on the trends for industrial cybersecurity, what they see as the most potent solutions available, the challenges that automation engineers are facing and what promises to be the leading industry applications. Here is what they have about

the technologies and trends shaping the next generation of industrial networks.

Keys to protecting industrial environments

OT visibility, software-based segmentation, zero-trust remote access, and unified IT/OT security platform.

According to Fabien Maisl, Marketing Lead, Industrial Security at Cisco, "the key technology trends in industrial cybersecurity include the adoption of enhanced OT visibility, software-based segmentation, zero-trust remote access, and unified IT/OT security platform. Vendors are addressing these concerns with innovative solutions designed to protect industrial

environments effectively."

Enhanced OT Visibility: Identifying and profiling OT assets is key to reduce the attack surface and build effective security policies. Traditional OT visibility solutions require deploying dedicated appliances or SPAN networks which are proving too complex and expensive. OT visibility capabilities can now be embedded in networking equipment to easily capture east-west traffic and gain comprehensive visibility on all OT assets

Software-based Segmentation: Segmenting industrial networks in small zones of trust is an efficient way to protect operations and avoid attacks to spread. But in many cases, it can be too complex to modify the network, deploy zone-based firewalls, and



VISIT US!

electronica 2024
12 - 15 November
Munich, Germany
Hall C4 - Booth 121

SPS 2024
12 - 14 November
Nuremberg, Germany
Hall 5 - Booth 110

 **ADI Chronous™**

INDUSTRY-LEADING SCALABLE ETHERNET. TIMED TO PERFECTION.

Delivering the Future of Time Sensitive Networking.

Analog Devices' Chronous™ family of Industrial Ethernet connectivity products enable best-in-class industrial automation solutions for the connected factory of tomorrow. ADI Chronous physical layer devices and embedded switches offer industry's lowest latency and power for the highest level of determinism and synchronization in high-performance factory, process and motion control applications.

Turn your vision of the connected factory into reality. Learn more and visit analog.com/chronous

[ANALOG.COM/CHRONOUS](https://analog.com/chronous)

ensure assets are placed in the proper segment without disrupting production. Software-based segmentation leverages networking equipment to easily enforce access policies that can be centrally configured and dynamically updated. Combined with enhanced IT visibility, this helps IT and OT work together to easily build a segmentation strategy.

Zero-Trust Remote Access: Machine builders, maintenance contractors, and the operations teams need remote access to OT assets for maintenance and troubleshooting. Cellular gateways or software products that IT is not controlling are security backdoors.

VPNs are too complex to manage at the scale of OT. Organizations are starting to deploy Zero-Trust Network Access (ZTNA) solutions to simplify the remote access workflow. Remote users log into a web portal where access policies are defined and enforced for the entire infrastructure, making it easy to define credentials and control access. The portal communicates with routers and switches in the infrastructure to ensure that remote users are only granted access to selected equipment which they need to configure, not to the entire network.

Unified IT/OT Security: Industrial operations are no longer working on air gapped environment. Industry 4.0 and OT digitization require seamless communications between OT, IT and cloud resources. As IT and OT networks are converging, IT and OT security also needs to converge. Organizations need to enable a cohesive security strategy that includes having global visibility on both IT and OT environments to detect modern threats faster, unifying security policies to avoid gaps in defense, and leveraging IT security tools and practices to enable advanced protection of OT assets and orchestrate faster remediation and recovery.

Technology benefits

Maisl said that the newer solutions offer specific benefits for industrial cybersecurity offer, and potential impact on manufacturing networks. These benefits include:

Enhanced OT Visibility: Embedding OT visibility capabilities in networking equipment allows manufacturing networks to gain comprehensive insights into all OT assets. This leads to improved asset management, better threat detection, and streamlined security operations, making the network more secure and resilient.

Software-based Segmentation: Implementing software-based segmentation in manufacturing networks enables the creation of small, manageable zones of trust without extensive network modifications. This minimizes production disruptions, enhances collaboration between IT and OT teams, and improves the containment of cyber threats, thereby protecting critical operations.

Zero-Trust Remote Access: Deploying Zero-Trust Network Access (ZTNA) solutions in manufacturing networks simplifies remote access management. It ensures that remote users only access necessary equipment, reducing the risk of unauthorized access and enhancing overall security. This streamlines the management of remote access policies and credentials and safeguards OT assets from potential threats.

Unified IT/OT Security: Converging IT and OT security strategies in manufacturing networks provides global visibility across both environments, enabling faster threat detection and unified security policies. This results in improved defense against modern threats, seamless communication between IT, OT, and cloud resources, and a cohesive security posture that enhances overall operational resilience.

Cutting edge cybersecurity

“To gain visibility on OT assets and their activities, you need to capture network traffic to extract information from communication flows,” Maisl said. “Traditional security solution providers typically configure SPAN ports on network switches to duplicate traffic and send it to a central server or dedicated appliances. Not only is this complex to manage, it’s also very expensive to deploy at scale as you would need to SPAN traffic from all switches to gain visibility on east-west traffic in addition to north-south traffic.”

He added that, with Cyber Vision, Cisco embeds visibility capabilities into switches and routers, eliminating the need to duplicate network flows or to deploy additional appliances. Obtaining visibility is a matter of activating a software feature. Cost, traffic, and operational overhead are all minimized.

“Segmenting industrial networks is key to protect operations and avoid attacks to spread. It is a key requirement of the ISA/IEC62443 security standard. Firewalls are perfect for building an industrial demilitarized zone (iDMZ). But deploying rugged firewalls in each product cell in factories leads to deployment issues like those IT faces with visibility appliances. Not only can it be very expensive, maintaining these firewall rules can become a challenge,” Maisl said.

Solutions such as Cisco Identity Services Engine (ISE) work with your network switches, routers, and wireless access points to restrict communications according to the zones and conduits you have defined. It leverages groups defined in Cyber Vision to allow or deny communications for each asset. When a change is required, you can just move the asset to another group in Cyber Vision. ISE will automatically instruct the network to apply the corresponding security policy.

When it comes to remote access, in many cases machine builders, maintenance

contractors, or the operations teams themselves have installed their own solutions: cellular gateways or software products that IT is not controlling. These backdoors are at odds with the OT security projects undertaken by the IT/CISO teams and create a shadow-IT situation that makes it difficult to control who is connecting, what they are doing, and what they can access. On the other hand, VPNs have the drawbacks of being always on, with all-or-nothing access, and requiring complex configurations to control what remote users have access to.

With Secure Equipment Access (SEA), Cisco is solving the challenges of deploying secure remote access to OT at scale. It embeds the gateway function into Cisco industrial switches and routers. Enabling remote access is now a software feature to activate. There is no dedicated hardware to install and manage. Configuring and enforcing security policies is done in a central console, making it easy to control who can access what and when across all sites. Distributing the gateway functionality anywhere in the network enables remote access to any assets, even those being NAT boundaries. The switch or router that provides connectivity now also provides remote access to these assets. And the same network equipment can enforce segmentation policies to prevent lateral movement to other assets.

Responding to challenges

Maisl said that one major concern for customers is the lack of visibility into OT assets. Many organizations do not have a complete inventory of all their OT and ICS devices, making it difficult to monitor and secure them effectively. This lack of visibility can lead to blind spots in the network, where vulnerabilities may go undetected, or unknown assets becoming the source of an attack. Without a detailed inventory of assets and their roles in the industrial process, it is becoming almost impossible to design and enforce security policies that will effectively protect the environment without disrupting production.

Another concern is the complexity and diversity of industrial environments which generally include legacy systems that were not designed with cybersecurity in mind. Protecting these systems is a significant challenge and requires precise mitigation measures you can only implement if you have a detailed asset inventory.

Additionally, the convergence of IT and industrial networks increases the attack surface, requiring comprehensive security measures that address both domains. Gone are the days when OT security could be managed in its own silo. Organizations now also need to converge their IT and OT security practices and implement a unified cybersecurity strategy.



“The integration of IT and OT systems requires a robust communication infrastructure that can handle the demands of both realms. Current technology trends in industrial cybersecurity include the increased adoption of AI-driven threat detection, zero-trust architectures, and advanced network segmentation,”
Michael Metzler, Vice President Horizontal Management Cybersecurity for Digital Industries, Siemens.

However, there is still a lack of collaboration between IT and OT teams. This siloed approach makes it challenging to design, implement, and maintain effective cybersecurity strategies.

Targeted applications

“As manufacturers accelerate digitization of their factories, they realize that both industrial networking and cybersecurity technologies are growing in complexity,” Maisl said. “As they increasingly use data to drive software-defined industrial operations and adopt AI technologies, there is a clear need for a converged strategy that incorporates not only IT and OT but also security.”

He added that, to enable smart manufacturing operations, the factory network must adopt modern IT technologies. Only this can simplify managing and reconfiguring the infrastructure, virtualize functions that used to run on dedicated hardware, support the fast and reliable transmission of large volumes of data to AI applications, and more. This IT infrastructure must be supported by comprehensive cybersecurity capabilities that are made simple and cost effective to deploy at scale.

Cisco is converging network and security functionality to reduce complexity, enable unified IT/OT security practices, and help accelerate adoption of AI-driven factories. Our network designs include centralized management of networks and security policies, unified visibility into both OT and IT,

automated network segmentation, zero-trust remote access, and more... all embedded into rugged industrial networking equipment purpose-built for the constraints of advanced manufacturing operations.

IT-OT Convergence

Robust communication infrastructure needed to handle the demands of both realms.

Michael Metzler, Vice President Horizontal Management Cybersecurity for Digital Industries at Siemens said that “the convergence of Information Technology (IT) and Operational Technology (OT) is a rapidly evolving trend in the industrial sector. As companies increasingly look for ways to optimize their operations and improve efficiency, the need for seamless communication between traditionally separate systems becomes paramount. It lays the foundation for data-driven decision making.”

“The integration of IT and OT systems requires a robust communication infrastructure that can handle the demands of both realms. Current technology trends in industrial cybersecurity include the increased adoption of AI-driven threat detection, zero-trust architectures, and advanced network segmentation,” he said.

To this end, Siemens – a major supplier for industrial cybersecurity – is offering solutions that offer real-time monitoring, automated response capabilities, and enhanced visibility

across both IT and OT environments. These solutions are designed to be scalable, allowing companies to protect both modern and legacy systems without significant overhauls.

Solutions for industrial cybersecurity

“Industrial networks are the nerve pathways in production; they are becoming in sum ever more complex. Hardware alone no longer determines their performance. Software-based network management and the use of cybersecurity tools have become indispensable,” Metzler said.

He added that new industrial cybersecurity solutions offer several benefits including improved threat detection, reduced response times, and enhanced protection against both internal and external threats. These solutions can significantly reduce the risk of costly downtime due to cyber incidents, thereby improving overall operational efficiency. The potential impact on manufacturing networks is substantial, as these solutions enable a more resilient and secure production environment, which is crucial in an era of increasing cyber threats.

“The risk of cyberattacks on industrial plants is real - and the frequency continues to increase. To comprehensively protect industrial plants against cyberattacks from inside and outside, all levels must be addressed simultaneously - from the operational to the field level, from data protection to secure



“Artificial intelligence and machine learning—tools enabled by the vast power of cloud computing—are where we are headed. The problem is that these solutions are only useful with huge amounts of consistent, quality data from the plant floor,” Dan White, Director of Technical Marketing at Opto 22.

communication,” Metzler said.

With Defense in Depth, Siemens provides a multi-layered security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the international IEC 62443 standard.

It is aimed at plant operators, integrators and component manufacturers and covers all relevant aspects of industrial cybersecurity. Cutting-edge cybersecurity technologies in industrial environments are characterized by their ability to seamlessly integrate with existing systems, including legacy OT devices. Technologies such as machine learning-based anomaly detection, industrial firewalls with deep packet inspection, and secure remote access solutions are being applied in factories to provide real-time threat detection and automated incident response. What makes these technologies unique is their focus on the specific needs of industrial environments, where uptime and safety are paramount.

Customer concerns

A key issue is addressing the primary concerns that automation engineers and companies are facing when implementing industrial cybersecurity strategies.

“The special framework conditions in Operational Technology (OT), including continuous operation, high performance requirements, and availability, demands an in-depth understanding of industrial processes so that security concepts can be optimally introduced and implemented,”

Metzler said. “For many companies, this task has become too complex. They need a partner who is familiar with and has mastered the special requirements of industry and cybersecurity.”

He said that when implementing industrial cybersecurity strategies, challenges include protecting legacy systems that were not originally designed with cybersecurity in mind, ensuring the secure integration of IT and OT (Operational Technology) networks, managing the growing complexity of industrial networks, and addressing the shortage of skilled cybersecurity professionals.

Additionally, companies must ensure that all components, including new and legacy devices, are equipped with robust security functionalities. This includes implementing technologies like industrial firewalls, intrusion detection systems, and secure remote access solutions that are specifically designed for industrial environments. Companies must also balance the need for robust security with the requirement for minimal disruption to production processes and safety systems.

“Beyond technology, the correct handling of cybersecurity measures by personnel is crucial,” Metzler said. “This involves training staff to adhere to defined policies and procedures, such as incident response protocols and regular security audits. A lack of cybersecurity awareness or poor adherence to security protocols by employees can undermine even the most advanced

technical defenses. Overall, the shortage of skilled cybersecurity professionals presents a challenge, making it essential for companies to not only invest in technology but also in ongoing training and education for their workforce.”

Critical infrastructure protection

Metzler said that the newest industrial cybersecurity solutions are specifically targeting areas such as critical infrastructure protection, secure remote access for industrial control systems, and the protection of industrial IoT devices. These solutions are also being applied to ensure compliance with stringent regulatory requirements and to safeguard sensitive production data. With the increasing convergence of IT and OT, traditional defense concepts are increasingly reaching their limits. Software-based network management and the use of cybersecurity tools have therefore become indispensable.

To be able to detect potential vulnerabilities in OT networks at any time, Siemens has designed a complementary tool set for plant operators with the SINEC software family. The SINEC Security Inspector determines the security status of individual components or entire production networks. The SINEC Security Monitor analyzes network traffic and detects anomalies through passive, non-intrusive continuous security monitoring. The latest tool in the SINEC portfolio is the SINEC Security Guard, an intuitive cloud-based software-as-a-service that displays vulnerabilities for OT-Assets



“Interestingly the cybersecurity needs in the industrial area seem to be driven by the IT world. Top keywords are asset management, patch management, intrusion detection, security operations center, none of which is specific to the OT environment,” Dr. Lutz Jänicke, Phoenix Contact.

and enables optimized security management for industrial operators without dedicated cybersecurity expertise. The SINEC NMS network management system also enables centralized monitoring and configuration of networks as well as security through encrypted data communication and local documentation.

Impact of AI and machine learning

Tools enabled by the power of cloud computing.

Dan White, Director of Technical Marketing at Opto 22 told IEB that “artificial intelligence and machine learning—tools enabled by the vast power of cloud computing—are where we are headed. The problem is that these solutions are only useful with huge amounts of consistent, quality data from the plant floor.”

He added that, in response, automation vendors have developed sophisticated control platforms that not only securely transmit data to the cloud but also ensure its accuracy right from the source. Edge controllers, positioned directly at the data origin, play a crucial role in this process. They filter and process raw data on-site, ensuring only relevant and refined information is sent to the cloud. Using a modern publish/subscribe protocol like MQTT Sparkplug, which also supports SSL/TLS security certificates, companies can rest easy knowing their plant data is getting to the cloud safely and securely.

More data at the edge

“As more data is collected at the edge of the network, from the plant floor and remote equipment, and moved into cloud computing platforms, AI tools and algorithms can make sense of it far more quickly and effectively than humans,” White said. “Finding operational anomalies, predicting equipment failures, and optimizing energy and raw material usage are just a few examples of the benefits.”

For too long, manufacturing networks have been isolated from the outside world. Companies now understand that manufacturing data must be democratized within the organization to unlock cost and efficiency savings. Manufacturing networks need to be reimaged to incorporate secure democratization of that data, which today’s modern edge gateways and PLCs can achieve.

White added that the “cutting-edge” cybersecurity technologies that factory environments are now discovering have been used by IT and internet companies for years. Online banking uses secure SSL/TLS encryption and certificates. VPNs, firewalls, and MQTT pub/sub architectures have existed since the 1990s. So what makes them unique is that factory environments are now embracing them.

“Don’t forget factories have used networks since the 1970s, before Ethernet and the Internet. Those were serial networks and usually proprietary, and we didn’t have great ways to democratize data back then,” White said. “In the 1990s, Ethernet wasn’t even

viewed as viable for plant floor operations due to its latency, sensitivity to noise, and nondeterminism. But the new obsession with data—and the not-yet-realized benefits that AI and ML can provide once we have a lot of data to analyze—have led the factory floor to start catching up.”

Primary concerns that automation engineers and companies are facing when implementing industrial cybersecurity strategies fall into a series of categories including support for legacy systems.

“Legacy systems, often characterized by outdated hardware, software, and security protocols, pose significant cybersecurity risks to industrial organizations. These systems were designed in an era when security was less of a concern, leaving them vulnerable to modern attack vectors,” White added.

Lack of Security Features: Most legacy systems lack built-in security features such as zero-trust user authentication, VPNs, firewalls, encryption, SSL/TLS certificate support, and network segmentation. Without security features, they’re easy targets for hackers who can exploit known vulnerabilities.

Vendor Lock-in: Reliance on legacy systems often involves vendor lock-in, which limits the options for upgrading or replacing the system, making it difficult to implement modern security measures.

Limited Scalability: Legacy systems, which typically rely on a poll/response architecture, may not be able to handle the increased data demands of modern IIoT applications,



"The key to effective industrial cybersecurity solutions is the development of resilient network infrastructure based on a defense in depth security approach is critical in ensuring the continuity of operations after any kind of major cybersecurity incident," Dr. Al Beydoun, ODVA President and Executive Director.

making them more susceptible to failures and security breaches.

As a result, organizations must carefully evaluate the risks associated with legacy systems and develop strategies to mitigate them. These strategies may involve upgrading to more modern systems or using modern edge devices to create a secure layer between OT and IT networks.

Targeted solutions

Application areas that the newest Industrial Cybersecurity solutions are targeting cover a variety of needs for smart manufacturers.

"Let's look at some of the low-hanging fruit. Right away, we are seeing a huge move toward energy data collection," White said. "Most companies don't understand their electric bill or how peak demand charges and variable rates work for their utility. Regardless of industry—from automotive to aerospace and from agriculture to electronics—there's one thing everyone has in common: they all use electricity. More granular analysis can help firms reduce costs and assign electricity costs to the process that's using them."

"After that, I would say operational equipment effectiveness (OEE). By adding a simple edge device onto an existing piece of machinery, which can be done for about \$1,000, companies can start to see when and why their factory equipment isn't running at full capacity," he added.

IT solutions moving to the OT world

Implementations specifically targeting the industrial environment are needed.

"Interestingly the cybersecurity needs in the industrial area seem to be driven by the IT world," Dr. Lutz Jänicke, Corporate Product & Solution Security Officer, Phoenix Contact, told IEB. "Top keywords are asset management, patch management, intrusion detection, security operations center, none of which is specific to the OT environment. Implementations specific to the industrial environment are needed."

Jänicke said that specialized products for OT are established, like firewalls, remote maintenance solutions, intrusion detection systems. However, the trend is moving away from "security products" to protect the OT world and the future will rather be "secure products". These follow security by design rules and implement security functions like access control and secure communications instead of relying on add-on products.

"IT solutions are moving into the OT world. A very important topic is the management of cybersecurity in the IT as well as in the OT environment. Connected systems need to be monitored for vulnerabilities, patches and updates need to be rolled out," Jänicke said. "Accounts needed for authentication and authorization require central management.

Communication security via secure protocols must be supported by centrally managed PKI or similar solutions, as communication does occur between IT and OT. A final ingredient for concepts like zero trust is endpoint security."

He added that all of these measures need to be implemented in a centralized manner unless in a very large factory an OT specific setup might be possible. If this is not the case, attacks must be remediated in a central Security Operations Center and security management needs to be coordinated between IT and OT. Of course, tooling on the shopfloor might be technically different but its operation needs to be integrated into the overall security management.

Engineering challenges

"Only few automation engineers have a solid cybersecurity background and experience," Jänicke said. "That makes it difficult to have the necessary 'holistic approach' within both cybersecurity and for the automation solution as a whole. Depending on the setup of the company, cybersecurity is typically organized in the IT departments, but both OT and IT need to work together. This often is a significant challenge due to different cultures."

"However, due to the convergence of IT and OT, IT technologies will move farther into the OT world as will cybersecurity threats," he added. "Overarching cybersecurity strategies

therefore need to integrate both worlds, requiring automation engineers to fully adopt the IT world."

Resilient network infrastructure

Based on a defense in depth security approach.

Dr. Al Beydoun, ODVA President and Executive Director, told IEB that that "the key to effective industrial cybersecurity solutions is the development of resilient network infrastructure based on a defense in depth security approach is critical in ensuring the continuity of operations after any kind of major cybersecurity incident."

"The greater the number of potential hurdles that any threat actor must overcome increases the odds that a potential incident will be discovered early on and therefore will minimize the potential damage," Beydoun stated. "Stopping attacks can come in many forms including employee training, physical security, firewalls, switch based deep packet inspection, network segmentation via separate security zones and communication conduits between zones, and end point security that supports zero trust with authentication for each connection. One potential option for automation devices is CIP Security, which provides end point security

including device authentication, message integrity, traffic encryption, role-based access, and a device level firewall."

Beydoun said it's important to not lean too heavily on any one kind of security system and to have experts available to review logs when suspicious behavior is identified by an automated system. Even the concept of air gapping is starting to unravel with the ability to remotely detect radiation signatures from physical electronic equipment. The significant value provided from taking advantage of edge and cloud connectivity for business optimization combined with the increase in potential threat vectors make defense in depth and zero trust security vital investments for the future.

Zero Trust Approach

He added that adopting a zero-trust approach makes it much more time consuming and difficult for a bad actor to continue to expand privileges and access within a breached network given that each new connection must be authenticated. The addition of role-based access to end point authentication reduces the privileges of a given user and further limits the potential damage a cyber threat actor can inflict.

It is important to make sure that even the most privileged of root and administrative

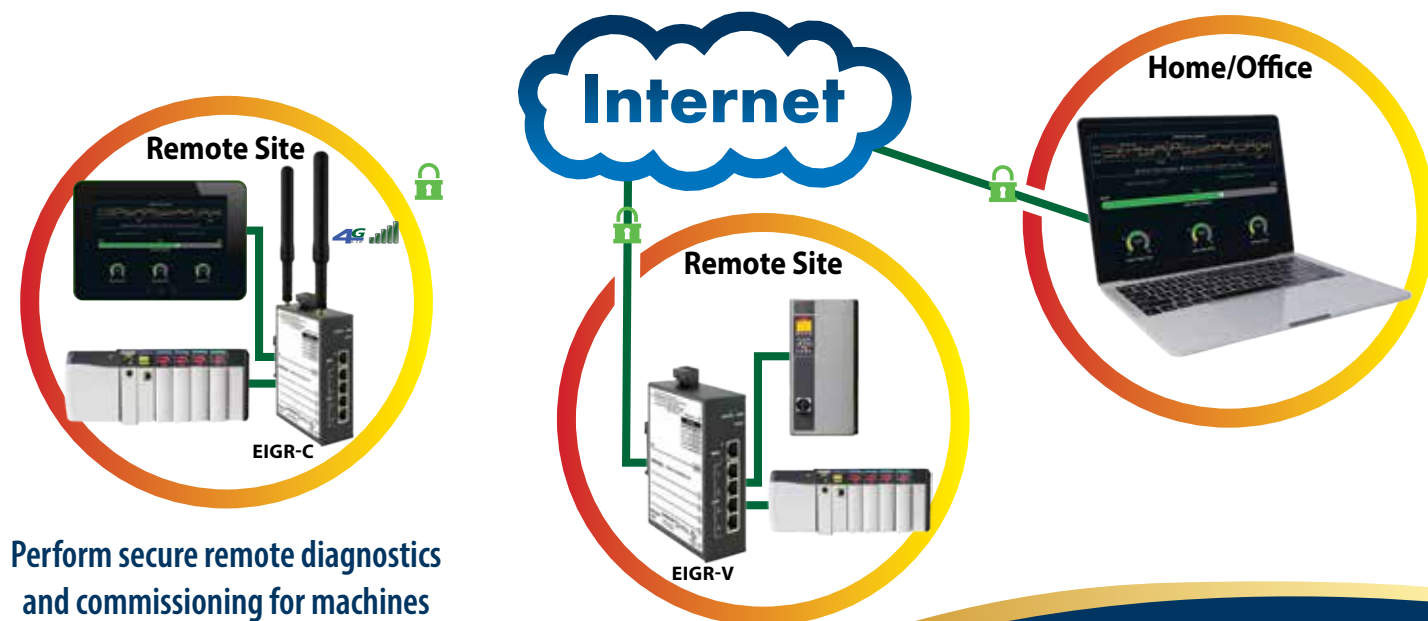
super users still must rely on the zero-trust approach to access confidential data and control potentially dangerous equipment in case their access is compromised. A systemic way to ensure a high level of network security is to rely on the ISA/IEC 62443 cybersecurity standards for industrial automation and control systems. Looking for automation networks that adhere to the security principles of IEC 62443, such as CIP Security, and devices that are certified to IEC 62433 standards is another way to bolster an organization's defense in depth security approach.

Impact of AI

"One of the newest additions to security is the implementation of Artificial Intelligence systems to look for abnormalities in network traffic to identify suspicious behavior as early as possible," Beydoun said. "AI systems can see if someone is accessing the network from unexpected locations, outside of normal working hours, or in areas that are not a part of an employee's job responsibilities. While false positives are sure to come to light from dedicated workers going above and beyond, the early detection of cyber threat actors can significantly limit potential damage caused."

The advantage of AI systems is that they can crunch vast amounts of data and see

Remote Machine Diagnostics and Commissioning



Perform secure remote diagnostics and commissioning for machines over wired or wireless using a Skorpion IP Router.

CONTEMPORARY CONTROLS®

Providing Solutions to Your Automation Needs

630-963-7070 • info@ccontrols.com

Learn more at www.ccontrols.com/machine



SOURCE: ISTOCKPHOTO

"Implementing cybersecurity strategies is a very involved process. These strategies need to consider the entire landscape of the network including local networks as well as the integration of remote sites. Everything needs to be considered in a layered approach," Mike Willet, Network Engineer, Red Lion.

when there are deviations outside of the norm in production processes and machinery operations that would be hard to detect by a person. Experts are still required to validate the findings and to determine the next steps that need to be taken. One of the disadvantages of AI systems is that they will need to be redesigned and retrained over time as the networks change given that models are trained to fit a given set of data from a time period in the past. It's important to note that AI will just be another tool, albeit a valuable one, in securing networks and operations.

Challenges for automation engineers

Beydoun said that controls engineers are tasked with the immense challenge of ensuring that complex networks aren't compromised in a way that will result in the loss of throughput, quality, or proprietary information. While an automation company must work to prevent a multitude of potential entry points, a bad actor just needs to find one successful way to enter a network.

Once inside the network, whether by phishing for the credentials of a company's trusted employee or through technical exploits, the cyber threat actor can then choose to stay silent while working to elevate their access privileges, waiting for an advantageous time like a company shutdown to initiate an attack.

A network that may appear to be secure

could already be compromised, which has led to the rise of security concepts such as zero trust that always requires verification for each connection. The potential for economic, environmental, or loss of life and limb, combined with the challenge of guarding networks that have a staggering number of potential entry points, has also given rise to the importance of end point security such as CIP Security for EtherNet/IP.

Key applications focus

"Automation applications where misuse can result in harm to employees and environment or seriously jeopardize the economic viability of a company are the most important to protect in case of a cyberattack from a bad actor," Beydoun said. "Critical application examples that require the most stringent security include metal stamping or rolling equipment, chemical mixers, oil distillation towers, and water treatment plant disinfectant and corrosion control processes."

He added that it is imperative to utilize zero trust security to protect control devices at the lowest level for vital applications. CIP Security for automation devices offers flexible protection via profiles that can be implemented as needed, allowing for high overhead encryption for critical applications while only using authentication for other less important processes. Security has become a key enabler of automation device to cloud connectivity that is allowing for increases

in productivity and growth. Therefore, security policy, training, and protections are an invaluable investment in the future of industrial operations, especially as security threats continue to grow and evolve.

Flexible hardware solutions

Integrate local networks and serve as hub of automation network.

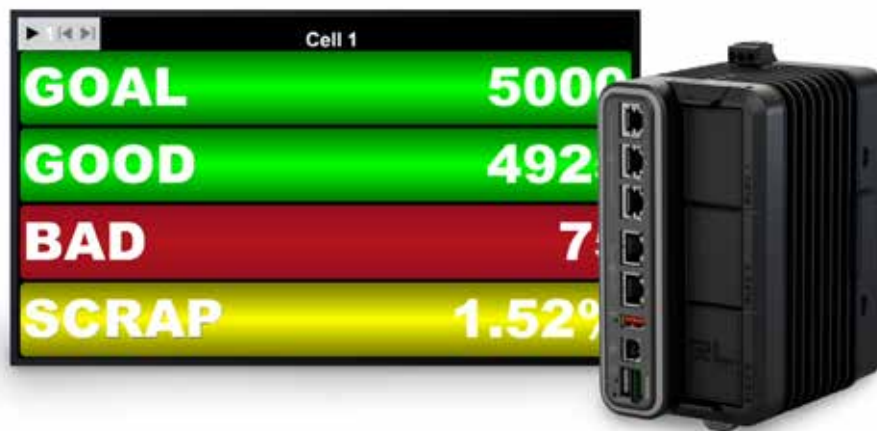
Mike Willet, Network Engineer for Red Lion said that a "key technology trend is implementing hardware that can serve many purposes in the landscape of the topology, security and the overall industrial network."

He cited FlexEdge from Red Lion as a key product that can be used as a firewall to secure the edge of the network, connect remote sites securely, integrate the local networks and also serve as the hub of the automation network with Crimson.

"It is an overall solution that can be the focal point of the industrial network. Red Lion is addressing these concerns with products like FlexEdge and NT5000 switches to build out the industrial network," Willet said.

Industrial cybersecurity solutions

Willet said that new solutions can offer advancements to security for industrial networks. Users can have the ability to better secure entry and exit points into the industrial network and also keep the local segment of the network secure. New



SOURCE: RED LION

The FlexEdge Intelligent Edge Automation Platform from Red Lion is powered by the company's Crimson Configuration Software.

Advanced security features are also becoming more prevalent. Modern solutions offer features such as network segmentation, real-time traffic inspection, and secure communication protocols. They protect manufacturing networks from diverse cyber threats while maintaining operational efficiency.

"Lastly, there is a growing emphasis on embedding security measures directly into the network infrastructure. Moxa focuses on foundational elements like authentication, access control, and segmentation, enabling a robust defense-in-depth strategy. This approach ensures that security is not an afterthought but a core component of the network design, enhancing overall resilience," Liou added.

Impact on manufacturing networks

"New industrial cybersecurity solutions offer significant benefits, particularly in terms of regulatory compliance and operational resilience," Liou said. "By adopting horizontal standards like ISO/IEC 27001 and IEC 62443, organizations gain clarity and structure in implementing cybersecurity measures. These standards simplify compliance, helping organizations navigate complex regulatory landscapes more effectively."

One of the key benefits is the adaptation of these solutions to the specific needs of operational technology (OT) environments. For example, Moxa's IEC 62443-certified solutions are designed to meet the unique requirements of industrial control systems (ICS), ensuring that security measures are relevant and effective in these settings.

Another major advantage is the ability to maintain operational continuity while enhancing security. Moxa's solutions incorporate redundant network architectures, which allow for secure maintenance and upgrades without disrupting critical operations. This approach is vital for managing risks and ensuring continuous availability in industrial environments.

Furthermore, integrating foundational security elements directly into the network infrastructure provides a solid base for additional security measures. Moxa's solutions reduce the attack surface and support a comprehensive defense-in-depth strategy, which is crucial for improving the overall resilience of manufacturing networks.

New solutions offer a structured approach to cybersecurity, tailored to the needs of industrial environments, while ensuring continuous operations and enhancing overall network security.

Cybersecurity technologies

"Cutting-edge cybersecurity technologies distinguish themselves by integrating advanced security features directly into

solutions can also empower industrial network users and administrators to manage the industrial network and maintain better insight into monitoring and ongoing status of the network.

"When Red Lion products are implemented into the industrial network, users can build out a new solution for cyber security with the ease of use and functionality that the devices bring. When a FlexEdge device is installed as a firewall and automation device with Crimson, it can also monitor NT5000 switches using N-View and port statistics can be mapped to tags to view and build alarms," Willet said.

"This solution can build a secure network with the advantage of passive monitoring to gain insight into the health of the network. Manufacturing networks can benefit from this because they can implement a secure network properly and gain the added benefits of a secure network with the ease of use factor of Red Lion products."

Cybersecurity strategies

"Implementing cybersecurity strategies is a very involved process," Willet said. "These strategies need to consider the entire landscape of the network including local networks as well as the integration of remote sites. Everything needs to be considered in a layered approach. So, with all of this comes quite a bit of planning."

During the implementation of the security plan all the outside or untrusted traffic must be defined and properly secured for specific inbound or outbound connections and protocols. Also, the local and private side of the networks where end devices are connected must also be properly secured. So, the overall concerns could emerge in the development stage of the security implementation plan itself and during the configuration stage of the firewalls, routers, switches and other devices in the network. It is critical to implement the proper security measures and

if Red Lion products such as FlexEdge and NT5000 switches are implemented into the network the ease-of-use factor can be very helpful while building the foundation of the network.

He added that security at various points and areas in the network is very important. Targeting the edge segments of the network are crucial because those areas are often connected to public networks and are usually connecting various sites together.

"It is important to maintain security at those points because those are the main entry and exit points from untrusted sources. But it is also important to build out a security architecture throughout the entire network," he said. "Making sure that the network switches connected downstream in the network that are connecting end devices have the proper security measures in place is also very important."

Structured framework for cybersecurity

Standards including ISO/IEC 27001, NIST CSF, and IEC 62443.

"One major trend is the adoption of horizontal standards like ISO/IEC 27001, NIST CSF, and IEC 62443," Laurent Liou, Product Marketing Manager, Cybersecurity at Moxa told IEB recently. "They provide a structured framework for cybersecurity, bridging the gap between IT and OT requirements. Vendors like Moxa incorporate these standards into their solutions, ensuring compliance with regulations while aligning with industry best practices."

Liou said that another trend is the integration of best practices directly into cybersecurity solutions. For instance, Moxa's adoption of IEC 62443 enhances the security of industrial control systems by addressing their unique challenges. This helps organizations build a robust cybersecurity posture that meets both regulatory and operational demands.



SOURCE: ISTOCKPHOTO

“One major trend is the adoption of horizontal standards like ISO/IEC 27001, NIST CSF, and IEC 62443. They provide a structured framework for cybersecurity, bridging the gap between IT and OT requirements.” Laurent Liou, Product Marketing Manager, Cybersecurity at Moxa.

the network infrastructure, particularly in industrial environments,” Liou said. “These features include secure communication protocols, robust access controls, and real-time traffic inspection, all of which are designed to protect operational technology systems from a wide range of cyber threats.”

A critical component of these technologies is network segmentation and redundancy. By creating isolated network segments and utilizing redundant pathways, these solutions help mitigate the impact of potential breaches. For instance, Moxa’s IEC 62443-compliant devices are engineered to ensure continuous operational availability even in the event of a cyber incident. This segmentation also supports secure maintenance and upgrades by isolating changes from critical operations.

Liou said that another defining characteristic is the defense-in-depth approach. This strategy involves multiple layers of security controls, starting with foundational measures like network segmentation and secure communication protocols. Moxa’s solutions enhance this foundation with additional protective layers to address various attack vectors, reducing vulnerabilities across the network.

Performance and availability are also prioritized in these advanced solutions. Moxa designs its technologies to integrate security measures without compromising network efficiency, ensuring that manufacturing operations remain smooth and uninterrupted. This balance between performance and security is crucial for maintaining high

productivity levels while safeguarding against cyber threats.

Primary customer concerns

The European Union’s NIS2 Directive and Cyber Resilience Act (CRA) imposes strict cybersecurity requirements, especially for critical infrastructure. Navigating these regulations can be overwhelming, particularly when considering the additional guidelines issued by organizations like ENISA (European Union Agency for Cybersecurity) and sector-specific bodies like EMSA and ENTSO-E.

Moreover, national laws such as Germany’s IT Security Act 2.0 further complicate the landscape by adding country-specific obligations. These regulations often require the integration of various industry standards, like IEC 62443, which focuses on OT security. Compliance with these standards is essential for addressing disaster recovery, safety, and secure communication protocols within industrial environments. Another major concern is maintaining operational continuity while implementing new security measures. Enhancing cybersecurity often necessitates significant changes to existing OT systems, which can disrupt operations. Ensuring that these measures integrate seamlessly without compromising performance or availability is a critical and resource-intensive task.

Automation engineers must navigate a multifaceted regulatory landscape, align with multiple standards, and ensure that cybersecurity measures do not disrupt ongoing operations, all while adapting to the specific needs of industrial environments.

Industrial cybersecurity solutions

“A primary focus is securing OT environments, which include industrial control systems (ICS) and other critical industrial networks,” Liou said. “Moxa’s IEC 62443-certified solutions are specifically designed to protect these systems from cyber threats while ensuring they operate efficiently and reliably. This is essential for industries where the integrity and availability of control systems are paramount.”

Sectors such as energy, water, and transportation face stringent regulatory requirements, and Moxa’s solutions help organizations in these industries achieve compliance while protecting essential services from cyber threats. These solutions are particularly important for maintaining the security and reliability of critical systems.

Additionally, Moxa’s solutions simplify compliance management by aligning with horizontal standards like ISO/IEC 27001 and IEC 62443. This alignment helps organizations manage cybersecurity risks more effectively and streamline the compliance process, which is crucial in regulated industries.

“By focusing on these application areas, Moxa’s industrial cybersecurity solutions enhance overall security, ensure regulatory compliance, and protect critical systems from evolving cyber threats,” Liou said. “These solutions provide a comprehensive and integrated approach to cybersecurity, supporting both operational resilience and regulatory adherence in complex industrial environments.”

Al Presher, Editor, Industrial Ethernet Book

Building futureproof industrial network security

The major stages for building effective OT cybersecurity include a solid foundation with secure networking devices, deploying solutions that offer OT-centric layered protection and developing an ability to monitor network status and identify cyberthreats.

TODAY, INDUSTRIAL ORGANIZATIONS ARE embracing digital transformation to gain a competitive edge and boost business revenue. To achieve digital transformation, industrial operators must first address the daunting task of merging their information technology (IT) and operational technology (OT) infrastructure.

However, businesses trying to streamline data connectivity for integrated IT/OT systems often encounter challenges such as lacking performance, limited network visibility, and lower network security from existing OT network infrastructure. Building a robust, high-performance network for daily operations that is easy to maintain requires thorough planning.

In this article, we will focus on the importance of strong OT network security and provide some tips on how to strengthen cybersecurity for industrial operations.

Why ramping up OT network security is a must

Nowadays, industrial applications are facing more and unprecedented cyberthreats. These threats often target critical infrastructure in different industries all across the world, including energy, transportation, and water and wastewater services. If successful, such attacks can cause significant damage to industrial organizations in the form of high recovery costs or production delays.

Before building IT/OT converged networks, asset owners must define the target security level of the entire network and strengthen measures to minimize the impact of potential intrusions. Poor network security exposes critical field assets to unwanted access and allows malicious actors to breach integrated systems.

However, strengthening OT network security is not that straightforward. IT security solutions require constant updates to ensure they can protect against the latest cyberthreats.

Applying these necessary updates often means interrupting network services and systems, which is something OT operations cannot afford. Operators need an OT-centric cybersecurity approach to protect their industrial networks without sacrificing network or operational uptime.



SOURCE: ISTOCKPHOTO

Building secure industrial networks requires careful strategy and planning. But the key is implementing a multi-layered defense strategy in several stages.

Three major stages of building OT cybersecurity

Building a secure industrial network can be done with the right approach. The key to strong cybersecurity is implementing a multi-layered defense strategy in several stages.

Stage One: build a solid foundation with secure networking devices

When developing secure networking infrastructure, start with choosing secure building blocks. The increasing number of cyberthreats has also led to the development of comprehensive OT network security standards.

Industrial cybersecurity standards, such as NIST CSF and IEC 62443, provide security guidelines for critical assets, systems, and components. Implementing industrial cybersecurity standards and using networking devices designed around these standards provides asset owners with a solid foundation for building secure network infrastructure.

Stage Two: deploy OT-centric layered protection

The idea of defense-in-depth is to provide multi-layered protection by implementing

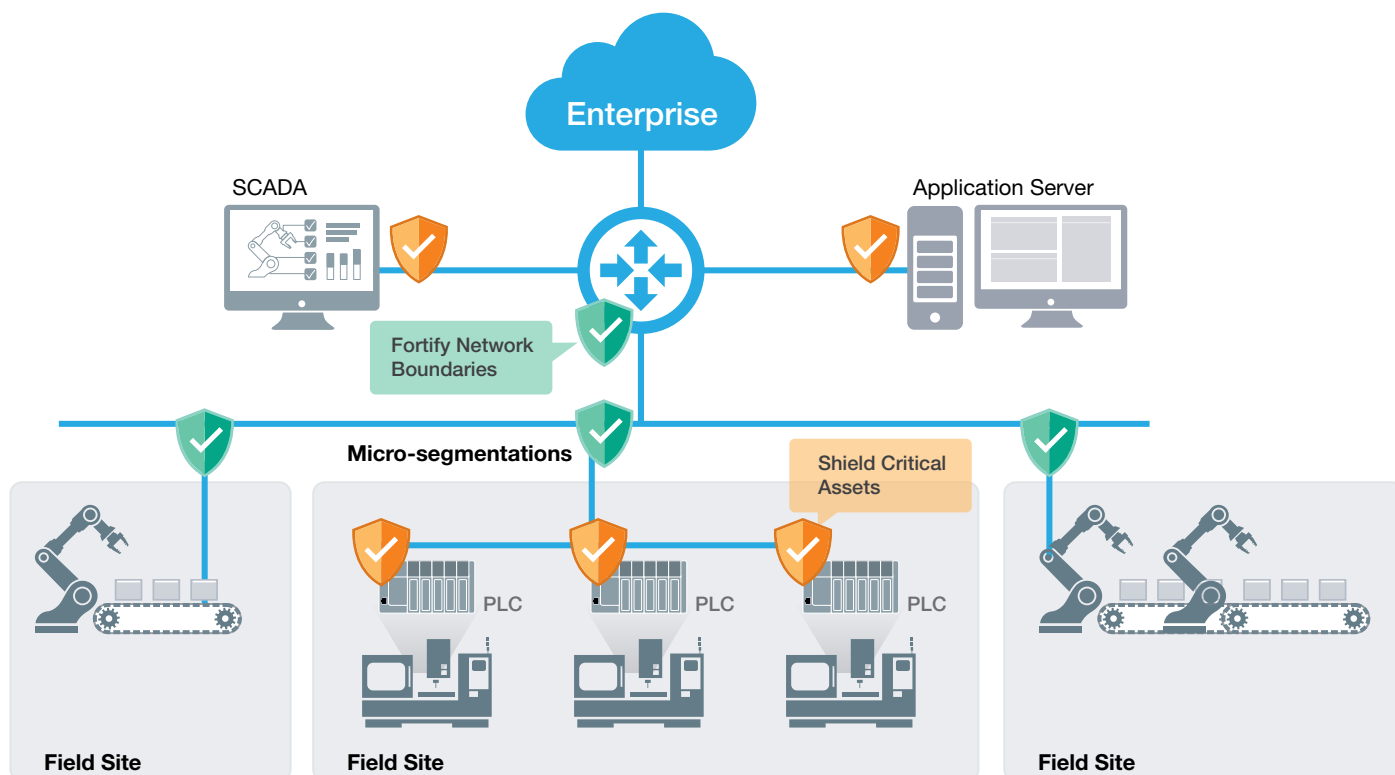
cybersecurity measures at every level to minimize security risks. In the event of an intrusion, if one layer of protection is compromised, another layer prevents the threat from further affecting the network. In addition, instant notifications for security events allow users to quickly respond to potential threats and mitigate any risk.

When deploying multi-layered network protection for OT networks and infrastructure, there are two key OT cybersecurity solutions to consider, namely industrial firewalls and secure routers.

Shield critical assets with industrial firewalls

An efficient way to protect critical field assets is using industrial firewalls to create secure network zones and defend against potential threats across the network. With every connected device being the potential target of cyberthreats, it's important to deploy firewalls with robust traffic filtering that allow administrators to set up secure conduits throughout the network.

Next-generation firewalls feature advanced security functions such as Intrusion Detection/Prevention Systems (IDS/IPS) and



When deploying multi-layered network protection for OT networks and infrastructure, there are two key OT cybersecurity solutions to consider, namely industrial firewalls and secure routers

Deep Packet Inspection (DPI) to strengthen network protection against intrusions by proactively detecting and blocking threats.

Advanced security functions tailored for OT environments help ensure seamless communications and maximum uptime for industrial operations. For example, OT-centered DPI technology that supports industrial protocols can detect and block unwanted traffic, ensuring secure industrial protocol communications.

In addition, industrial-grade IPS can support virtual patching to protect critical assets and legacy devices from the latest known threats without affecting network uptime. Designed for industrial applications, IPS provides pattern-based detection for PLCs, HMIs, and other common field site equipment.

Fortify network boundaries with industrial secure routers

IT/OT converged networks require a multi-layered and complex industrial network infrastructure to transmit large amounts of data from field sites to the control center. Deploying powerful industrial secure routers between different networks can both fortify network boundaries and maintain solid network performance. Featuring built-in advanced security functions such as firewall and NAT, secure routers allow administrators to establish secure network segments and enable data routing between segments. For optimal network performance, a powerful industrial

secure router features both switching and routing functions with Gigabit speeds, alongside redundancy measures for smooth intra- and inter-network communication.

The demand for remote access to maintain critical assets and networks has also been on the rise. Industrial secure routers with VPN support allow maintenance engineers and network administrators to access private networks remotely through a secure tunnel, enabling more efficient remote management.

Stage Three: monitor the network status and identify cyberthreats

Deploying a secure industrial network is just the start of the journey towards robust cybersecurity. During daily operations, it takes a lot of time and effort for network administrators to have full network visibility, monitor traffic, and manage the countless networking devices. Implementing a centralized network management platform can provide a huge boost to operational efficiency by visualizing the entire network and simplifying device management. It also allows network administrators to focus more resources on ramping up network and device security.

In addition, a centralized network security management platform for cybersecurity solutions can boost efficiency even more. Such software allows administrators to perform mass deployments for firewall policies, monitor cyberthreats, and configure notifications for when threats occur. The right combination

of cybersecurity solutions and management software offers administrators an invaluable way to monitor and identify cyberthreats with a holistic view.

Futureproof network security with effective solutions

Network security is imperative for industrial network infrastructure. Moxa has translated over 35 years of industrial networking experience into a comprehensive OT-centric cybersecurity portfolio that offers enhanced security with maximum network uptime.

Moxa is an IEC 62443-4-1 certified industrial connectivity and networking solutions provider. When developing products, designs adhere to the security principles of the IEC 62443-4-2 standard to ensure secure product development. The goal is to provide users with the tools necessary to build robust device security for industrial applications.

To defend against increasing cyberthreats, OT-focused cybersecurity solutions can maximize uptime while protecting industrial networks from intruders. Network management software can simplify management for networking devices and OT cybersecurity solutions, allowing administrators to monitor the network security status and manage cyberthreats with ease.

Technology article by Moxa.

[Visit Website](#)

IEC 62443 standards: defending against infrastructure cyberattack

By putting together and adopting the IEC 62443 standard, industrial automated control system stakeholders have paved the road for dependable and safe infrastructures. Secure authenticators are the bedrock of the future of IEC 62443 standard-compliant components requiring robust hardware-based security.



SOURCE: ISTOCKPHOTO

Industry 4.0 calls for highly connected sensors, actuators, gateways, and aggregators. This increased connectivity increases the risk of potential cyberattacks, making security measures more critical than ever. The creation of organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) illustrates the importance and demonstrates a commitment to safeguarding critical infrastructures and ensuring their resilience against cyberattacks.

THE FOUNDATIONAL REASONING AND BENEFITS of the IEC 62443 series of standards is that it provides a set of protocols designed to ensure cybersecurity resilience and protect critical infrastructures and digital factories.

This leading standard offers an extensive layer of security; however, it raises several challenges for those seeking certification. We will explain how security ICs provide essential assistance to organizations striving to reach certification goals for industrial automated control systems (IACS) components.

Introduction

Despite the potential for increasingly sophisticated cyberattacks, IACS have previously been slow to adopt security measures. This has been partly due to the lack of common references for designers and operators of such systems. The IEC 62443 series of standards offers a way forward towards more secure industrial infrastructures, but firms

must learn how to navigate its complexities and understand these new challenges in order to make use of it successfully.

Industrial systems at risk

The digitalization of critical infrastructures such as water distribution, sewage, and power grids has made uninterrupted access essential for everyday life. However, cyberattacks are still one of the causes of disruption to these systems and they are expected to grow.

Industry 4.0 calls for highly connected sensors, actuators, gateways, and aggregators. This increased connectivity increases the risk of potential cyberattacks, making security measures more critical than ever. The creation of organizations such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) illustrates the importance and demonstrates a commitment to safeguarding critical infrastructures and ensuring their resilience against cyberattacks.

Why IEC 62443?

In 2010, the emergence of Stuxnet thrust industrial infrastructures into a state of vulnerability. Stuxnet was the world's first publicized cyberattack indicating that attacks could successfully target IACSs from afar. Subsequent attacks have solidified the realization that industrial infrastructures can be harmed through remote attacks that can target a specific type of equipment.

Government agencies, utilities, IACS users, and equipment makers quickly understood that IACS needed to be protected. While governments and users naturally leaned towards organizational measures and security policies, equipment makers investigated possible hardware and software countermeasures. However, adoption of security measures was slow due to:

- the complexity of the infrastructures
- the different interests and concerns of stakeholders

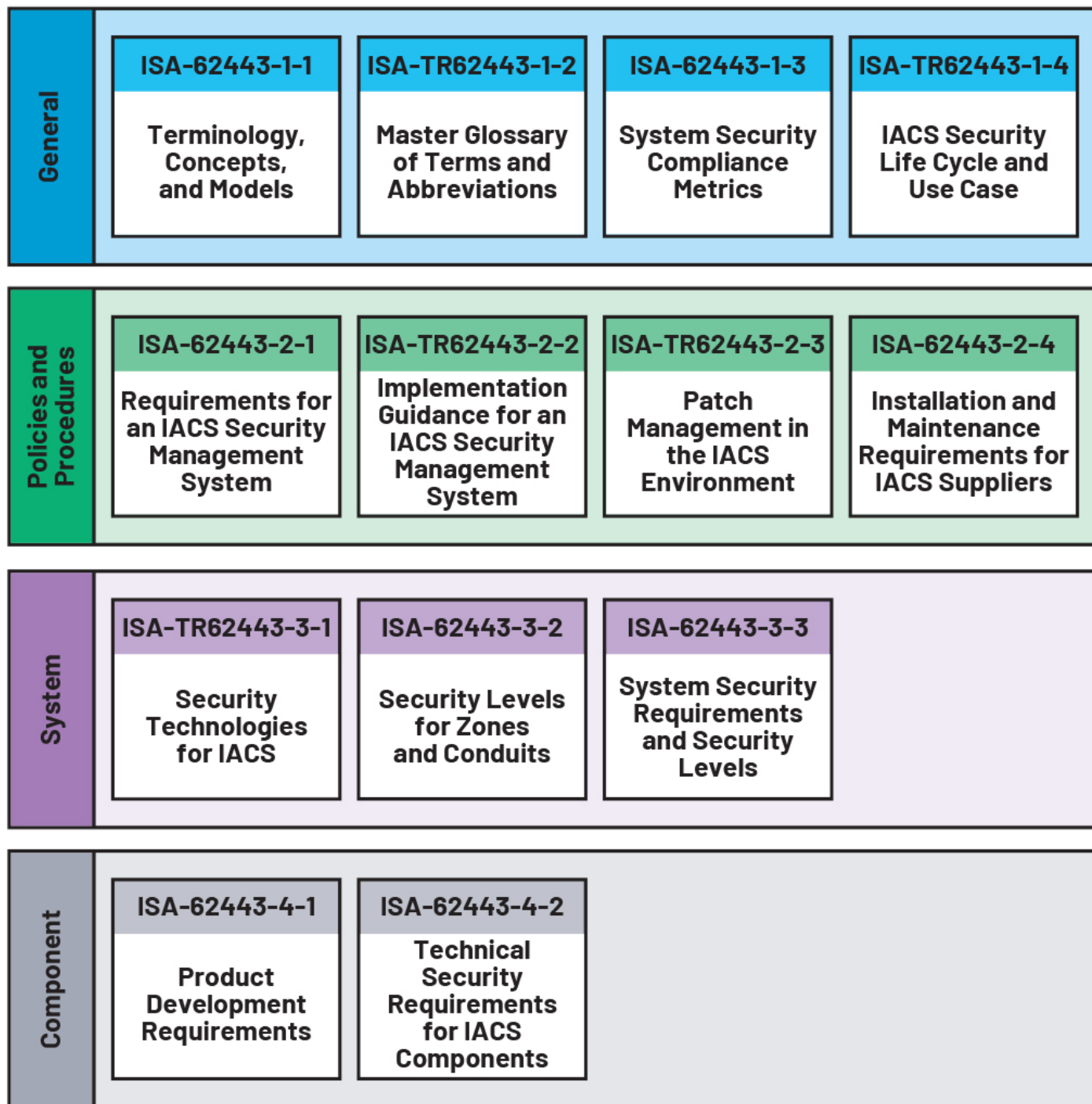


Figure 1. The IEC 62443 is a comprehensive security standard.

- the variety of implementations and available options
- the lack of measurable objectives

Overall, stakeholders faced uncertainty about the right level of security to target, one which carefully balanced protection with costs.

The International Society for Automation (ISA) launched working groups to establish common references under the ISA99 initiative, which finally led to the release of the IEC 62443 series of standards. This set of standards is currently organized into four levels and categories, shown in Figure 1.

Thanks to its comprehensive scope, the IEC

62443 standard encompasses organizational policies, procedures, risk assessment, and security of hardware and software components.

The complete scope of this standard makes it uniquely adaptable and reflective of current realities. Additionally, the ISA has taken a comprehensive approach when addressing the various interests of all stakeholders involved in an IACS. In general, security concerns are different from one stakeholder to another. For example, if we think about IP theft, the IACS operator will be interested in protecting manufacturing processes while an equipment maker may be concerned with protecting an

artificial intelligence (AI) algorithm from being reverse engineered.

Also, because IACS are complex by nature, it's essential to consider the entire security spectrum. Procedures and policies alone are insufficient if not supported by secure equipment, while robust components are useless if their secure usage is not properly defined by procedures.

The chart in Figure 2 shows the adoption rate of the IEC 62443 standards through ISA certifications. As expected, a standard defined by industry key stakeholders has accelerated the implementation of security measures.

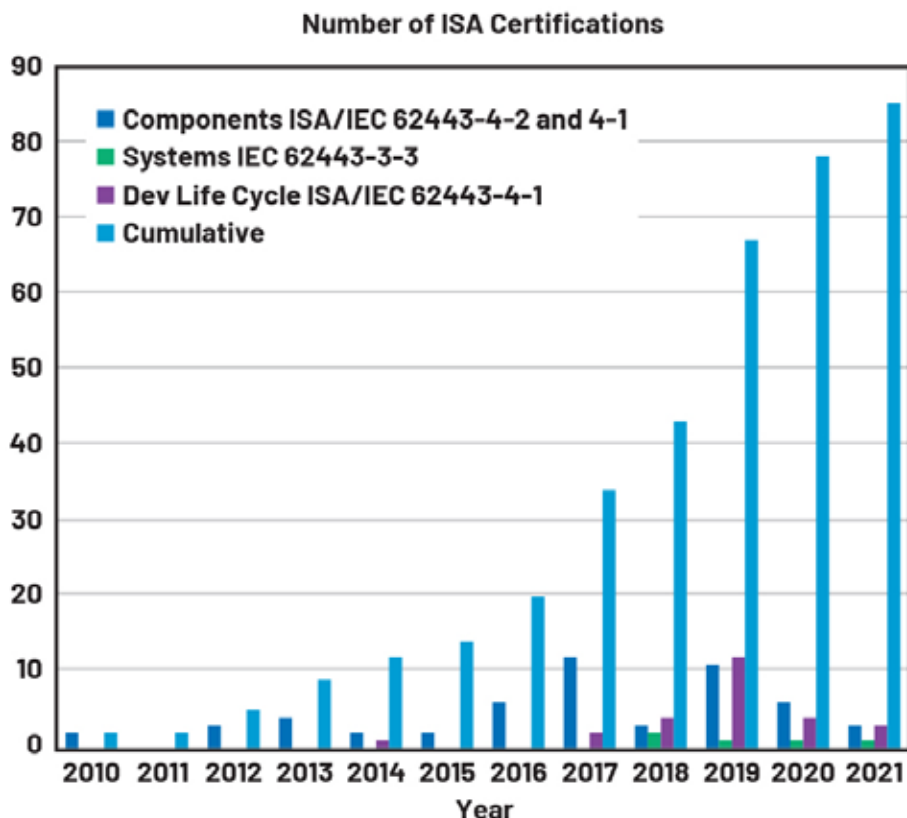


Figure 2. The number of ISA certifications over time.

IEC 62443 compliance: a complex challenge

The IEC 62443 is an incredibly comprehensive and effective standard for cybersecurity, yet its complexity can be overwhelming. The document itself is nearly 1000 pages in length. Acquiring a clear understanding of cybersecurity protocols involves a learning curve and reaches beyond absorbing the technical language. Each section within IEC 62443 must be understood as a part of a larger whole, as the concepts are interdependent (as shown in Figure 3).

For example, as per IEC 62443-4-2, a risk assessment targeting the entire IACS must be conducted and the outcomes will condition the decisions that determine the target security levels for equipment.

Designing IEC 62443 compliant equipment

Highest Security Levels Call for Hardware Implementation

The IEC 62443 defines security levels in straightforward language as shown in Figure 4.

The IEC 62443-2-1 mandates a security risk assessment. As an outcome of this process, each component is assigned a target security level (SL-T).

As per Figure 1 and Figure 3, some parts of the standard deal with processes and procedures while IEC 62443-4-1 and IEC 62443-4-2 address the components' security. Component types as per IEC 62443-4-2

are software applications, host devices, embedded devices, and network devices. For each component type, IEC 62443-4-2 defines the capability security level (SL-C) based on the component requirement (CR) and requirement enhancement (RE) they meet. Table 1 summarizes SL-A, SL-C, SL-T, and their relationship.

Let's take the example of a network-connected programmable logic controller (PLC). Network security requires that the PLC is authenticated so that it does not become an entry door for attacks. A well-known technique is public key-based authentication. With regards to the IEC 62443-4-2:

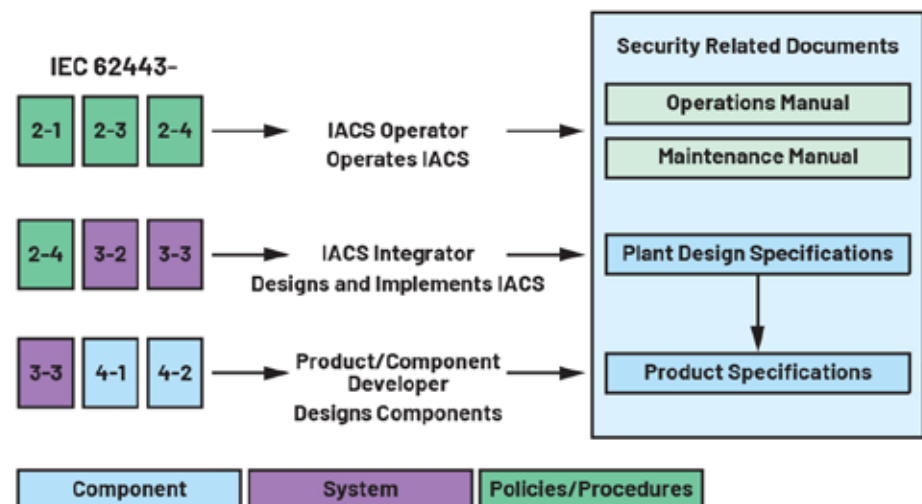


Figure 3. A high level view of the certification process.

SOURCE: ANALOG DEVICES

- Level 1 does not consider public key cryptography
- Level 2 requires the commonly adopted processes such as certificates signature verification

Levels 3 and 4 call for hardware protection of the private keys used in the authentication process

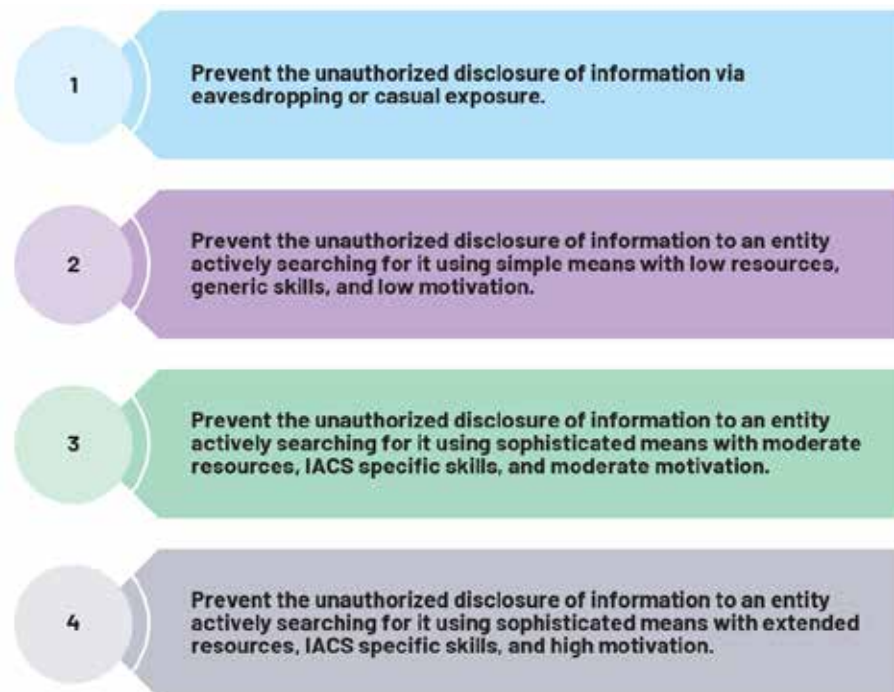
Starting at Security Level 2, many security functions are required, including mechanisms based on cryptography involving secret or private keys. For security levels 3 and 4, hardware-based protection of security or cryptography functions is required in many cases. This is where industrial component designers will benefit from turnkey security ICs, embedding essential mechanisms such as:

- Secure key storage
- Side-channel attacks protection
- Commands for functions such as:
 - Message encryption
 - Digital signature computation
 - Digital signature verification

These turnkey security ICs relieve IACS component developers from investing resources into complex security primitive design. Another benefit of using security ICs is to inherently take advantage of the natural isolation between general-purpose functions and dedicated security functions. The strength of security functions is more easily evaluated when security is concentrated in an element rather than spread throughout the system. Also gained from this isolation is the preservation of the verification of the security function across software and/or hardware modifications of the component. Upgrades can be performed without the need to reassess the complete security function.

Furthermore, secure ICs vendors can implement extremely strong protection techniques that are not accessible at the PCB or system level. This is the case of hardened EEPROM or Flash memory or physical unclonable function (PUF) that can achieve the highest level of resistance against the

SOURCE: ANALOG DEVICES



SOURCE: ANALOG DEVICES

result, the IACS accumulates and is exposed to all their vulnerabilities, as illustrated by the MITRE ATT&CK database⁶ or the ICS-CERT advisories.

Moreover, with the Industrial Internet of Things IoT (IIoT) trend of embedding more intelligence at the edge,⁸ devices are being developed to make autonomous system decisions. Therefore, it is even more critical to ensure that device hardware and software can be trusted given these decisions are critical to safety, operation of the system, and more.

Additionally, protecting the R&D IP investments of device developers from theft—related to AI algorithms, for example—is a common consideration that can drive the decision to adopt the protection that a turnkey security IC can support.

Another important point is that insufficient cybersecurity may negatively impact functional safety. Functional safety and cybersecurity interactions are complex and discussing them would deserve a separate article, but we can highlight the following.

IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems mandates cybersecurity risks analysis based on IEC 62443.

While IEC 61508 focuses primarily on hazard and risk analysis, it mandates subsequent security threat analysis and vulnerability analysis each time a cybersecurity occurrence is serious.

The IACS edge devices we listed are embedded systems. IEC 62443-4-2 defines specific requirements for these systems such as malicious code protection mechanisms, secure firmware updates, physical tamper resistance and detection, the root of trust provisioning, and integrity of the boot process.

Figure 4. The IEC 62443 levels of security.

most sophisticated attacks. Overall, security ICs are a great foundation to build system security.

Securing at the edge

Industry 4.0 means sensing everywhere, any time, and thus calls for the deployment of more edge devices. IACS edge devices include sensors, actuators, robot arms, PLCs with their I/O modules, etc. Each edge device is connected to a highly networked infrastructure and becomes a potential entry point for hackers. Not only does the attack surface expand proportionally with the number

of devices, but the diverse composition of devices inherently expands the variety of attack vectors.

“Given existing platforms, there’s a lot of viable attack vectors and increased exposure of both the endpoint and the edge devices,” said Yaniv Karta, CTO of the app security and penetration-testing vendor, SEWORKS.

As an example, in a complex IACS, not all sensors come from the same vendor, nor do they share the same architecture in terms of microcontrollers, operating systems, or communication stacks. Each architecture potentially carries its own weaknesses. As a

Secure Authenticator Features	IEC 62443 High Level Requirements	SL1	SL2	SL3	SL4
ECDSA/HMAC/AES MAC	Communication Integrity	X	X	X	X
Secure Boot	System Integrity: Boot Firmware, Configuration Data Integrity	X	X	X	X
AES Encryption	Data Confidentiality (at Rest, in Transit)	X	X	X	X
ECDSA Verification	User Authentication	X	X	X	X
ECDSA Signature/Verification	Device Authentication		X	X	X
Dedicated ECDSA/SHA/AES Engines	Hardware Security for Authentication			X	X
x.509 Certificate Verification	Certificate-Based Authentication, Standard PKI		X	X	X
ECDSA Signature	Protection of Audit Information		X	X	X
ECDSA Signature	Multifactor User Authentication			X	X
External Tamper Input	Tamper Resistance and Detection, Notification of Attempts			X	X
Security IC Firmware Update + System	Secure Updates (Security Module and System)		X	X	X
ChipDNA-Based Secure Storage	Hardware Secure Storage for Private Keys			X	X

SOURCE: ANALOG DEVICES

Figure 5. Secure authenticators features mapping to IEC 62443 requirements.

Table 1. Security Levels Summary

	Target Security Level	Capability Security Level	Achieved Security Level
Acronym	(SL-T)	(SL-C)	(SL-A)
Definition	The security level equipment should reach according to the system-level risk assessment	The security level equipment is capable of according to the CRs it supports as per IEC 62443-4-2	The security level that equipment achieves
Objective	SL-T ≥ level defined by risk assessment	SL-C ≥ SL-T	SL-A ≥ SL-T

Table 2. DS28S60 and MAXQ1065 Key Parameters Summary

Device Features	DS28S60/MAXQ1065
Operating Temperature	−40°C to +105°C
Host Interface	SPI (I ² C in development)
Supply Voltage	1.62 V to 3.63 V
Maximum Active Current	3 mA
Typical Idle Current (25°C)	0.4 mA
Power Down Current (25°C)	100 nA

add high grade security to an existing design. They save the R&D effort of rearchitecting a device for security for a low BOM cost. For example, they do not require changing the main microcontroller. As examples, the DS28S60 and MAXQ1065 secure authenticators address all levels of the IEC 62443-4-2 requirements as illustrated in Figure 5.

The DS28S60 and MAXQ1065 3 mm × 3 mm TDFN packages make them suitable for the most space-constrained design and their low power consumption perfectly addresses the most power-constrained edge devices.

IACS component architectures already featuring a microcontroller with the security functions to address IEC 62443-4-2 requirements can also benefit from secure authenticators for keys and certificate distribution purposes. This would save the OEMs or their contract manufacturers from investing in costly manufacturing facilities needed to handle secret IC credentials. This approach would also protect keys stored in microcontrollers to be extracted through debugging tools such as JTAG.

Conclusion

By putting together and adopting the IEC 62443 standard, IACS stakeholders have paved the road for dependable and safe infrastructures. Secure authenticators are the bedrock of the future of IEC 62443 standard-compliant components requiring robust hardware-based security. OEMs can design with assurance, knowing that secure authenticators will help them achieve the certifications they seek.

Christophe Tremlet, Director, Business Management, Analog Devices.

[View Product Portfolio](#)

Meet IEC 62443 objectives with ADI's Secure Authenticators

Secure authenticators, also referred to as secure elements, from Analog Devices have been designed to address these requirements with ease of implementation and cost efficiency in mind. Fixed-function ICs that come with a full software stack for the host processor are turnkey solutions.

As a result, security implementation is delegated to ADI and components designers can focus on their core business. Secure authenticators are the root of trust by essence, providing secure and immutable storage of root keys/secrets and sensitive data representative of the state of the equipment, such as firmware hashes. They feature a comprehensive set of cryptographic functions including authentication, encryption, secure data storage, life cycle management, and secure boot/update.

ChipDNA™ physically unclonable function (PUF) technology utilizes the

naturally occurring random variation in wafer manufacturing processes to generate cryptographic keys rather than storing them in traditional EEPROM of Flash. The variations exploited are so small that even the expensive, most sophisticated, invasive techniques used for chip reverse engineering (scanning electron microscopes, focus ion beams, and microprobing) are inefficient to extract keys. No technology outside of integrated circuits can reach such a level of resistance.

Secure authenticators also enable certificates and chains of certificate management.

In addition, ADI offers a highly secure key and certificate preprogramming service in its factories, so that original equipment manufacturers (OEMs) can receive parts already provisioned that can seamlessly join their public key infrastructure (PKI) or enable offline PKI. Their robust cryptographic capabilities enable secure firmware updates and secure boot.

Secure authenticators are the best option to

Effective strategies for keeping IoT environments secure

IoT devices can offer flexibility and convenience. However, in order to get the most benefit out of these solutions, they need to be adequately protected. By following effective strategies, organizations can ensure IoT devices don't become a source of a network breach and remain an asset that helps improve business operations.



SOURCE: ISTOCKPHOTO

Effective cybersecurity strategies are an important part of an overall program to develop IIoT and Industry 4.0 solutions.

THE INTERNET OF THINGS (IoT) HAS BECOME an integral part of modern-day society. From the smart devices we use in our homes to the sensors used in supporting intelligent factories and supply chains.

However, while IoT devices and the networks they support offer a number of advantages for everyone, they can pose a number of risks to organizations that don't adequately secure them.

The question is what are the security risks that IoT devices introduce?

Because of their "always on" functionality, IoT devices can bring a number of unique challenges to individuals and businesses by opening up a variety of security vulnerabilities. This can lead to:

Database security breaches

IoT devices operate by collecting a large amount of information - much of it can be sensitive information about connected networks or critical systems and databases. This information is typically in constant

motion and will usually be stored in caches on both the device itself and connected data storage locations.

If databases or networks are left unsecured, this can lead to potential security breaches, which are the primary sources of identity theft and other forms of fraud.

Remote controlled botnets

Cybercriminals will often look to recruit a number of IoT devices to conduct large-scale attacks on other organizations. These massive networks, known as "botnets" can be used for a variety of malicious purposes, including launching Distributed Denial of Service (DDoS) attacks that flood networks with a large volume of activity at once - downing servers and any connected applications or systems.

Botnets are often used to hijack the processing power of different devices and can be used to successfully accomplish a number of illegal activities - often without the device's owners even knowing it's happening.

Compromised network access

In the event a malicious source gains access to an unsecured IoT device, they can use this entry as a starting point to go deeper into networked systems and look for more valuable targets. Some of these targets could be computers or databases connected to the network, which could contain important elements of the underlying infrastructure.

A compromised network can lead to a wide range of issues for organizations, which can have long-term, negative operational and financial implications.

Injection points for dangerous malware

IoT devices offer organizations a high level of flexibility and convenience, especially when they're positioned in various locations around buildings and offices. However, if they are more accessible to individuals, this can also leave them open to tampering.

Cyberattackers are able to exploit software vulnerabilities in devices if they're able to



A compromised network can lead to a wide range of issues for organizations, which can have long-term, negative operational and financial implications.

access them directly. Using various tools and equipment, they can modify the device's software and firmware and inject malicious code that can be used to carry out their agendas.

Strategies for securing an IoT infrastructure

Although IoT devices come with their own level of risk when integrated into business environments, this doesn't mean organizations don't have options for reducing their digital attack surface.

Below are some effective strategies that can be put in place to keep an IoT infrastructure secure.

Best practices password policies

One of the most effective ways to keep devices secure is by applying best practices when creating authentication credentials. This includes establishing passwords at least 12 characters in length and using a combination of upper and lowercase letters as well as numbers and symbols.

Many out-of-the-box IoT devices will already have default administrative passwords in place. It's important to never leave these unchanged, as they are often easy to compromise.

Establishing stronger passwords for devices is important, but users should also remember to change their credentials regularly (every 90-180 days). This added step is an additional protection for networks that may have had certain credentials compromised over time.

Using network segmentation

Network segmentation, the practice of breaking up a larger network into smaller pieces, is a common security measure being used increasingly in modern business environments.

The purpose of network segmentation is to create isolation points in the event a particular endpoint is breached. In the event of successful network penetration, segmented networks make it much more difficult for attackers to move laterally into other more valuable systems or databases.

Organizations can begin segmenting their networks by making use of virtual local area networks (VLANs) in combination with firewalls and other security networking solutions. This process can be more time-consuming to set up, however, it can be well worth the effort to ensure IoT devices aren't a source of major security breaches.

Monitoring IoT devices

Another important part of keeping a more secure IoT network is by regularly monitoring the traffic coming too and from connected devices. This is an important step in not only being able to identify suspicious activities happening on a network, but also giving IT administrators an opportunity to contain them.

Networking monitoring solutions can use automated processes to monitor activity on system networks while setting up alerts tied to failed login attempts or malware detections.

Another critical feature of many network monitoring solutions is their ability to track

all IoT devices and report on their firmware versions. This allows you to have a unified view of all digital assets to make sure they're all getting the security updates and patches they need to keep the business network secure.

Implementing firewall protections

Firewalls are another important necessity when using IoT devices. They are another tool for helping to monitor incoming and outgoing network traffic while also having specific configurations in place to successfully block any unauthorized access.

Next-generation firewalls (NGFW) offer even more advanced features like intrusion prevention systems which filter traffic on a much more granular level. In these setups, firewalls will use deep packet inspection methods to add an additional layer of security that traditional firewalls won't support.

Make IoT devices more secure

IoT devices can offer a great deal of flexibility and convenience for individuals and businesses. However, in order to get the most benefit out of these solutions, they need to be adequately protected. By following the strategies discussed, organizations can ensure their IoT devices don't become a source of a network breach and instead remain an asset that helps improve business operations.

Guido Voigt is the Director of Engineering at Lantronix.

[Learn More](#)

Automatic CIP Security via Pull Policy

This article explores important use cases for automatic pull policy as a new approach to delivering CIP Security configuration, discussed requirements, and evaluated some technology options. The ability to pull all of the CIP Security configuration is important for enabling use cases which will be important in the future.



SOURCE: ISTOCKPHOTO

CIP Security provides important information assurance properties that are needed to mitigate threats in many industrial applications using EtherNet/IP.

THE CIP SECURITY PULL MODEL PROFILE provides a major benefit of allowing a device to automatically discover a certificate enrolment server and request a certificate for secure communication. However, secure communication with CIP Security requires additional configuration beyond just the certificate. Additional value could be realized by defining a mechanism for a device to request not just a certificate, but also the associated configuration for enabling CIP Security.

This configuration includes things like allowed cipher suites, trust anchors, certificate revocation lists, etc. One benefit of this ability would be the seamless application of device replacement, where a replaced device could automatically discover a security configuration server and request all of the configuration needed for CIP Security.

Furthermore, this would enable devices to work in network architectures where a configuration tool could not reach the device, like a NAT with the device on the private

network and the configuration tool on the public network. We will explore use cases and requirements for a feature such as this, as well as potential technology choices.

Introduction

CIP Security provides important information assurance properties that are needed to mitigate threats in many industrial applications using EtherNet/IP. However, prior to using CIP Security there must be a configuration step that takes place.

The CIP specification has defined a common way in which this configuration is delivered to a device via CIP objects and services. This works well in many cases, although there are some limitations. This is explored further in the use cases section, but briefly there are at least three situations where delivering CIP Security configuration via CIP objects and services presents a limitation:

- Network architectures where routing is not allowed like Network Address Translation (NAT)

- Software that only has CIP client capabilities and no server functionality
- Fully automatic device replacement with CIP Security enabled

In order to serve these use cases (and potentially others) a new mechanism for delivering CIP Security configuration is discussed here. Requirements for this mechanism are discussed in this article, but essentially it needs to be able to serve CIP Security configuration via a document that is requested by a client. In this context, the term “document” refers to a packaged data format that exists in one coherent file and can be transmitted to the consumer independent of the transport mechanism. Of course, this scheme must provide authenticity assurances and be resistant to cyber-attacks.

Besides discussing use cases and requirements, this article will also investigate potential technologies to realize this scheme for delivery of CIP Security configuration via a document format. A few technologies are weighed against how well they meet

the requirements, and a recommendation for a technology to use is given, as well as recommended future work.

Use cases

A consistent security configuration is required for devices to operate in a secure manner. Due to the need for clients and servers to have the same configuration, a mechanism for the clients and servers to request, or “pull” security configuration is useful to distribute this security configuration across multiple use cases that may even overlap.

The existing Push Model is useful in that a centralized tool can configure all the devices in the network, but it fails to accommodate some important use cases, which are explored below. Note that the Push Model as currently defined can provide a certificate as well as the necessary CIP Security configuration via CIP services and attributes. However, the current Pull Model only provides a certificate; therefore, this document format is necessary to provide parity of Push and Pull models.

In this use case, the PLC opens a client connection (not a CIP connection, rather some TCP or similar session) to the OT Configuration server and pulls its security configuration periodically. The routes through the router and the firewall can be simply configured and monitored.

Motor

Network topologies that enforce network segregation through routers with Network Address Translation (NAT) make it difficult for Push Model connections to be made through the router. In Figure 1, any devices that connect to the DMZ will have a translated IP address of 10.20.14.1.

The DMZ will not be allowed to make a connection through the router to the OT Network unless pre-configured routes are used. This requires substantial configuration and continuous maintenance as devices in the segregated network are added and removed. Preconfigured routes also weaken the security posture of the segregated network giving attackers a well-defined path to gain access to the network.

Deliver security config to “client-only” software

SCADA, HMI, Engineering, Configuration and Management tools, are often client only functionality. Unlike OT devices such as PLCs and IO, they have no ability to accommodate a Push Model for configuration. However, there is still a need for coherent security configuration for clients to be aligned with servers in the system. Much like the first use case where a client connection can be easily configured through routers and firewalls, the Pull Model provides simpler system configuration while ensuring a high level of security posture.

Ethernet LAN Diagram

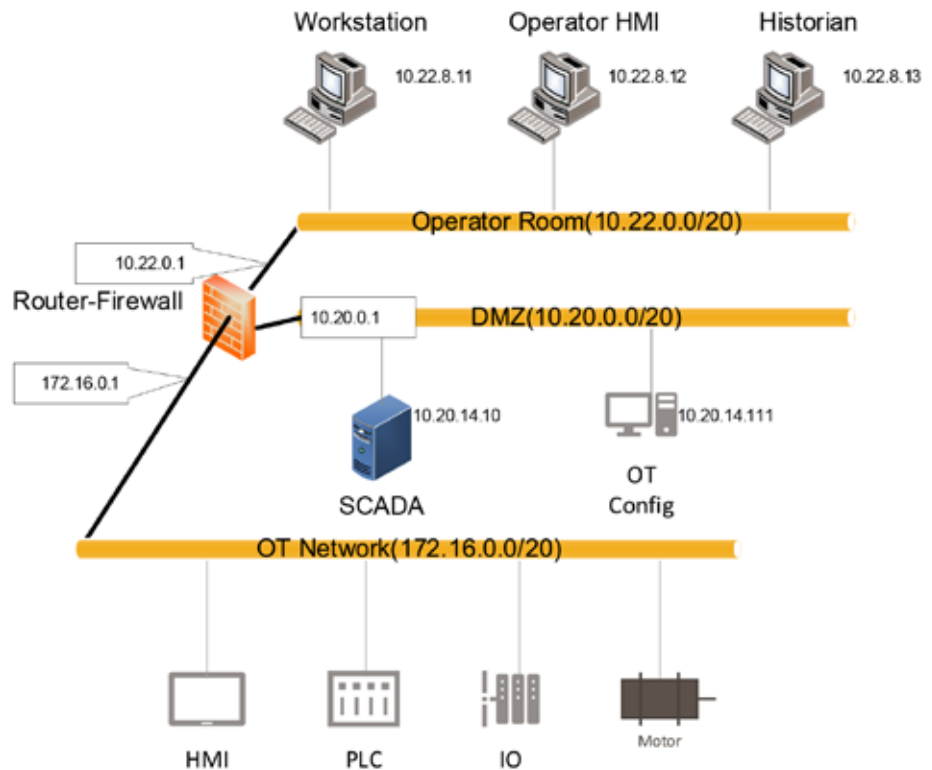


Figure 1.

Fully automatic device replacement

In one last use case regarding device replacement, allowing a device being replaced to retrieve its own configuration is a straightforward way to facilitate device replacement. The specifics of how a device may come to be trusted on the network are outside the scope of this article, but a simplified configuration to enable that process can be accomplished with a Pull Model.

As an example, an electric motor driver is replaced. The motor driver searches for a well-known address using mDNS (multicast DNS packets to discover a service) or DNS-SD (a specific protocol for discovering network services) in order to find the OT Configuration service address. After the address is resolved, the motor driver can then pull its initial security configuration from the OT Configuration service. This configuration may be enough to allow the full bootstrapping of trust of the new motor driver without manual intervention.

Requirements

This section outlines some of the crucial requirements ensuring the effective delivery of a robust security configuration. Here, a diverse set of requirements is outlined that encompass various aspects, including

technical specifications and practical use case considerations. By addressing these crucial prerequisites, a solid foundation can be established for implementing a reliable and tailored security configuration.

Document format

A comprehensive document format is essential for managing and communicating critical security parameters from the configuration server. This document format enables the inclusion of crucial information such as allowed cipher suites, trust anchors, and certificate revocation list together with the communication certificate.

Integrity and consistency are vital aspects when it comes to delivering the security related configuration. Bundling all the configuration options in one single document maintains the reliability and trustworthiness of the information. Both these attributes ensure that the content of the document remains accurate and unaltered. This allows for all of the configuration to be applied atomically, as it can be parsed and interpreted by the device and then applied at once. Furthermore, the document format abstracts the transport of configuration from the configuration itself, meaning that this

could be delivered over other transports (e.g. MQTT) if that was necessary or beneficial in some use cases.

A well-defined document format containing allowed cipher suites, trust anchors, and certificate revocation lists, delivered along with the device's identity certificate establishes a robust security configuration.

Authenticity

The authenticity of a document confirms its genuine origin and ensures that it has not been tampered with. It ensures that the document can be trusted as an accurate representation of its contents, i.e. the full security configuration delivered from the server.

The validation of the authenticity of a document is crucial and something that can be done using different mechanisms. In all cases there needs to be some provisioning done before the validation of the authenticity takes place. One common approach is the use of digital signatures. Digital signatures utilize cryptographic techniques to bind a unique identifier to the document. By verifying the digital signature, the device can authenticate the document and trust that it came from the expected sender and was not modified by an unauthorized party. However, in this case the device would need to be pre-provisioned with a key from the server generating the document.

In all cases the pre-provisioning requires that some trust provisioning with the device takes place before the authenticity of the document can be verified. Once the pre-provisioning of trust occurs this could allow for a fully automatic and seamless device replacement. To establish the initial trust, the process of a trust on first use (TOFU) approach would be required. Upon the first attempt to connect, to a configuration server the device is initially provisioned with cryptographic keys. These keys then facilitate validation of the authenticity of the signed configuration document, providing the replaced device with security configuration.

Confidentiality

In general, the security configuration isn't secret and doesn't need to be protected by encryption. However, the pre-shared keys are one attribute within the security configuration that needs to be protected and kept secret. Installations that use pre-shared keys are normally smaller installations with a limited number of nodes. In those cases, it's less likely that the Pull Model will be used, as a centralized configuration server may not be present.

If pre-shared keys are to be delivered via the Pull Model, at a minimum they need to be encrypted in some way. Alternatively, the whole document could be encrypted. This would protect the pre-shared keys in the case when they are used. Since only the pre-shared keys need to be protected and pre-shared

keys are not the normal use-case, it is an unnecessary burden to always encrypt the whole document.

There are however merits to allow for encryption of the whole document if additional configuration attributes that require protection, are added in the future. For this reason, it's preferable to make it an option for the end-user to protect the whole document with encryption.

Versioning

End nodes need to be aware of the specific version of the policy they are applying in order to ensure proper functionality and compatibility. This is crucial when implementing updates or modifications to policies while maintaining backward compatibility. There are two primary methods to accomplish version tracking; using a counter or using timestamps.

The counter-based approach involves assigning a numerical value to each new version of the policy document. Every time a new version is created, the counter increments by one. End nodes can then reference this counter value to determine the policy version they should apply.

Alternatively, timestamps can be employed to track policy versions. Each time a new version of the policy document is created, a timestamp indicating the date and time of the update is assigned. End nodes can compare their own timestamp with the latest timestamp in the document to determine which version to apply. This method provides more value, allowing for precise version identification when the configuration change in the document was done. However, it does require that consumers of the policy document have time set in a synchronous manner with the configuration server.

It's worth noting that choosing the counter-based approach initially does not preclude the utilization of timestamps in the future. Timestamps can be introduced for additional functionalities as needed in the future. For example, timestamps can be used to track the last modification time of the document or for auditing purposes, while the counter remains dedicated to policy versioning.

Automatic discovery

In the CIP Security Pull Model Profile, the initial setup involves locating an Enrollment over Secure Transport (EST) server through mDNS/DNS-SD and subsequently requesting identity and trust information using the EST protocol. The certificate and trust provisioning process in the Pull Model comprises two primary steps. Firstly, the EST server is discovered using mDNS/DNS-SD. Secondly, certificates are retrieved from the EST server.

Likewise, the new Pull Policy approach requires the discovery of a server to access

the policy document. Since mDNS/DNS-SD is already established in the CIP Security specification, it is preferable to continue utilizing these mechanisms. By reusing the same mechanisms and protocols, unnecessary burden on end nodes is eliminated. Generally, this requirement is meant to ensure that any technology chosen would not prevent the continued use of mDNS/DNS-SD.

Configuring retry

During the initial discovery process of the Pull Policy server, the end node will continuously attempt to find the server and request the policy document. However, it is crucial to avoid overwhelming the network with excessive traffic when the server is offline or temporarily unable to provide the policy document.

To address this issue, it is necessary to implement a mechanism that reduces network traffic generated by the end node's attempts to discover the server or obtain a policy document. This mechanism should include a sensible default value, which can potentially be modified by end users through configuration options. Additionally, incorporating a back-off algorithm could be a beneficial consideration.

Trigger a reconfiguration

Over time, it is expected that the configuration policy will undergo changes, necessitating the deployment of a new policy document on the end-nodes. To ensure proper functioning, this new policy deployment must be synchronized across the entire system or, at the very least, among all interconnected end-nodes.

Given the requirement for synchronization among the affected end-nodes, a triggering mechanism becomes necessary for initiating this reconfiguration. In many cases, it is advantageous for the reconfiguration trigger to be executed through a CIP command. This approach allows for the synchronization of reconfiguration with the control operation of the system, including the secure closure and re-establishment of IO connections. However, there are also advantages to triggering the reconfiguration through the policy server especially if it could be done through a non-CIP mechanism, as the policy server would not need to know about CIP at all.

Alternatively, it is possible for each end-node configured via the policy document to periodically check for policy updates. In many cases this will provide an acceptable level of synchronization, as changes across the system need not be synchronized atomically. Many security changes will result in connections being dropped and re-made, which will provide some amount of downtime. If this downtime extends by a few seconds that is likely acceptable, as these types of changes are likely not being applied during production.

	AutomationML	Custom JSON	Existing Policy Language like REGO	Encoded CIP Commands	Explanation
Document format	10	10	10	10	All options provide data in a document format
Authenticity	10	10	10	8	AutomationML, JSON, and most existing policy languages already have mechanisms for applying a digital signature. A custom file of encoded CIP commands would need to define a mechanism or choose from one of the many file signing formats.
Confidentiality	10	10	10	8	Essentially the same scoring and same reasoning as for authenticity
Versioning	10	10	10	8	Once again, the same reasoning holds; existing languages can use existing versioning.
Automatic discovery	n/a	n/a	n/a	n/a	None of these technologies provide this, it would need to be added through another means like DNS-SD.
Configuration retry	9	9	9	7	AutomationML, JSON and existing policy languages can easily encode this via a name-value pair, or encoded CIP commands as those don't have a seamless way to do this.
Trigger a reconfiguration	9	9	9	7	Same reasoning as for Configuration Retry.
Suitable for an embedded environment	6	10	2	10	JSON is a very lightweight technology and would be tailored to this use case, therefore it is highly efficient. Many of the existing languages are not well suited to an embedded space. AutomationML is used in some embedded applications, but is feature rich and built on XML, which is not very lightweight. CIP commands are already used in the embedded space, so this option is also very well-suited.
Human readable	8	9	9	3	JSON and many existing languages are very human readable, AutomationML is more complex but still fits here. CIP commands however are not generally human readable.
Optimized for CIP	6	9	1	10	A custom JSON for CIP Security policy is well suited to delivering CIP, and of course CIP commands are perfectly suited to this task. AutomationML is not, and many existing policy languages are not possible to use for this purpose.
Totals	78	86	70	71	

Ease of use with CIP configuration

Even if a technology was able to easily meet all of the aforementioned requirements, it would be useless if it could not be used to encode CIP configuration. This effort is focused on deploying CIP Security configuration as document-based policy in a secure manner, so it is very important that the document is able to encode CIP configuration. Some technologies may be optimized for other types of information and therefore are not able to easily encode CIP configuration, in which case they would not be suitable.

Configuring CIP Security involves several things, from simple setting of Boolean attributes to transmission of certificates for use as trust anchors. Although not strictly necessary for the minimum configuration, it is also helpful to be able to encode a request for the execution of a certain CIP service, as these might be necessary for the policy to be fully realized (for example, the policy may include running the Object_Cleanup service of the CIP Security object to clean up any unused certificates after a new policy is applied).

Suitable for embedded computing environments

Given that many of the CIP stacks execute on an embedded software platform, any technology chosen for pull policy must be able to execute within an embedded environment. Although this might not completely disqualify some possible solutions, it will likely make some less suitable. Technologies that rely on large files or require software agents to run would be less suitable for use in an embedded environment.

Human Readable

It is ideal to choose a technology that allows for the policy document to be human readable. This would provide a quick interpretation of a given policy document, and possibly even allow for manual editing in a simple system. Auditing would also be easier, as a human or machine could interpret the document without any additional decoding needed.

Technology

There are several possibilities for the technology used for the configuration policy

formatting. Given that the configuration policy is to be encoded and delivered in a document, the transport mechanism is not very important; a document can be transmitted over various communication protocols. However, the technology used to format this document is important to define. Various technologies offer trade-offs. A discussion of a few possibilities follows.

AutomationML

Automation Markup Language or AutomationML, is a data modeling language created specifically for industrial automation. AutomationML is object oriented and provides some powerful features like object inheritance. This is realized using role classes and interface classes. This provides a high degree of flexibility in modeling various data concepts, and it has been used successfully in many applications, such as in the Process Industry with CAEX via IEC 62424. However, with these features comes complexity, and given that CIP objects do not directly support object inheritance, AutomationML may not be



The ability to pull all of the CIP Security configuration is important for enabling use cases which will be important in the future.

the best fit for CIP configuration policy, as not all of the functionality can or will be realized. AutomationML relies on XML for the data encoding. XML is a well-used format, although it is not generally viewed as a compact format, especially in the context of embedded devices. However, AutomationML is already deployed in various use cases across the industrial automation space, often as a unifying format to ensure different engineering tools are able to use the same data. Although this is a very important use case it is quite different from the use case of distributing CIP Security configuration policy.

Custom JSON encoded document

A custom encoding could be defined using JSON to represent CIP objects, attributes and services. The downside of this is that it requires some upfront work to define this. However, it would likely be very well suited for CIP Security configuration policy, as it would be defined specifically for that purpose. JSON is a very popular data exchange format that is compact and has wide support in parsers, some being quite lightweight and optimized for embedded environments. JSON already has signing and encryption defined via the JOSE standard; that could be applied for authenticity and confidentiality. Furthermore, a JSON schema could be defined to better document the configuration policy format and to help possible future enhancement efforts. For all these reasons this is an attractive option if the upfront development cost is palatable.

Other policy languages

There are a number of “policy languages” that are already in use for various purposes. Although it is not practical to analyze all of these languages, it is possible to speak about

them generically. All of these were created for a use other than with CIP Security policy, so they will of course not be well optimized for that. It may be possible in some cases for them to still be used, but that is not the purpose of these languages and there will likely be limitations in using them for CIP Security policy.

An example of a language like this is Rego, which is used with Open Policy Agent (OPA). This language is well optimized for access control, and although it is flexible, it would be challenging to tailor it to work with CIP object/attribute configuration.

Encoded CIP services

Another possibility is to simply use the encoded CIP services within a document format. CIP already defines a format for calling services as a transmission protocol. This “on-the-wire” formatting could simply be encoded into a document and used there. This is quite straightforward from the standpoint of capturing the necessary configuration. However, it would not be human readable. Furthermore, it would not be straightforward to encode information that might not be part of a CIP object, such as the revision of the policy document. Signing and encryption would also need to be defined for this option. Although there are many ways to sign and encrypt a file, there is no standard way that this would be done since it is a custom file.

Technology comparison

Building on the discussion above, some scoring can be done of these different choices against the requirements. An arbitrary value of 0 – 10 is used for how well each requirement is met. A score of 10 means the requirement is met in an ideal way, 0 means it is not met at all.

Conclusions

This article explored some of the important use cases for automatic pull policy as a new approach to delivering CIP Security configuration, discussed requirements, and evaluated some technology options. The ability to pull all of the CIP Security configuration is important for enabling use cases which will be important in the future, including securing devices within a private NAT network and client-only software.

It is likely that client-only software will grow in usage as more IIoT applications are realized in practice, such as connecting software agents that harvest data or applications that reside on mobile devices.

Furthermore, the ability to replace a CIP device and deliver all of the CIP Security configuration seamlessly will enable better workflows and further ease of use. Although it is possible to realize this through a number of technologies, analysis shows that defining a JSON schema for encoding CIP Security configuration is the best technology choice.

Follow-on work will include defining a specification enhancement to Volume 8 of the CIP specification that defines a mechanism for this, likely using JSON. Other follow-on work includes an investigation into whether or not this might be suitable for delivering other CIP configuration via a policy document. It is likely that the same requirements would hold, although certain applications like CIP Motion or CIP Safety might have additional needs that were not explored.

Joakim Wiberg, Head of Technology, HMS Networks; David Smith, Cybersecurity Architect, Schneider Electric; and Jack Visoky, Principal Engineer and Security Architect, Rockwell Automation.

Cybersecurity basics: industrial security fundamentals

The fundamentals of industrial cybersecurity are based on key principles including confidentiality, integrity and availability. Cybersecurity often seems like an invincible Hydra but, with practical guidelines, users can setup systems and create strategies that significantly strengthen the security of company networks.



SOURCE: ISTOCKPHOTO

Cybersecurity is a never-ending task. With defined processes for continuous improvement, organizations create the preconditions for a continuous improvement cycle, including regular review and refinement of security protocols, incident response procedures, and monitoring mechanisms.

CYBERSECURITY IS A BARE NECESSITY, THAT much is clear. What is less clear, however, are the basic principles that form the foundation of a strong and effective cybersecurity strategy. If they are missing, the entire concept is rickety.

Part One: Confidentiality, Integrity and Availability

C.I.A. – these three letters stand for the classic understanding of cybersecurity. Even if others are sometimes added, these three form the core. The C stands for confidentiality. This means that only the authorised parties involved are allowed to read the content. The I stands for integrity, which states that the content of a message may not be changed. In addition, the A is availability: a message must be available for exactly as long as necessary, neither longer nor shorter.

When it comes to IT security, these three aspects are considered equally important. In

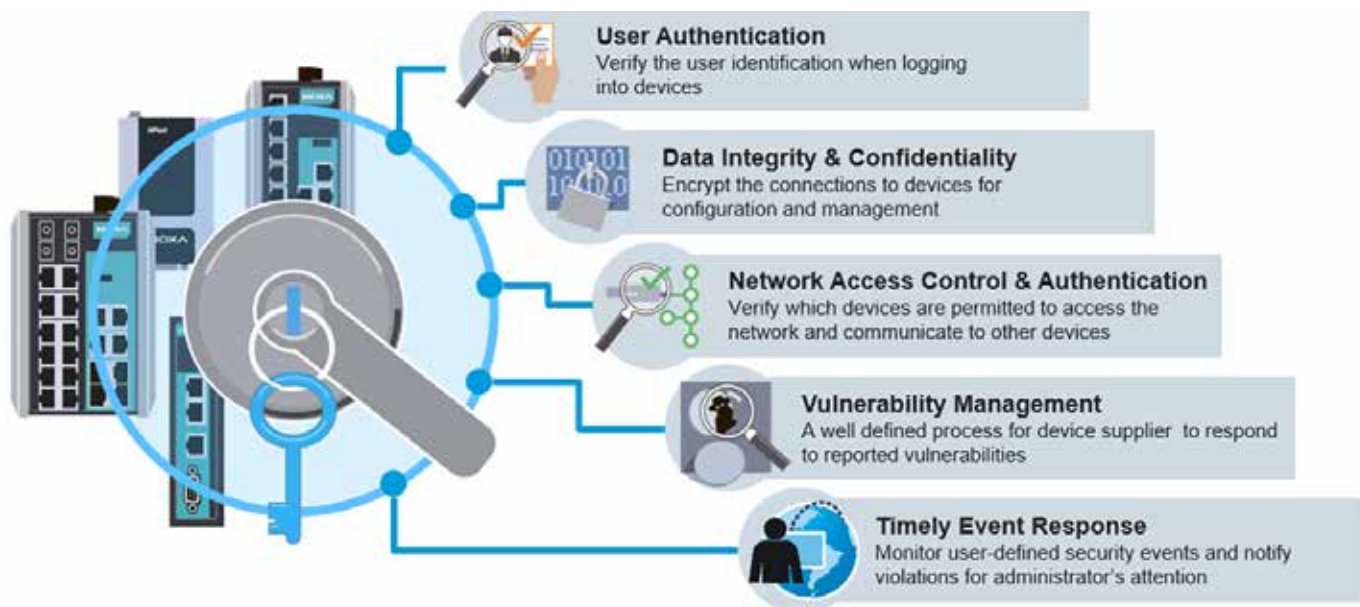
the area of OT, though, availability is the top priority. After all, if there are interruptions in a production line, this can result in vast financial costs. In an operating theatre, it can even be a matter of lives. This means that in the area of OT, not only the threat must be evaluated, but also the effects of security measures.

In an OT network, Principle C (confidentiality) requires the data flow between sensors, controllers and other devices in an OT network to be encrypted, e.g. by using TLS/SSL, so that no unauthorised party can access sensitive information. This might also include the encryption of firewall configurations that contain confidential details about the network's security design. I for integrity demands that only subscribed or purchased operating systems and software are run on the hardware – also known as secure boot. Moreover, A for availability refers to a network concept that guarantees redundancy to rule out a single point of failure (SPOF).

Controlling access to information ensures confidentiality and integrity. Here, it is important to distinguish between authorisation and authentication. Authentication is the process of checking whether a person or computer is actually who they say they are. This ensures everyone knows with whom they are sharing information. Authorisation, on the other hand, regulates the access rights or privileges of a person or software. Both – clearly defined authorisation guidelines and the systematic authentication of users – are crucial for preventing intrusions.

Types of threat – meaning well does not always equal doing well

The basis of a cybersecurity strategy also includes defining possible dangers. Obvious examples are powerful hacker organisations, international espionage and warfare. Still, this doesn't mean that anyone who isn't connected to the internet or company



Following the fundamentals of cybersecurity management creates the discipline required within an organization.

network is safe: around a fifth of threats arise from internal hazards. All it takes, for example, is a disgruntled, dismissed employee whose password hasn't been changed. In Maroochy, an administrative area of Australia, for example, a worker hooked up the network of a water treatment plant to a Wi-Fi router before switching jobs. Years later, when he was rejected for a position at the town hall, he flooded the park with 1,000 litres of wastewater.

Yet, even with good intentions, employees can cause harm. In terms of security, it makes no difference whether the intention is malicious or not – it is the result that counts. With the dramatic rise in sophisticated social-engineering and deepfake-phishing attempts, the risk of an employee trying to help their manager in a supposedly threatening situation that is actually fake and malicious is growing. In 2019, a major American bank made headlines when it accidentally exposed over 800 million private data records, including driving licence details and bank statements.

Another myth that needs to be invalidated is the idea that it takes powerful supercomputers and the latest technology to cause significant damage. The reality is much simpler: crime is already offered “as a service”. According to Forbes, paralyzing an internet-based asset for an hour on the darknet only costs USD 165, while you can obtain a valid credit card number linked to an account with at least USD 10,000 for as little as USD 25.

Cat-and-mouse game

The rapid development of criminal cyberattacks with ever more complex and precise forms of intrusion poses a challenge

for protective measures to keep pace. While brute-force attacks are still common, ransomware continues to grow and social engineering is becoming more sophisticated. Advanced persistent threats (APTs) are used to secretly collect private data over a longer period of time.

Once an attacker has found an easy victim, it is quite possible that they will look for further vulnerabilities. It is a well-known fact that it takes some time to make a weak infrastructure secure. However, even rudimentary cybersecurity measures can significantly reduce the potential extent of damage and the consequences of a successful attack.

Dealing with vulnerabilities

In this context, it's important to know how weak points are currently handled. During the development of a network component, they can be recognised at an early stage with static tests or peer reviews. Automated tests are used to check the system's resistance to common attacks. Intrusion tests are also common practice, in which a third party attempts to systematically and exploratively circumvent the defence measures. Should a vulnerability be discovered in a new product, the manufacturer can fix it immediately. If the product is already on the market, the person carrying out the test usually notifies the manufacturer and gives them time to create a patch before publicising the problem via groups such as MITRE. Although such responsible disclosure is not required by law, it is standard practice in the security industry.

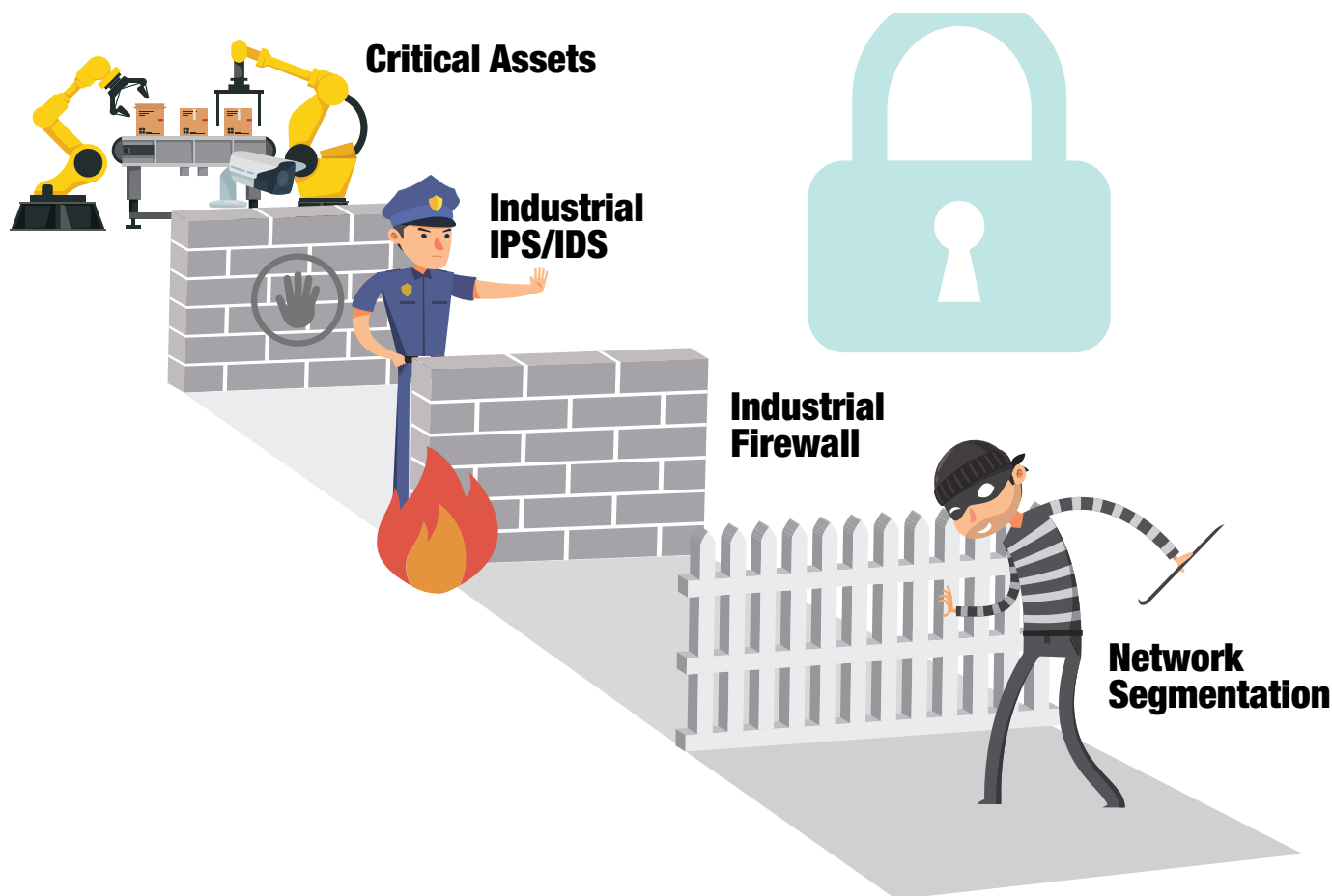
Not only are vulnerabilities publicly available, there are even free search engines that can be used to look for network

equipment based on vulnerabilities. This means that weak points in devices and software are known to the public. It is crucial to identify which ones need a firmware update and to execute it in a timely manner.

Protection mechanisms

One common shield against online threats is encryption. It prevents information from being intercepted during the communication between two nodes. For example, a Wi-Fi connection can be tapped, but if it uses WPA encryption, the transmitted content cannot be deciphered. Communication via open networks, e.g. in hotels or airports, must be encrypted to maintain confidentiality. However, even if the communication is private, e.g. between employees working from home, all intermediate networks that make up the internet must be considered a threat.

Another encryption application is signatures. In contrast to symmetric encryption, which uses the same key for encryption and decryption, asymmetric methods use different keys. This means that a communication can be encrypted with a secret key and anyone who decrypts it with the publicly available key can read its content. In addition, the recipient knows that the document originates from the owner of the secret key as the document bears a signature. This way, digital certificate authorities (CAs) can provide entities with certificates certifying the authenticity of this entity. This is the case, for example, with websites that use HTTPS. If their certificate is invalid, it cannot be decrypted with the CA's public key. In this situation, the browser cannot verify the identity of the website and doesn't display it. The reason is that the website could be an imitation of the original



Fundamentals of Defense in Depth strategies.

or a malicious intermediary between the user and the original website.

Security at network topology level

There are further measures that make network topologies resistant to cyberattacks. In the OT sector, air gapping is frequently found. The internal network and the globally networked outside world are separated. Nevertheless, air gapping is no longer considered sufficient because many potentially dangerous actors are located internally. If no physical access control is used in conjunction with air gapping – i.e. control over who can enter the building – anyone can join the network via a USB stick or the Wi-Fi. And do the network engineers have a list of all the computers that have activated Bluetooth? Most of them do not. This means the network is open and connected.

The expression “castle with moat” uses a medieval metaphor to describe a network with extremely robust perimeter security. It is based on the assumption that the outside world is hostile, while the inside is secure. Unfortunately, this model is no longer up to date. Since the COVID pandemic at the latest, many people have been using VPNs to work from home. This blurs the “secure perimeter”: Does it include the home network? Is that

secure?

A more advanced design is “defence in depth” with a multi-layer principle: each layer is slightly more secure than the last, with the most important operations and data that must not be compromised under any circumstances in the middle. The “defence in depth” method is the foundation for the Purdue model, which is also recommended in EU cybersecurity guidelines.

One modern architecture is SASE (Secure Access Service Edge). Here, all security functions, including authentication and authorisation, are not located in a central system, but at the edge of the network.

Part Two: specific steps for more security in industrial automation

Cybersecurity often seems like the invincible Hydra, constantly growing new heads as soon as one has been cut off. However, with practical guidelines, you can defeat it and significantly strengthen the security of the company network.

Threat modeling

The first step towards a stable cybersecurity framework is gaining a detailed overview of the existing network and identifying the potential vulnerabilities. To do this,

it is advisable to catalogue critical assets, including all machines, systems, and areas in which intellectual property and/or confidential information is saved.

This is followed by a thorough assessment of the direct and indirect consequences of potential threats, allowing you to define a response strategy that reduces immediate risks and prevents long-term consequences. To this end, the risks associated with each identified threat are categorized. Possible responses are considered for each threat:

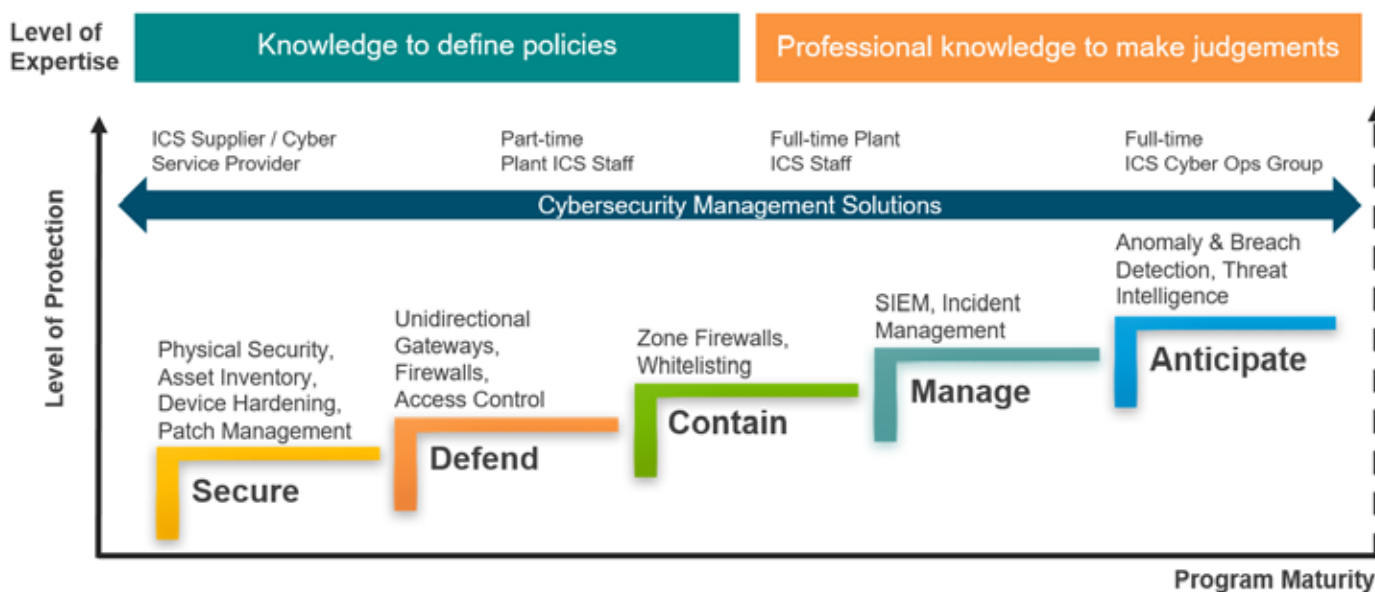
Acceptance: some risks may be considered acceptable; thresholds are then used to determine the point up to which the risk is tolerable and monitoring is sufficient.

Damage containment: a strategy to reduce the likelihood or impact of potential threats may include implementing security measures, protocols, and redundancies.

Elimination: structural changes to the network, the integration of advanced security technologies and the removal of vulnerable components help eliminate risks from the start.

Directives, laws, and standards

Compliance with EU directives, national laws and industry-specific cybersecurity standards is a must. However, by keeping up to date



ARC Cybersecurity Maturity Model.

with regulations and guidelines, companies not only fulfil their legal obligations, but also increase their own security.

On this basis, it is also important to define governance rules. These should include the policies, procedures and protocols that govern day-to-day operations of industrial automation. Effective cybersecurity governance includes solid risk assessment, ongoing identification of cybersecurity risks and up-to-date guidelines based on industry standards. Integral components include access controls, defined responses to incidents, and the sensitization and training of employees.

Once the governance rules are in place, it is important to monitor them continuously and carry out regular security checks and assessments. This is the only way to identify and resolve new vulnerabilities.

Setting up a resilient network

The fundamental step to a secure industrial automation network is to carefully assess the security requirements for each segment. Segmentation involves dividing the network into separate segments or zones to control traffic, improve security and mitigate potential attacks. Each segment can have its own security policies and access controls to increase security and minimize the risk of threats. This allows for a targeted security strategy focusing on specific parts of the network while improving overall system security.

When assessing each segment, consider the organization's critical assets and confidential information, identify potential vulnerabilities, and assess the potential impact of security breaches on each segment. That way, each segment can be assigned a security level based on the probability and possible impact of a successful attack.

Resources can thus be allocated effectively and protection prioritized where it is most urgently needed. On this basis, a plan for a secure network model can be created step by step.

To start with, it is advisable to begin with simple hygiene measures. These include regular software updates, password management, and basic access controls, e.g. restricting the use of certain resources to individual MAC addresses.

The next step will show solutions that are more sophisticated. According to the defense-in-depth principle, several layers of security measures can be combined to create a multi-layered defense strategy. A mix of firewalls, intrusion detection systems, and encryption is recommended.

By separating the floor plan from the corporate network with a DMZ (demilitarized zone), a buffer network, direct communication between the corporate and floor network is prevented and access is controlled with firewalls.

In addition, the isolation of critical segments is an important aspect for minimizing the movement and therefore the spread of threats within the network. To this end, the number of access points and the number of neighboring networks that can communicate with the most secure segments are kept to a minimum. This maintains the integrity of the entire network, even if one area is compromised.

Furthermore, authorization mechanisms should be adapted to the functional roles to ensure that people only have access to resources that are necessary for their tasks. It is advisable to separate administrative roles from other functions and thus strictly limit access to critical configurations and sensitive information.

Software upgrades

It makes sense to approach the topic of software upgrades with a meticulous inventory of the firmware versions of all important devices. This demands caution, professionals should check the authenticity of upgrades with the respective provider. Otherwise, the door is open for counterfeit malware.

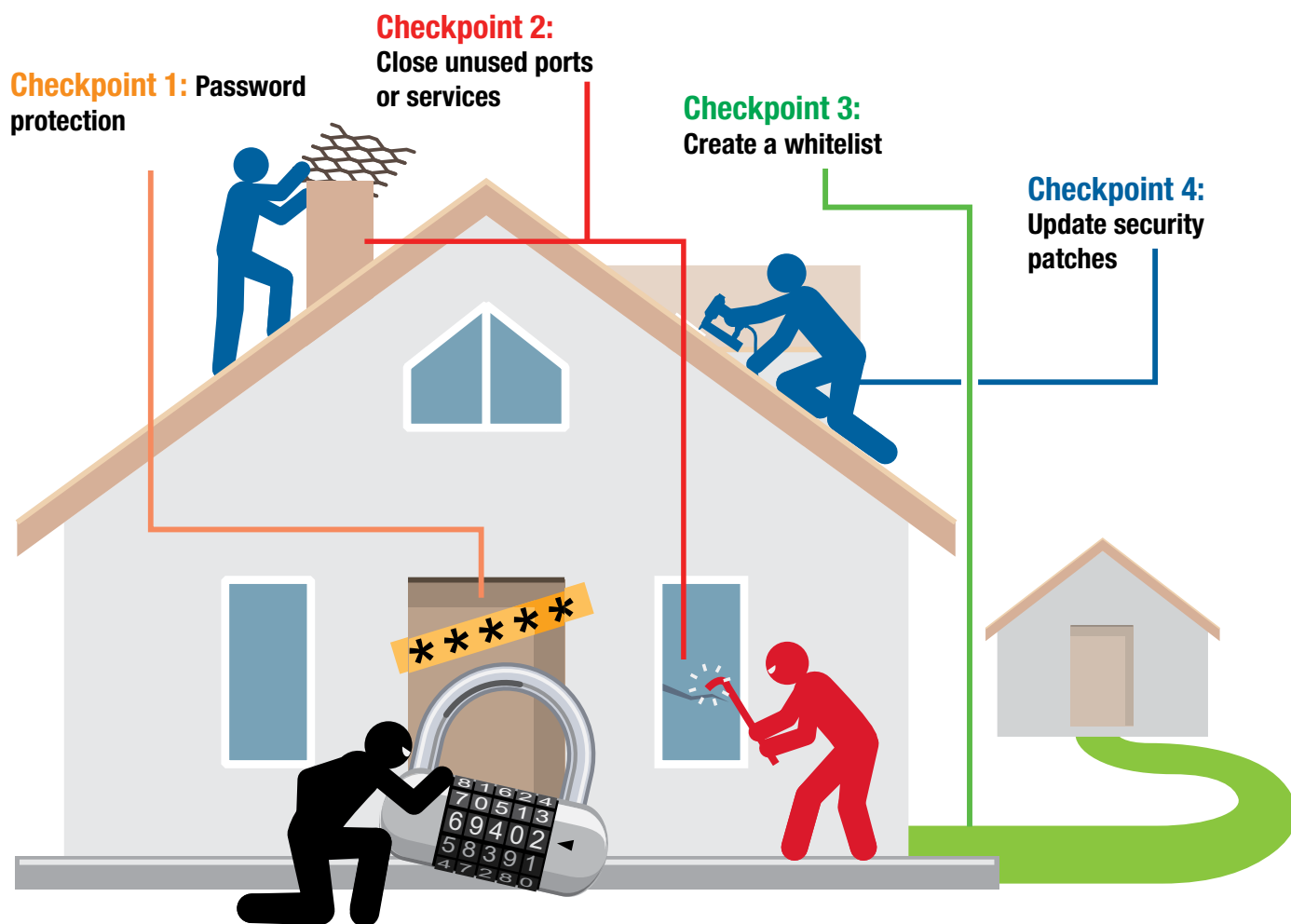
The upgrade process should be carried out in stages so that the effects of upgrades can be monitored and evaluated on a smaller scale before they are applied to the entire network.

In many cases, an immediate firmware update is not possible. The recommended alternative is virtual patching. This involves implementing security measures at network or application level so that no changes to the firmware are required. Hence, network traffic can be actively monitored, malicious patterns identified, and vulnerabilities prevented from being exploited by outdated firmware.

Foster security awareness

In addition to technical measures, the human factor is crucial. Teams must be equipped with the necessary resources to master the intricacies of different types of attack. This starts with creating checklists and step by step procedures that act as practical guides for each type of attack. These materials should be simple and practical, and complex security measures should be broken down into practicable steps. This will enable cybersecurity specialists to empower other teams to respond effectively to threats.

In order to embed cybersecurity awareness in the minds of employees, regular training programs are needed that cover theoretical aspects as well as practical exercises on real-life scenarios.



Device security checkpoints.

The corporate culture is also an important pillar for security awareness, emphasizing an environment where team members can report security concerns without fear of reprisals, which is crucial. Placing blame for security incidents is counterproductive. Instead, the focus should be on understanding the causes and taking corrective action. Praise is also an effective way of encouraging positive behavior. Recognizing vigilance and responsiveness encourages employees to actively contribute to the safety of the company.

Security in the ecosystem

A solid security strategy also takes all of the company's partners into account. This starts with defining clear rules. Authentication should be one of the non-negotiable security aspects, as it is proof of the legitimacy of interactions within the industrial ecosystem. Of course, authentication protocols must comply with industry standards and regulations. Apart from that, partner assessments, audits and security practices should be continuously scrutinized by experts.

Based on the principle "Together we are stronger", actively sharing threat intelligence

and best practices is also recommended to ensure that security measures are mutually reinforcing.

Network monitoring

The first step of network monitoring is gaining a comprehensive understanding of the activities within the industrial ecosystem. With the help of modern tools and technologies, network traffic, device interactions and communication patterns can be observed in real time. This allows anomalies, potential vulnerabilities, and unauthorized access to be detected.

Monitoring security breaches requires robust intrusion detection systems, log analysis, and an active search for signs of unauthorized access, malware, or other security breaches. This is where the aforementioned culture of encouraging employees to report security incidents comes into play.

Every security incident should be meticulously documented, even (seemingly) minor incidents. It is helpful to develop a standardized process for recording the details of the incident, the measures taken, and the lessons learned. Such documentation not only ensures compliance with regulations, for example during audits, official inspections, or

internal reviews, but also provides valuable insights for the continuous improvement of cybersecurity.

Continuous improvement

Cybersecurity is a never-ending task. With defined processes for continuous improvement, organizations create the preconditions for a continuous improvement cycle. This should include the regular review and refinement of security protocols, incident response procedures, and monitoring mechanisms. The evaluation should involve team members from different departments and hierarchical levels, and suggestions should be considered without reservation. Training programs, awareness campaigns, and collaboration frameworks should also be part of continuous improvement.

At the same time, the threat landscape is constantly changing. Active participation in threat intelligence networks and industry forums as well as continuous training help prepare people for evolving threats.

Laurent Liou, Product Marketing Manager, Moxa.

[Learn More](#)

IT-OT convergence leverages advanced technology solutions

Advanced technology is driving the latest solutions for IT-OT convergence. In this special report, industry leaders speak out about the impact of artificial intelligence, the move to software-based solutions, virtual controllers and the ongoing push for more efficient, interconnected and agile operations.



SOURCE: ISTOCKPHOTO

“From a technology perspective, IT-OT Convergence remains critically important as industries increasingly seek to harness the full potential of digital transformation. The progress made in this area is significant with advancements in edge computing, cloud platforms, and advanced analytics paving the way for more integrated and intelligent manufacturing environments.” -- Ronny Hendrych, Program Manager, Industrial Operations X, Siemens.

TO TACKLE IT/OT CONVERGENCE CHALLENGES, smart manufacturing companies are leveraging new technologies including use of Artificial Intelligence, software-based solutions and virtual controllers to achieve a blending of IT and OT systems that deliver more efficient, interconnected and agile operations.

In this special report, the Industrial Ethernet Book reached out to industry experts to gain their perspectives on how IT-OT convergence efforts are continuing to focus on enabling seamless data connectivity, interoperability and scalability.

Here is what they had to say about bridging the gap between IT and OT, and driving greater operational efficiency and security in today's complex industrial environments.

Impact of Artificial Intelligence Accelerating the cycles of innovation.

“Driven by faster innovation cycles, higher cost and quality pressures and facing a lack of talent combined with the sustainability challenge, companies need to be able to adapt their product development and manufacturing in a speed that only software is capable today. AI is shaping up to be a strong driver to bring this needed change also to the shopfloor,” Ronny Hendrych, Program Manager, Industrial Operations X at Siemens told IEB recently.

Hendrych said that, for that, the key technology trends in the IT-OT Convergence discussion include the increasing integration

of cloud computing, simulation, Industrial Internet of Things (IIoT), and edge computing into industrial environments. These technologies enable real-time data collection, processing, and analysis directly at the production level (shopfloor), which significantly enhances decision-making and operational efficiency.

Another trend is the evolution of advanced Manufacturing Execution Systems (MES) and Manufacturing Operations Management (MOM) systems that bridge the gap between operational technology (OT) on the shopfloor and information technology (IT) systems, such as Enterprise Resource Planning (ERP). These trends are driving the need for seamless data connectivity, interoperability,

and scalability across diverse industrial setups.

Technology solutions

Potential solutions to IT-OT Convergence include Industrial Edge computing, advanced SCADA (Supervisory Control and Data Acquisition) systems, and IIoT platforms. Especially Industrial Edge computing, for example, enables data to be processed and analyzed closer to the source (on the shopfloor), reducing latency and bandwidth issues, which are crucial for real-time applications. Advanced SCADA systems act as a data integration layer, harmonizing and contextualizing data from various OT sources before transmitting it to higher-level IT systems. IIoT platforms facilitate connectivity and data exchange across different systems and locations, enabling centralized monitoring, predictive maintenance, and optimization of production processes.

The importance of these technologies lies in their ability to break down data silos, improve real-time decision-making, and enhance overall operational efficiency. By implementing these technologies, industries can achieve higher levels of automation, reduce downtime, and meet regulatory requirements more effectively, ultimately leading to increased competitiveness and sustainability. To succeed, this has to become a culture of data-driven decision-making based on IT/OT integration. However, many IT/OT projects fail due to various inefficient IT/OT collaboration solutions. For this, these technologies have to be embedded in a systematic approach going from small use cases enrolling it to the whole organization at the speed of relevancy for those companies.

Technology benefits

"The specific technical benefits of these solutions include enhanced data transparency, improved scalability, and increased flexibility in industrial operations," Hendrych said. "For example, Industrial Edge computing allows for localized data processing, which minimizes latency and ensures that critical operations can continue even if there is a disruption in cloud connectivity. This is particularly important for applications requiring real-time control and monitoring."

SCADA systems with integrated Industrial Edge solutions provide seamless Southbound-Northbound communication, enabling a smooth flow of data between OT and IT systems. This ensures that data from sensors and controllers on the shopfloor is accurately captured, processed, and transmitted to enterprise-level systems for further analysis and decision-making. These technical benefits translate into tangible improvements in enterprise/automation integration, such

as more efficient resource utilization, faster response times to production issues, and the ability to implement predictive maintenance strategies. This level of integration also supports the adoption of AI-driven applications, which can further optimize processes and reduce costs.

"To address the challenges of IT-OT integration, it's essential to understand how these technologies work together," Hendrych added. "For instance, an Industrial Edge solution typically involves the deployment of edge devices, such as industrial PCs or dedicated edge gateways, on the shopfloor. These devices collect data from sensors, PLCs (Programmable Logic Controllers), and other OT components. The data is then processed locally on the edge device, where it can be aggregated, filtered, and analyzed before being sent to IT systems or cloud platforms."

A SCADA system or an HMI (Human-Machine Interface) system often acts as the intermediary, managing the flow of data between OT and IT systems. It provides a unified interface for operators to monitor and control industrial processes while ensuring that the data is formatted correctly and securely transmitted to higher-level systems. Data integration layers like the Siemens Industrial Edge Information Hub (IIH) further enhance this process by providing additional tools for data processing, visualization, and integration with cloud or IT systems. These technologies open new possibilities for addressing IT-OT integration challenges, such as ensuring data consistency, managing the increasing volume of data generated by modern industrial systems, and providing secure and scalable solutions that can grow with the needs of the business.

Looking ahead

Given the challenges of IT-OT Convergence from a technology perspective, Hendrych gave his opinion on the continuing importance and progress made on this issue.

"From a technology perspective, IT-OT Convergence remains critically important as industries increasingly seek to harness the full potential of digital transformation," Hendrych said. "The progress made in this area is significant, with advancements in edge computing, cloud platforms, and advanced analytics paving the way for more integrated and intelligent manufacturing environments."

He added, however, that the challenges are still substantial, particularly in terms of ensuring seamless interoperability between legacy OT systems and modern IT infrastructures, maintaining data security, and managing the complexity of these integrations. Despite these challenges, the ongoing development of flexible, scalable, and secure solutions demonstrates that the

industry is moving in the right direction. The continuous innovation in this space is helping companies to not only meet current operational needs but also to position themselves for future growth and technological evolution. The importance of IT-OT Convergence will only increase as industries strive for greater efficiency, sustainability, and competitiveness. The progress made so far is encouraging, but ongoing efforts and collaborations between technology providers and industrial companies will be essential to fully realize the potential of this convergence.

"One aspect we need more focus on is the change on how collaboration between IT and OT personal can be improved and how IT working modes (e.g. DevOps and stronger use of simulation & test technologies) can be applied to fully benefit from those data driven paradigms in production," Hendrych concluded.

Focus on scalability and flexibility

IT and OT stakeholders share data and insights more effectively.

According to Jessica Forguites, Technical Platform Lead at Rockwell Automation: "In the age of AI there are many technology trends shaping collaboration or convergence of IT and OT groups and the technologies they use. Common discussions with our customers include investment in software targeted toward specific outcomes, investment in infrastructure and networks to account for new requirements, and data streams associated with their company's goals."

Forguites said that potential solutions to IT/OT convergence include integrated network infrastructure, edge computing solutions, and software and services that support a unified framework in critical areas like security and data management. These solutions enhance scalability and flexibility, help ensure consistent regulatory compliance, improve collaboration among stakeholders, and accelerate data-driven decision-making.

"The technical benefits include enhanced reliability and uptime, improved data integrity and consistency, and optimized asset utilization, such as network resources, servers, and storage capacity," Forguites said.

The technology operates by offering flexible segmentation options to manage data flows during system integration, ensuring scalable and manageable asset and data identification over time. It also enables IT and OT stakeholders to share data and insights effectively, avoiding multiple sources of truth, and supports operational continuity throughout ongoing system integrations.



SOURCE: ISTOCKPHOTO

"Potential solutions to IT/OT convergence include integrated network infrastructure, edge computing solutions, and software and services that support a unified framework in critical areas like security and data management." -- Jessica Forguites, Technical Platform Lead, Rockwell Automation.

"Businesses are increasingly reliant on data driven insight to achieve the outcomes they are looking for. This makes IT and OT convergence a necessity for organizations to remain competitive and secure, while managing long term total cost of ownership of their assets. The rapid progress of IT/OT convergence has laid a foundation for more efficient operations, improved resiliency, in addition to other digital transformation goals," Forguites said.

Blending of IT and OT systems

More efficient, interconnected and agile operations.

According to Krishna Diwakar, Technical Marketing Engineer at Cisco, "Traditionally, IT and OT teams have operated in silos, but recognition of integrating these two domains are bringing them to work closer together and help the organization succeed. IT-OT convergence involves blending of IT systems which handle data management and business analytics with OT systems which manage and control physical processes and machineries in verticals such as manufacturing, utilities, transportation, etc."

Diwakar stated that IT-OT convergence fosters more efficient, interconnected

and agile operations driven by a series of technology trends:

Industrial IoT developments: vast availability of smart sensors and connected industrial assets to collect real-time data for better monitoring and controlling the physical processes

The need for large scale industrial networking: higher speed connectivity with low latency to support ever more advanced process automation powered by seamless and secure communication between the IT and OT systems to unlock the promises of industry 4.0

The rise of AI & ML enabled software applications that need operational data to predict anomalies, optimize operations, and enhance decision making.

Unified cybersecurity across IT and OT to protect both operations and enterprise networks and ensure that any security breaches remain contained and not spread from one domain to the other

Increasing use for hosted applications in datacenters, private, and public clouds for scaling resources for data storage, analysis, as well facilitating automation across IT and OT systems.

Solutions to IT-OT convergence

"In the coming years manufacturers will continue to invest in smart network

initiatives that provide higher performance, edge compute, easy installation, security, and troubleshooting capabilities," Diwakar said. "The expectation from their networks will be such that it contributes to more cohesive, responsive and secure operational environment alongside increase productivity and helping them stay competitive in the marketplace."

Therefore, the technologies that can help in IT-OT convergence are: (1) Standardized networking hardware and software across IT and OT, (2) A common network management platform, (3) Embedded security in network equipment, and (4) unified IT/OT security platform to detect faster and better orchestrate response.

Standard networking equipment across IT and OT can eliminate patchwork of networks that offer different capabilities and require multiple tools to manage and secure. A single management system for the standardized environment can automate networking tasks across the entire network increasing consistency and reducing OpEx. Embedded security in network equipment rather than point products, and common security operations streamline architectures and provide a more holistic view of threats across the organization for better correlation, detection, and response.



"The convergence of IT and OT offers numerous benefits, including increased efficiency, improved security, enhanced reliability, and the ability to leverage digital technologies for innovation. As industries continue to evolve and become more technologically advanced, the trend towards IT and OT convergence is likely to accelerate." -- Krishna Diwakar, Technical Marketing Engineer, Cisco.

Diwakar said that solutions like the above help organizations bridge the gap between IT and OT, driving greater operational efficiency, security, and adaptability in today's complex industrial environments.

Enterprise/automation integration

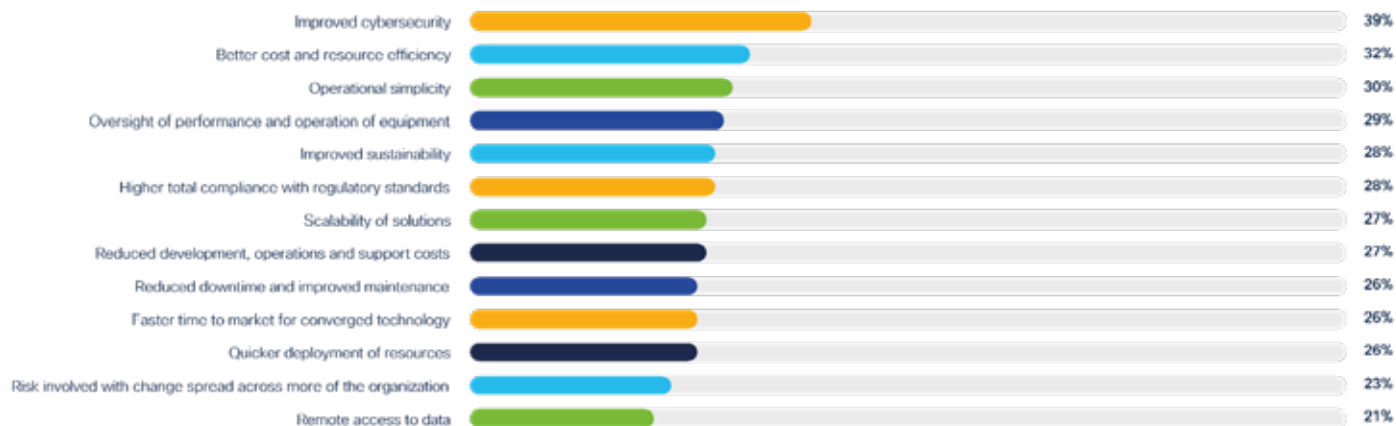
"When IT/OT collaborate, each team focus on their unique skill sets to define together the right strategies and the technologies supporting them. OT knows industrial

automation. IT knows networking and security. This collaboration reduces the need for separate support teams and tools and in most cases prevents re-inventing the wheel," Diwakar said. "OT teams can leverage the automation expertise from IT and avoid manual repetition of tasks with a huge reduction in errors enabling quicker time to market and adopt technological advancements with ease."

For example, Cisco networking products

for enterprise and operations, while purpose-built for their respective environments and use cases, share components from the same ASIC family and run the same operating system (IOS XE). Cisco industrial switches, routers, and wireless equipment are all managed by the same Catalyst Center that uses machine learning for predictive insights and automated troubleshooting, minimizing downtime not just for the enterprise but also for the OT networks in single management pane.

Q. What do you think are the main benefits of IT and OT collaboration? Select all that apply



Benefits of IT and OT collaboration led off by improved cybersecurity.



SOURCE: ISTOCKPHOTO

“Driven by the ever-increasing performance of computing hardware, IT and OT are moving from specialized hardware to software implemented products. This is true, for example, in IT with virtualization and containerization or software defined networks. In OT, products like PLCs are moving from specialized runtimes to support standard programming languages.” -- Dr. Lutz Jänicke, Corporate Product & Solution Security Officer, Phoenix Contact.

Diwakar said that a recent survey conducted by Cisco and detailed in 2024 State of Industrial Networking Report, shows the benefits that respondents recognize that closer alignment of IT and OT would yield as shown in the chart below.

He added that Cisco industrial switches and routers are the only industrial networking equipment on the market to offer OT visibility capabilities. The embedded Cyber Vision sensor inventories and profiles industrial assets and enables real-time monitoring of application flows, without the need for dedicated security appliances or SPAN networks. This comprehensive visibility into industrial networks provides the basis of automated network segmentation in OT as required by ISA/IEC 62443 standards and enables adopting a common zero-trust framework across IT and OT networks to control which device can access what.

Reporting events to a single SOC platform, such as Splunk, provides a comprehensive view of potential threats across IT and OT environments which allows detecting advanced threats faster and better coordinated response and mitigation efforts.

Addressing challenges

Diwakar said that commonality between the network devices used in both IT and OT, for instance the Cisco Industrial Ethernet switches, offer the ruggedization and compliance standards for industrial use, but run the same IOS XE software as Cisco Catalyst enterprise switches making it easier to use the common set of protocols like NETCONF, RESTCONF and programmable APIs to automate and gain insights into the OT network. This common functionality makes it easier for the organization since they could leverage the skills IT already possesses, and no time is needed for learning new skills or ramping-up.

Moving from unmanaged to managed switches in the OT deployments helps focus on features like VLANs to segment the network and QoS ensuring the traffic flow gets the best treatment they would require and conserving bandwidth. Effective bandwidth utilization facilitates the efficient network resource usage, reduce latency and achieve operational efficiency in Industrial settings.

Informed by the visibility that Cyber

Vision provides Identity Services Engine (ISE), a network access control and policy enforcement engine, predominantly used in IT can now be used to automate and push security policies to the devices in the OT network in a consistent manner. It also simplifies the tools needed to secure and optimize OT operations.

Continuing importance and progress

“The convergence of IT and OT offers a powerful combination of benefits, including improved operations, better data analytics, and enhanced security. Cisco as the networking and security market leader is building OT products that are both enterprise-grade and industrial-strength. Using Cisco networking products, OT and IT teams can forge a better partnership as Cisco meets the needs of both,” Diwakar said.

He added that a unified view of both IT and OT cybersecurity threats is undoubtedly a huge win from a technology perspective. It offers unified threat management that allows for coordinated response and mitigation efforts, a shared perspective that allows building of consistent security policies, and

reduced risk of blind spots by monitoring of both IT and OT environments.

“Looking beyond technology, a single vendor solution for IT and OT may also reduce overall licensing and support costs resulting in lower OpEx, provide a more predictable and manageable environment compared to multiple vendors, and help organizations create a networking and security blueprint that they can replicate across their operations,” Diwakar said.

“The convergence of IT and OT offers numerous benefits, including increased efficiency, improved security, enhanced reliability, and the ability to leverage digital technologies for innovation. As industries continue to evolve and become more technologically advanced, the trend towards IT and OT convergence is likely to accelerate.”

Moving to software solutions

OT becoming more closely connected to enterprise systems.

Dr. Lutz Jänicke, Corporate Product & Solution Security Officer, Phoenix Contact said that “generally driven by the ever-increasing performance of computing hardware, IT and OT are moving from specialized hardware to software implemented products. This is true, for example, in IT with virtualization and containerization or software defined networks. In OT, products like PLCs are moving from specialized runtimes to support standard programming languages. This also includes the usage of (IT) standard communication protocols instead of or in addition to specific OT protocols.

Jänicke said that OT devices and services are more closely connected to enterprise systems to support the management and monitoring of the systems and of course the production.

“An obvious technology trend is the implementation of artificial intelligence (machine learning). Impressive results can be seen in drafting and translating texts or in videos. As there is a strong dependency on material to learn from, application in the OT area might be challenging. Still, the processing of such data would be an IT-topic,” he added.

IT-OT convergence

Jänicke said that both IT and OT are moving towards IT technologies. Communication is based on IP and web services, for example, using REST interfaces. This allows for a seamless integration. Standardization is most important and is underlined by the role of OPC UA. Additional synergies might be found in the use of digital twin technologies improving the exchange of data.

Processing of data using cloud services and/or container technologies makes deployments more effective. Of course, this integration comes with additional security challenges due to increased connectivity.

“IT environments are becoming more and more service oriented,” Jänicke said. “By packaging operations into microservices functions become very modular and can be developed, deployed, and updated in small increments. Concepts like DevOps would not be thinkable without these environments. In addition, by using standard libraries and offerings available in many languages like Java, C#, ... a new function can be built without digging into lower-level details.”

Jänicke said that the same is not fully applicable to lower-level automation systems. They still need to be developed to support real-time operations and the deployment needs to be stable. Using above mentioned technologies however allows to implement “glue logic” that is easier to interface to the enterprise systems. Virtual PLCs that will be a very visible move in the convergence have been discussed for quite some time and seem to become available now.

“The convergence is ongoing and will not stop,” Jänicke concluded. “It offers advantages in effectiveness and efficiency of OT operations.”

Impact of virtual controllers

Automation and control software that is fully independent of the hardware.

According to Steven Fales, Director of Marketing at ODVA, “virtual controllers are an emerging technology in Industrial Automation that are set to enable greater IT-OT convergence going forward.”

Fales said that what differentiates a virtual controller from a traditional controller is that the automation and control software is fully independent of the hardware. This is made possible by using standalone, executable packages of software that include the code, runtime, system tools, system libraries, and settings to run the desired applications.

This is like the way that cloud servers run software independently so that different servers can be used to scale up the possible number of connections or to switch over to a different server in case there is trouble with the existing hardware. Industrial personal computers (IPC) were the initial basis for decoupling the software from the hardware in industrial controllers since standard personal computers were used to run industrial software for control applications. This led to the development of soft controllers that were originally based on IPC hardware and are capable of both traditional control as well as gateway, human-machine interface (HMI), web server connectivity, and more.

Soft controllers then evolved into Programmable Automation Controllers (PACs) that combine the advantages of controllers and PCs. Virtual controllers are essentially PACs that run within a virtual machine managed by a real-time hypervisor or virtual machine monitor on a commercial-off-the-shelf (COTS) server. Virtual controllers, PACs, soft controllers, IPCs, and traditional PLCs can all run industrial Ethernet communication networks including EtherNet/IP.

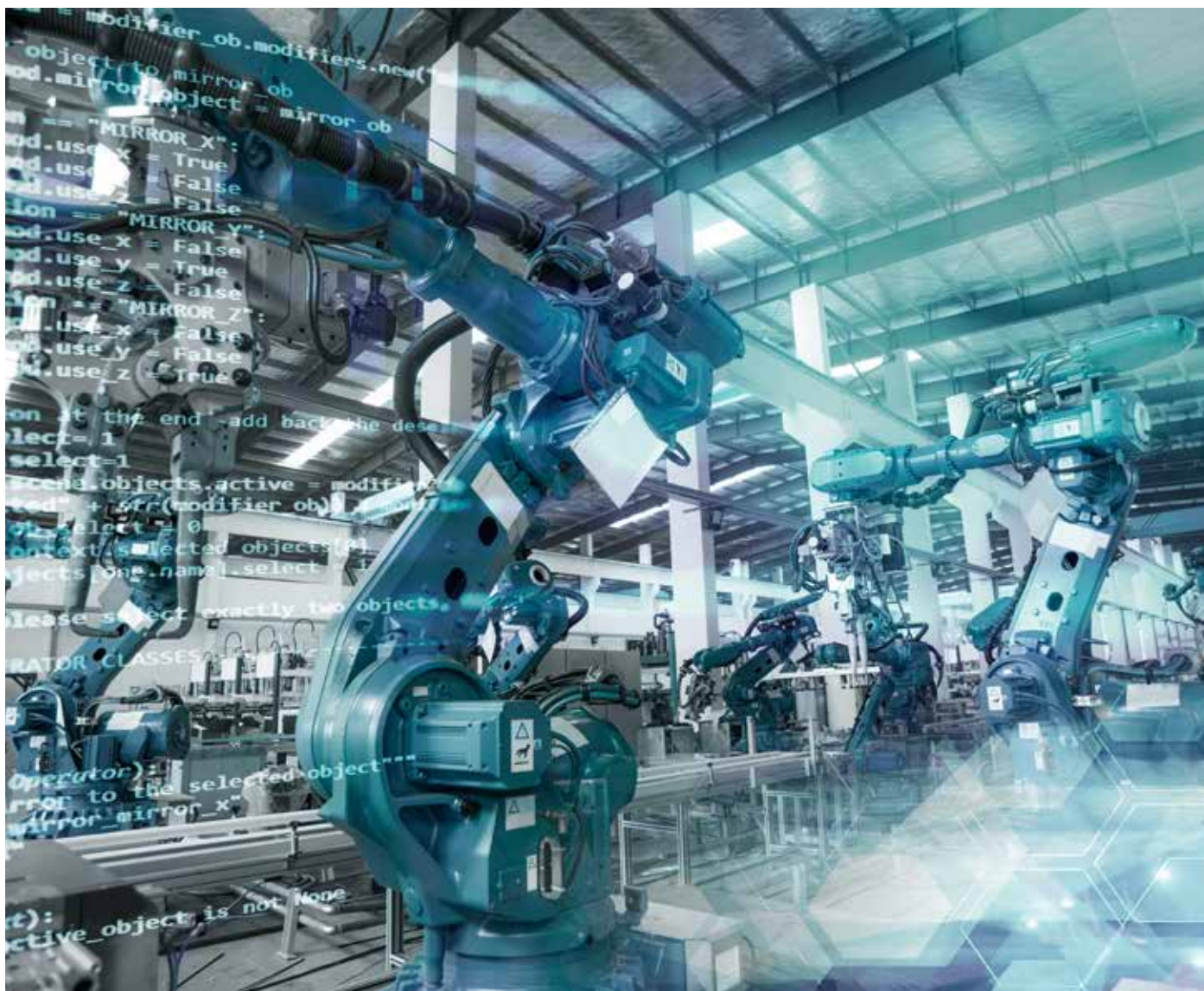
Advantages of virtual controllers

The advantages of virtual controllers stem from the fact that they are not tied to the underlying hardware that the control software runs on and that they rely on internet connectivity. This enables virtual machines to keep operating in the case of a hardware failure by switching over to a different server. Additionally, applying software patches for security or stability upgrades has traditionally been very difficult to accomplish with traditional controllers that are spread throughout plants and not typically connected directly to the internet.

In contrast, virtual controllers can be updated much faster in comparison when a security vulnerability or operational improvement is identified. Further, the updates can be verified in a test environment before pushing the patch to production in the same way that traditional IT software updates are made. Another significant benefit of virtual controllers is that remote management will allow for a larger amount of data to be available for operations analysis and improvement as well as maintenance management.

Specific technical benefits

“Virtual controllers will allow for a much greater level of IT-OT convergence than previously possible by bringing the full advantages of containerized software to industrial control. The ability to manage thousands of virtual controllers in the same way that traditional PCs are by IT will provide much faster software bug fixes and a more complete picture of an organization’s operations,” Fales said. “Traditional PLCs are limited to running embedded firmware on specialized hardware that can make changes or data gathering more challenging. The use of virtual controllers could also open the development and maintenance of the programming language code to a much wider group of professionals from the IT world using more commonly used coding languages. While the development of specific control loop algorithms would be best left with experienced OT engineers there are other less critical tasks that can be done by software developers with a smaller amount of domain expertise. Additionally, the implementation



"The advantages of virtual controllers stem from the fact that they are not tied to the underlying hardware that the control software runs on and that they rely on internet connectivity. This enables virtual machines to keep operating in the case of a hardware failure by switching over to a different server."
 -- Steven Fales, Director of Marketing, ODVA.

of artificial intelligence would also be easier with virtual controllers given the ability to more easily update the software as changes are made."

He added that the downside of virtual controllers is that there are serious concerns regarding security, safety, and real time capability. While the historical security by obscurity of traditional controllers has long since been rejected, there are definite reliability advantages to having a physically onsite controller that adheres to IEC/ISA 62433 security standards and has limited connectivity to the internet.

Additionally, the reliance on internet connections could lead to challenges keeping an operation running properly either because the machine would be constantly returning to a safe state or would simply shut down in the middle of a process in the case of an intermittent internet connection. Traditional

PLCs that leverage embedded firmware and are located on machine offer a level of reliability that is critical to operations uptime.

Automation applications that can tolerate periods of unavailability are the initial target for virtual controllers. It remains to be seen whether traditional controllers will stay in their current form or if the advantages of virtual PLCs will start a shift toward decoupling hardware from software and adding more reliance on internet connectivity to all controllers.


Progress being made

Fales said that automation has made significant strides moving from pneumatic controls in the 1950s to PLCs in the 1970s and then from fieldbus to Industrial Ethernet and PLCs to PACs in the 2000s. Industrial Ethernet communication networks such as EtherNet/IP will remain relevant going forward due to their adherence to IEEE

specifications, usage of TCP/IP, real time capabilities, media independence, and safety and security services.

"However, they will likely be running in new virtual controller and cloud environments in the future to take advantage of the lessons learned in IT of virtual patching and remote management," Fales said. "IT and OT technologies have and will continue to converge toward each other slowly but surely enabling industry to smoothly transition to the full advantages of cloud computing, artificial intelligence, and the new technologies of tomorrow. As has been constant in industrial automation for decades though, the new will need to coexist with the old to keep the industries humming along that provide for our basic needs including water, food, and transportation."

Al Presher, Editor, *Industrial Ethernet Book*.

The background of the cover is a photograph of a modern industrial facility, likely a data center or a high-tech manufacturing plant. It features complex piping, structural beams, and various digital displays. In the top left, a large blue circular gauge shows '85%'. In the top right, several smaller digital screens show green progress bars and numbers like '1.188' and '1249'. On the right side, a larger screen displays a green interface with the word 'Nutrients' and two circular gauges showing '83%' and '73%'. The overall lighting is a mix of cool blues and warm oranges, creating a high-tech, futuristic atmosphere.

Industrial Ethernet Solutions

2024 Corporate Profiles

Learn about the companies
and technologies shaping the
future of Industrial Ethernet,
the IIoT and Industry 4.0.

The logo consists of a green square at the top, connected by a horizontal line to two smaller green squares below it, forming a stylized 'E' or a network structure.

industrial ethernet book
Industrial Networking & IIoT

Beckhoff Automation: New Automation Technology

Beckhoff implements open automation systems using proven PC-based control technology. The main areas that the product range covers are industrial PCs, I/O and fieldbus components, drive technology, automation software, control cabinet-free automation, and hardware for machine vision.



SOURCE: BECKHOFF

PRODUCT RANGES THAT CAN BE USED AS separate components or integrated into a complete and mutually compatible control system are available for all sectors from Beckhoff Automation. New Automation Technology stands for universal and industry-independent control and automation solutions that are used worldwide in a large variety of different applications, ranging from CNC-controlled machine tools to intelligent building control.

PC-based control technology

Since Beckhoff's foundation in 1980, the development of innovative products and solutions on the basis of PC-based control technology has been the foundation of the company's continued success. We recognized many standards in automation technology that are taken for granted today at an early stage and successfully introduced to the market as innovations. Beckhoff's philosophy of PC-based control as well as the invention of the Lightbus system and TwinCAT automation software are milestones in automation technology and have proven themselves as powerful alternatives to traditional control technology. EtherCAT, the real-time Ethernet solution, provides a powerful and future-oriented technology for a new generation of control concepts.

Worldwide presence on all continents

The corporate headquarters of Beckhoff Automation GmbH & Co. KG in Verl, Germany, is the site of the central departments such as development, production, administration, sales, marketing, support and service. Beckhoff's presence in the international market is guaranteed by its subsidiaries. Beckhoff is represented in more than 75 countries by worldwide cooperation partners.

EtherCAT – the Ethernet Fieldbus

Selecting the communication technology is important: it determines whether the control performance will reach the field and which devices can be used. EtherCAT, the Industrial Ethernet technology invented by Beckhoff, makes machines and systems faster, simpler and more cost-effective. EtherCAT is regarded as the "Ethernet fieldbus" because it combines the advantages of Ethernet with the simplicity of classic fieldbus systems and avoids the complexity of IT technologies. The EtherCAT Technology Group (ETG), founded in 2003, makes it accessible to everyone. With over 7,000 member companies from 72 countries (as of March 2023), the ETG is the world's largest fieldbus user organization.

EtherCAT is an international IEC standard that not only stands for openness, but also for stability: until today, the specifications

have never been changed, but only extended compatibly. This means that current devices can be used in existing systems without any problems and without having to consider different versions. The extensions include Safety over EtherCAT for machine and personnel safety in the same network, and EtherCAT P for communication and supply voltage (2 x 24 V) on the same 4-wire cable. And also EtherCAT G/G10, which introduces higher transfer rates, while the existing EtherCAT equipment variety is integrated via the so called branch concept: even here there is no technology break.

Beckhoff Automation at a glance

- 2023 global sales: €1.75 billion (+16%)
- Headquarters: Verl, Germany
- Managing owner: Hans Beckhoff
- Employees worldwide: 5,500 (FTE, March 2024)
- Engineers: 2,000
- Subsidiaries/representative offices worldwide: 40
- Sales offices in Germany: 23
- Representatives worldwide: >75

Beckhoff Automation GmbH & Co. KG

info@beckhoff.com

Phone: +49 5246 963-0

[Visit Website](#)

Analog Devices: accelerating your digital transformation journey

Access new insights from the Intelligent Edge with innovative solutions that solve the toughest industrial automation challenges.



SOURCE: ANALOG DEVICES

ANALOG DEVICES (ADI) IS A GLOBAL LEADER in the design and manufacturing of analog, mixed signal, and DSP integrated circuits. We intelligently bridge the physical and digital worlds with a cutting-edge portfolio of technologies that sense, measure, interpret, connect, power, and secure. ADI is not a typical semiconductor company. We push the boundaries of silicon technology, investing heavily in software, systems expertise, and domain knowledge within our key markets such as industrial automation. The combination of this knowledge with that unmatched set of analog-to-digital capabilities enables ADI to approach challenges at the system-level and help our customers get to market faster, create and capture more value, and make sound investments with a roadmap to tomorrow.

Industry-leading, scalable Ethernet – timed to perfection

We turn your vision of connected factories into reality. ADI's portfolio of compatible and interoperable industrial Ethernet connectivity products enables best-in-class industrial automation solutions for the connected factory of tomorrow.

From complete Time Sensitive Networking solutions for high-performance motion control in factory automation to innovative single pair Ethernet products for robust edge connectivity in process/factory and building automation – our market-leading Ethernet portfolio of combined software and hardware solutions are scalable and timed to perfection.

ADI's Ethernet solutions encompass a range of advanced Industrial Ethernet technologies from real-time Ethernet switches to physical transceivers and network interface solutions that include protocol stacks. Designed to support scalable and flexible system development, the ADI Ethernet product portfolio offers multiple port count, low power consumption, and flexible bandwidth. Being multiprotocol, these solutions are compatible with the majority of existing industrial protocols while also providing the ability to future-proof for TSN networks.

ADI's Ethernet solutions are designed and verified for robust operation in harsh industrial environments and offer effective security at each node point within a system. Our suite of industrial Ethernet products includes technologies, solutions, software,

and security capabilities designed to connect the real world to factory networks and beyond to the cloud.

Why ADI?

Our long history, rich industrial expertise, and system design knowledge combines with advanced technologies to deliver seamless and secure connectivity across the automation network, turning your vision of the connected factory into reality. ADI ensures your time-critical automation and control data is delivered perfectly on time, every time. Get to market fast by using ADI's complete solutions that provide predictable, trusted results you can depend on every time. For deterministic, verified robust, scalable and flexible solutions that simplify system design and reduce the development burden, look no further than Analog Devices.

Analog Devices

Email: EMEAMarketing@analog.com
Phone: +49 89 769030

Visit Website

Opto 22: Your Edge in Automation

Let the engineers at Opto 22 help you build your connected automation system.

READY TO CONNECT AUTOMATION, ENTERPRISE, and cloud data? Opto 22's *groov* family of industrial edge controllers and I/O gives you the integrated control, connectivity, and cybersecurity tools to do it.

With *groov* EPIC and *groov* RIO, you can bring brownfield systems into the next generation of industrial automation.

Create cohesive OT data systems from multi-vendor networks with OPC UA, MQTT, and more.

Secure PLC, I/O, and equipment data with built-in cybersecurity features like encryption, mandatory user authentication, and configurable device firewalls.

And you can collect, process, and publish OT data where it's needed, into on-premises and cloud-based applications like databases, CMMS, SCADA, and ERP.

Control and I/O options at the edge

For *groov* EPIC, develop real-time control programs in a language you know: ladder logic, function block diagram, flowcharts, Python, C/C++, and more. Build HMI screens for embedded or external touchscreens, PCs, and mobile devices. Run Inductive Automation's Ignition Edge on the EPIC programmable industrial controller.

groov RIO edge I/O combines security,



SOURCE: OPTO 22

An edge programmable industrial controller, groov EPIC® is much more than a PLC or a PAC. It can secure and simplify automation and IIoT projects, while reducing cost and complexity.

software-configurable I/O, embedded software, and even CODESYS control programming in a single compact edge device.

Why choose groov?

Built on Opto 22's nearly 50 years of experience, *groov* products are backed by lifetime guarantees on solid-state I/O, UL Hazardous Locations approval, ATEX compliance, and a wide -20 to 70°C operating temperature range.

Count on free pre-sales engineering help and product support as well. All Opto 22 products are developed, manufactured, and supported in the U.S.A.

Contact our engineers today, and let's talk about what you want to do.



RIO MM1
Universal I/O

RIO MM2
Universal I/O
with Ignition
IgnitionEDGE

RIO EMU
Energy
Monitoring



SOURCE: OPTO 22

groov RIO® edge I/O offers over 200,000 software-configurable I/O combinations plus optional real-time control in a single, compact, PoE-powered industrial package.

Opto 22

www.opto22.com

Visit Website

Contemporary Controls: Your Trusted Partner

Providing innovative and reliable solutions to the industrial automation industry for more than 49 years, Contemporary Controls has been a leader in innovative solutions for industrial automation.

WITH MORE THAN 49 YEARS OF experience, Contemporary Controls has been a leader in innovative solutions for industrial automation. Contemporary Controls' CTRLink products are designed for unattended operation in environments not conducive to office-grade equipment.

The products provide convenient DIN-rail mounting in control panels, 24VAC/DC power, UL 508, improved EMC compliance and reliability. Contemporary Controls' repeating hub, switches, media converters and IP routers adhere to IEEE 802.3 standards and more. Specialty regulatory needs are addressed in selected models.

Rugged Ethernet Switches

Whatever the Ethernet infrastructure need, a solution is available from CTRLink products. For simple systems, plug-and-play unmanaged switches provide a cost-effective method for expanding Ethernet networks. Most models include features such as auto-MDIX and auto-negotiation. For demanding applications, managed switches provide features such as VLANs, SNMP, Quality of Service, port security, port mirroring, alarming and cable redundancy.



SOURCE: CONTEMPORARY CONTROLS

to the LAN side while keeping the same IP settings for the devices and the application, lowering installation cost and eliminating trouble shooting.

The IP address for the WAN port on the IP router is the only setting that requires modification allowing multiple machines to reuse the same configuration on the LAN side. Skorpion routers have been successfully used in Robotics, Automated Guided Vehicles (AGVs), Packaging and Scientific Equipment.

Simplified, Secure Remote Communication

Utilizing the EIPR/EIGR series VPN routers, Contemporary Controls offers three VPN solutions that deliver secure, remote access—RemoteVPN subscription service, and Self-HostedVPN and BridgeVPN solutions. Hosted on the Internet and maintained by Contemporary Controls, RemoteVPN provides secure communication and the convenience of remote access without having to maintain a VPN server.

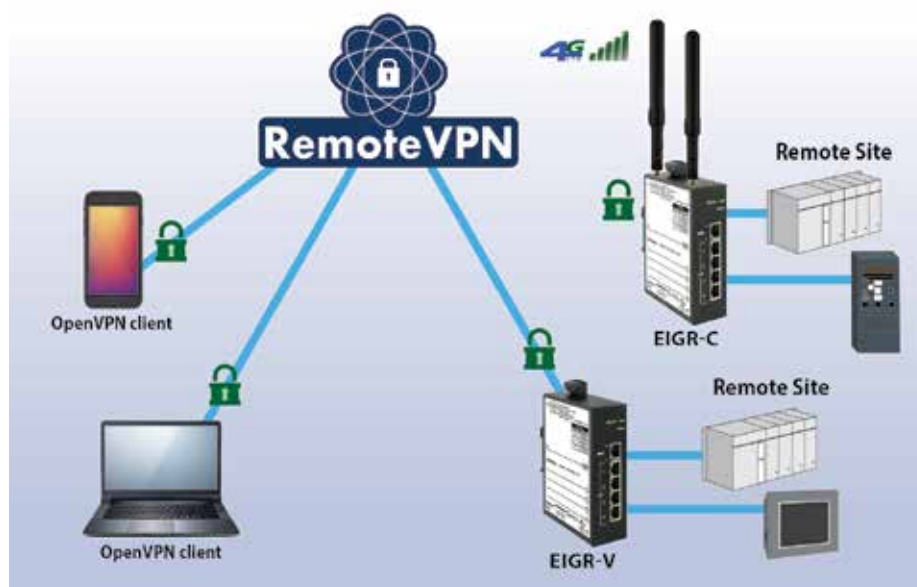
Contemporary Controls' Self-HostedVPN and BridgeVPN solutions allow users to set up and maintain their own secure remote access without subscription fees and without the need for a cloud-based VPN server.

Innovative Diagnostic Switches

For troubleshooting, diagnostic switches allows a network sniffer to attach to an unused port on a switch and observe all traffic on the network.

Cost-Effective, Trusted IP Routers

Contemporary Controls' Skorpion series of IP routers ease the integration of new machines into the existing network. Each machine consisting of multiple IP devices connects



SOURCE: CONTEMPORARY CONTROLS

Solutions You Can Depend On

With automation systems, applications vary and can require a special product or need. Contemporary Controls has worked with OEMs in obtaining UL 864 compliance with some CTRLink switches, and can help in other areas such as private-labeling, unique packaging or extreme environmental design.

Contemporary Controls' customers are systems integrators, contractors and OEMs seeking simple, reliable networking and control products from a dependable source. With headquarters based in the US, Contemporary Controls also has operations in the UK, Germany and China and is well suited to fulfil your application needs.

Contemporary Controls
www.ccontrols.com

Visit Website

Machine and Device Connectivity

Providing data-driven OT Insights.

SOFTING INDUSTRIAL OFFERS ADVANCED AND easy-to-use products and solutions for the digitalization and networking of industrial systems and processes. Our innovative solutions help to increase the efficiency of production and provide users with secure and flexible connectivity between machines and systems. They enable optimized data exchange, efficient OT/IT integration, and seamless connections to edge and cloud platforms.

Controller connectivity

Our controller connectivity products improve the scalability and reduce the operating costs of your applications, whether for brownfield or greenfield projects. They provide access to controllers from leading manufacturers and IoT devices and improve connectivity at the interface between OT and IT.

Connectivity for field devices

Our software and hardware gateways enable you to unlock HART, PROFIBUS, and other device data in Plant Asset Management applications to optimize your commissioning, maintenance and diagnostic processes.

OPC UA Unified Name Spaces

Use our solutions to collect and consolidate data to make it available in a consistent and structured format for applications such as



SOURCE: SOFTING INDUSTRIAL/SHUTTERSTOCK

Seamless OT-IT Integration Drives Data-Driven Insights for Optimized Processes.

SCADA, MES or ERP via the OPC UA Unified Name Space (UNS).

CNC machine connectivity

We provide products to securely read data from CNC machines without changing the machine configuration, and efficiently integrate it into IoT and cloud applications.

Embedded Industrial Ethernet and Ethernet-APL

Our solutions enable you to seamlessly integrate Industrial Ethernet and Ethernet-APL into your industrial devices. We support you in implementing real-time Ethernet protocols for reliable communication. Additionally, we offer flexible software solutions for various embedded systems. This allows you to design your network connection efficiently and future-proof.

Empowering Your Digital Transformation with Seamless Industrial Connectivity

With Softing Industrial, you gain a trusted partner dedicated to enhancing your industrial connectivity, ensuring your operations are more efficient, secure, and future-ready. Together, we can drive the digital transformation of your business.

Softing Industrial Automation GmbH

Email: info.automation@softing.com

Web: <https://go.industrial.softing.com/softing-ieb>

[Visit Website](#)



SOURCE: SOFTING INDUSTRIAL/SHUTTERSTOCK

Softing offers Advanced, Easy-to-Use Solutions for Digitalizing and Networking Industrial Systems.

Cisco - Powering smart industries

Cisco transforms critical industries by bridging the gap between IT and OT, and enabling AI-driven solutions that empower smarter, safer, and more sustainable operations.



SOURCE: CISCO

Figure 1: Cisco industrial networking portfolio.

AN INDUSTRIAL NETWORK WITH SCALE, flexibility, performance, determinism, security, and resiliency is the key to reliable operations where operational data can be easily harnessed for industrial agility and increased profitability.

Accelerate digital transformation

For over 20 years, Cisco has offered a comprehensive portfolio of industrial switches, routers, and wireless which are purpose-built for every industrial sector. Cisco industrial switches enable resiliency to minimize downtime, support communications protocols between control systems and machinery with minimal delay, and protect operations with visibility, data encryption, and network segmentation. Cisco industrial Wi-Fi, Ultra-Reliable Wireless Backhaul, and LoRaWAN solutions extend the wired network with dependable connectivity to mobile devices and sensors. Cisco industrial routers help securely connect your distributed field operations over 4G/5G and SD-WAN to your enterprise and the cloud.

All Cisco industrial switches, routers, wireless

network devices are managed and secured by the same proven tools that IT has used and trusted for many years. Network innovations allow OT teams to run advanced services within the equipment obviating the need for additional servers, networking complexity, and expense, while increasing the collaboration between IT and OT.

Protect operations

Cybersecurity is paramount in industrial operations due to the critical nature of the systems involved. A breach can lead to significant disruptions, financial losses, and even physical harm. Deeper integration between IT, cloud, and industrial networks is creating many cybersecurity issues that are becoming the primary obstacle to industry digitization efforts.

Cisco's approach to industrial security starts with gaining deep visibility. Cisco Cyber Vision runs within Cisco industrial networking equipment, analyzes traffic, identifies assets, discovers security vulnerabilities, and helps

define policies for effective segmentation in conjunction with Cisco Identity Services Engine or Cisco Secure Firewalls. Cisco leverages its unique enterprise security portfolios of products and solutions, together with threat intelligence from Talos®, one of the world's largest security research teams, to make security inherent and embedded in the industrial network.

Enable AI strategies

Cisco industrial network provides the high performance, low latency, and highly reliable infrastructure for data collection, transmission, and analysis, enabling AI applications to drive innovation, improve efficiency, and facilitate data driven decisions.

Deploy confidently

Cisco makes designing, implementing, and securing your industrial network easier by publishing tested architectures, including those built with our partnerships with leading Industrial Automation and Control Systems (IACS) vendors so you can deploy confidently and minimize risk.

Cisco is the only IT/OT networking company

Cisco's industrial automation and control networking solutions integrate industrial-strength networking equipment with enterprise-grade network management and security tools and provide validated and field-proven guides designed to accelerate your adoption of and benefit from IIoT. Cisco IIoT converges IT management and security technologies with industrial networks, drawing on both IT expertise and operational intelligence.

Cisco

[Visit Website](#)



Figure 2: Cisco connects and protects operations.

Rugged instrumentation for reliable measurement and control

Moore Industries is a world leader in the design and manufacture of exceptionally rugged, reliable and high-quality field and DIN rail-mounted instrumentation for the process monitoring and control industries.

MOORE INDUSTRIES WORLDWIDE SALES AND support offices provide first rate customer service and solutions for the chemical, petrochemical, utilities, petroleum extraction, refining, pulp and paper, food and beverage, mining and metal refining, pharmaceuticals, and biotechnology industries.

IIoT Solutions built to Deliver Field Data to your Host Systems

HART and MODBUS industrial communication protocols have dramatically increased access to device and process information that allows you to make more effective operational process decisions. Our Remote I/O systems including the NCS Net concentrator System® and HART gateways and converters such as the HES HART to Ethernet Gateway System and HCS HART to MODBUS Converter help integrate valuable data into your monitoring and control system strategy.

Instrument Panels and Systems Engineering

Moore Industries can specify, procure, and assemble your multi-vendor electronic and pneumatic instrumentation/hardware into custom-built instrument panels, systems and enclosures. We will provide complete documentation, expert technical assistance, and the assurance that complete and thorough testing has been performed.

Complete Temperature Solutions

Moore Industries Universal PC-Programmable, Smart HART® Temperature Transmitters



SOURCE: MOORE INDUSTRIES

convert and send RTD or thermocouple signals ready for direct interface with an indicator, recorder, PLC, DCS, or SCADA system. Temperature assemblies and measurement components include The WORM® flexible RTD and thermocouple sensors, connection heads and enclosures, thermowells and fittings. Our TCS Temperature Concentrator System provides precision measurements via HART or MODBUS RTU while significantly reducing hardware, wiring, and installation costs.

Programmable Alarm Trips

Provide on/off control, warn of trouble, or provide emergency shutdown with one or more programmable alarm (relay) outputs when a monitored process signal falls outside of a selected high and/or low limit. Our SPA2

Programmable Limit Alarm Trip accepts inputs from over thirty RTD and Thermocouple sensor types, provides two or four independent and individually-configurable alarm relay outputs, and offers an analog output (-AO) option for transmitter functionality to reduce installation costs/time.

Functional Safety Solutions

Our spectrum of SIL 2 and SIL 3 capable FS Functional Safety Series instruments include signal isolators and splitters, single and multi-loop alarm trips and logic solvers, temperature transmitters and more.. Every instrument is built and approved for use in Safety Instrument Systems and are third-party certified by exida to IEC 61508 standards.

More Than 55 Years Designing and Manufacturing Rugged and Reliable Instruments

Moore Industries has been proudly serving the process instrumentation needs of global manufacturers and automation companies since 1968. Designing, building and supporting more than 170 products across 14 product lines with unmatched systems, support and services expertise.

Moore Industries Worldwide

www.miinet.com

Email: info@miinet.com

[Visit Website](#)



SOURCE: MOORE INDUSTRIES

KLG Smartec: Makes Industry Smarter

KLG Smartec specializes in industrial communication solutions, integrating high-quality Ethernet switches and Smart Control Systems for reliable, high-performance industrial networking.

AT KLG SMARTEC (KLG), WE ARE DEDICATED to advancing industrial communication by integrating AI-powered solutions with top-notch Industrial Ethernet Switches and comprehensive Smart Control Solutions. Our focus on Industrial Automation drives us to prioritize high-quality Industrial Communications, seamlessly blending them with advanced industrial networking technologies. Our expertise shines through our commitment to developing AI-powered Industrial Networking Solutions and efficient Smart Control systems. This dedication ensures peak performance and unwavering reliability in our Industrial Network Infrastructure, adapting to the ever-evolving landscape of industrial internet.

Our Solutions

AUTBUS is a newly standardized IEC industrial broadband multidrop fieldbus. It supports both balanced cables, such as twisted single-pair cables, and unbalanced cables, such as coaxial cables. With a qualified twisted pair cable, AUTBUS can connect up to 254 multidrop data network nodes over a distance of up to 500 meters, at a data transmission speed of 100 Mbit/s. Using OFDM technology on the physical layer, AUTBUS is ideal for demanding communication environments. Its characteristics of broadband capability, low latency, and determinism make AUTBUS well-suited for industrial wired data communication.

AUTBUS Converter - ABN300 Series: The ABN300 series, powered by AUTBUS, supports data tunneling, which allows Ethernet-based transmission protocols and other communication protocols, such as CAN bus, to be transparently transmitted from one data connection point to another via the passive



The ABN300 series powered by AUTBUS, the newly standardized IEC industrial broadband multidrop fieldbus.

multi-drop data network without protocol translation. This integration enhances safety, reliability, and operational efficiency.

Industrial Ethernet Solutions

Industrial Ethernet Solutions are essential for maintaining robust and reliable communication in various industrial environments. Kyland's industrial Ethernet solutions ensure high-speed data transfer, resilience to harsh conditions, and adaptability to evolving technological demands.

Kyland Aquam Series: This series meets the stringent reliability requirements of both rail transit and factory automation sectors. It is ideal for applications where resistance to vibration and electromagnetic compatibility (EMC) are critically important.

Kyland Opal Series: This series consists of unmanaged Ethernet rail-type switches designed for applications in power, intelligent transportation, factory automation, video surveillance, and other fields. These switches

ensure fast and stable data transmission even in harsh industrial environments.

Kyland SICOM Series: This series includes DIN-rail managed Ethernet switches, rack-mounted managed Ethernet switches, Power over Ethernet (PoE) switches, and Layer 3 managed rack-mounted backbone switches. These products are widely used across various sectors, including factory automation, transportation, petrochemicals, wind power, and more.

Kyland Ethernet solutions offer high-speed data, durability, and adaptability to changing technologies.

Our Applications

Our applications deliver tailored solutions across multiple industries. In railway systems, we ensure exceptional reliability and safety, adhering to international standards. For factory automation, our advanced solutions support multiprotocol connectivity and enhance operational efficiency. In the power sector, we provide comprehensive support for reliable and efficient generation and distribution. Additionally, our solutions optimize operations in the oil and gas industry, focusing on safety and efficiency.



Kyland Ethernet solutions offer high-speed data, durability, and adaptability to changing technologies.

KLG Smartec GmbH

Arbachtalstrasse 6, 72800 Eningen, Germany

Telephone: +49 (0) 7121 6952 804

Inquiry: marcom@klgsmartec.com

[Visit Website](#)

One network, one solution

CC-Link IE TSN from the CC-Link Partner Association is the first and only open industrial Ethernet technology to provide a converged network architecture by combining Time Sensitive Networking with gigabit bandwidth.

THE CC-LINK PARTNER ASSOCIATION (CLPA) IS an international organization dedicated to the technical development and promotion of the CC-Link family of open automation networks. The CLPA was founded over 20 years ago in November 2000, when it introduced CC-Link, its highly respected industrial fieldbus technology. This was followed in 2007 with the widely adopted CC-Link IE, the first open industrial Ethernet to offer gigabit bandwidth. CLPA has since grown to be an acknowledged industrial automation network technology leader globally.

Today, CLPA's key technology is CC-Link IE TSN, the world's first open industrial Ethernet that combines gigabit bandwidth with Time-Sensitive Networking (TSN), making it the leading solution for Industry 4.0 applications and providing the foundation of the converged network architecture necessary to address the ever-changing challenges of 21st century manufacturing.

In order to meet demanding productivity and quality targets, current production trends demand cost effectiveness, better process insights, the shortest cycle times and the management of large amounts of process data. Complying to IEEE 802.1 standards, CC-Link IE TSN provides this capability by combining gigabit performance with the integration of control, safety and motion data along with general TCP/IP traffic on a



SOURCE: CLPA

single network architecture, all without compromising performance. This is the key to future industrial network convergence and only CC-Link IE TSN offers this functionality today. This translates to key business benefits:

- Simpler, more cost-effective network architectures and system designs
- Greater process transparency and better management
- Higher productivity
- Better integration of OT and IT systems

Currently the CLPA has over 4,300 member companies worldwide, and more than 3,000 certified products available from over 390

manufacturers. Together, these form a global installed base of about 43 million devices. The CLPA's technologies have found application in a wide variety of industries including but not limited to automotive, consumer electronics, semiconductor, food & beverage, packaging, material handling, water treatment and more.

CLPA offers development support and certification for device makers and product developers wanting to take advantage of CC-Link IE TSN's advanced capabilities in their own compatible products.

The CLPA has also been active in forming relationships with other industry leading associations such as the OPC Foundation and PROFIBUS & PROFINET International and is a member of the TIACC organisation.

SERVICES

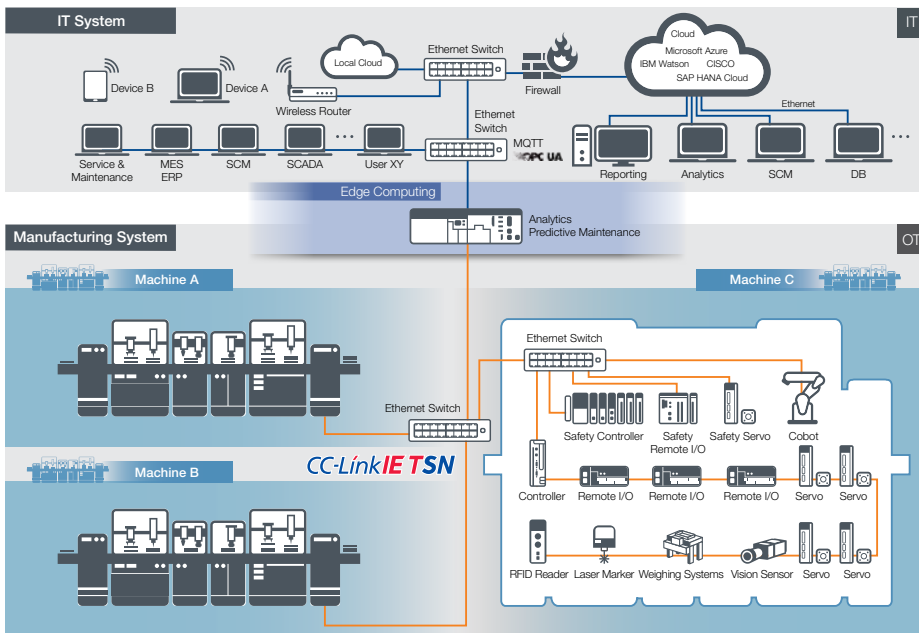
- Open industrial Ethernet
- Time-Sensitive Networking
- Gigabit & 100Mbit bandwidth
- Support for Industry 4.0
- Open fieldbus
- Safety networks
- Motion control networks
- Product certification
- Product development support
- Product promotion opportunities
- PROFINET interoperability

CC-Link Partner Association

Email: partners@eu.cc-link.org

Website: eu.cc-link.org

[Visit Website](http://eu.cc-link.org)



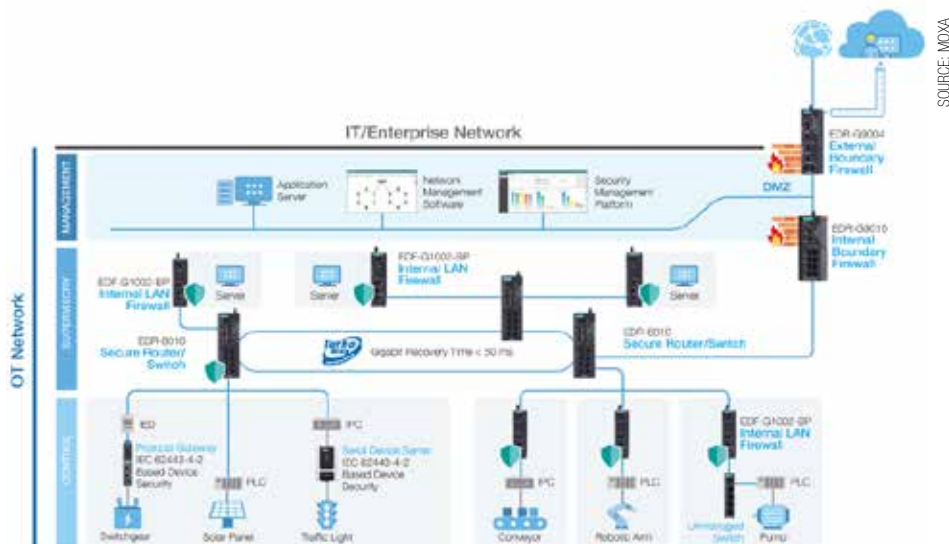
SOURCE: CLPA

Enabling the Future of Industrial Networking

Moxa offers scalable, secure and reliable solutions that help enterprises strengthen their digital operations, drive IT/OT convergence and build future-proof industrial organizations.

WITH OVER 35 YEARS OF INDUSTRY EXPERIENCE, Moxa is a global leader in edge connectivity, industrial computing, and network infrastructure solutions that empower the Industrial Internet of Things (IIoT). The company has connected more than 102 million devices worldwide and serves customers in over 85 countries, delivering reliable networking solutions and unparalleled customer service.

As industries navigate the challenges of digital transformation, Moxa remains at the forefront by providing resilient and future-ready networking solutions, specifically designed for IT/OT convergence. Moxa helps businesses optimize their network infrastructure to support the integration of advanced technologies such as AI, IIoT, TSN, and 5G, ensuring uninterrupted connectivity, enhanced security, and simplified management.



Factory network diagram: Dual firewall DMZ and secure devices for assessment.

Defense-in-Depth Network Security

Industrial control systems are increasingly targeted by cyberattacks as industries shift towards remote and distributed operations. Robust network security is now essential to maintaining operational resilience and ensuring safety. Moxa offers a defense-in-depth approach to security, delivering multi-layered protection across all levels of industrial networks.

In adherence to the IEC 62443 cybersecurity standards, Moxa provides tailored security solutions, including OT-centric firewalls, real-time visibility, and proactive threat detection and response. The MXsecurity platform enables industries to defend their operations from cyberthreats, ensuring

maximum uptime and operational reliability.

Advanced Solutions for Futureproof Networks

Industrial networks need to evolve to meet growing demands for performance, scalability, and resilience. Moxa's EDS-4000/G4000 Series industrial managed Ethernet switches offer a flexible and scalable solution that supports future network expansions. With 68 models certified under the IEC 62443-4-2 standards, these switches allow for seamless integration of additional bandwidth, PoE power, and enhanced security features — all within a compact, unified design. These futureproof switches are designed to support both current

and future network demands, ensuring robust network resilience and operational efficiency.

Simplified Industrial Network Management

Effective management of industrial networks is crucial for maintaining operational uptime and efficiency. Moxa's MXview One platform provides deep visibility and control over IT/OT networks, offering real-time monitoring of wired, wireless, and IEC 61850 substation networks. By simplifying network management, MXview One helps industries enhance operational efficiency and uptime at all stages of network deployment, management, and maintenance.



MXview One Central Manager: Real-time visibility and management of multi-site networks.

Delivering Lasting Business Value

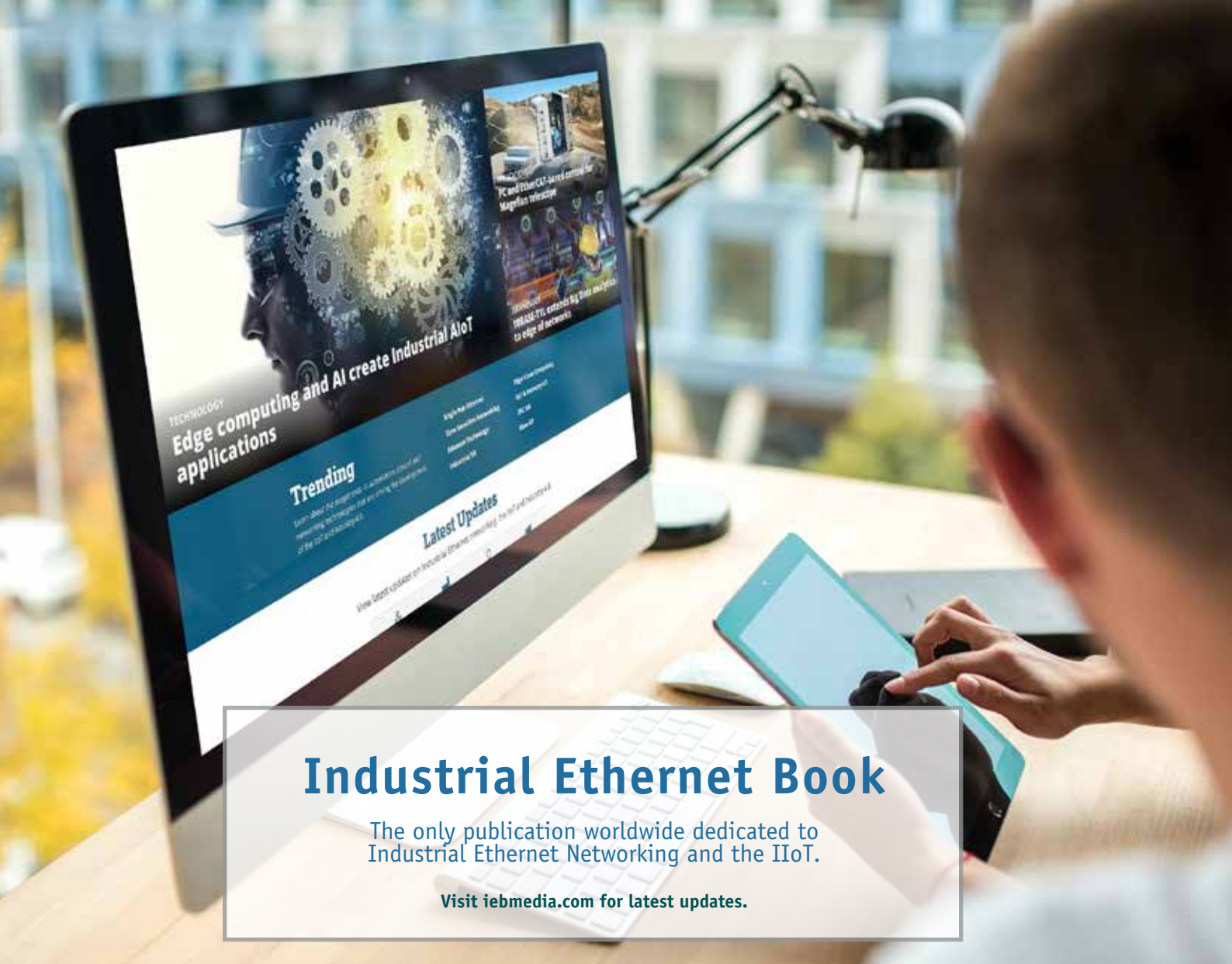
Moxa empowers industries with solutions that drive long-term success. With a focus on reliability, security, and scalability, Moxa continues to be a trusted partner in digital transformation for industrial automation. By enabling industries to optimize their network infrastructure, Moxa supports businesses in staying competitive, secure, and ready for the future.

Moxa GmbH

www.moxa.com

europe@moxa.com

Visit Website



Industrial Ethernet Book

The only publication worldwide dedicated to Industrial Ethernet Networking and the IIoT.

Visit iebmedia.com for latest updates.

New website offers deepest, richest archive of Industrial Ethernet and IIoT content on the web.



eBook Archive



Technical Articles



Latest Updates



Trending Topics

View and/or download latest issue of Industrial Ethernet Book and past issues.

Search our database for in-depth technical articles on industrial networking.

Learn what's trending from 5G and TSN, to Single Pair Ethernet and more.

Keep up-to-date with new product introductions and industry news.

Digital tool life monitoring: making machine data transparent

Metal machining is a standard process in the manufacturing of parts for the automotive sector. This is where digitalization in manufacturing can help to optimize process flows and boost efficiency. In its production work, Schlote Group utilizes the edgeConnector 840D from Softing to monitor tool life in its machining centers.



SOURCE: FOTOGRAFIE HANUSCHKE

The medium- and large-volume processing of metal parts for the automotive sector is a key business segment for Schlote Group.

HIGH-VOLUME PRODUCTION OF AUTOMOTIVE parts often involves the use of machining to further process cast parts. This particular area is a specialty for the midsize enterprise Schlote Group. At nine facilities around the world, the company operates an extensive machine pool for metal processing and other manufacturing processes.

Drilling, turning, milling, and other cutting methods are part of the standard repertoire here for processing engine, transmission and drivetrain components. To secure outstanding quality and high levels of efficiency, advanced CNC machining centers and automated production lines are used.

True to the company slogan "Innovative technology for success," Schlote Group works continuously towards improving production and optimizing its process flows. "This is where digitalization offers us huge potential," says Sascha Carell, who is responsible for shopfloor IT as the Group's MES Team Lead.

Regular tool changes

At Schlote Group's Harsum facility, the focus is on processing parts made from steel. Tools in the machining centers here are therefore subject to high levels of wear. Depending on the specific circumstances, individual tools may only have a life of a few thousand processing cycles.

On average, employees in production need to change two to three tools every minute at one of the many machining centers in use. For each tool responsible for handling a specific processing step, a maximum number of processing cycles is defined – after this time, the tool must be swapped out. Changing out the tool in time is the most effective way of avoiding unplanned system downtime due to tool breakage.

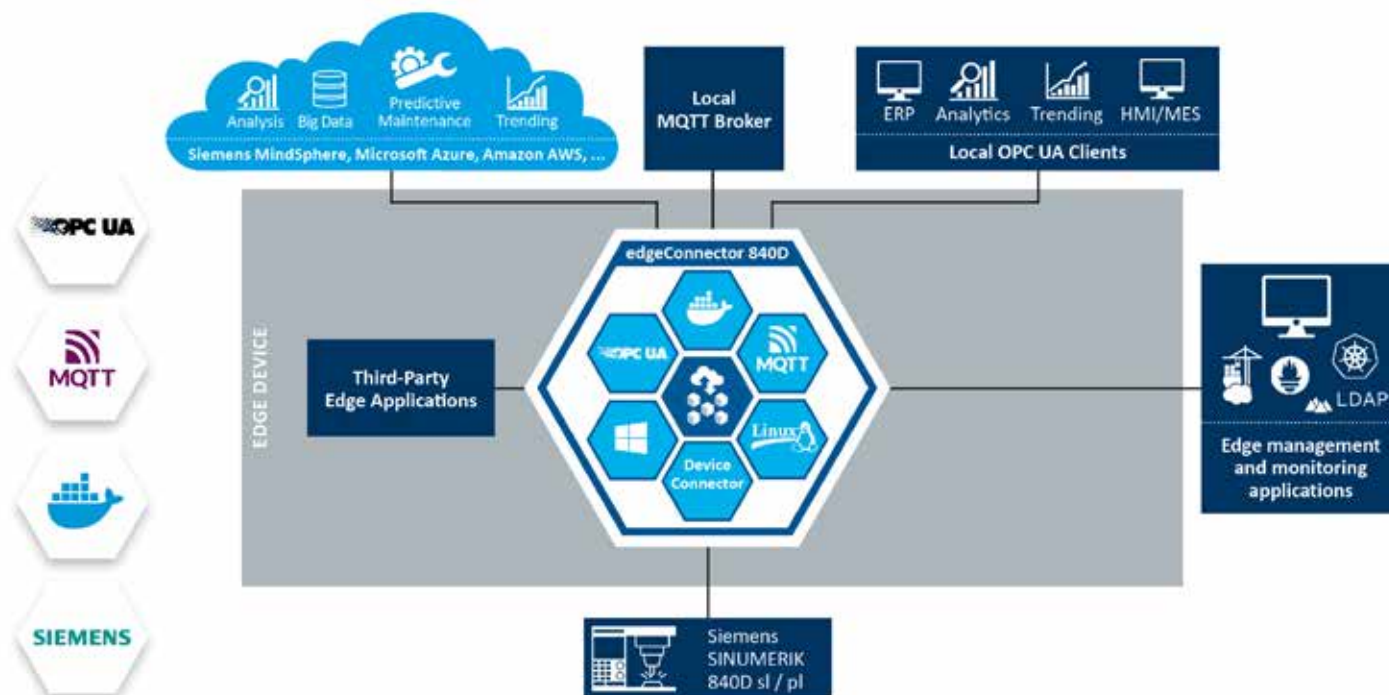
Carell: "The challenge here is monitoring all of the machining centers at the same time, so that tool changes can be carried out well in advance of any issues. So we were on the lookout for a digitalized solution to handle this task."

Data from the machine tool control

The data needed – in this case, the number of processing cycles since the last tool change – can be found in the CNC control inside the machine tool. However, the challenge here is ensure the right data are extracted from the machines in question and transferred to a higher-level system.

While solutions are also offered by the machine tool makers, these are manufacturer-specific. This makes it impossible to obtain an overview of the data from the overall machine pool, which includes machines from several makers. With the edgeConnector 840D from Softing, Schlote Group has found a solution that can retrieve the data from the Sinumerik controls used in its machining centers.

"We use Windows servers as our standard IT systems," Carell explains. "These provide a Linux subsystem on which we can install the edgeConnector 840D as a Docker container." Communication with the machine pool is then easily handled via the company-internal



The edgeConnector 840D from Softing accesses data from machine tools and supplies them to data consumers via an OPC/UA server (for example).

network. For machines featuring a Sinumerik 840D Powerline control without an Ethernet port, Softing offers a compatible adapter for the control's serial interface.

The software is configured very quickly and easily via a browser-based interface. The variables as well as the control and NC component can be selected in the corresponding tools, which generate the data files that the edgeConnector can import.

Carell: "One thing that we wanted to get right here was to have a solution that can also access data from the NC component and make these data easily available. Softing's edgeConnector formats these process data into a clean and tidy process data tree." A key factor for Schlote in this application is the tool monitoring counter, which indicates how many parts can still be processed before the

next tool change. As soon as this counter with a stored maximum value approaches zero, an employee has to change the tool.

Visualization without programming

Further processing of the data supplied by the edgeConnector is unproblematic, as Softing makes use of open industry standards and protocols such as MQTT and OPC/UA. Schlote uses the Peakboard Designer to visualize the data for employees working in production. This low-code application can be used to create visualizations even without extensive knowledge of coding.

Within the user-friendly interface, users work with building blocks to map out more complex process flows. To process the data from the edgeConnector, the OPC UA server is selected as a data source in Peakboard

Designer.

Large screens showing dashboards with the tool data have been installed in several places in the production areas at the Schlote facility. The employees responsible for the machines only need to glance up to see when the tools are due to be changed. Other status data are also visualized alongside the tool data. These screens supplement the traditional "traffic lights" on the machines. And operators are more likely to use the screens and dashboards, as they offer much more information. As one example, the screen tells them why the traffic light has just turned yellow or red. "Being able to skim through all of the key data at a glance is a real help for our production team," says Carell in conclusion.

Better integration with platforms

Integrating the edgeConnector 840D with the Peakboard solution was also a positive experience for Schlote's MES Team Lead. "I didn't have to stop and work out a software networking strategy, because the manufacturers offer solutions that are designed to fit together. This kind of architectural compatibility and collaboratively developed solutions package really offers great value for end users. Carell was also highly impressed by the experience of working with the Softing team. "Softing responded promptly to new requirements, also typically implementing these over a short timeframe. At the end of the day, this project was really like working as part of a single development team."

Dr. Jörg Lantzsch, Agentur, **Softing Industrial**.

[Visit Website](#)

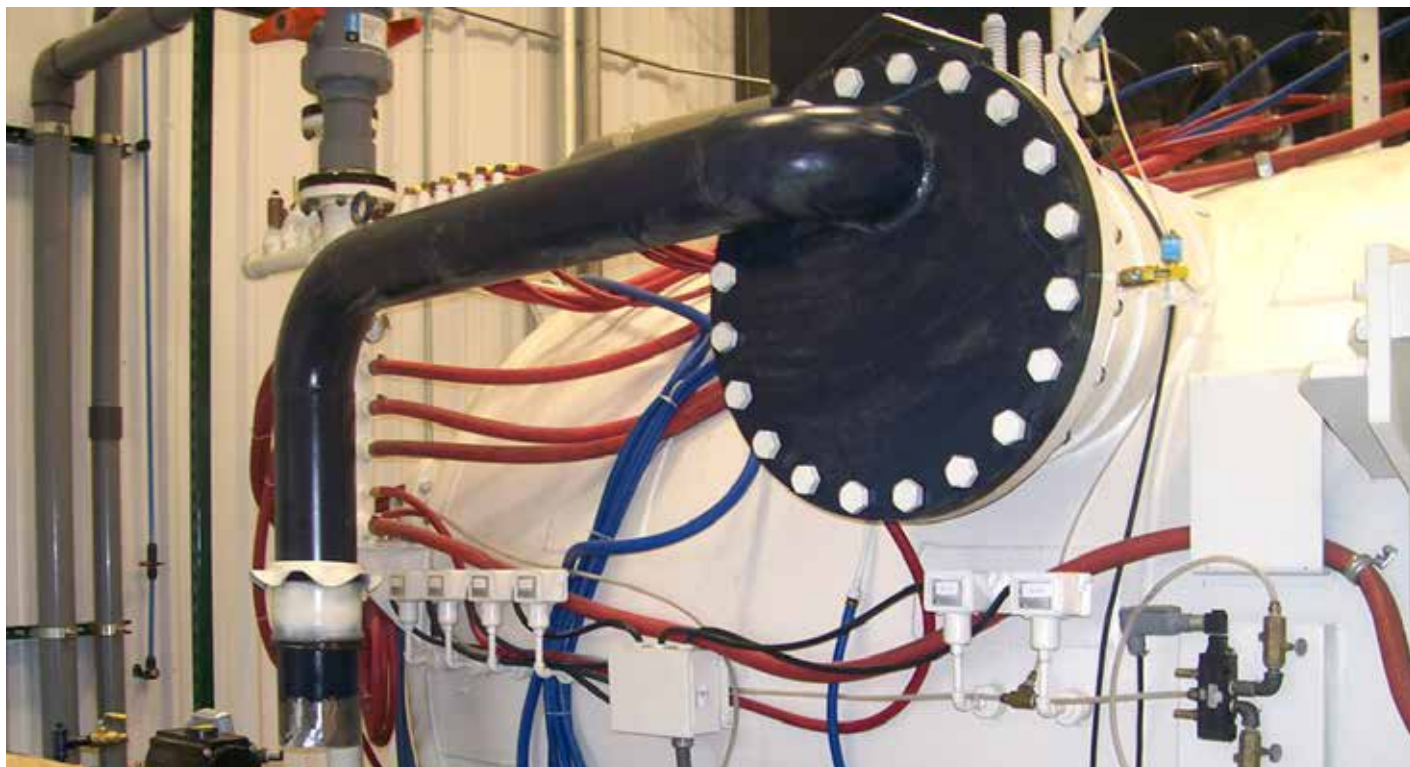


SOURCE: SCHLOTE GROUP

Thanks to the data visualizations provided by Peakboard dashboards, employees can check tool and machine data at any time.

Heat treatment OEM chooses flexibility and scalability

Heat treatment machinery OEM Mercer Technologies continues to innovate, adding energy cost per part. Using energy monitoring, the company is able to calculate in real time how much it costs to heat treat parts, and can accurately and effectively assign the cost of energy to the production of a particular component.



SOURCE-OPTO 22

Mercer Technologies' vacuum furnace utilizes Opto 22's groov EPIC system with a variety of I/O modules.

INDUSTRIES LIKE AEROSPACE AND POWER generation, where the margin for error is virtually nonexistent, utilize heat treatment to enhance the performance, durability, and reliability of critical components. Heat treating can improve strength, wear resistance, and lifespan of commonly used parts like camshafts, crankshafts, and turbines.

Mercer Technologies, a veteran owned and operated company in Terre Haute, Indiana,

is an expert on heat treatment processes. At Mercer, they not only perform heat treatments on parts, they build full heat treatment systems that they provide to their customers, and they refurbish existing heat treatment systems, breathing new life into existing machinery to extend service life and enhance performance.

"All projects are different. Every furnace is different," explains Cody Young, Mercer

Technologies' Controls and Automation Engineer. "There's annealing, brazing, pre-welding, post-welding, and so on. For that reason, we wanted a platform that was flexible and scalable. Customization is a must."

Heat treatment challenges

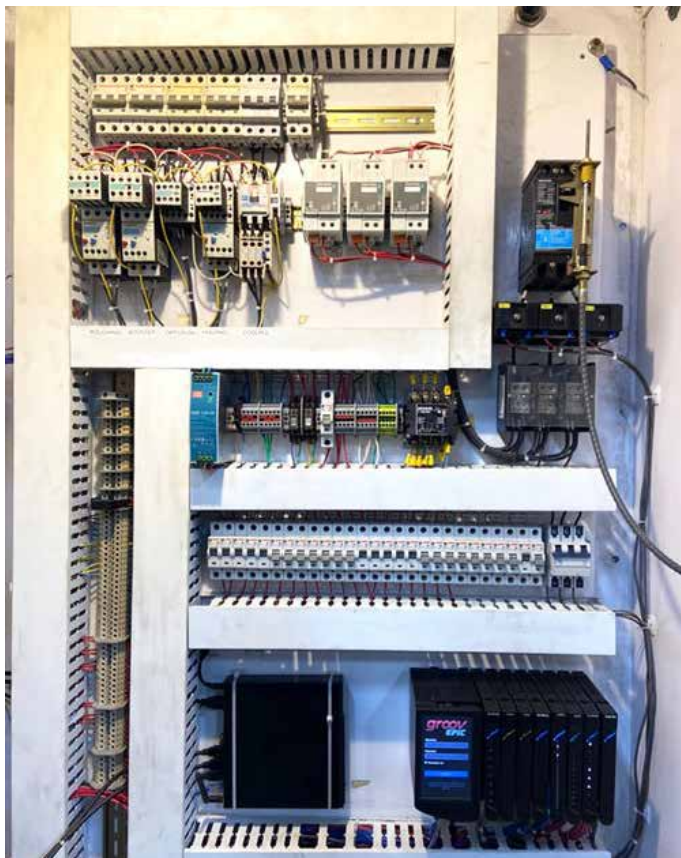
The heat treatment process involves heating and cooling materials, typically metals, in a controlled manner to alter their physical and



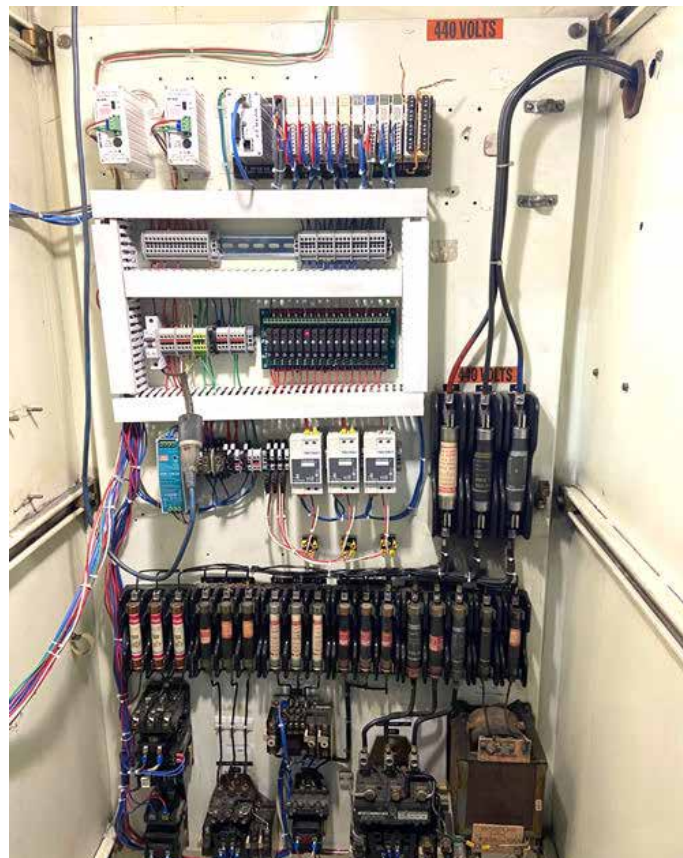
Vacuum furnace (exterior)



Vacuum furnace (interior)



Mercer's most recent hardware design uses a groov EPIC System for control.



Mercer's older systems, still running reliably, use an Opto 22 SNAP PAC System.

mechanical properties without changing their shapes. Heating to temperatures in excess of 1000° C requires a high degree of care and precision.

Ridding the chamber of contaminants

before the treatment begins is a key part of the process, and it can be accomplished in various ways. The atmospheric method, which is done by purging the furnace with an inert gas like nitrogen, is generally safer but takes

longer and increases the overall cost of the process. Vacuum furnaces, on the other hand, which use vacuum pumps to decontaminate the chamber, can reach their deepest vacuum level in just a few minutes, but the operation is a bit more perilous.

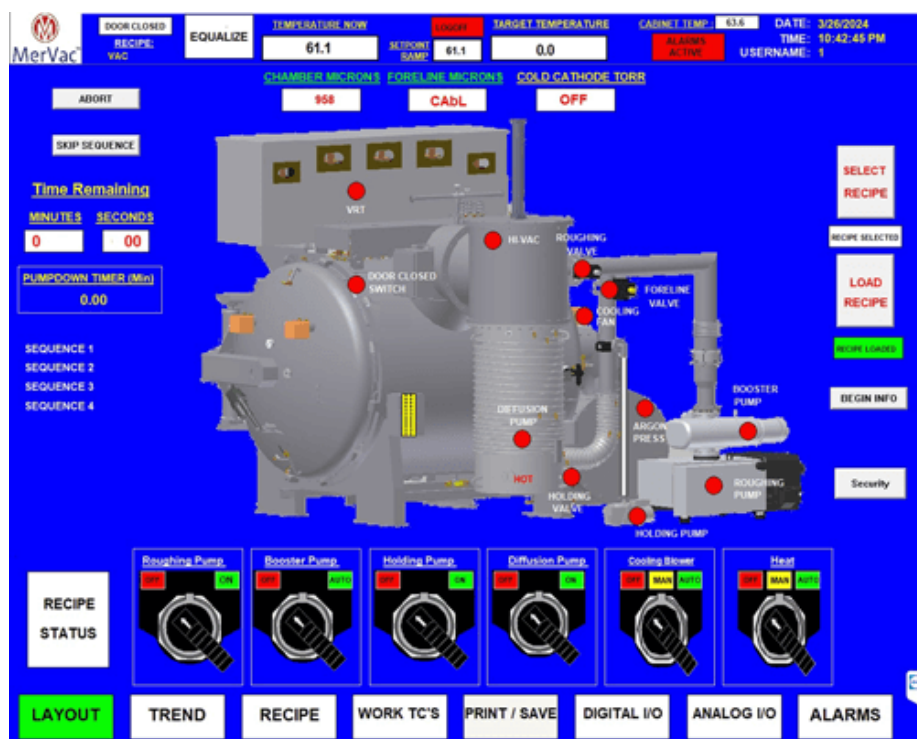
"Improper valve sequencing during vacuum furnace operation can cause oxygen in the air to go where it's not supposed to. Oxygen in the wrong place can lead to potential explosions or implosions, which is obviously a very bad situation," explains Young.

Application solutions focus

Back in 1994, when Mercer Technologies was starting out, they needed a control solution that could do two things: flexibly adapt to a variety of applications and safely ensure proper sequencing of valves to prevent dangerous accidents.

Young found that the modular design of Opto 22 products offered the hardware scalability that Mercer needed. And OptoScript, a scripting language found within Opto 22's PAC Control flowchart-based programming software, offered the flexibility Mercer was looking for. "Back in my college days at Ivy Tech, we learned C++, so I was familiar with a similar scripting language. I can customize it however I want to," Young recalls.

Beyond capable products, Mercer needed a platform that offered local support. Based in the USA with free product support, Opto



Mercer HMI screenshot.

22 fit the bill. Young explains, “Opto 22 has competitors, but they are unmatched in support, and using products made in the USA is important to our mission. Every issue I’ve ever had with Opto 22 products was resolved quickly, usually with help from the OptoForums [Opto 22’s factory-supported online community forum for exchanging ideas and application support].”

30 years later ...

Opto 22 has been providing solutions for Mercer since the firm’s inception in 1994, and today, Mercer has over 100 heat treatment systems operating in the field at various customer sites and 8 systems running in their Terre Haute facility.

Young explains, “Vacuum chambers in heat treatment systems used to be manually controlled with pushbuttons and switches. Automating with Opto 22 products has enabled us to build a less error-prone system, but most importantly, a safer environment for our operators and customers.”

New products enhance heat treatment process

While the heat treatment process itself hasn’t changed much since 1994, better instrumentation and technology have opened the door to further enhancements in safety, reliability, and intelligence.

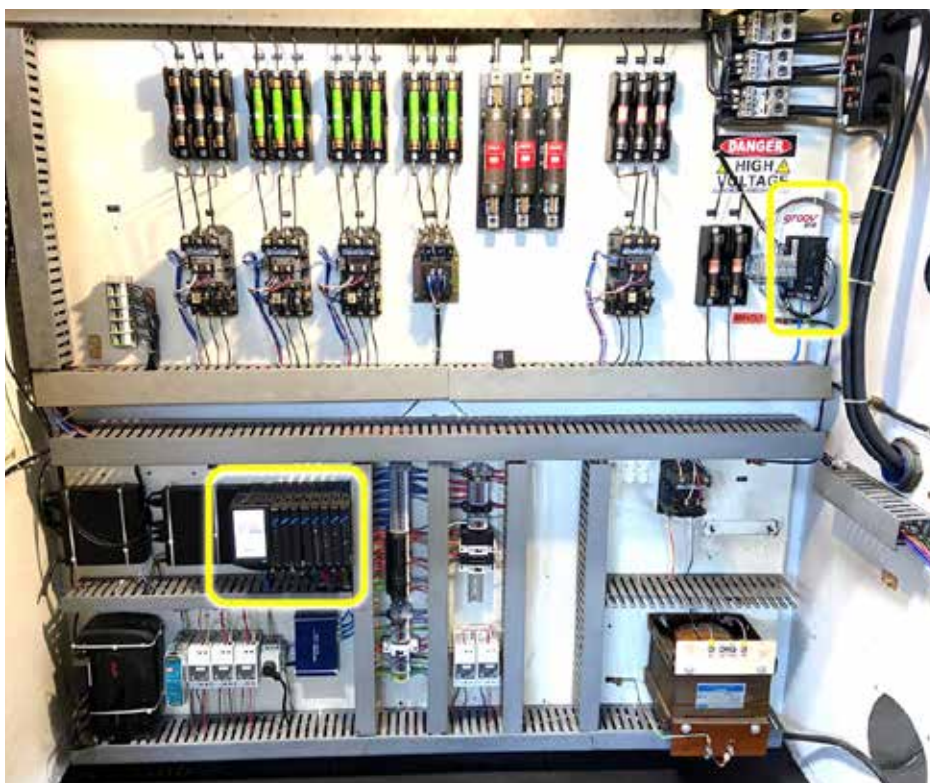
Hardware Design

Mercer’s most recent hardware design utilizes Opto 22’s groov EPIC system with a variety of I/O modules that serve the following functions:

- The GRV-CSERI-4 module (and in some cases, a USB-to-serial converter from Gearmo®) provides RS-232 communication to a EuroTherm® temperature controller, which includes PID loops for control, and a Televac® vacuum measurement instrument, which ensures proper vacuum levels.
- The GRV-OVMALC-8 module outputs a 4–20 mA signal to provide fine-tuned control of heating elements.
- The GRV-OMRIS-8 module’s relay outputs, with a 5 amp capacity, control higher current valves on the vacuum chamber.
- The GRV-OACS-12 similarly controls lower current rated valves on the chamber.
- The GRV-IDCS-24 provides input from pushbuttons and on/off feedback from valves.
- The GRV-ITM-8 provides valuable temperature data through thermocouple inputs.

Software Design

Most of Mercer’s systems utilize Microsoft® Windows® 11 PCs running AVEVA® software [formerly WonderWare®] for visualization.



Mercer's latest design incorporates a groov RIO EMU and a groov EPIC system.

AVEVA’s OPC drivers provide seamless communication to Opto 22’s groov systems and also to legacy Opto 22 SNAP systems.

Onboard the groov system, Node-RED, an open-source flow-based programming tool for IIoT applications, handles the RS-232 serial communication between the groov EPIC and third-party instrumentation.

At the heart of the application is still Opto 22’s PAC Control. The flowchart programming environment is designed for safely controlling a sequential operation like heat treatment.

PAC Control handles all of the critical valve sequencing, and runs independently of the PC.

“For fail-safe reasons, the HMI is only used to view operations and to transfer recipes into the PAC Control strategy. Once the values are transferred and the process begins, the PC could be unplugged, but the groov EPIC system will remain running to keep the furnace in a safe state,” explains Young.

Powering through: the energy dynamics of heat treating

“In our most recent design, we’ve utilized a groov RIO EMU [Opto 22’s IIoT-ready power and energy monitoring module] to monitor energy consumption of a particular furnace,” says Young. “At max output, this furnace consumes nearly 350 kVA per hour, roughly 420 amps at 480 volts—enough to power an entire residential subdivision!”

Young goes on to explain, “With energy monitoring, we can calculate in real time how much it costs to heat treat parts, and we can

now accurately assign the cost of energy to the production of a particular component.”

With this new energy data, Mercer Technologies can make informed decisions on how to optimize energy consumption and ensure pricing strategies are accurate and competitive.

New opportunities

Mercer Technologies isn’t done. Their recent foray into groov products has opened the door to new opportunities to enhance their product offering and better serve the industry.

One of Mercer’s customers, an Inductive Automation® Ignition® user, recently expressed interest in adding their Mercer Technologies equipment into their Ignition application. “I haven’t crossed that bridge yet,” Young says, “but my experience with Opto 22’s support has been phenomenal. I’m sure when the time comes, I’ll be able to find most of what I need on the OptoForums.”

Reflecting on the 30-year history using Opto 22 products, Young declares, “We’ve done a lot of refurbishing of older systems where we replaced older, outdated controls with SNAP and groov systems. We know they’ve been a success because of all the repeat business. I almost never deal with failed systems. We have systems that have been in the field for over 20 years that are still running.”

Application report by Opto 22.

[Visit Website](#)

Maximizing automation efficiency with Industrial PoE switches

This article explores how industrial PoE switches can maximize efficiency and flexibility in automation by simplifying cabling, reducing installation time and centralizing management.



SOURCE: ANTAIRA TECHNOLOGIES

Use of Power Over Ethernet in car manufacturing.

INDUSTRIAL AUTOMATION IS A COMPLEX AND rapidly evolving field that requires robust and versatile networking solutions. One technology that has emerged as a key enabler of automation is Power over Ethernet (PoE), which combines power and data transmission over a single Ethernet cable.

PoE in industrial automation

The PoE standard was first approved by the Institute of Electrical and Electronics Engineers (IEEE) more than 20 years ago. This standard, known as IEEE 802.3af, allows for up to 15.4W of DC power per port. Since then, IEEE has released updated standards. The most recent is IEEE 802.3bt Type 4, also known as 4-pair PoE (4PPoE) or PoE++. IEEE 802.3bt can supply up to 90W of power per port to a range of devices such as IP PTZ cameras, gas analyzers, video monitors and embedded computers that require higher wattage.

PoE has rapidly gained traction in the industrial sector for a variety of reasons, just as it has in enterprise and commercial networks. For one, it significantly lowers infrastructure complexity, especially in remote locations or areas of the plant without available power outlets. An electrician is not needed to install or maintain a PoE cable due to the low voltages

involved, nor does the installation require long runs of steel conduit or earthing enclosures, reducing initial deployment costs. Another advantage of PoE is that it gives network managers the ability to centrally monitor a device's PoE power consumption and other power-related data. Nonessential devices being monitored by a managed PoE switch can have their power automatically decreased or turned off entirely when not in use. Flexibility is yet another benefit. Network devices can be mounted in previously inaccessible locations since power outlets no longer restrain their placement. Swapping existing devices on the network entails a little more than plugging in the device's Ethernet cable into a PoE network switch port. Also, PoE is standards-based, for vendor interoperability.

An area of automation where PoE is paying dividends is Supervisory Control and Data Acquisition (SCADA) networking. SCADA is a means of remotely monitoring and controlling equipment in automation processes in industries such as manufacturing, oil and gas distribution, utility power, and wastewater management.

One of the largest shifts in SCADA has been its evolution from serial networking protocols to the Internet protocol (IP). Adopting IP has meant equipment costs are less expensive,

and bandwidth can scale up to 10 Gbps for end stations and up to 100G bps for backbone networks. It also means a SCADA network that deploys Ethernet as an access network can benefit from PoE. A SCADA's array of PLCs, RTUs, sensors and other end devices can all be supplied with power simply by connecting the device's cable to an open switch port.

Industrial safety

While PoE is frequently touted for its flexibility and infrastructure savings, this technology also contributes to industrial safety.

It is not unusual for the electrical systems powering industrial facilities to be 480V or 600V, more than enough to injure an employee from electrical shock, arc flash, explosions or other hazards. Low-voltage PoE reduces or eliminates the risks of short circuits, exposed wiring, or accidental contact with live voltage. Overload protection, which guards against high power consumption and consequent damage to devices or cables, is also built into PoE devices. If an overload is detected, power distribution is reduced or turned off to safeguard or repair the connected equipment and lower the possibility of overheating or a fire.

Is electrical safety important in automation projects? Overwhelming, the answer is yes.

According to the National Fire Protection Association (NFPA), electrical accidents in the workplace cause thousands of injuries annually and nearly one fatality per day.

Selecting a PoE managed network switch

Network architecture, capacity, and scalability must all be carefully considered when designing an industrial automation network that can accommodate PoE devices. This will require configuring several PoE managed switches in order to guarantee dependable and effective network operation. So, what should you be looking for in a managed PoE switch?

Ruggedized equipment

Numerous risks confront switch operation such as electrical noise, humidity, corrosive chemicals, vibrations, and extreme temperatures. To mitigate or reduce these factors, confirm that you are purchasing industrial-grade PoE managed switches featuring ruggedized, environmentally hardened packaging with the appropriate ingress protection (IP) rating. Although less common, another threat is the presence of classified areas within a plant where volatile flammable liquids or gases are handled, processed or used. In these environments an explosion-proof switch will be required by Class 1 Div 2 and ATEX codes.

Bandwidth requirements

Switch bandwidth determines the data-carrying capacity of a network, influencing the speed and reliability of data transmission. Inadequate switch bandwidth can lead to network congestion, latency, and compromised device functionality. Whether a 10/100, 2.5G, Gigabit, or 10G switch is necessary will depend on your application. It is also a good strategy to plan for extra bandwidth in case needs increase.

Power requirements

Ensure the industrial PoE switch's overall power budget can simultaneously support all of the devices by factoring in each device's power consumption. Industrial network devices, including optical sensors, APs, networked lighting, and IP cameras, have significant variation in wattage requirements, typically swinging between 15 watts to 100 watts.

Confirm that the industrial PoE switches have enough PoE power and power budget to support your devices. You'll also need to factor in that the maximum distance for PoE is 100 meters (328 feet) and that energy loss can occur over longer distances. If that's the case, you'll need to install additional network infrastructure, such as intermediate switches, PoE extenders or power injectors.

Port configuration and types

A switch's required PoE port count depends on the number of PDs you plan to power, although



Antaira PoE managed Ethernet switches featuring 16 Gigabit PoE+ ports integrating robust M12 connectors and capable of supplying 30 watts per port (IEEE 802.3 af/at) with two 10G SFP slots.

it is good practice to have more to allow for expansion. Port count and the PoE standard will significantly impact the quality, scalability and flexibility of your network. Having a mix of Gigabit and Fast Ethernet ports allows you to cater to devices with varying bandwidth requirements.

Compatibility

Before power transmission can begin, the industrial PoE switch and the powered device must negotiate to determine the device's power requirements. The outcome of the negotiation establishes whether the two are compatible and whether the device can safely get the power it needs. If successful, negotiation keeps the powered device from receiving too much or too little power; both conditions can damage the device or cause it to malfunction.

Security features

Having advanced security features in an industrial PoE switch, such as port security and access control lists (ACLs), is essential to protecting a network in light of growing concerns surrounding cybersecurity.

Case history: PoE in car manufacturing

Let's look at the actual case of an Antaira customer to get a better sense of the importance of PoE in automation. In this instance, the customer was an automaker seeking to add visual guidance to its robotics systems by installing new GigE Vision products and machine vision cameras. In order to simplify wiring, many GigE Vision cameras will use PoE for power so only one cable needs to be run, for instance, on a robotic arm with the camera able to recognize objects or to localize them for welding.

Aggregating multiple GigE Vision cameras

into one link into the Industrial PC (IPC) will often require a 10G link from the PoE switch to the IPC running the software.

Among the challenges facing the manufacturer in deploying its machine vision system was ensuring reliable connections from the industrial PoE switches. Harsh conditions prevented use of the standard RJ45 connections found on most network switches since they lack ingress protection and could disconnect due to vibrations from the heavy machinery. The automaker company also needed a powerful switch solution that transmitted image data at high frame rates, along with a special low voltage power (12-24V DC) needed for the GigE Vision cameras to properly operate.

To help make this project a reality, the automaker selected Antaira LMP-1802-M12-10G-SFP-67-24-T PoE managed Ethernet switches featuring sixteen Gigabit PoE+ ports integrating robust M12 connectors and capable of supplying 30 watts per port (IEEE 802.3 af/at) with two 10G SFP slots. M12 designs provide extremely tight connections in areas subject to high vibration, shock, dust, liquid or gases.

Besides the M12 connectors, LMP-1802-M12-10G-SFP-67-24-T industrial switches are IP67 rated as waterproof and dust-tight, plus operate in an extended temperature range from -40°C to 70°C for withstanding extreme conditions. Low voltage power requirements of the GigE Vision cameras were met by the Ethernet switch's 24~55VDC power input. In addition, a separate Antaira switch offering two 10G SFP slots for fiber connections was installed as the high-speed link to the IPC.

Henry Martel, field application engineer, Antaira Technologies.

[Visit Website](#)

TSN component certification from Avnu

TSN Component Certification for switches advances unified communication for Time-Sensitive Networking.



MOXA®



Moxa obtains the world's first TSN Component Certification from Avnu Alliance.

MOXA HAS ANNOUNCED A GROUNDBREAKING milestone in obtaining the world's first TSN Component Certification from Avnu Alliance for components used in its TSN-G5000 Series industrial Ethernet switches. Moxa's TSN-powered switches enable users to design interoperable, deterministic, reliable end-to-end communications to achieve time-sensitive networking (TSN) for critical industrial applications without the limitations of proprietary systems.

"The Component Certification Program is the first of its kind to certify TSN capabilities and serves as the industry platform for verifying conformance and cross-vendor interoperability of TSN components," said Dave Cavalcanti, President of Avnu Alliance. "Moxa's expertise and experience in industrial Ethernet and networking, as well as the global TSN standardization projects, brings crucial advancement to the program and improves deterministic and reliable end-to-end networking over TSN for various industrial applications across vertical markets."

As an industry forum for integrating

deterministic capabilities into open, standards-based networking, the Avnu Alliance Component Certification Program focuses on core TSN standards, including timing and synchronization (802.1AS) and enhancements for scheduled traffic (802.1Qbv). Manufacturers from different markets can now verify the compliance of their components with the core TSN standards, resulting in improved interoperability and easier integration with other systems.

Leveraging its expertise in bridging the gap between standard Ethernet and industrial applications, Moxa supports the Component Certification Program by providing testing products and completing test cases for network devices such as Ethernet switches, to help develop the program. Moxa's experience with worldwide TSN projects such as the IEC/IEEE 60802 TSN profile for industrial automation and the IEEE 802.1 TSN Task Group, also played a crucial role in translating IEEE SA 802.1 TSN standards into test specifications. Moxa's contributions helped ensure that these component-level TSN technologies can be

widely and effectively adopted across different markets around the world.

Moxa's TSN Ethernet switches with Avnu-certified components have been deployed in success cases all around the world. Featuring a compact design and user-friendly interface, these Ethernet switches are ideal for a variety of applications such as factory automation, dynamic mass customization, hydropower plants, and CNC machines. The TSN-G5000 Series not only helps customers reduce production times and increase efficiency, but also showcases the benefits of TSN in real-world applications, accelerating the digital transformation across various sectors.

Through the TSN Component Certification Program, Moxa believes that its commitment to advancing TSN technologies will continue to set new industry benchmarks and drive innovations to meet the ever-changing needs of industrial automation.

Moxa

[Visit Website](#)

Intelligent manufacturing hub

OpreX Intelligent Manufacturing Hub offers a proven data integration and visualization solution.

Sample KPI dashboards for personnel at all levels of the organization



Sample KPI dashboards for personnel at all levels of the organization offers connectivity with RPA.

YOKOGAWA HAS ANNOUNCED THE GLOBAL release in all markets other than Japan of OpreX™ Intelligent Manufacturing Hub. By utilizing robotic process automation (RPA) implemented in a low-code / no-code environment or through customization by Yokogawa, this data integration solution can significantly reduce reporting time.

OpreX Intelligent Manufacturing Hub covers the full range of key performance indicators (KPIs), workflows, and reporting at every level of the organization, from the C-suite to the plant floor, and employs a single database to integrate and display on dashboards data that customers need to make the right decision at the right time.

Development background

Companies everywhere are looking for the right digital transformation (DX) solutions that will help them to run their businesses more efficiently. One common issue is that the data they need is often scattered across different systems, with no interface available for automatic integrated access.

Business intelligence tools are available that can meet this need, but they must be optimized based on each company's unique infrastructure to minimize incidents, eliminate manual operations, reduce the amount of time needed to generate reports, and ensure

a sufficient return on investment, but all this requires considerable domain knowledge and consulting expertise.

As a trusted provider and integrator of industrial automation solutions with deep domain knowledge, Yokogawa has the ability to provide consulting on manufacturing and process control in a wide variety of industries. Based on the company's understanding of its customers' infrastructure and business processes, it is able to verify and propose tailor-made solutions that utilize intelligent business tools.

Main features

User-friendly dashboards that visualize data for decision makers at each layer of the organization

Data from diverse operational technology (OT) and IT data sources that has been securely integrated in a single database is visualized on feature-rich dashboards. Covering the full range of KPIs, workflows, and reporting at every level of the organization from the C-suite to the plant floor, this gives customers access to all the information they need to make informed and timely decisions.

Drastic reduction in reporting time

By incorporating the use of RPA technology, this solution eliminates the need for manual

processes and thereby significantly reduces the amount of time required to generate reports. Leveraging a low-code/no-code environment, customers can create their own RPA software, or turn to Yokogawa for the provision of a customized RPA solution.

The OpreX Intelligent Manufacturing Hub also allows for the drilling down through data to find root causes and gain insights. It is well suited for use in a wide variety of industries, from oil & gas to chemicals and pharmaceuticals. Along with this solution, Yokogawa will provide holistic support and services through its global network that are essential for the success of any intelligent business tool project, including definition of specifications, training, maintenance, and technical support.

Kunimasa Shigeno, a Yokogawa Electric Senior Vice President & Executive Officer and head of the company's Digital Solutions Headquarters, said, "I am pleased to announce the official launch of this solution. Using a pre-release version

of OpreX Intelligent Manufacturing Hub, our skilled digital transformation consultants and subject matter experts have already demonstrated their ability to identify and solve issues. In keeping with our aim of being a leader in the system of systems field, this solution allows for the integration of multiple corporate assets, eases collaboration across the organization, and creates a single source of trusted data, giving our customers the information they need to make the right decisions at the right time. And by utilizing RPA, they can dramatically reduce reporting time. This is a proven solution that will enrich user experience and provide both value and a solid return on investment."

Major Target Markets

Oil & gas, petrochemicals, chemicals, renewable energy, power, pulp & paper, mining & metal, pharmaceuticals, food & beverage, water

Applications

Data integration and visualization, workflow automation, management of business and plant process data

Yokogawa

[Learn More](#)

Enhanced CNC functionality

Siemens is paving the way for digital twins to acquire greater flexibility, productivity, and sustainability.

Siemens is introducing hardware and software for the Sinumerik 828D CNC specifically designed for the compact and mid-range machine market. The new PPU271.5, PPU270.5, PPU290.5, and PPU272.5 processor units and the redesigned Sinumerik 828D MCP (Machine Control Panel) operating concept offer a wide range of functions and options that increase the productivity, sustainability, and efficiency of manufacturing processes.

Run MyVirtual Machine

The new processor units allow the Sinumerik 828D to be upgraded to software version 5.24, paving the way for Sinumerik Run MyVirtual Machine. As with Sinumerik One, the digital native CNC, Run MyVirtual Machine allows NC programs to be created, validated, and optimized using a digital twin of the machine without interrupting production. This reduces the set-up time on the real machine by up to 20 percent and minimizes production risks.

In addition, the working area of the machine, clamping, tool, and material removal can be visualized in detail in all phases of the NC program. Potential collisions can therefore be recognized and eliminated in advance. Training new employees with Run MyVirtual Machine also saves machine time and minimizes the risk of damage due to incorrect operation or programming errors.

Redesigned operating concept

The redesigned Sinumerik 828D MCP operating concept is being introduced to



Sinumerik 828D PPU272.5.

match the new generation of processor units. This launches a more intuitive machine operation for the Sinumerik 828D from Siemens, which offers CNC users greater user-friendliness, efficiency, and flexibility.

The redesigned Sinumerik 828D MCP operating concept includes significantly larger and innovatively designed control panels with 12.1-inch and 15.6-inch screens as well as mechanical keys. Create

MyHMI/3GL can also be used to further customize the user interface for specific areas of application.

Enhanced connectivity, energy efficiency, and security functions

The new processor units have an X120 interface, which enables connection to external devices like Sinumerik HT (Handheld Terminal) 10 or edge devices. This extends the range of applications and increases productivity.

The Ctrl-E key combination also provides the user with a comprehensive analysis function that makes energy consumption transparent. In the area of cybersecurity, the new processor units offer security functions like a security archive, user management, and certificate storage, which offers protection from manipulation and product piracy.

With the new hardware and the associated new software for the Sinumerik 828D, Siemens is paving the way for digital twins to acquire greater flexibility, productivity, and sustainability. At the same time, the range of applications for the control of turning, milling, and grinding technology is expanding to the areas of power and energy, electronics and 5G, automotive, and more.

Siemens

[Visit Website](#)



Sinumerik 828D PPU271.5 and Sinumerik 828D PPU270.5 and redesigned operating concept Sinumerik 828D MCP.

GenAI automation platform

Transformative GenAI automation platform delivers powerful tool for power and water industries.

The Ovation Automation Platform with GenAI will empower workforce, optimize operations. As part of its release of the Ovation™ 4.0 Automation Platform, global automation and technology leader Emerson is delivering transformative generative artificial intelligence (GenAI) that will enhance data to inform decisions, helping power and water companies accelerate growth, improve efficiencies and drive more predictive, reliable and resilient performance to their operations.

With the digital transformation of the power and water industries, utilities and municipalities now have vast amounts of rich production, reliability, safety and sustainability data for their operations – yet much of it is fragmented and siloed. Operators require a modern, future-proof computing environment that can confidently mine large and complex data sets and harness the power of GenAI for better, more efficient operational insights.

Ovation 4.0 Automation Platform

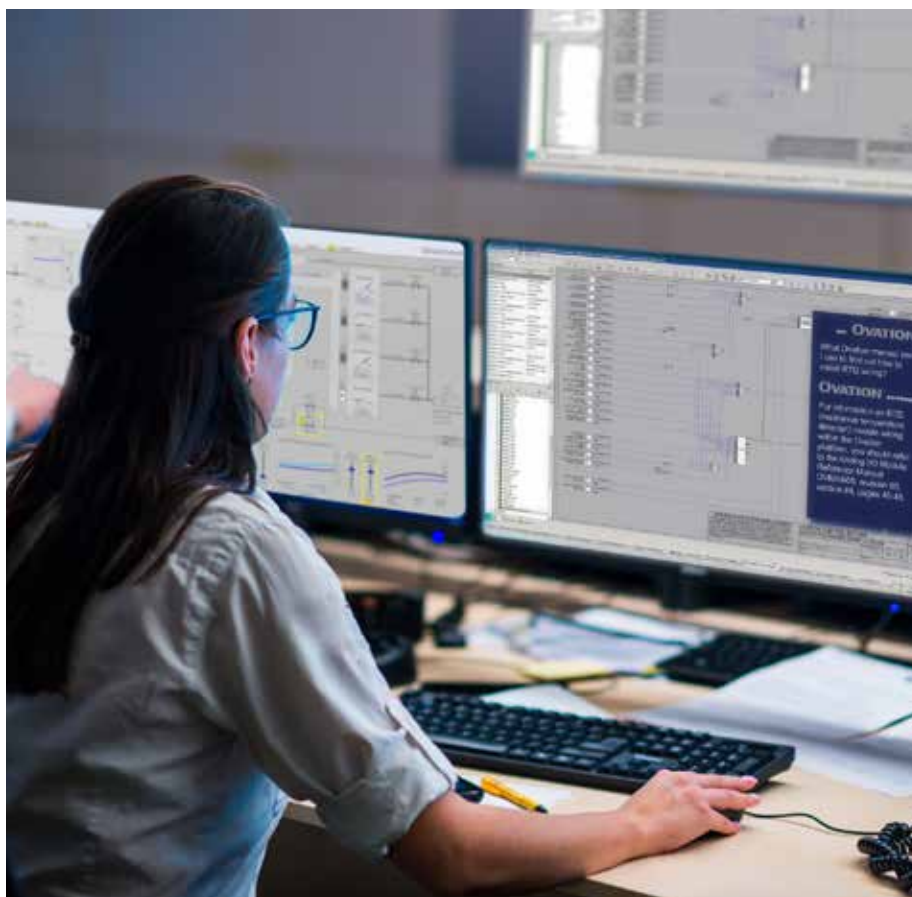
Emerson's Ovation 4.0 Automation Platform with integrated and dedicated GenAI deployment, trained on a secure foundation of knowledge-based data, will augment workforce expertise and thought processes to enhance productivity by prioritizing and automating tasks. The platform will provide predictive guidance and recommend appropriate actions to increase reliability, improve customer experiences and optimize overall operations.

"While global power operators are experiencing unprecedented demands, we are also on the precipice of technological advances that will forever change how we and our customers work," said Bob Yeager, president of Emerson's power and water business.

"The digital revolution is generating so much valuable data that our Ovation Automation Platform with GenAI can harvest to create accessible, usable insights to inform smarter and more timely action."

Through its AI-based capabilities, the new platform will help support:

- **Workforce empowerment:** AI assistants will work side-by-side with operators of every experience level to optimize workflows for more effective operations and help diagnose issues and suggest or implement control actions to return to normal, safe operating conditions.
- **Remote operations:** AI will work in tandem with operators at centralized



Transformative generative artificial intelligence (GenAI) will enhance data to inform decisions, helping power and water companies accelerate growth, improve efficiencies and drive more predictive, reliable and resilient performance.

control centers that monitor multiple assets, acting as autonomous guardians that provide prescriptive guidance to help with information processing and decision support.

- **Reliable, continuous operations:** The Ovation GenAI assistant will predict maintenance requirements, helping mitigate the impacts of common reliability issues such as faulty sensors, mechanical wear, temperature fluctuations and pressure deviations. In addition, real-time digital twin simulation, coupled with AI models trained on plant-specific historic operations and maintenance, will recognize abnormal conditions to identify how and why processes are diverging from baseline operations.
- **Grid optimization:** Facilitated by AI-assisted predictive maintenance, the platform will offer advanced situational awareness that improves decision-making from power generation to delivery, resulting in increased grid stability.

- **Security:** Robust AI models will be used as a tool to enhance cybersecurity by improving threat detection, response automation, vulnerability management and overall security protocols.

Initially released on Microsoft Azure's OpenAI service, the Emerson Ovation GenAI will also be available on other large language models that rely on closed, proprietary and secure data sets.

"Today's most forward-thinking power and water companies will use our new Ovation 4.0 Automation Platform with GenAI to help sort through their vast amounts of data," Yeager said. "By contextualizing data from the intelligent field, edge and cloud to make better, safer decisions, this technology will enable what is called 'Boundless Automation™' – breaking down data silos to liberate data and unleash the power of software."

Emerson

[Learn More](#)

Private 4G/5G network solution

CORE Network and RAN software with ME1310 platform for secure connectivity in harsh environments.

A Kontron and Amarisoft partnership is promoting the use of private 5G solutions for defense and security applications. The integration combines the robust ME1310 Edge platform from Kontron with the CORE and RAN software from Amarisoft. This ensures uninterrupted connectivity reliable in isolated and complex environmental scenarios.

The robust Kontron's ME1310 edge platform is designed for demanding applications and is characterized by an exceptional durability, performance and a reliable operation under the toughest conditions. The platform combines switching and timing for 4G/5G Open RAN networks in a very robust, temperature-independent (-40 °C to +65 °C) Platform that can withstand extreme temperatures, shocks and vibrations. The high processor performance of the ME1310 and the comprehensive connectivity options enable seamless integration and optimal performance.

The platform allows can be easily integrated into the Amarisoft software and offers operators and system integrators benefit significantly in terms of performance, flexibility and Cost efficiency. The purely software-based approach enables high



SOURCE: KONTRON

configurability of Amarisoft Core Network and RAN, allowing adaptation to a wide range of use cases with different TDD patterns, cell bandwidths, number of cells and MIMO levels. They also offer more than 1000 active UEs. New functions can be implemented

within a very short time by installing a software upgrade.

Kontron

[Visit Website](#)

Anybus protocol converter

Protocol converter connects serial devices to EtherCAT, EtherNet/IP, Modbus TCP or PROFINET controllers.

Bosch Rexroth has combined the Anybus Communicator protocol converter with its Smart Flex Effector to offer a highly versatile compensation module.

To enable robots to perform new tasks, the Smart Flex Effector needs to exchange position measurement data with the robot controllers, including information about the deflection of the tool and control signals for the module's locked and unlocked states.

To solve these connectivity challenges, Bosch Rexroth turned to HMS Networks who provided the Anybus Communicator Common Ethernet, a ready-made protocol converter capable of connecting serial devices to EtherCAT, EtherNet/IP, Modbus TCP or PROFINET controllers.

A key benefit of the Anybus Communicator Common Ethernet was that the same unit can connect to all the major Ethernet protocols. The Anybus protocol converter was a solution because it can be reconfigured with a firmware update and provide connections to the wide range of different protocols.

The Smart Flex Effector and Anybus Communicator have worked so well together



SOURCE: HMS NETWORKS

that Bosch Rexroth includes the Anybus Communicator as part of its complete solution. "We decided to create an order number for the Anybus converter, so that customers could buy it directly from us. So, we sell both devices together as a complete

solution," reported David Lehmann, System Architect at Bosch Rexroth.

HMS Networks

[Learn More](#)

Current measuring transducers

Precise measurement: new current measuring transducers with user-guided web-based management.

New current measuring transducers from the ECM UC product family from Phoenix Contact save users plenty of time with the intuitive device configuration via web-based management. The products measure direct, alternating, and distorted currents in four measuring ranges, starting from 0 to 100 mA through to max. 0 to 100 A, with a transmission error of <0.5%. Modbus versions enable the digital further processing of the measured data.

Because the ECM current measuring transducers can be configured via web-based management, cumbersome software downloading is no longer necessary. Here, the device is simply connected to the PC via a standard USB-C cable. During the configuration process, both data transmission and power is supplied to the device via the USB-C cable. An external 24 V DC supply is not required to operate the current measuring transducer.

The intuitive menu navigation simplifies the settings on the device. In addition, the live measured data of the current components, such as the AC and DC currents, can be visualized simultaneously in different windows. The device settings are saved in



SOURCE: PHOENIX CONTACT

a configuration file and can be imported easily to other devices, enabling the rapid commissioning of several measuring transducers with the same configuration.

The current measuring transducers of the ECM UC series measure direct, alternating,

and distorted currents in accordance with the true RMS value measurement principle.

Phoenix Contact

[Visit Website](#)

All-band GNSS antennas

Antenna provider u-blox introduces new all-band GNSS antenna for high-precision applications.

A global provider of leading positioning and wireless communication technologies and services, u-blox, has announced a new external GNSS antenna ANN-MB2 for wide coverage, multi-constellation high-precision applications.

Optimized for the u-blox high-precision GNSS technology, ANN-MB2 is well-suited for industrial automation, surveying, autonomous vehicles, mobile robotics and other applications requiring centimeter-level position accuracy in challenging environments.

The u-blox ANN-MB2 is a compact, high-precision real-time kinematic (RTK) antenna that supports L1, L2, E6/B3, L5, L-band, and all major GNSS systems. This all-band antenna features a robust architectural design, superior multipath mitigation, and versatile mounting options.

With its excellent price-to-performance ratio, ANN-MB2 is suitable for easy evaluation and fast design-in of wide-band high-precision positioning applications, paving the way for mass-market adoption.

ANN-MB2 includes a high-performance,

multi-band, RHCP dual-feed stacked-patch antenna element, a built-in high gain LNA with wide-band SAW pre-filtering, and a 5-meter antenna cable with an SMA connector.

ANN-MB2 engineering samples are

available; production starts in Q4 2024.

u-blox

[Learn More](#)



SOURCE: UBLOX