September/October 2023 138
ISSN 1470-5745

industrial ethernet book

Industrial Ethernet Automation Networking & IIoT

Corporate Profiles

Industrial Ethernet Automation Solutions

Page 35

Industrial Cybersecurity Special Report: 2023 6

Industrial Control with Remote I/O

RIO MM1
Universal I/O

RIO MM2
Universal I/O with Ignition
IgnitionEDGE

RIO EMU
Energy Monitoring

groov® RIO

now with CODESYS and Sparkplug COMPATIBLE

10 Channels of software-configurable I/O:

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

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

Learn more at www.opto22.com.

GET CONNECTED…

Visit our new website at: www.iebmedia.com

Industrial cybersecurity

THE INDUSTRIAL CYBERSECURITY MARKET size was valued at USD 16.3 billion in 2022 and is expected to reach USD 24.4 billion by 2028; it is expected to grow at a CAGR of 7.7% from 2023 to 2028 according to a new report by MarketsandMarkets™. The major factors driving the growth of industrial cybersecurity market are increasing focus on integrating into industrial control systems.

Wireless Security is projected to have largest market size during forecast period.

The industrial cybersecurity market for wireless security is expected to have the largest market size during the forecast period. Wireless intrusion prevention systems (WIPS) or wireless intrusion detection systems (WIDS) are commonly used to comply with wireless security policies.

Factors such as increased use of radio frequency identification (RFID) technology and other wireless communication technologies, easy availability and low-cost accessibility of wireless 4G mobile devices, rise in small office home office (SOHO) trend, and intensified need for SaaS-based wireless security solutions stimulate the growth of the market for wireless security.

Software solutions and services will have the highest growth in coming years.

Professional services and managed services are covered under the industrial cybersecurity market for services. In professional services, risk management is the most prominent service.

In industrial organizations, industrial control systems are designed not only to monitor and control industrial processes but also to manage network and system devices. These systems are now more exposed to cyber threats due to the increased connectivity with third-party service providers, a growing number of network-enabled devices, and enhanced sophistication of security attacks. As a result, the demand for risk management services is growing.

Transportation Systems is expected to have highest CAGR during the forecast period.

The industrial cybersecurity industry for the transportation system industry is expected to grow at the highest CAGR during the forecast period.

To improve performance, the transportation sector has started using advanced technologies, and the systems are being shifted from standalone to newer interconnected systems.

Download MarketsandMarkets™ PDF Brochure: https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=3764676

Al Presher

SCADA is Dead, or is it?: 52

New Products: 60

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **November/December 2023.**
Deadline for editorial: November 13, 2023 **Advertising deadline:** November 13, 2023

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., Box 1221, Fairport, NY, 14450 USA ISSN 1470-5745

Wi-Fi 7 to play fundamental role in how people live and work

Wireless Broadband Alliance report explores how new Wi-Fi 7 technology will transform how people worldwide live, work and play.

SOURCE: ISTOCK

WI-FI 7 WILL ENABLE INDUSTRY 4.0, enterprise, medical, smart city and other applications that are impractical or impossible with other wired and wireless technologies, providing twice the bandwidth and three times the speed of Wi-Fi 6, deterministic network support, and more.

The Wireless Broadband Alliance (WBA) has announced the public release of *Get Ready for Wi-Fi 7: Applying New Capabilities to the Key Use Cases*, a report that explores how this new technology will transform how people worldwide live, work and play.

Based on the IEEE 802.11be (Extreme High Throughput) standard, Wi-Fi 7 has a wide variety of advanced capabilities that will improve existing use cases or enable new ones that are not possible with existing wired and wireless technologies. The 43-page paper, led by WBA members Broadcom, CableLabs, Cisco, and Intel, explores many of Wi-Fi 7's major new capabilities and applications, such as:

Double the bandwidth and three times the speed of Wi-Fi 6

Wi-Fi 7 supports channel widths up to 320 MHz, while Wi-Fi 5 and Wi-Fi 6 are limited to 160 MHz. It also supports 4k QAM, which is an upgrade over prior standards. With wider channels and 4K QAM capabilities, Wi-Fi 7 can deliver speeds over three times faster than Wi-Fi 6. This is critical for enabling whole-home multi-Gigabit Wi-Fi service.

Advanced support for latency-sensitive use cases

Wi-Fi 7 devices can use multi-link operation (MLO) in the 2.4 GHz, 5 GHz, and 6 GHz bands to increase throughput by aggregating multiple links or to quickly move critical applications to the optimal band using seamless switching between links. Fast link switching allows Wi-Fi 7 devices to avoid interference and access Wi-Fi channels without delaying critical traffic. This and other new features also make Wi-Fi 7 ideal for immersive XR/AR/VR, online gaming and applications that require high throughput, low latency, minimal jitter, and high reliability.

Wi-Fi 7 Industry Trials Program

The WBA is actively collaborating with its members to conduct field trials of these technologies in real-life Wi-Fi 7 networks. These trials are open to all interested industry players and are a crucial platform for mobile device and AP vendors, operators, and service providers to collectively test Wi-Fi 7 capabilities in key deployments scenarios.

In these trials, participants will gain invaluable hands-on, real-world insights into deploying Wi-Fi 7 across operator, residential, and enterprise networks. As with its Wi-Fi 6 trials, the WBA will share comprehensive reports that offer indispensable knowledge and serve as a reference for industry stakeholders.

Tiago Rodrigues, President and CEO, Wireless Broadband Alliance, said: "Get Ready for Wi-Fi 7 showcases the revolutionary capabilities that will enable Wi-Fi 7 to help bridge the digital divide and enable new use cases across consumer, business, education, government, medical, industrial, hospitality, public venues and transportation."

Gabriel Desjardins, Director of Product Marketing, Wireless Communications and Connectivity Division, Broadcom, said: "With Wi-Fi 7, business, service providers and smart cities now have a new option for quickly deploying enterprise-grade gigabit broadband outdoors, such as to connect buildings around an office campus, apartment complex or downtown. For example, MLO-enhanced multi-link single-radio (eMLSR) mode enables link redundancy to maximize reliability, while MLO simultaneous transmit and receive (STR) mode with 5 GHz+6 GHz bands can meet demanding enterprise backhaul requirements such as 10 Gbps throughput."

Matt MacPherson, Wireless CTO, Cisco, said: "Wi-Fi has never been a more important technology. Building on the advancements made by the Wi-Fi 6 and Wi-Fi 6E standards, Wi-Fi 7 represents the next big leap towards more deterministic Wi-Fi. The next generation of wireless use cases – AR/VR, autonomous and intelligent vehicles, streaming 4K video – will rely on a trustworthy connection. The Wi-Fi 7 standard will allow Wi-Fi to be that reliable, secure connection that enterprises and service providers need to unlock the next generation of use cases."

Lili Hervieu, Principal Architect, CableLabs, said: "Wi-Fi 7 will provide higher throughput and reliability and lower latency to deliver a better user experience in residential deployments. These three components are also key pillars of the 10G platform developed by CableLabs and the industry. CableLabs is an active participant in the Wireless Broadband Alliance and is looking forward to participating in the WBA Wi-Fi 7 residential field trial to demonstrate the benefit of the technology."

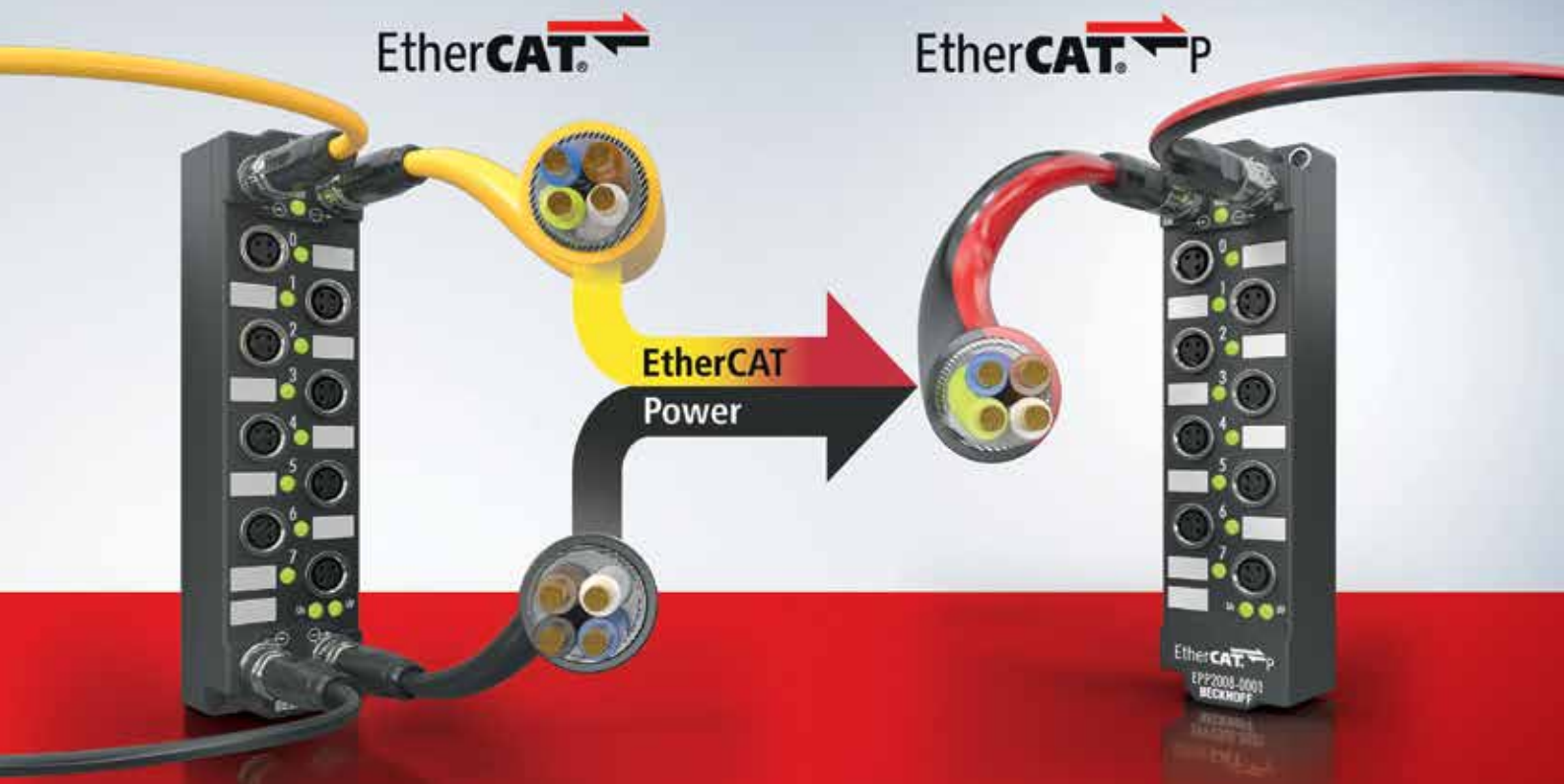
Eric McLaughlin, VP & GM Wireless Solutions Group, Intel, said: "Wi-Fi 7 will deliver another major leap in client device capabilities enabling multi-gigabit speed, lower latency, and more robust and deterministic behavior. It will help accelerate innovation for new applications and use cases which will further enhance user experiences across many segments which include personal computing and IoT. As in the past with Wi-Fi 6 and Wi-Fi 6E technologies, we are looking forward to showcasing amazing real-world benefits with industry partners via future WBA Wi-Fi 7 trials."

*News report by **Wireless Broadband Alliance**.*

Visit Website

EtherCAT P: reduces cabling and costs

Ultra-fast communication and power on one cable



EtherCAT P integrates EtherCAT communication as well as system and peripheral voltage supply in a 4-wire standard Ethernet cable. The I/O system for EtherCAT P with IP 67 protection takes full advantage of EtherCAT P: material and installation costs, as well as the required installation space in drag chains, cable trays and control cabinets are significantly reduced. The compact and robust I/O modules cover a wide signal range, from standard digital I/Os to complex analog and measurement technology.
More than 100 additional components are available for EtherCAT P. Find out more now!

Scan to discover all you need to know about the competitive edge offered by EtherCAT P

New Automation Technology **BECKHOFF**

2023 Industrial Cybersecurity Progress Report

Industrial cybersecurity has become "Job One" for manufacturers to enable secure use of modern IT technologies in industrial networks, and seamless communications between IT, OT and cloud resources that require highly granular security policies based on identity and context for people, devices, and applications.

SOURCE: ISTOCK

"With comprehensive visibility, you can restrict communications between assets by using software solutions creating security policies to segment the industrial network into smaller zones of trust as recommended by the ISA/IEC62443 security standard," -- Andrew McPhee, Solution Architect - Industrial security, Cisco.

INDUSTRIAL CYBERSECURITY HAS BECOME AN overarching, top priority for manufacturing as the move to the Industrial Internet of Things and cloud computing has created an environment where the traditional air-gap approach to security is not sufficient.

In this special report, the Industrial Ethernet Book reached out to industry experts to gain their insights into the megatrends driving Industrial Cybersecurity technology, industry standards and the challenges facing automation engineers.

Adoption of Cloud Services

Driving the need for distributed security architectures and no single points of control.

According to Andrew McPhee, Solution Architect - Industrial security at Cisco, key technology trends and growth of the IIoT are creating a need for new industrial cybersecurity solutions.

"The growing adoption of cloud services for running operational processes is driving the need for distributed security architectures and no single points of control. The traditional air-gap approach to industrial security, enforced by firewalls in the industrial DMZ is still needed but not sufficient," McPhee told the Industrial Ethernet Book recently.

"Enabling secure use of modern IT technologies in industrial networks, and seamless communications between IT, OT, and cloud resources require highly granular security policies based on identity and context, for people, devices, and applications," he said. "This means being able to identify and profile every connected device, as well as local and remote users, and define least privilege access policies for each one of them."

McPhee added that, fortunately, the latest advances in edge computing enables industrial networking equipment to embed software capabilities making automated asset discovery, software-based network segmentation, or zero-trust network access (ZTNA) simple to deploy at scale without the need for dedicated security appliances or additional network resources which would typically raise the cost and complexity of such cybersecurity architectures to unbearable levels.

Impact on manufacturing networks

McPhee added that most industrial organizations do not have comprehensive or up-to-date inventory of connected OT assets. You can't secure or monitor what you don't know. Modern network equipment such as Cisco industrial networking products automatically build and maintain the inventory at scale without any addition to the industrial network. It makes it easier to have the visibility required to build security policies, monitor assets and communications, comply with cybersecurity regulations, and meet cyber-insurance requirements. It is the foundation to a robust OT cybersecurity strategy.

"With comprehensive visibility, you can restrict communications between assets by using software solutions creating security policies to segment the industrial network into smaller zones of trust as recommended by the ISA/IEC62443 security standard. Cisco industrial networking equipment can enforce these policies to prevent unauthorized communications or avoid attacks to spread. This means there is no need to deploy firewalls

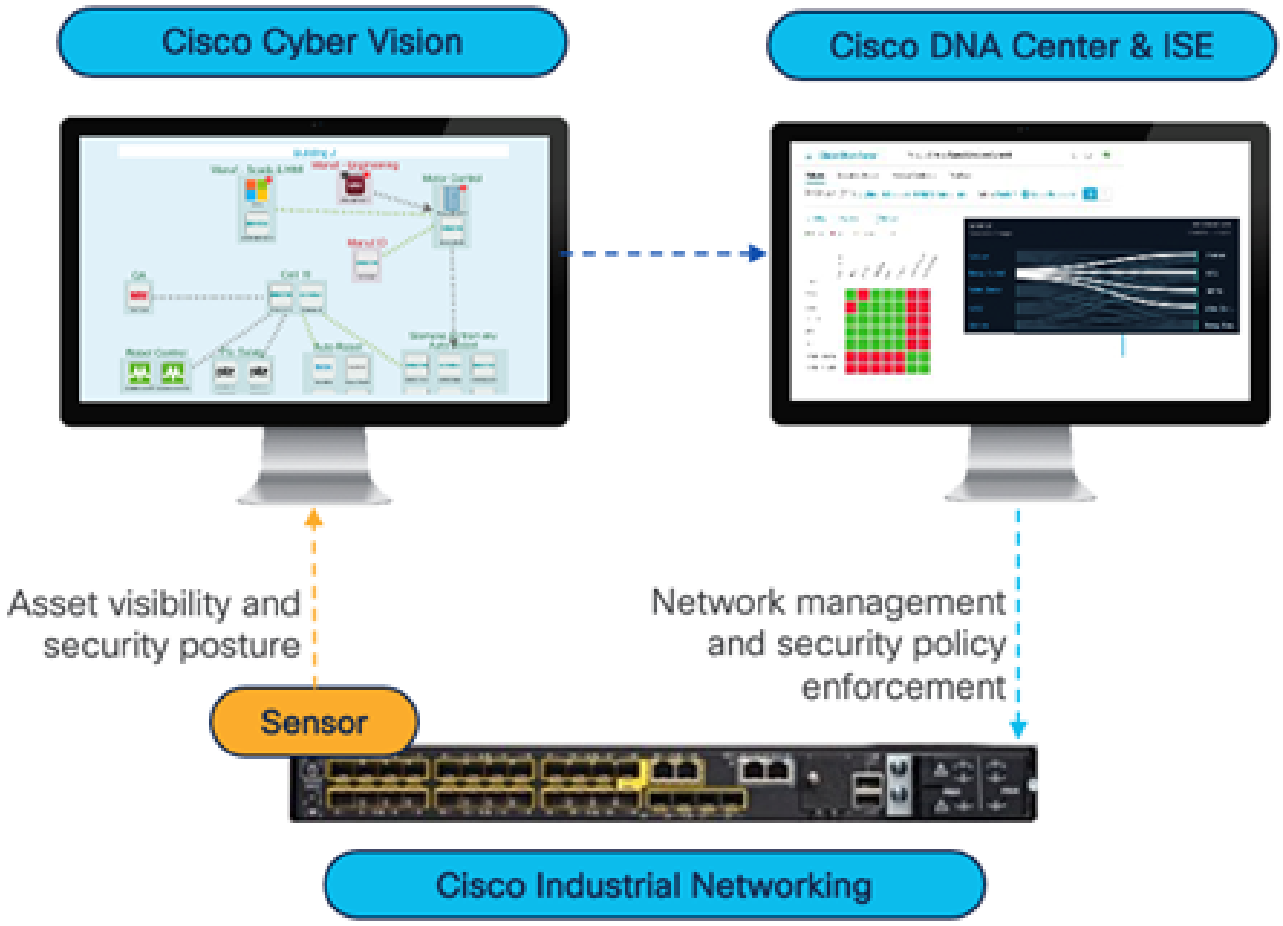
Cyberattacks can happen.

Are you prepared?

Cyberattacks are targeting industrial control and automation systems more and more. The only way to protect your plants and systems with enough security is to use a holistic 360° approach. Phoenix Contact will help you with secure products, services, and industrial solutions.
Let us get prepared together!

For more information on our 360° security concept, visit **phoenixcontact.com/security**

PHOENIX CONTACT



SOURCE: CISCO

Advanced cybersecurity provides tools for asset visibility as well as network management and security policy enforcement.

for zone segmentation, greatly simplifying network setup, as assets move, are replaced, or added"

Similarly, edge computing enables zero-trust network access (ZTNA) to operational spaces. Rather than using 4G/LTE gateways or ad-hoc remote access software that are too complex to control and secure, Cisco industrial networking equipment gives you access to remote OT assets to manage or troubleshoot them. The embedded ZTNA agent provides granular access controls based on identity and context policies with audit capabilities.

Having edge computing capabilities embedded into industrial networking equipment allows to use of the network as the sensor and the enforcer. Eliminating the need to deploy, maintain and power dedicated appliances also drives sustainability and simplicity. It also addresses the skills shortage issue, helping small teams managing advanced infrastructures.

Unique technology resources

McPhee summarized a series of areas where the latest technologies are providing unique benefits and solutions that can be applied in industrial environments.

Segmentation: OT assets should only communicate with resources they need to perform their tasks. In industrial environments the focus is on creating smaller trust zones to prevent malware propagation as recommended by the ISA/IEC-62443 security standards. Solutions such as Cisco Identity Services Engine (ISE) for instance, work with your network switches, routers, and wireless access points to restrict communications as per the zones and conduits you have defined, without having to deploy and maintain firewall appliances within the industrial network. It leverages groups defined by the OT team using the Cisco Cyber Vision asset inventory capabilities to allow/deny communications for each asset. When a change is required, just move the asset to another group in Cyber Vision for ISE to automatically apply the corresponding security policy.

Zero Trust Network Access (ZTNA): Remote access is key for operations to manage and troubleshoot OT assets. Zero Trust Network Access (ZTNA) is the future of remote access architectures. It lets you configure least privilege access based on identity and context: Remote users connect to a cloud portal and have access only to the devices you choose, using only the protocols you specify, only in the time window you allow, and only after they have passed a series of security controls such as multifactor authentication or verification of the computer's security posture. Edge computing allows Cisco Secure Equipment Access to run in Cisco industrial networking equipment to simplify deployment of ZTNA in OT networks at scale.

Specific application areas are also being targeting with the newest Industrial cybersecurity solutions, and contribute to overall network performance. These include:

Network performance: OT visibility solutions such as Cisco Cyber Vision help understand network and configuration issues in addition to malicious traffic and abnormal behaviors. They track all communications to provide operational insights that can help troubleshoot operations.

The move to cloud: As the industrial network uses more cloud services, the attack vector increases, and it is critical to continuously verify trust of remote resources. Security service edge (SSE) solutions help organizations provide secure connectivity between IT, OT, and cloud domains by enforcing granular access controls and security policies. SSE solutions enable security administrators to offload computationally expensive tasks from on-prem hardware to scalable cloud resources and provide centralized policy management which increases network performance and minimizes administrative errors that result in downtime. Combined with visibility solutions, they offer the ability to react to changes in trust upon the discovery of new information.

ANALOG DEVICES

AHEAD OF WHAT'S POSSIBLE™

ADI Chronous™

INDUSTRY-LEADING SCALABLE ETHERNET. TIMED TO PERFECTION.

ANALOG.COM/CHRONOUS

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**

Secure remote access: Historically, 4G/LTE gateways or ad-hoc remote access software have been deployed, making it nearly impossible to enforce security controls. These shadow IT solutions must be identified (using the visibility capability of the industrial network) and replaced with a secure solution. Zero-trust network access (ZTNA) built into industrial networking equipment makes it easier to enforce granular access controls.

"New OT cybersecurity solution provides network telemetry and visibility into asset that operations team can leverage to identify device misconfigurations, unexpected changes to industrial processes and overall equipment effectiveness (OEE)," McPhee said.

He added that using edge computing capabilities built into industrial networking equipment to benefit from visibility, segmentation and secure remote access drives cost reduction, simplicity, and agility. Fewer appliances and network resources to deploy and manage means lower CAPEX and OPEX. It is also much easier to deploy and operate at scale, helping OT teams run advanced facilities even if they cannot find new skilled personnel to hire.

"Implementing such visibility solutions also helps IT and OT teams gain a factual understanding of the situation and facilitate effective collaboration between both teams. In turn, this will generally lead to proactive vulnerability management, network segmentation projects, and events monitoring which are regulatory requirements in many industries," McPhee said. "Even insurance companies can require these OT cybersecurity best practices to be implemented to provide cyber insurance."

SOURCE: ISTOCK

"Creating zones and conduits within an application will minimize the likelihood of a successful attack by creating multiple layers of protection against an attack vector," Barry Turner, Technical Business Development, Red Lion.

Creating zones and conduits

New segmented sections within the application represent a new layer of defense.

"Many industrial controls engineers are benefiting from creating zones and conduits to create more segmentation within their industrial applications," Barry Turner, Technical Business Development at Red Lion, told IEB.

"These new segmented sections within the application represent a new layer of defense. As part of a Defense in Depth strategy, customers are creating multiple layers between key assets and would-be hackers. Grouping key resources for speed with an added benefit of access control in and out of this segmented section of the network, which is known as a zone," he added.

Turner said that the biggest hurdle to overcome in implementing this is making changes to the network components themselves. Using network segmentation solutions like Red Lion's RA10C, users can create segmented portions of their network without making changes to the existing network components. So, there is no need to change the IP address of the 10-year-old PLC that is working perfectly fine just to increase security on the plant floor. Using the RA10C in bridge mode makes this possible.

New solutions, technology benefits

"Creating segmented areas within a plant floor must be done with extreme care to avoid interrupting the speed requirements of the industrial devices on the floor. It is crucial to keep PLCs and the devices they directly control within one zone or segmented area of the network to ensure the most reliable network and application," Turner said.

"When data needs to leave the zone, it will take a conduit or path out through a firewall or router. These conduits provide access control, offering users the ability to allow or disallow traffic as well as log activity. Using a solution like the RA10C, users can create segmentation without making changes to the network components already in production. Therefore, there is no need to change the IP address of the PLC or VFD that has been running for years. Simply place the RA10C in the application in bridge mode and use the firewall to graphically allow or disallow traffic," Turner said.

Zones and conduits

The concept of zones and conduits has been around for a while but Turner said it is just now being implemented in industrial applications. This concept is covered quite extensively in the ISA 62443 standard, as it is something IT has been using for a while now. The limiting factor in implementing this type of solution is the fear of making changes to the network that jeopardizes the uptime of the application.

Making a change to the PLC that has been running without fail for many years is not something a controls engineer takes on lightly. Traditionally, to implement zones and conduits, one would need to create a new VLAN, change the IP addresses of the newly segmented devices, create a route for the new segment, and perform some type of access control. Red Lion's RA10C makes this much easier, faster, and without the risks. Users using the RA10C in bridge mode do not need to change the IP address of the devices or create VLANs. They simply put the device in line, and the graphical firewall makes it easy to decide which devices should communicate and which ones should not. This segmentation creates a layer of security without negatively impacting downtime.

Industrial cybersecurity solutions

"As a controls engineer, one needs their application to run smoothly without interruption. The best way to ensure that is to keep the application safe from would-be attackers. Creating zones and conduits within an application will minimize the likelihood of a successful attack by creating multiple layers of protection against an attack vector," Turner said.

"A factory floor using a flat network has one large attack vector, which is the single VLAN or subnet the process is running on. If an attacker gains access to that one network segment, they will have some access to the entire application. Breaking the plant floor into smaller segments will limit the potential success of a hacker or malicious software. Then, utilizing conduits with access control and logging will enable the ability to control traffic and alert if things are out of the norm."

IIoT increases network exposure

Industrial cybersecurity requires state-of-the-art security patch management, intrusion monitoring, and security logging capabilities.

"The increasing professionality of cybercriminals has led to the creation of convenient toolkits that make attacks of all kinds – e.g., denial of service, data theft, and extortion – more likely because many front-line attackers do not need to have deep technical knowledge to successfully use these toolkits," Georg Stöger, Director Training & Consulting at TTTech Industrial, told IEB.

"Advances in AI make super-convincing impersonation and phishing attacks more likely. Therefore, industrial cybersecurity requires state-of-the-art security patch management, intrusion monitoring, and encompassing security logging capabilities," Stöger added.

Stöger said that, although emerging quantum computing encryption mechanisms sound exciting, the major security challenges in industrial systems are not related specifically to broken encryption of data transmissions. Rather it is the wide range of technical and organizational weaknesses in heterogenous, networked control and management components across all layers of the automation pyramid which makes hardening the industrial system against cybercrime so difficult.

"Therefore, we recommend not to look for a specific technology solution first, but rather to adhere to standards for secure design and operation of industrial control systems, Stöger said.

Major security challenges

A major security challenge for manufacturing systems is the trend toward Internet of Things, which not only increases network exposure but also brings a lot of new software to the industrial edge. Solutions for industrial cybersecurity must therefore address not only network security but also software management, specifically patch management.

Stöger said that security patches related to vulnerabilities of any component in the plant need to be identified based on the system's Software Bill of Material (SBOM) and installed in the shortest possible timeframe - certainly within days, not months or years after becoming available. This applies both to the application software and the underlying operating systems. Ideally, such patch management should be supported with minimal or no downtimes, although sometimes a reboot of controllers may be unavoidable after installing some OS security patch. This helps to avoid two worst-case examples of how software security management might be performed: either by shutting down production to check for, and apply, patches and updates for each component in the system – or to skip software security management altogether.

Beyond network-based security

Advanced industrial cybersecurity goes beyond network-based security and user-based authentication; it needs to address all areas of system security including:

- user and component/device identification and authentication (using device certificates);
- maintaining and enforcing access restrictions;
- enhancing and checking system and software integrity and authenticity;
- keeping data secure during use, during communication, and even when taking a component out of service;
- protecting the industrial system against service degradation and denial of service;
- and providing robust event logging and timely analysis of unusual events to ensure that countermeasures are initiated in case of a security incident.

This list indicates that more than one technology will be required to achieve good cybersecurity for a complex industrial system and that the application of these technologies in a specific system and situation cannot easily be described in a generic way. The good news is that for most common threats, comprehensive technical and/or organizational solutions exist. They are sometimes cumbersome

to implement properly, and cutting-edge solutions will simplify this as much as possible.

Security at the industrial edge

"Industrial cybersecurity solutions for manufacturing and discrete automation systems provide enhanced security measures at the industrial edge where data is generated," Stöger said. "They offer real-time threat detection, local access controls, and network segmentation, helping to safeguard critical processes against cyber threats. Edge security solutions ensure data privacy through anonymization and aggregation, while also enabling real-time patching and integration with legacy systems. With scalability and support for heterogeneous systems, the newest edge cybersecurity solutions are well-suited for diverse manufacturing operations. By focusing on local threat detection, access controls, and compliance, these solutions contribute to secure, resilient, and efficient manufacturing processes."

In addition to discrete automation, advanced cybersecurity solutions addressing IIoT and industrial edge security requirements are seeing increased adoption in process automation, transportation and infrastructure systems, and energy production and utilities. As these application areas are becoming more connected, the paradigm of a well-defined security perimeter is getting challenged, and more "zero trust" elements need to be included in the system security architecture.

Challenges for plant personnel

Stöger said that industrial cybersecurity addresses challenges including cyber threats, data privacy, system disruptions, legacy systems, interconnected networks, supply chain risks, human errors, regulatory compliance, remote access vulnerabilities, and incident response. As automation systems become more interconnected and reliant on digital technologies, the risk of cyberattacks, data breaches, and operational disruptions increases and must be addressed consequentially and systematically by automation engineers.

"Industrial cybersecurity involves implementing measures such as network segmentation, encryption, access controls, and intrusion detection systems to protect critical infrastructure and manufacturing processes," he said. "It also focuses on training personnel, securing remote access, and complying with regulations. By integrating cybersecurity into automation design, implementation, and maintenance, industrial cybersecurity mitigates these challenges and ensures the integrity, availability, and security of industrial systems."

To address cybersecurity effectively, engineers need comprehensive knowledge of cybersecurity principles for industrial control systems (ICS). Proficiency in programming languages, risk assessment, incident response, and regulatory compliance is essential.

"Effective communication, problem-solving abilities, and a commitment to continuous learning are vital for collaborating with teams, addressing vulnerabilities, and staying current in this evolving field. An ethical approach, ideally combined with relevant cybersecurity certifications enables engineers to design, implement, and safeguard secure automation systems against the complex challenges of cybersecurity," Stöger concluded.

SOURCE: ISTOCK

"Advances in AI make super-convincing impersonation and phishing attacks more likely. Therefore, industrial cybersecurity requires state-of-the-art security patch management, intrusion monitoring, and encompassing security logging capabilities," Georg Stöger, TTTech Industrial.

Digitalization driving new security solutions

Significantly enhanced state-of-the-art security capabilities required to protect plant networks successfully.

"The main driver for industrial cybersecurity is digitalization, as it requires and enforces new security solutions. Everything gets connected and becomes part of the IoT including the formerly mostly isolated automation systems," Franz Köbinger, Marketing Manager Industrial Cybersecurity for Siemens Digital Industries, told IEB.

"But this also increases the surface for cyber-attacks and therefore automation systems and industrial networks need significantly enhanced state-of-the-art security capabilities to protect them successfully against the new cyber-threats."

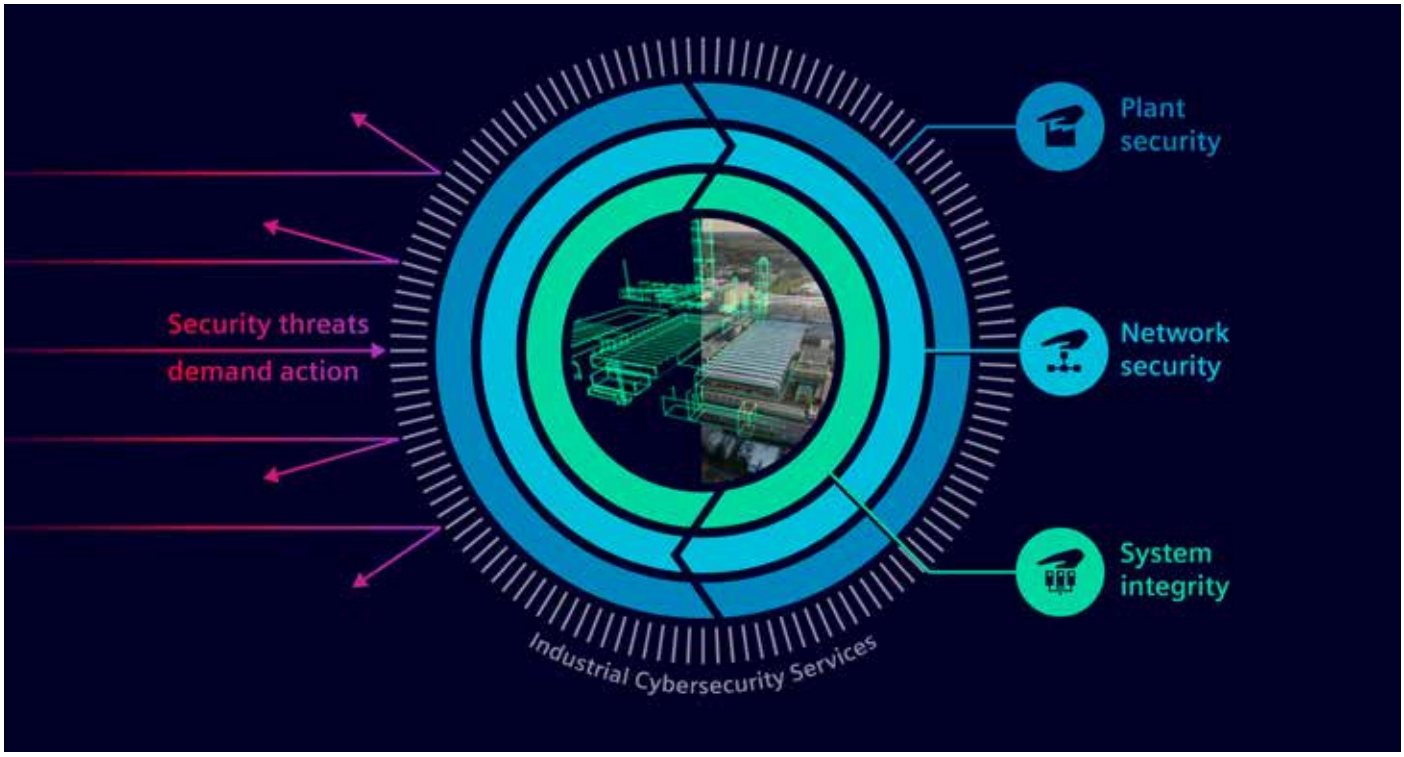
Köbinger said that this means, for example, that unprotected communication will be replaced with protected protocols and security features like user management and access protection become mandatory for automation systems.

He added that this is the reason for new upcoming or tightened security regulations like the NIS 2 directive in the EU, which will

SOURCE: SIEMENS

State-of-the-art security capabilities are protecting automation systems against the new cyber-threats.

SOURCE: SIEMENS



"Specific benefits can be created when new solutions for industrial cybersecurity are based on integrated security features and functions from OT components and automation system," Köbinger said," if the vendors of these products consider the 'Security by design' and 'Security by default' principles, users get already hardened and secure products out of the factory," Franz Köbinger, Marketing Manager Industrial Cybersecurity for Siemens Digital Industries.

become mandatory also for industrial plants in October 2024. To comply with this, it is not necessary to invent new security technologies, but the proved and state-of-the-art security technologies which are used already in IT need now also to be applied and integrated into OT components and networks. But as OT has other conditions and requirements than the Office-IT, this needs to be done by experts, who understand the challenges in the OT, but also how to apply the latest cybersecurity technologies.

Industrial cybersecurity innovations

"Specific benefits can be created when new solutions for industrial cybersecurity are based on integrated security features and functions from OT components and automation system," Köbinger said," if the vendors of these products consider the 'Security by design' and 'Security by default' principles, users get already hardened and secure products out of the factory."

In this way, the risk of wrong configuration and incorrect operation is reduced, the usability is better and the effort is lower as the security functions are already activated or pre-configured. Of course, it is also necessary to keep the products secure during operation. As vulnerabilities and exploits are unavoidable, vendors need to provide security updates quickly and reliably. A vulnerability management helps to detect and to apply necessary security updates.

Köbinger said that the impact on manufacturing networks is that the networks are no longer alone responsible for the protection of production sites and automation systems. This is the pre-condition to open the networks and connect OT with IT, Internet and IoT, which is a must-have for the digitalization. This can be achieved with the same or an even better protection as this concept is based on the defense-in-depth principle, which means there is not only one security layer, but more in place.

"One example is the secured communication. While it is very common in IT environments to use secure protocols, many OT devices still lack these capabilities," Köbinger said. "In this context, TLS (transport layer security)-based communication, which is used to protect the data transfers between automation systems, engineering station and HMI enhances the protection of the transferred data tremendously."

Additionally, and with respect to IT/OT convergence, user management and access

SOURCE: SIEMENS

As OT has other conditions and requirements than the Office-IT, this needs to be done by experts.

control gets also more and more important for automation systems. Most of the automation systems have already a local user management, but this is not practicable for large plants with many different systems. Because if there is a change of a user or access rights it must be changed locally in every other system. But if there is a connection to a central user management (e.g. active directory) the changes need to be made there only once.

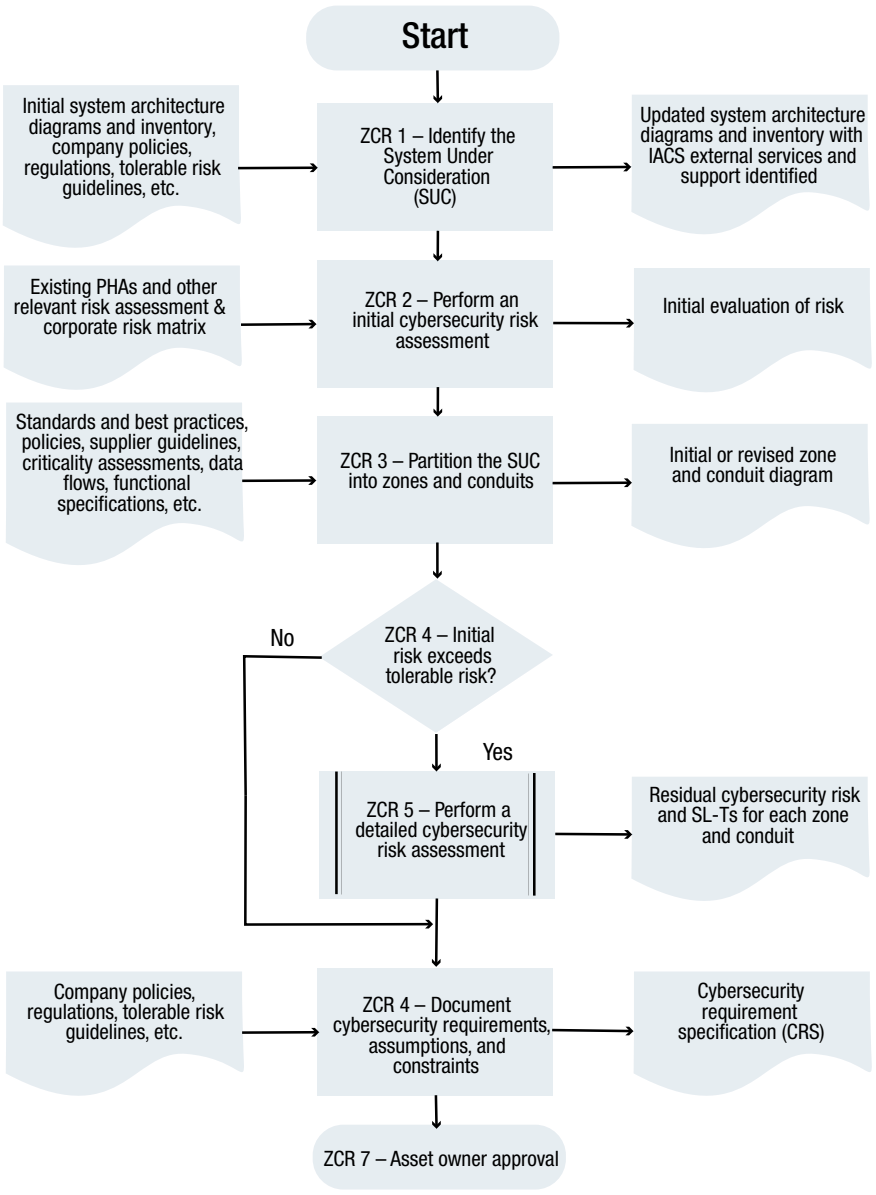
Targeted application areas

Köbinger said that the newest industrial cybersecurity solutions aim to improve the protection of automation systems through access control, encrypted communication, vulnerability management and endpoint protection as well as to improve the network security through anomaly detection, secure remote access, secure OT/IT data exchange and end-to-end OT/IT security based on Zero Trust principles. The overall network performance should not be affected significantly by these measures. Most of them are already used and proven in an IT environment.

"Automation engineers are responsible for a trouble-free operation of their production plants. To avoid disturbances, plant standstills, data and production loss, industry espionage or sabotage a comprehensive cybersecurity concept must be in place, which also includes the protection of automation systems," Köbinger added.

"A challenge could be, that automation engineers may not be security experts and do not know exactly, what measures need to be applied or how they have to be configured to operate correctly. In these cases, an automation engineer can be supported by providing a configuration support (e.g. security wizard), which explains all available security functions, suggests settings and security features are already pre-configured and must not be forgotten," he added. "In addition, security trainings or security assessments can also be useful for automation engineers to address the new challenges of industrial cybersecurity."

ISA/IEC 62443 Risk Assessment Process



SOURCE: ISA/IEC

"We are in the age of 'pervasive AI,' and businesses in all sectors are capitalizing on the advantages of AI in all areas of their business, from generative design to process optimization and even employee safety. The importance of AI in cybersecurity becomes increasingly critical as we transition into a more interconnected and data-rich world," Scott Pepper a member of the International Society of Automation (ISA) and Sector Head for the Process Instrumentation & Control sector at GAMBICA

Security Drives Innovation

Connected technologies brings cybersecurity risk and need for effective solutions.

"The common thread among technological advancements benefiting manufacturing is connectivity. However, this connectivity also brings cybersecurity risks. Therefore, it's fair to say that the widespread adoption of connected technologies is a primary driver for the development of cybersecurity solutions," Scott Pepper a member of the International Society of Automation (ISA) and Sector Head for the Process Instrumentation & Control sector at GAMBICA, the UK's trade association for instrumentation, control, automation and laboratory technology, told IEB. "In this context, the need for security drives innovation, as the saying goes, 'necessity is the mother of invention'."

Areas of innovation

Pepper cited a series of the key trends that are specifically exciting in terms of cybersecurity solution developments and how they can be applied to modern manufacturing:

Artificial intelligence

"We are in the age of 'pervasive AI,' and businesses in all sectors are capitalizing on the advantages of AI in all areas of their business, from generative design to process optimization and even employee safety. The importance of AI in cybersecurity becomes increasingly critical as we transition into a more interconnected and data-rich world. AI-driven algorithms can continuously monitor network traffic and identify anomalies,

SOURCE: ISTOCK

The expansion of edge computing brings about cybersecurity concerns, potentially introducing vulnerabilities into networks, so expect new edge cybersecurity solutions and edge computing to evolve in tandem.

detecting cyber threats and responding in real time," Pepper said.

Applied AI in the form of machine learning can help enhance threat intelligence, enabling models to predict future cyber threats based on historical data and emerging trends, allowing businesses to proactively address vulnerabilities before they are exploited.

Quantum computing

While quantum computing is still in its relative infancy, the immense processing power it could offer can potentially break widely used encryption methods in a matter of hours or minutes.

To counter this, quantum-resistant cryptography is emerging, which employs algorithms designed to withstand quantum attacks. Post-quantum cryptography is being developed and tested to protect sensitive data in the quantum era, where traditional cryptographic methods may become vulnerable.

Edge computing

While not necessarily an enabler, edge computing deserves recognition as a technology that is spurring the development of new cybersecurity solutions. Edge computing brings data processing closer to the source of data generation, (typically at or near the "edge" of a network), shifting processing and decision-making tasks from central locations to local devices or edge servers.

Edge computing offers notable advantages, including the capacity to harness advanced analytics, deliver lower-latency control, and enhance bandwidth efficiency. Nonetheless, the expansion of edge computing brings about cybersecurity concerns, potentially introducing vulnerabilities into networks, so expect new edge cybersecurity solutions and edge computing to evolve in tandem.

Cybersecurity benefits

"Enhanced cybersecurity is an indispensable enabler of technological advancement across all sectors. For manufacturers, it serves as the foundational cornerstone for embarking on their digital transformation journey with confidence," Pepper said.

He added that emerging technological innovations offer the potential for substantial benefits, including reduced downtime, increased productivity, cost savings, innovation, elevated customer trust, and long-term sustainability. However, these benefits remain unrealized if a foundation of trust in security is not in place.

"Cybersecurity serves as the guardian of this trust by safeguarding manufacturing systems, digital assets, and sensitive data from threats and vulnerabilities. As such, new solutions bringing about improved cybersecurity allow manufacturers to harness the full potential of emerging technologies, making them a crucial aspect of modern manufacturing," Pepper added.

Cutting edge solutions

Pepper said that cutting-edge cybersecurity technologies are able to rapidly detect and

SOURCE: ISTOCK

As companies advance in their digital transformation efforts, the demand for improved cybersecurity solutions becomes critical. Many industrial facilities are "brownfield sites" which have been in operation for a while so the first step in this journey involves understanding the potential risks, especially in operational areas where cybersecurity concerns may not have received adequate attention in the past.

respond to threats and mitigate risks in real-time, they are able to effectively evolve over time to safeguard sensitive data and systems against increasingly sophisticated threats, and they strive towards ease of deployment and upkeep.

As Pepper discussed previously, AI-based cybersecurity solutions effectively handle most current threats. However, attackers are also harnessing AI for more targeted and nuanced attacks. The ability of AI solutions to adapt to these and other unforeseen cybersecurity risks places them at the cutting edge. While being on the cutting edge offers the highest level of security, it may not always be necessary for many manufacturing sites.

Employing a risk-based approach – such as that outlined in the ISA/IEC 62443 3-2 standard developed by the International Society of Automation – is vital to ensure appropriateness for specific needs and circumstances. This includes an ability to:

1. Assess the risk to the facility in terms of consequence to the organisation.
2. Define the security level (SL) appropriate to that level of risk.
3. Map the security requirements for that level of risk to the environment's technology and identify gaps.
4. Review cybersecurity solution capabilities against the gap assessment.

When considering cutting edge solutions, it is essential to assess:

1. How realistic are the claims?
2. Does the gap assessment require the new features offered?
3. What is the risk/reward assessment for choosing a cutting-edge solution against a proven, but perhaps less capable solution?
4. What is the total lifecycle cost for the cutting-edge solution, especially considering the long-term maintenance requirements?
5. Is the underlying technology proven, or is there a possibility that it could become obsolete, requiring a replacement solution?

Specific application areas

Pepper said that, as companies advance in their digital transformation efforts, the demand for improved cybersecurity solutions becomes critical.

Many industrial facilities are "brownfield sites" which have been in operation for a while so the first step in this journey involves understanding the potential risks, especially in operational areas where cybersecurity concerns may not have received adequate attention in the past. There is no one-size-fits-all solution for addressing cybersecurity concerns at any site. Therefore, it's crucial to view solution providers as partners in crafting a comprehensive cybersecurity strategy.

"Industrial cybersecurity solution providers can assist in thoroughly assessing an entire system for specific vulnerabilities and security risks, and an essential part of this process involves understanding the hardware and software bills of materials (HBOM/SBOM)," Pepper said. "These documents provide a detailed breakdown of the technical components that comprise today's Industrial Automation and Control Systems (IACS). This understanding is critical for quickly identifying and addressing technical vulnerabilities within a manufacturing environment."

These vulnerabilities can then be mitigated by developing effective business processes, fostering a culture of cybersecurity, and implementing the appropriate technologies.

Challenges facing automation engineers

Pepper concluded by stating that "the modern automation engineer is responsible for an incredibly diverse range of technology, from PLC and Fieldbus I/O, through virtualised HMIs and servers, to historian and advanced analytics software for condition monitoring."

"The technical and procedural vulnerabilities in these complex environments are almost impossible to manage without modern cybersecurity solutions. The modern automation engineer requires solutions that can help them identify and prioritize cybersecurity issues," he said.

Effective Cybersecurity Standards

Zero trust security and single sign-on infrastructure and services.

Randy Armstrong, Chair of the OPC UA Security Working Group, told the Industrial Ethernet Book that the major trends in new industrial cybersecurity solutions are:

1) Emergence of industrial devices and applications that support standards for zero trust security infrastructure. These allow factory owners to reduce the impact of security breaches by ensuring each device only has access to resources it needs to do its job.

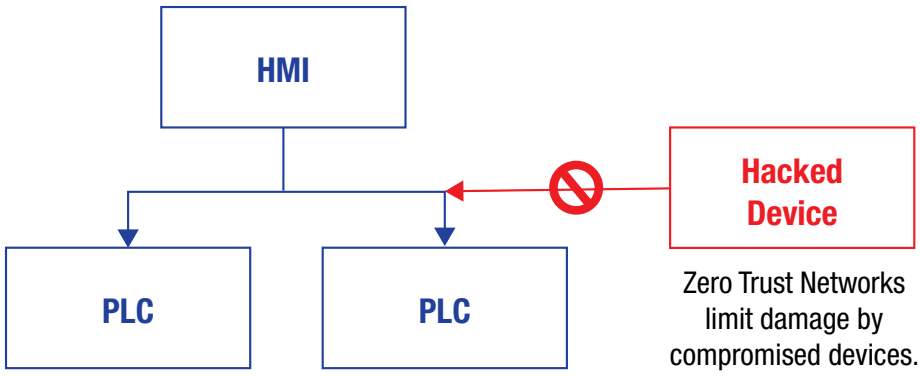
2) Standards for single sign on infrastructure that can be implemented in industrial devices. These standards allow factory owners to eliminate the need to store passwords on devices which often become a huge vulnerability when a password is acquired by a malicious actor. They also allow the use of factory specific roles to determine what rights are assigned to a user which means users can be added or removed from the system without affecting the configuration of individual devices.

3) Standards for onsite services to manage the zero-trust security infrastructure. These services allow the factory owner to retain control over their networks even if external connections are blocked and to reduce the risk that a compromised IT network could allow access to the factory network. More importantly, these services ensure the factory stays secure by automatically updating device security configuration when requirements change.

Benefits for factory automation

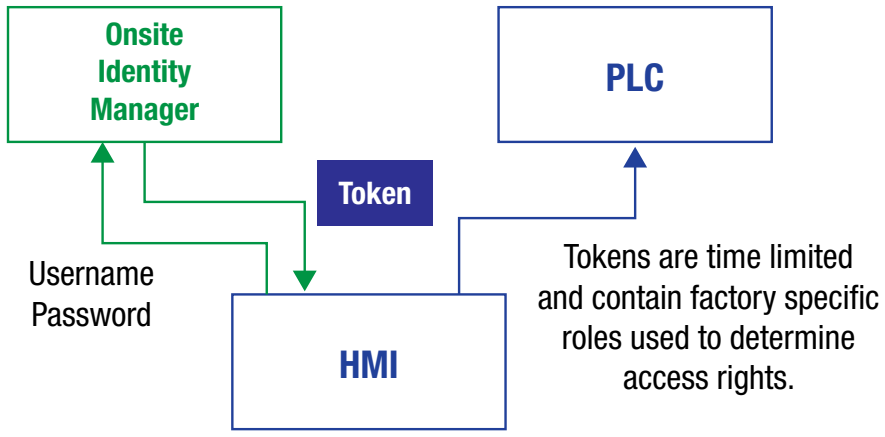
"The new solutions allow factory owners to better protect against cybersecurity threats which can often arise from within the factory network via compromised devices or employees," Armstrong said. "These solutions ensure the factory owner maintains control over their networks and does not require that they depend on cloud or enterprise services while being able to benefit from the standards that the cloud/enterprise services use."

Armstrong said that today most factories are kept secure by physically isolating their networks. If passwords are used to authenticate devices the passwords are fixed and never changed even if an employee leaves the company. While this model does provide some security the protection fails completely once an attacker is able to access the factory network. The new cybersecurity technologies provide another layer of protection that limits the damage that an attacker can cause even when they gain access to the network. The new cybersecurity solutions also benefit all types of industrial automation applications.

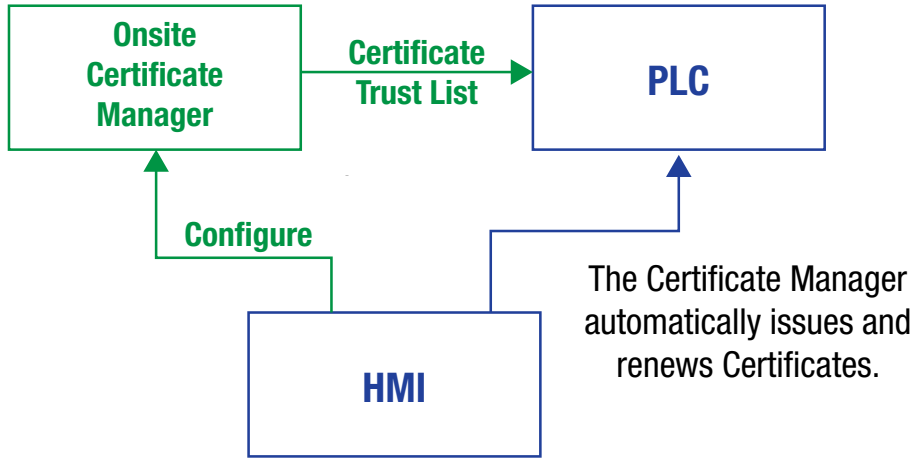


SOURCE: OPC FOUNDATION

Emergence of industrial devices and applications that support standards for zero trust security infrastructure.



Standards for single sign on infrastructure that can be implemented in industrial devices.



Standards for onsite services to manage the zero-trust security infrastructure. These services allow the factory owner to retain control over their networks even if external connections are blocked and to reduce the risk that a compromised IT network could allow access to the factory network.

Effective system implementation vital to success

"Automation engineers know that deploying secure systems is a requirement for their job today but configuring and maintaining secure systems is a challenge," Armstrong said. "Automation engineers need open standards that not only provide protocols that ensure the integrity of their devices but make it possible to manage the security configuration for networks of devices provide by different vendors."

*Al Presher, Editor, **Industrial Ethernet Book***

Cybersecurity protects clinical trials

Manufacturing medicines for clinical trials is a complex, lengthy, and costly process. As the global demand for medicine continues to grow, the pressure is on for the pharma industry to produce in ever-quicker cycles.

SOURCE: SIEMENS

Collaborative innovation will ultimately benefit patient health (copyright: CPI).

THE MEDICINES MANUFACTURING INNOVATION Centre in the UK was conceived to relieve this pressure. "We operate a model in which the pharmaceutical industry and its supply chain work together to identify and overcome major industry hurdles, or Grand Challenges, to reduce the time, resources, and cost of medicines manufacturing – to ultimately deliver benefits to patients," explains Dave Berry, Head of Digital Business Systems, at CPI's Medicines Manufacturing Innovation Centre.

The Medicines Manufacturing Innovation Centre is a collaboration led by CPI. Its mission is to safeguard UK's place as a technology and innovation leader in pharmaceutical manufacturing. The center will initially focus on translating technology for small molecule drug manufacture. With a collaborative innovation culture and state-of-the-art facilities, the new facility allows industry, academia, healthcare providers and regulators to work hand-in-hand to address challenges and maximize technology opportunities in the supply of medicines.

CPI, headquartered in Wilton, Redcar, UK, is a pioneering social enterprise that accelerates the development, scale-up and commercialization of deep tech and sustainable manufacturing solutions.

Through their incredible innovation experts and infrastructure, CPI looks beyond the obvious to transform healthcare and drive towards a sustainable future. CPI brings together pharma giants including GSK and AstraZeneca, the University of Strathclyde, UK Research and Innovation and more than 25 technology companies to fast-track clinical trial manufacturing. As a result of this collaboration, Siemens technologies – from the Digital Twin to industrial automation, to Cybersecurity – now ensure seamless digital processes and a secure Digital Enterprise.

Industry problems, digital solutions

As a greenfield site, the center is leveraging the potential of the Digital Enterprise to tackle these challenges. Fully integrated best-in-class technology from Siemens was deployed. The Digital Twin created with Tecnomatix Plant Simulation, for example, allows pharma companies to implement the automation module that they need, to conduct tests, and avoid bottlenecks. "Modeling allows us to stay within tight specifications," Dave Berry says. "From a Grand Challenge perspective, we are reducing waste."

SOURCE: SIEMENS

Automation technology is key to reducing waste (copyright: CPI).

A paperless Opcenter Execution Pharma – a manufacturing execution system (MES), automation and enterprise resource planning systems in one – informs personnel how and when to execute each step, likewise speeding up the process to real-time release, while ensuring full compliance.

Secure automation

Siemens' industrial automation system was applied to all layers, from the demilitarized zone (DMZ) and network to the MES down to the control level. The Simatic RTLS (real time location systems) tracks materials, cutting down the time needed to locate parts and objects, and optimizing inventory.

Deploying Simatic controllers with integrated security functions and the Totally Integrated Automation Portal (TIA Portal) opens the doors to comprehensive digital automation services and forms the basis of a secure IT/OT (operational technology) environment.

Fully integrated, defense in depth security approach

At Medicines Manufacturing Innovation Centre, where there's the potential to manufacture clinical trial batches all the way down to the individual level, security is paramount.

Protecting personal and company data in this era of cyberattacks is crucial. "Siemens' Defense in Depth security approach provides comprehensive and extensive protection on three levels – the plant, the network, and the system – leading the way to a secure Digital Enterprise," comments Michael Metzler, Vice President, Horizontal Management Cybersecurity for Digital Industries at Siemens.

A Scalance-based security architecture, including Scalance W for wireless, was deployed all across the center's operational technology network. A customizable Mendix-based dashboard allows Qualified Persons (QP) – who are authorized to legally certify medicines to market – to access information quickly and flexibly. The secure, integrated IT/OT network delivers information from the manufacturer back to the QPs, allowing them to legally release a batch in real time.

Compliant to EU and UN standards

Siemens' cybersecurity approach complies with both the UN-endorsed IEC 62443 standard and the new NIS 2 EU cybersecurity directive. Siemens Industrial Cybersecurity Services conducted special trainings for the center's employees to increase awareness.

Optimizing sustainably into the future

With its operations secure, the team at the center can focus on swiftly optimizing. "To improve really quickly, what we have to do is create a lot of waste. By automating and digitalizing processes, we can reduce that waste," adds Dave Berry.

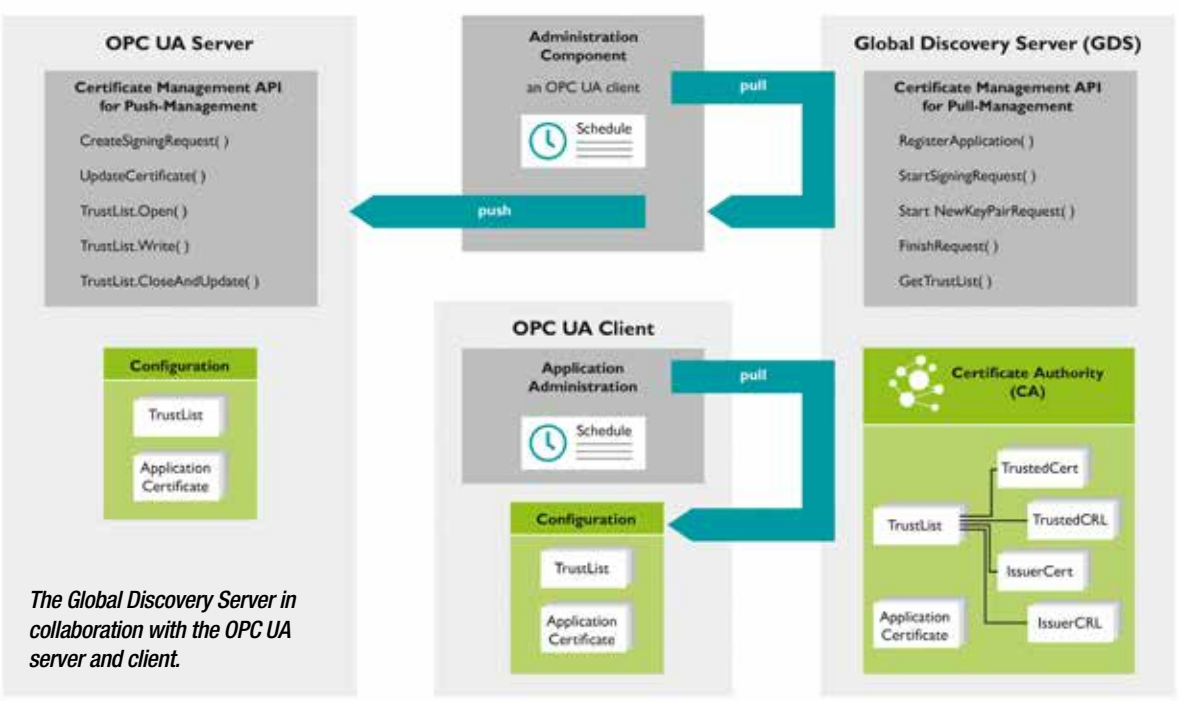
"From a sustainability perspective, what we can't do really very well as an industry yet is look at Scope Three Carbon Emissions. By creating a bubble where we readily and rapidly understand digitally what's happening in Scope One and Two, it enables us to work out the best methodology for implementing Scope Three within the pharma industry. I'm really excited about working with Siemens to help get that done," Berry concludes.

Ben Caley, Product Manager - Industrial Communication and Cyber Security, ***Siemens Digital Industries Process Automation.***

Learn More

Easier identification, management and security for OPC UA devices

Dynamic certificate management with the OPC UA GDS can be developing using a Device and Update Management system. The OPC UA information model enables new processes to be set up efficiently between a controller and any higher-level, business-oriented software layer.

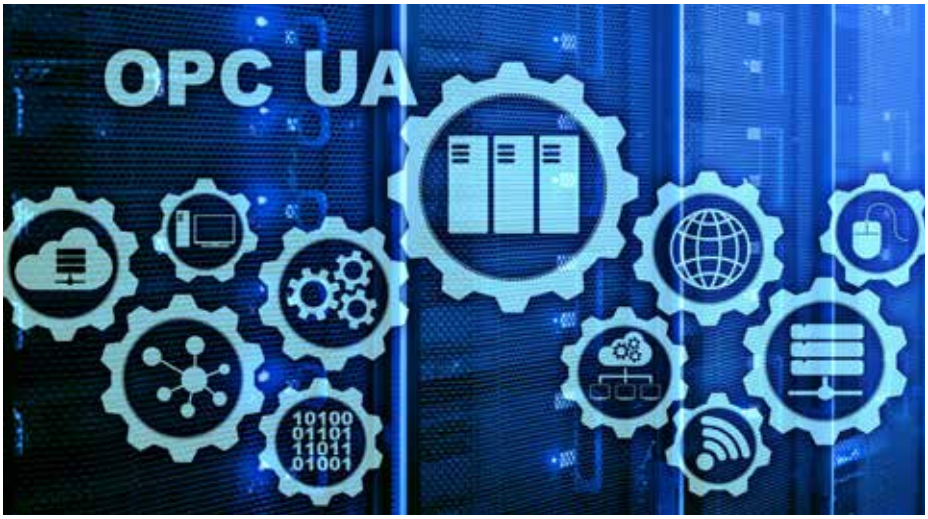


The Global Discovery Server in collaboration with the OPC UA server and client.

SOURCE: PHOENIX CONTACT

OFTEN, OPC UA IS ONLY ASSOCIATED WITH a machine-to-machine communication protocol for industrial automation. However, the standard is also a good solution for connecting machine networks and company networks. This is because OPC UA not only transmits machine information - for example, target values, measured values, and process parameters - but also defines and describes the data (lead).

The OPC UA information model enables new processes to be set up efficiently between a controller and any higher-level, business-oriented software layer. In addition, the software update model specified in the OPC UA specification 10000-100 can be used to realize a software management system for an asset. This system includes, for example, installing new software, updating existing software, updating firmware, and performing a limited backup and recovery of parameters and firmware whenever this is necessary for the update process. However, to exchange data with an asset securely and with a high level of trust, OPC UA offers the option of certificate-based communication. This is where the OPC UA Global Discovery Server (GDS) comes into play.



(Image source: Funtap@shutterstock.com)

SOURCE: PHOENIX CONTACT

Access point to the central certificate management

First, the GDS concept of OPC UA allows the configuration of cross-subnet Discovery Services. Second, it provides interfaces for a central certificate management system. A Global Discovery Server includes mechanisms for the central management of CA-signed (Certificate Authority) and self-signed certificates, as well as for the management of trustworthy lists and certificate revocation lists (certificate revocation list, CRL). This means that the GDS is an access point to the central certificate management system and therefore takes on the role of a security server within an OPC UA network.

The main application of the Global Discovery Server is the administration of CA-signed certificates with the associated CRLs. For this purpose, the GDS can generate initial OPC UA

application certificates, regularly update the associated CRLs and trust lists, and renew the OPC UA application certificate. All in all, the OPC UA Global Discovery Server plays a critical role in ensuring the hardened and efficient operation of OPC UA systems by providing key identification, management, and security capabilities.

Real-time client notification

The GDS Push Service is a function of the OPC UA Global Discovery Server that notifies clients in real time when new endpoints or applications are added to the GDS or when existing endpoints and applications are changed or deleted. With the GDS Push Service, clients can subscribe to notifications regarding specific events or changes, such as when a new OPC UA server is added to the network or the end point URL of an existing server changes. This means that the clients are always up to date on adaptations in the OPC UA network and can automatically adjust their configurations when necessary.

The GDS Push Service can also work alongside the OPC UA Pub/Sub protocol, which enables the efficient and scalable communication of event notifications. Clients can subscribe to specific topics or events that are of interest to them. The GDS then automatically sends messages if these events occur. Overall, the GDS Push Service is a powerful feature of the OPC UA Global Discovery Server. This is because the service allows the real-time identification and management of OPC UA applications and endpoints, which is a huge boost to efficient and secure data transmission in industrial and IoT systems.

Identification of devices in a network

Implementing the OPC UA Global Discovery Server is a great benefit to a device management tool, such as the Device and Update Management system from Phoenix Contact. First of all, the GDS supports the user in identifying and managing OPC UA-enabled devices and applications more easily. The Global Data Server provides a central location for the identification and administration of OPC UA endpoints and applications, meaning that the device management tool can identify the devices in the network more easily and connect with them.

In cooperation with a device management tool, the GDS is also available for managing the security of OPC UA-enabled devices and applications. The Global Discovery Server includes functions for the management of certificates and security directives, thus ensuring that communication between the devices is secure and trustworthy. Last but not least, the GDS Push Service can deliver real-time notifications regarding changes in the network, meaning that the device management tool is always up to date in terms of changes to OPC UA-capable devices and applications. This enables the device management tool to automatically adjust its configuration when necessary.

SOURCE: PHOENIX CONTACT

Manufacturer-independent and industrial networking and security with OPC UA.

OPC UA server certificates in PLCnext controllers

The embedded OPC UA server built into the PLCnext controllers from Phoenix Contact requires X.509 certificates to ensure trustworthy communication with OPC UA clients. There are four main types of certificates that can be used:

Automatically generated self-signed certificates
The necessary certificates are generated automatically by the controller. This function is easy to set up and is particularly useful for tests and permanent use in secure LANs.

Manually generated self-signed certificates
These have no additional security advantages over automatically generated self-signed certificates. However, the manager has greater control over certificate management.

Certificates signed by the company's own certification authority (CA)
Compared with automatically and manually generated self-signed certificates, these have no security advantages. However, a structured certification management system can be set up.

Certificates issued by a trusted certification authority
These certificates must be purchased from a trusted certification authority, such as GeoTrust or Symantec, for example. This option is recommended for public or unsecured networks, because all clients should accept a certificate signed by a trusted certification authority.

Remote configuration

There are a large number of applications that will require automated commissioning of new or replacement devices in the future - in particular as we move toward a networked world in the All Electric Society. The buzz phrase zero-touch or one-touch provisioning is often used here. Within a company network, intelligent end devices (edge devices) can be configured remotely – without human intervention on site. This saves time and money.

In combination with an OPC UA Global Discovery Server, an intelligent device management tool enables a decisive step to be made here. This is because identifying new devices via the GDS, trusting them, or issuing them with a trustworthy identity, and then installing a previously defined global configuration on the devices are essential functions for automated commissioning. Using the OPC UA standard is a key advantage here. This is the only way that corresponding scenarios can be implemented regardless of the device manufacturer.

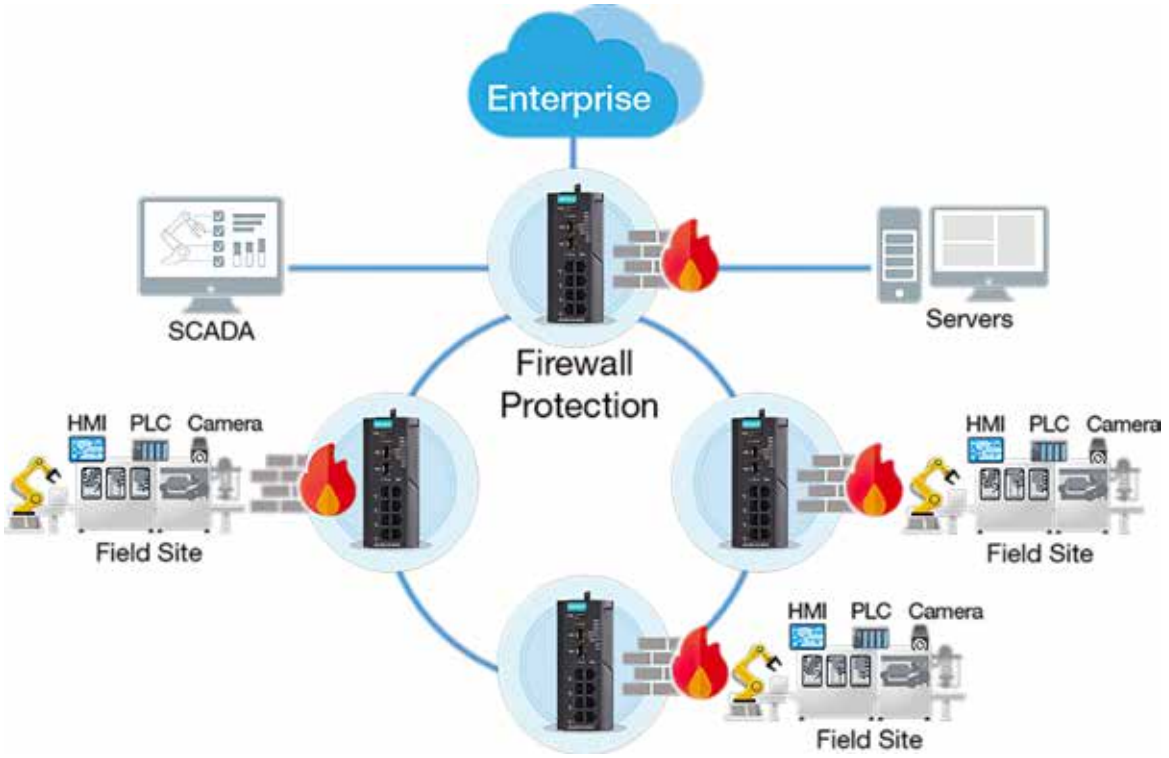
Even if a device management tool does not necessarily need an OPC UA Global Discovery Server, it can still benefit from its functions and the ability to identify, manage, and secure OPC UA-enabled devices and applications, as well as provide real-time notifications of changes in the network.

Arno Martin Fast, B. Eng., Senior Specialist Digital Services in the Business Unit Automation Systems, ***Phoenix Contact Electronics GmbH.***

Learn More

Building security boundaries to enhance industrial cybersecurity

A defense-in-depth concept allows companies to leverage their existing network infrastructure and investment to build the first line of their network defense. Industrial intrusion prevention systems and security boundary concepts can also further protect OT systems from a wide range of cyberattacks.



SOURCE: MOXA

THE RISE OF INTERCONNECTED OT AND IT systems is often attributed to how business models have evolved with the purpose of enhancing operational efficiency. For instance, SCADA networks deployed along oil pipelines now collect oil output data that is essential to billing and pricing systems.

This increase in data collection allows companies to predict with higher levels of accuracy not only levels of oil production and output but also expected revenue. However, it should be noted that these interconnected systems do not only bring benefits -- a downside is that the likelihood of introducing cybersecurity threats to OT systems increases significantly.

What is compounding this complex issue even further is that ransomware attacks are increasing in their severity. This type of malware exploits Windows vulnerabilities and attacks insufficiently protected systems.

With increasingly similar cybersecurity incidents occurring in OT systems, business owners and regulators are keen to seek solutions that enhance industrial cybersecurity and allow businesses to keep functioning normally. In this article, we will introduce the defense-in-depth concept that allows companies to leverage their existing network infrastructure and investment to build the first line of their network defense. Later in the article, we will discuss the benefits and advantages of how industrial intrusion prevention systems can further protect OT systems.

What is the security boundary concept?

When enhancing cybersecurity, it is vital to understand how your industrial systems are exchanging data within different systems and how they connect to IT-level systems. In an ideal scenario, when traffic crosses other systems, there should be boundaries between each design to ensure the traffic has good "cyber-hygiene" even if it is authenticated and authorized.

However, it is challenging, and often unrealistic to build boundaries between every system, as it involves significant expenditure, and often has a detrimental effect on the efficiency of network communications. For these reasons, it is highly recommended to divide OT systems into different digital cells and zones and build up the boundaries to find the right balance between expenditure and acceptable levels of risk.

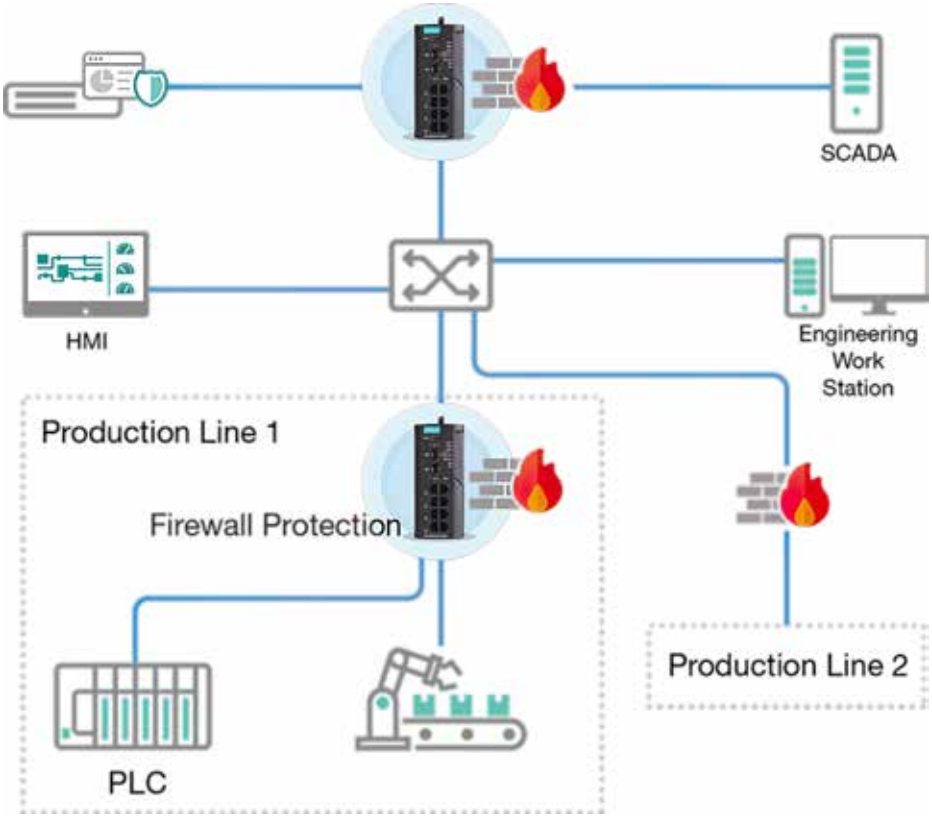
The defense-in-depth approach, which is recommended by the IEC 62443 cybersecurity standard committee, is widely used across industries and has a good track record of helping build up multiple layers of protection to fulfill operational requirements. In the picture below, the critical assets and operations are considered the most important. As they perform vital roles for businesses, it is wise to take additional security precautions, such as adding more layers of protection, to secure them further.

How to build security boundaries

Network Segmentation

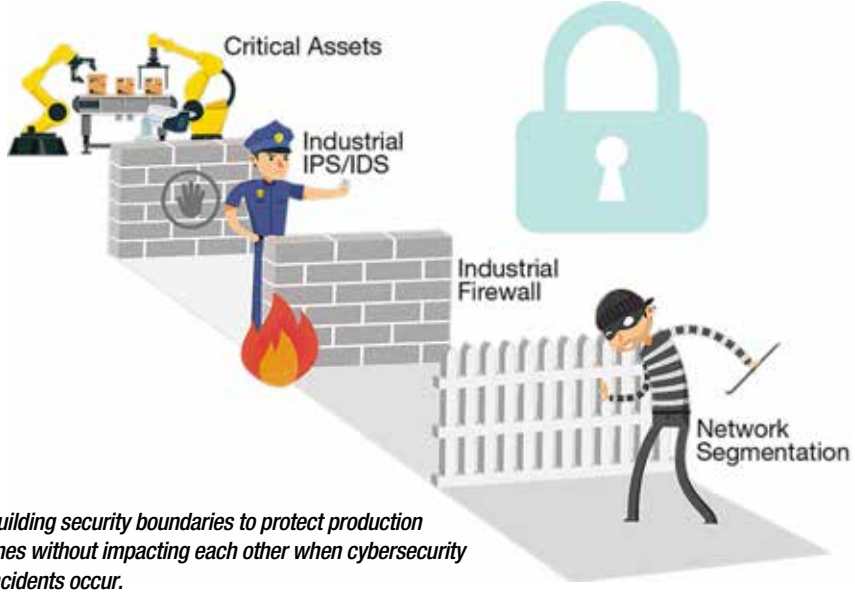
Physical layer segmentation: This is known as air gapping when two networks are physically isolated. When the operations and security of one system need to be independently maintained, an air gap is a potential solution. However, as mentioned earlier, it is increasingly difficult to arrange networks this way due to business and operational requirements.

SOURCE: MOXA



Data link/network (Layer 2/Layer 3) segmentation: As industrial control systems may have been built decades ago, one of the key challenges, but also essential requirements for network administrators, is to leverage existing infrastructure while ensuring industrial control systems remain secure. One approach that is frequently deployed is to segregate traffic between different network segments using a VLAN (Virtual LAN), which is one of the functions of managed Ethernet switches. Some Ethernet switches feature Access Control Lists (ACL) at the port level, which can help improve VLAN security as data enters the switch. An alternative is to deploy firewalls to protect industrial applications and data especially when you need to deal with traffic on Layer 2 and Layer 3 networks.

Layer 4-7 network segmentation: Further segmentation can be applied through Deep Packet Inspection (DPI). DPI offers granular control over network traffic and helps you filter industrial protocols based on the requirements of the application. When you have multiple devices on the same network, theoretically, they all have the ability to communicate with each other. However, there are certain scenarios, when for example, Controller A should only communicate with Robotic Arm A at a specific time, then DPI technology can help engineers to define which controllers can perform read/write commands or even the direction of traffic.



Building security boundaries to protect production lines without impacting each other when cybersecurity incidents occur.

SOURCE: MOXA

Micro-segmentation

In some situations, additional protection for critical assets is necessary, and a good way to achieve this is to use an intrusion prevention system to micro segment the network. What makes micro-segmentation particularly helpful for industrial networks is that it can be used to segregate the network into even smaller sub-networks. What is beneficial about this approach is that the virtual patch function of an IPS can help mitigate the risk of known vulnerabilities. For example, some systems might be operating on Windows XP, which Microsoft does not provide security updates for anymore. Under this scenario, even though there are known vulnerabilities, it may not be feasible to perform security updates. Watch the video to see how IPS virtual patch works.

Secure remote access

According to cybersecurity experts, remote desktop protocols are sometimes exploited to spread malware or conduct unauthorized activity. As remote connections have become more and more prevalent due to the necessity of increasing operational efficiency and the need to perform troubleshooting quickly, it is unsurprising that building security boundaries between two field sites is being talked about more frequently. Instead of using software to build the remote connections, which can easily lead to vulnerabilities in the long term, it is highly recommended to build VPN tunnels and ensure that access control mechanisms are maintained properly.

Typical scenarios

Manufacturing: Interconnected factory networks need proper network segmentation to reinforce industrial network security. Furthermore, network redundancy is also required to ensure the availability of the industrial control system.

Secure Substation Monitoring: A power grid that covers a vast area needs IEC 61850 certified VPN solutions to monitor the intelligent electronic devices (IEDs) at each remote substation.

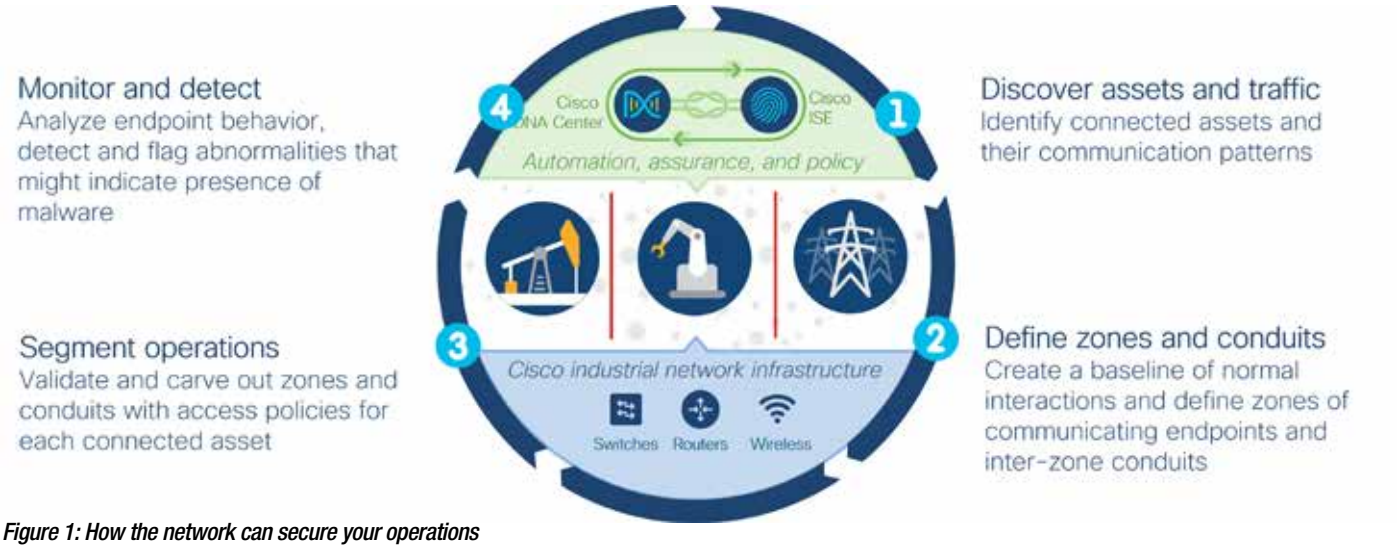
As business owners are no longer able to enjoy the benefits and security of completely air-gapped networks, it is imperative for business owners and engineers to enhance security boundaries through different approaches including network segmentation, micro-segmentation, and secure remote access. Each of these approaches fulfills additional network requirements and helps improve cybersecurity not just by forming perimeter protection but also by preventing lateral movement of unauthorized traffic.

*Technical article by **Moxa**.*

Learn More

From data to defense: the evolving role of industrial network security

Converging networking and security in industrial operations can enhance visibility within the organization, improve threat prevention, detection and response, simplify management, provide scalability and flexibility, and offer a crucial platform for IT-OT collaboration that can be built upon.



SOURCE: CISCO

Figure 1: How the network can secure your operations

TRADITIONALLY TO PROTECT INDUSTRIAL operations, manufacturing organizations kept the operations network isolated from the enterprise and from the outside world. But with increasing connectivity required to achieve the promise of Industry 4.0, the airgap approach to securing operations is obsolete.

Firewalls have traditionally been the mainstay against cyberthreats. While firewalls are an essential component, they are not sufficient to provide comprehensive cybersecurity, as they only provide limited perimeter protection and cannot defend against sophisticated attacks or existing vulnerabilities in industrial assets. Neither can they protect against insider threats. They can also be cumbersome to set up and manage, especially in large networks.

The network that connects industrial assets, their control systems, and applications is in the best position to defend operations against threats. In this article we will discuss how you can empower your network to prevent, detect, and mitigate cyberthreats as shown in Figure 1.

Securing operations is not a job for OT or IT teams alone. Each team brings different skill sets to the table and must work collaboratively to achieve desired outcomes.

Network as a sensor

Industrial operations have typically been built over several years, even decades, frequently by vendors and 3rd parties, often without much regard to cyberthreat protections. Often, operations teams do not have an accurate inventory and there might be assets that were added but are no longer used or updated. In short, there could be a lot of lingering unknown vulnerabilities.

Fortunately, the technology to identify connected assets is available today. Deep Packet Inspection (DPI) decodes all communication flows and extracts message contents and packet headers, providing the visibility and detailed information on assets to understand your OT security posture. DPI can also help identify software vulnerabilities.

To work, DPI needs to analyze traffic in the network, and if you are using a separate server

SOURCE: CISCO

Figure 2: The Cyber Vision sensor runs in the Cisco industrial network equipment.

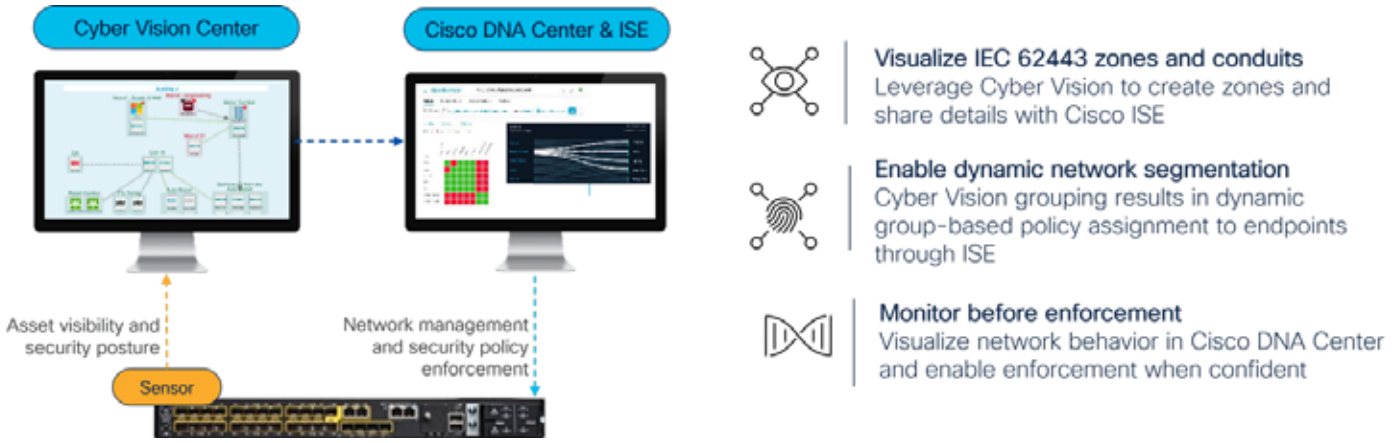


Figure 3: Cisco industrial network as a security enforcer.

for DPI, you will need to duplicate all traffic from your industrial switches, all the way down to access switches otherwise you will miss the "East-West" traffic that is exchanged between machines. In a larger network, you will essentially need to build a parallel network to support this additional traffic, adding complexity and expense.

A better way would be to run the DPI sensor and analyze the traffic right in those access switches. You will not need to duplicate any traffic but only send the results of that analysis to a central dashboard where you can visualize your assets, traffic, and vulnerabilities to fix. With that intelligence, the dashboard application could also spot and alert you to any abnormalities, helping you to identify potential threats and act on them quickly.

Cisco has embraced this approach. Cyber Vision leverages a unique edge computing architecture that enables DPI to run within Cisco Industrial Ethernet switches giving comprehensive visibility at scale while minimizing cost, traffic, and operational overhead.

Network as an enforcer

The ISA/IEC-62443 Series of security standards requires segmenting the industrial network into zones and conduits to restrict communications between unrelated assets and restrict any malware that finds its way into a zone from spreading and disrupting entire operations.

A zone is a collection of assets that have common security requirements. For example, an automobile plant may have a production line for welding and another for painting. There is no reason that equipment in welding and paint shops would need to interact.

Under the least privilege principle, OT assets can only communicate with other assets in their zone. Conduits between zones must be defined to all inter-zone communications.

Visualizing network traffic gives you insights into normal communication patterns, that can help you create a baseline of normal network flows. This reference, that supplements the operations team knowledge of their assets, can help you define zones and conduits.

Once accurate flows necessary for proper functioning of operations have been determined, you can define policies that will enforce these flows and restrict others, thus dividing operations into zones, and creating conduits between zones.

Now this enforcement can be accomplished by placing firewalls around these zones, but in a large network with many zones, firewall placements and configurations could quickly become very complex. A better approach will be to have the industrial switches themselves enforce these policies to segment the network, thereby creating zones, and allow only defined connectivity between zones, creating conduits.

An easy and well-known segmentation method is to create VLANs, but they have limitations. They only work at Layer 2, have limited scalability, and can get very complex to administer. There is a better approach. You can use Cisco industrial switches to segment the network in a much more automated and scalable manner. You can set segmentation policies that you have defined as rules in Cisco Identity Services Engine (ISE). ISE then sends these rules to Cisco industrial switches.

Based on these rules the switches act on incoming packets, either allowing them to proceed to their destination or to discard them. The combination of Cyber Vision, ISE, and Cisco industrial switches provides an automated, scalable, cost-effective, and granular alternative to VLANs or firewall-based approaches.

Towards complete industrial security

Using your industrial network as a security sensor and enforcer are necessary steps for building a complete security framework for your operations. After establishing and enforcing trust, continuous monitoring of assets through Cyber Vision helps quickly identify and flag any abnormal behavior that could be indicative of malware presence.

Converging networking and security enhances visibility, improves threat prevention, detection and response, simplifies management, provides scalability and flexibility, and provides a crucial platform for IT-OT collaboration that they can build upon.

Vivek Bhargava Product Marketing Manager, ***Cisco.***

Visit Website

Can IoT development go hand in hand with cybersecurity?

Cybersecurity is not a tick-box exercise but a fundamental part of grid modernisation in smart utilities and in smart city development. It needs to be a continuous effort from the beginning and then carefully considered at each stage of the design.

SOURCE: ISTOCK

We know threats are constantly changing and cyber attackers are finding new and innovative ways to develop their techniques.

ENERGY SECURITY TOPS THE LIST OF THE MOST exciting areas of IoT development for utilities, according to a poll Wi-SUN Alliance conducted earlier this year. The idea behind this survey of senior professionals in the industry was to find out what was top of mind for those working in and developing smart utilities services and applications in what has in the past been seen as a sector largely resistant to change.

More recent modernisation of our utilities, enabling increased efficiencies and reliability through digital transformation and open connectivity, means that smart utilities are now changing the way the industry operates. Smart systems, devices and customer services are replacing an ageing infrastructure to help create a more efficient, more affordable, and more sustainable energy future.

But will this transformation come at a price? Security and data privacy are always a worry for an industry that is increasingly open to attack. According to ABI Research a couple of years ago, both water and power utilities have reported an increase in advanced persistent threats (APTs) which can exploit vulnerabilities in industrial control systems. While other cyber threats like ransomware and DDoS (dedicated denial of service) attacks are able to infiltrate systems and cause significant damage once inside.

The evolving threat landscape

We know threats are constantly changing and cyber attackers are finding new and innovative ways to develop their techniques. As you increase connectivity and open up systems to multiple parties in an effort to increase efficiency and reduce costs, you also open up potential attacks vectors that need to be secured.

Attackers could get access to customer data leading to data privacy breaches but could also manipulate data and readings. At this stage, consumers then lose trust in the technology which could impact smart meter deployments. There's also the bigger risk of the smart meter network becoming compromised with the potential to bring down the grid or leading to power outages. As our cities become increasingly smart and networks increasingly interconnected, a compromised grid could affect other applications like smart lighting, traffic and transport systems or even healthcare systems.

Then factor in regulation and compliance in an already highly regulated industry. With multiple cyber initiatives in Europe, there could the risk of too much complexity.

Changing attitudes

In our *Journey to IoT Maturity* report published last year, we can start to see how perspectives and attitudes to IoT technologies are changing among those developing and implementing smart cities and smart utilities. The report –

SOURCE: ISTOCK

As you increase connectivity and open up systems to multiple parties in an effort to increase efficiency and reduce costs, you also open up potential attacks vectors that need to be secured.

a study of 300+ IoT adopters in the UK and US – is a revisiting of our first state of the nation report published in 2017.

The market has gathered momentum during this period. Our latest report shows that over 90% of respondents recognise they must invest more in IoT to remain competitive as the market continues to evolve. But some of the core concerns five years ago have started to ease. One of these is security, with those respondents ranking security as one of their top three challenges when rolling out IoT falling by over half (from 58% in 2017 to 24% in 2022).

This change in attitude is particularly interesting considering the threat environment, with concerns growing among policy makers and industry leaders due to current global economic and political turmoil, including the war in Ukraine potentially putting energy supplies at risk.

What's interesting, however, is that concerns around data privacy are growing. In our most recent IoT study, data privacy regulation was ranked the second highest political, economic or social challenge by respondents, while almost one fifth (up from 11% in 2017) placed big data in their top three IoT rollout challenges. Most IoT initiatives, from smart metering to rollouts of streetlighting, rely on increasingly large amounts of data, so capturing and storing it securely presents its own challenges.

The General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and other privacy regulations have also come into force since our 2017 report, which may be driving up concerns. With stricter data protection laws come greater pressures for utilities and energy providers to protect sensitive data. Those that fail to do so risk running into compliance issues that can lead to serious financial penalties and damage to reputation.

Security by design

The question of smart utility development going hand in hand with security is not a case of whether it can, but how it can.

Cybersecurity is not a tick-box exercise but a fundamental part of grid modernisation in smart utilities and in smart city development. It needs to be a continuous effort from the beginning and then carefully considered at each stage of the design, from the network infrastructure that provides a robust foundation for secure IoT implementations, to the devices and applications sitting on the network.

If security hasn't been baked in from the start it can be difficult and expensive to solve security issues retrospectively.

This is very close to our hearts as an industry alliance. IP-based security technologies, which form part of the Wi-SUN protocol, ensure that data communications across the network are protected from security threats. Our own commitment to security is embodied by our global members who prioritise secure communication within their product offerings.

This commitment in turn inspires innovation and collaboration, which are critical to the success of IoT development.

Phil Beecher, CEO and President, ***Wi-SUN Alliance.***

Visit Website

Operational technology security at a glance

Establishing a complete and effective OT security program is a complex endeavor that differs from typical cybersecurity strategies. Ultimately, the goal is to maximize uptime by enabling operators to take targeted action to reduce and, where possible, minimize security breaches in OT environments.

OT SECURITY USES TECHNOLOGIES TO MONITOR and detect changes in the operational technology infrastructure , such as in critical infrastructures - what is important here? Palo Alto Networks explains the basics and aspects of OT security.

OT (Operational Technology) stands for operational engineering or technology in the English-dominated engineering language. The term refers to hardware and software systems used to monitor and/or control industrial plants and processes.

These are OT devices (servers, industrial robots, PLCs, conveyor belts), 5G OT devices (such as drones) and IT/IoT devices (endpoints, printers, security cameras, heating and cooling systems). These industrial processes and devices are used in critical infrastructure, utilities, power grids, manufacturing plants and traffic control systems.

The generic term OT includes many specialized systems such as process control domains, programmable logic controllers (PLCs), physical access controls, and distributed control, security, and transportation systems. This also includes SCADA systems (Supervisory Control and Data Acquisition) and building management/ Automation systems, often summarized under the term ICS (Industrial Control Systems).

Although OT and IT security share some similarities, there are characteristics that differentiate OT from traditional IT systems. Perhaps the most obvious difference between IT and OT security is the direct connection of OT to the outside world. OT has the potential to impact the physical elements of society through production disruptions, public health and safety risks, environmental damage, and financial damage.

SOURCE: PALO ALTO NETWORKS

The generic term OT includes many specialized systems such as process control domains, Programmable logic controllers (PLCs), physical access controls, and distributed control, security, and transportation systems.

Unique requirements and ongoing convergence of IT and OT

OT environments rely on applications and operating systems that IT professionals may be unfamiliar with. When developing and operating OT systems, security and efficiency are sometimes at odds with security.

Operational technology systems have special requirements for connectivity and security, e.g. B. Uptime with high availability, security and integrity. Vulnerability patching is slow to non-existent and cyber forensics limited, if at all.

Security breaches not only affect business operations as in IT, but can also lead to process fluctuations, equipment and environmental damage or endanger personnel safety.

In the past, IT and OT were managed by separate groups and had no interdependencies. In recent years, however, the paradigm has changed. Today it is common for OT systems to be equipped with network and computer technologies. The worlds of IT and OT are converging, laying the foundation for the Industrial Internet of Things (IIoT).

The IIoT is a matrix of interconnected sensors, instruments and devices that collect and exchange data. Many industries use this data, e.g. For example, in manufacturing, oil and gas, transportation, energy and utilities, and more.

Modern OT environments must facilitate the exchange of data between machines and applications. At the same time, OT environments must be able to scale processes across physical and virtual systems. Because of this, OT systems are beginning to converge with IT systems.

The IIoT will play a key role in Industry 4.0. Converged IT/OT ecosystems will serve as conduits embedding the IIoT into the 4IR ecosystem. The integration promises numerous benefits such as improved information flow, process automation, advances in managing distributed processes, and easier compliance.

Why is OT security so important?

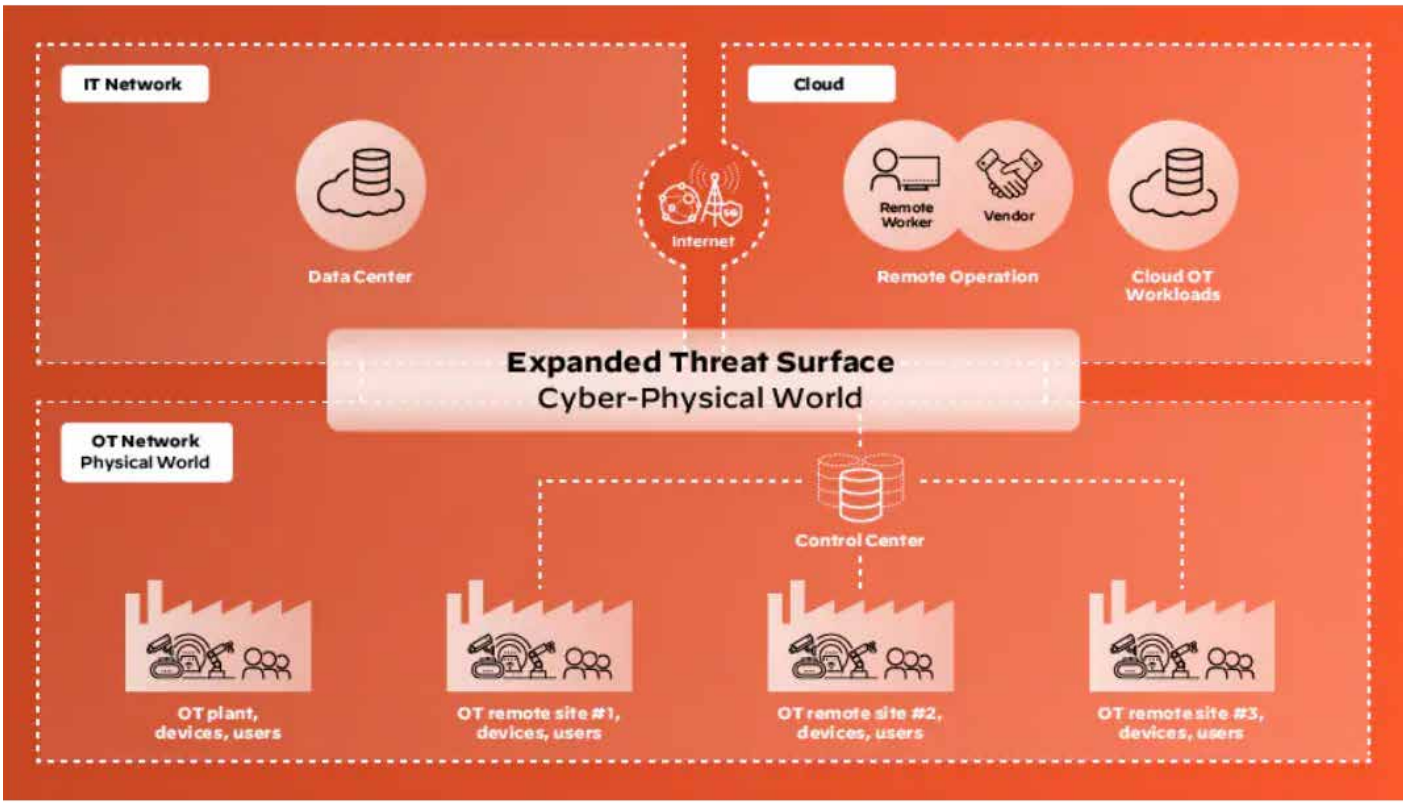
As the boundaries between IT and OT disappear, the attack surface for networked IT/OT systems increases. The most common attack vector for hackers is the internet. ICS sensors, instruments, and OT devices that can be accessed over an OT network are vulnerable to malicious actions. Botnets can be used for targeted attacks on critical infrastructures.

Typically, Human Machine Interfaces (HMI) that connect human operators to industrial control systems are also networked to IT infrastructures. Accessibility of HMIs over the Internet poses a major risk to ICS security. Consequently, HMIs are vulnerable to IP-based vulnerabilities such as B. Bypassing authentication, weak session management.

According to the experience of Palo Alto Networks, attackers usually penetrate ICS systems with malware. This can be generic malware or malware specifically designed to attack critical infrastructure. These infiltrations often lead to denial-of-service (DoS) attacks that paralyze or bring industrial networks and processes to a standstill. ICS and IIoT devices are also a valuable target for hackers. Whether attackers are looking to extort ransom or to sabotage rival nations by gaining access to confidential data, this is a target.

OT security risks and challenges

One of the current challenges in OT security is that it's not possible to secure what you



SOURCE: PALO ALTO NETWORKS

can't see. Invisible vulnerabilities create exponential risk. The threats exceed the possibilities of prevention. The promise of digital transformation and connectivity in OT environments also comes with significant risks. A flood of connected devices will further increase the opportunities for attacks.

This is especially true in OT environments as OT devices are vulnerable and unprotected. There are more than 1,000 common vulnerabilities and compromises in industrial control systems, more than 80 vulnerabilities in the devices of the four largest OT vendors, and 29 percent of OT devices are vulnerable due to internet connectivity.

The consequences of security breaches in ICS are very different from typical cyber attacks. A manipulated OT system can cause damage to devices that cannot be easily replaced. Other risks include malicious changes to alert thresholds, commands, or instructions, as well as OT software infected with malware, or improperly changed OT configuration or software settings.

Disrupted or delayed data flow through OT networks could also disrupt OT operations. Erroneous data sent to system operators to disguise unauthorized changes or induce operators to take inappropriate actions is another problem.

OT security best practices

According to NIST, there are nine OT security recommendations for creating, implementing, maintaining, and continually improving an OT security program. By implementing and maintaining these best practices, organizations can create an OT security roadmap for risk management:

1. Establish OT security governance.
2. Established and trained a cross-functional team to implement the OT security program.
3. Defining an OT security strategy.
4. Definition of OT specific policies and procedures.
5. Implemented a security awareness training program in the OT organization.
6. Implementation of a risk management framework for OT.
7. Developing a maintenance tracking capability.
8. Develop Incident Response capability.
9. Development of recovery skills (recovery and restore).

Regardless of whether the environments are partially separated by air gaps or connected via a cloud, Palo Alto Networks has found that this can be achieved with a Zero Trust OT security approach.

This consists of (1) minimally privileged access control with micro-segmentation and granting of minimal access, (2) continuous trust assessment that assesses the security posture and behavior of OT devices, as well as the behavior of applications and users, and (3.) a continuous security review. The latter means that all traffic is inspected, even on allowed connections, and all threats, including zero-day threats, are prevented.

Establishing a complete and effective OT security program is a complex endeavor that differs from typical cybersecurity strategies. Ultimately, the goal is to maximize uptime by enabling operators to take targeted action to reduce and, where possible, minimize security breaches in OT environments.

Technology article by ***Palo Alto Networks.***

Visit Website

SOURCE: PALO ALTO NETWORKS

IT-OT convergence drives technology innovation

Cybersecurity has become one of the primary challenges for IT/OT convergence. But the ongoing effort to integrate information technology with factory automation systems faces a wide range of challenges including connectivity, data collection, cloud integration, applications and updating issues.

SOURCE: PALO ALTO NETWORKS

The breadth of Operations Technology (OT) encompasses many specialized systems such as discrete and process control domains, all types of industrial controllers, physical access controls, connections to enterprise systems and the cloud -- along with distributed control, security and transportation.

IT-OT CONVERGENCE ENCOMPASSES THE integration of information technology (IT) and operational technology (OT) systems. IT systems are used for data-centric computing; OT systems monitor and control automation processes and devices, and provide vital connections to enterprise and manufacturing systems.

Connecting information technology with manufacturing operations enables efficient use of the data generated in the modern smart factory. IT-OT network connectivity means linking plant or machinery automation with IT as seamlessly and fully as possible.

For this IT-OT technology trends and solutions update, we reached out to industry experts to gain their perspective on the state of convergence in modern factories. Vivek Bhargava, Product Marketing Manager at Cisco and Dr. Al Beydoun, ODVA President and Executive Director, share their thoughts on questions about key technologies, trends, applications and the challenges of the ongoing quest for effective IT-OT convergence.

Industry Experts Q&A

What are technology area(s) that represent potential solutions to IT-OT Convergence, and how are they contributing to both the importance of these initiatives and make an impact for industry?

Vivek Bhargava, Product Marketing Manager, Cisco: Historically, IT and OT teams have worked in separate domains with different priorities. But rapid digital operations transformation requires skills in networking and security that IT has perfected over decades in the enterprise space. OT, being more focused on safety, efficiency, and continuity, generally lacks these skills. For the organization to achieve positive outcomes, it is important the IT and OT teams collaborate and share their skills.

While there are several cultural, communications, budget, and leadership challenges that must be addressed, technology can help bridge the gap between IT and OT by helping them build a common framework, share expertise, and develop trust.

In my opinion, there are three technology areas that stand out that can help IT and OT collaborate better: network equipment, operations security, and machine-to-cloud communications.

Dr. Al Beydoun, ODVA President and Executive Director: 5G is a technology that can help break down traditional barriers between IT and OT through connecting devices and their associated data with higher level systems, including the cloud, for analysis

SOURCE: ISTOCK

Some potential quick wins for 5G in industrial applications include connectivity into discrete machines and process skids for 24/7 status and maintenance management purposes, direct sensor connectivity for vibration and temperature measurement, and machine control for remotely located process equipment.

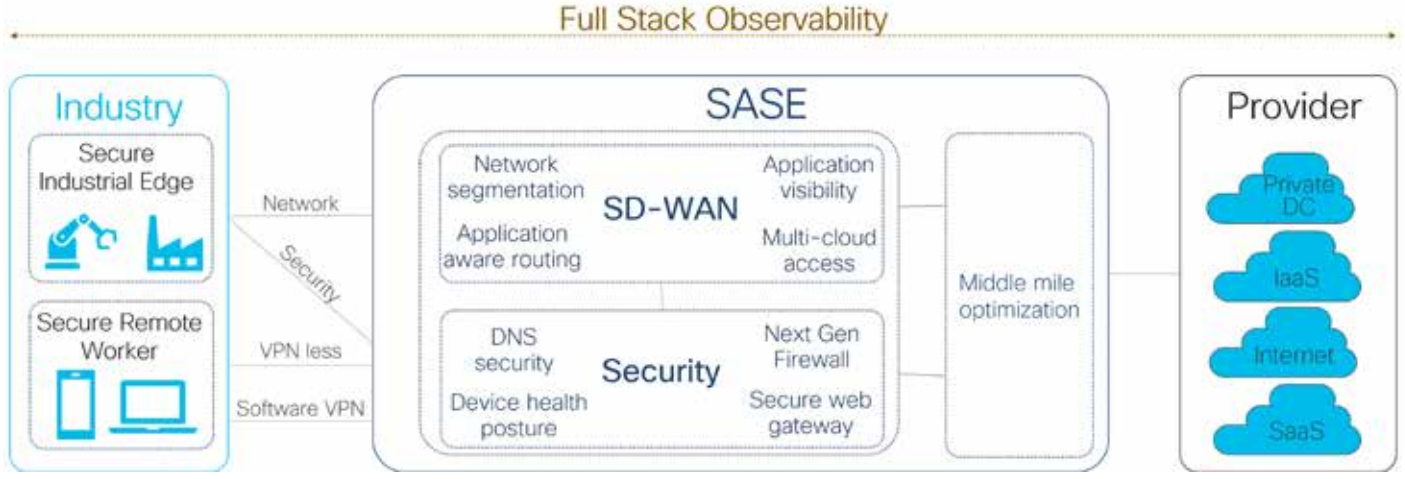
and action. Unlike previous generations of mobile technology, 5G is designed to move beyond simply connecting mobile/cellular phones. 5G now includes Quality of Service (QoS) for message prioritization, the ability to be used for Augmented Reality and Virtual Reality (AR/VR), and even real time control for automation. In fact, the 5G Alliance for Connected Industries and Automation (5G-ACIA) is working to enable 5G for use in more and more industrial automation applications.

Some of the potential quick wins for 5G in industrial applications include connectivity into discrete machines and process skids for 24/7 status and maintenance management purposes, direct sensor connectivity for vibration and temperature measurement, and machine control for remotely located process equipment. The ability to have constant remote access enables the population of operations dashboards with critical machine health information.

This can make it much easier to see when an issue arises and this awareness can allow for quicker and therefore lower cost resolution. 5G connected applications include Automated Guided Vehicles (AGVs) that can carry components and finished goods around industrial operations and other standard automation applications on the plant floor such as tool changers.

However, there are still challenges that remain to be solved regarding the high amount of electrical noise and reflections from metal equipment such as moving robot arms. Some potential solutions to undesired interference are Massive Multiple In Multiple Out (MIMO) that provide a large number of 5G antennas from a single base station and Coordinated Multi-Point (CoMP) that provides MIMO across multiple 5G base stations for greater coverage.

What specific technical benefits do these solutions provide, and how can it make a difference in implementing new levels of enterprise/automation integration?

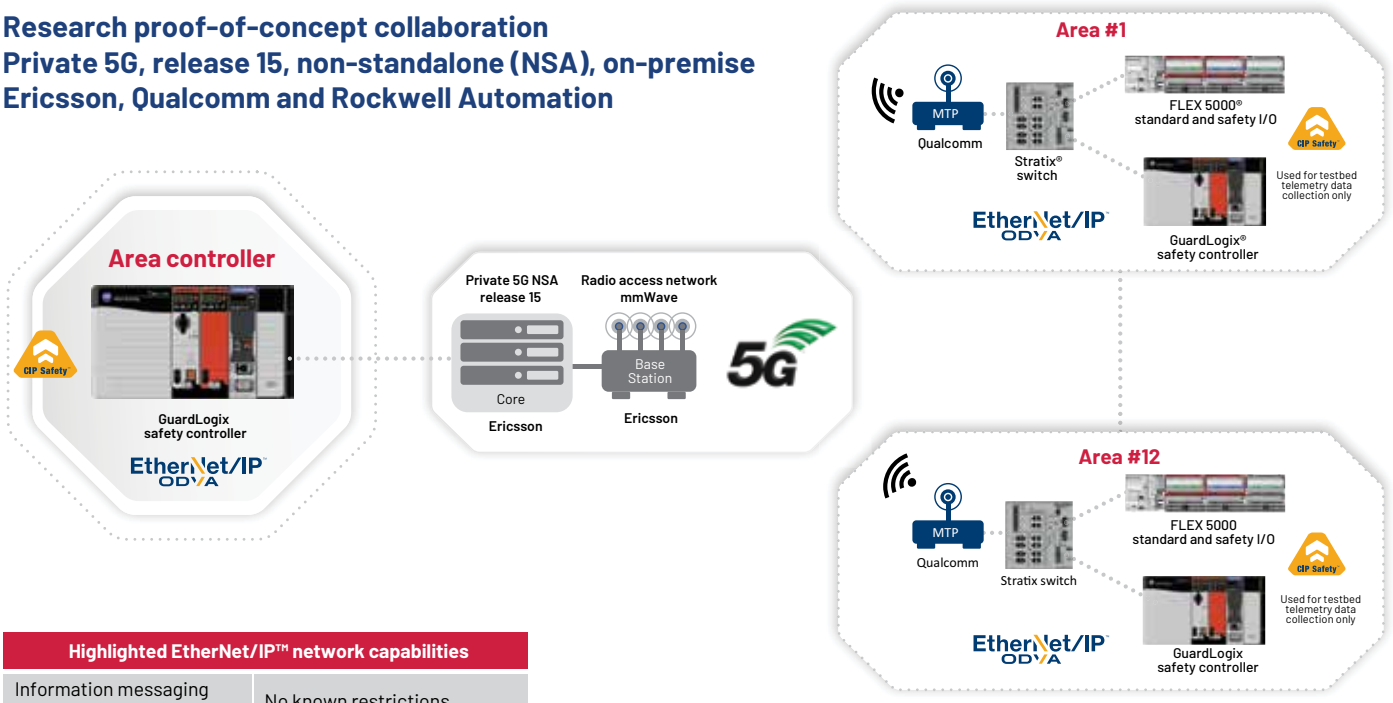


SOURCE: CISCO

Machine to cloud architecture with SASE.

SOURCE: ODVA

Research proof-of-concept collaboration
Private 5G, release 15, non-standalone (NSA), on-premise
Ericsson, Qualcomm and Rockwell Automation



Highlighted EtherNet/IP™ network capabilities	
Information messaging (configuration, monitoring)	No known restrictions
CIP™ standard I/O	RPIs down to 5 ms
CIP Safety™ I/O	RPIs down to 8 ms

MTP: Mobile test platform, 5G to Ethernet adapter, referred to as user equipment (UE)
CIP: ODVA Common Industrial Protocol
RPI: Requested packet interval (rate at which the owner-controller and the I/O exchange data)
Qualcomm 5G technology is licensed by Qualcomm Incorporated.
Qualcomm 5G products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

EtherNet/IP Private 5G Proof of Concept Illustration.

***Bhargava**: Network equipment:* Building modern OT networks starts with equipment that brings together the best of enterprise-grade and industrial-strength features which can be a catalyst for better IT-OT integration. Such devices provide the scale, flexibility, and performance perfected over decades by IT, but are hardened for harsh environments, equipped with support for industrial protocols, and offer extremely high availability. Cisco networking equipment even have essential services built in that further boost IT-OT collaboration such as visibility and secure remote access. IT can now gain OT's trust and better help them with building, scaling, managing, and securing their network.

Operations security: With increased connectivity, OT can no longer ignore security threats or software vulnerabilities. Technology advances in visibility, segmentation, threat detection and remediation, that IT has been using, can be applied to OT too. Cisco industrial networking equipment can double as security sensors by running Deep Packet Inspection (DPI) within themselves. The visibility it provides into assets and network traffic helps IT teams define and enforce access policies, segment the network without disruption to operations, and help OT keep operations secure, fostering trust and even better collaboration.

Machine-to-cloud: More operations are utilizing the cloud for applications such as SCADA, Historian, and Manufacturing Execution System (MES), as well as analytical applications that operate on real-time data. The insights these provide facilitate data-driven decisions. IT has been running applications in the cloud for many years now and has developed secure and robust ways for data exchange. Technologies such as Secure Access Service Edge (SASE), SD-WAN, Security Service Edge (SSE), and Full Stack Observability (FSO) ensure that this exchange is secure and meets required SLAs.

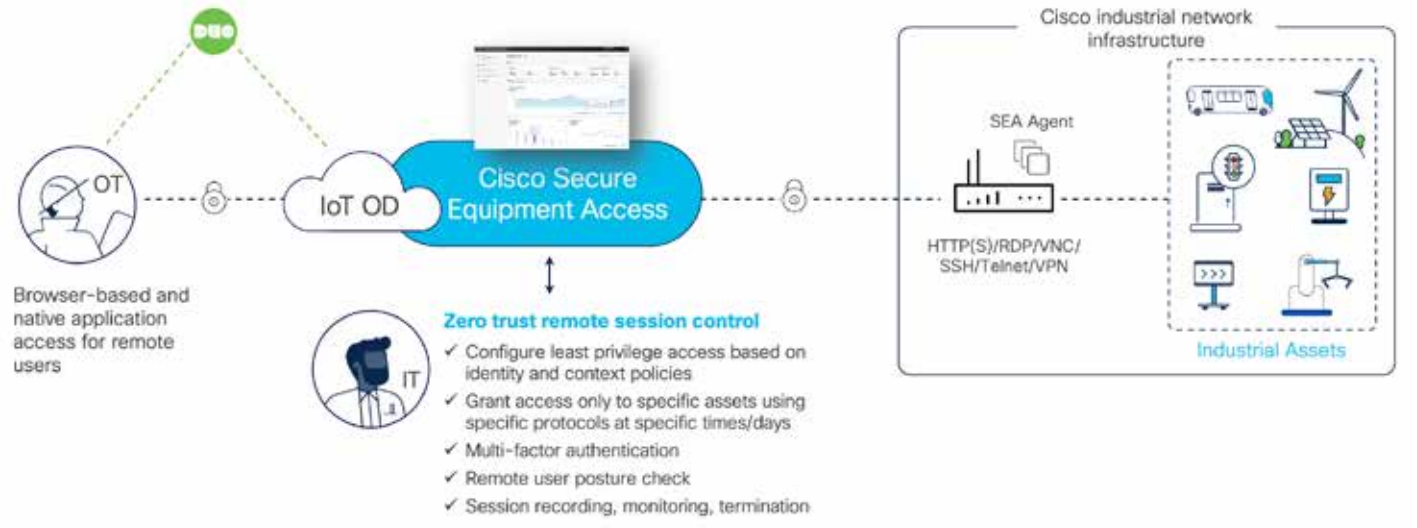
Beydoun: 5G is designed to connect to many different types of devices that can allow for minimizing energy consumption in battery powered sensors with low-band radio frequencies while minimizing latency for automation equipment with high-band radio frequencies. Private 5G networks also open up the possibility of transporting data from a user to an edge compute device for processing and then back again for usage.

The value of this approach is that the user's device can be much lighter due to not requiring as heavy of a battery to support built in processing capabilities. An example use case is Augmented Reality (AR) where a user could have a wearable that would allow them to access devices status and maintenance instructions connected to the plant equipment. This use case can result in reduced training requirements for workers and decreased time required to repair down equipment.

Provide technical details and on how the technology works to help educate readers on new possibilities for address the challenges of IT-OT integration.

***Bhargava:** Network equipment:* Commonality between enterprise and operations networking equipment such as the operating system, configuration and control protocols make it easier for utilizing the common set of tools and leverage the skills IT already has, making it easier for IT to help OT. Equipment that provides insights into the traffic with network telemetry (NetFlow) capabilities, automation of tasks with configuration with RESTCONF, NETCONF, etc., APIs, and support for software-based segmentation capabilities as well as remote access to industrial assets, help place IT in a better position to make the OT network scalable, flexible, and high performing.

Operations security: Cybersecurity is on top of everyone's minds and both teams realize the need to protect operations. Tools that perform deep packet inspection (DPI) on network traffic can provide granular visibility into connected assets, traffic patterns, and vulnerabilities. This insight can be used to make operations secure by addressing vulnerability issues, defining, and enforcing segmentation policies, continuous monitoring for identifying potential threats, and taking



SOURCE: CISCO

A well-reasoned infrastructure and plans for secure equipment access can effectively use zero trust remote session control technology.

proactive actions to mitigate these threats.

For example, Cisco Cyber Vision sensor resides withing Cisco industrial switches, performs DPI, and provides insights that can be used by Cisco Identity Services Engine (ISE) and Cisco DNA Center to set policies that are enforced by Cisco industrial switches.

Machine-to-cloud: Cloud technologies under the umbrella of SASE architecture deliver converged networking and security-as-a-service capabilities. The architecture includes SD-WAN which brokers between WAN links such as MPLS, 4G/5G, etc., for the best possible connection, helping improve application performance. Another part of SASE is SSE which provides a set of security services to defend against threats and enforce user, data, and application access policies.

FSO helps identify performance issues that IT teams can quickly address before they become a problem. It goes beyond visibility of performance in a single part of the network but provides insights into the entire "technology stack" that includes endpoints, operations network, enterprise network, SD-WAN, and even cloud applications. This is another area that operations can benefit from IT expertise.

Beydoun:

5G networks are able to accomplish the task of multiple specialized networks through a technology called network slicing. Portions of a network can be optimized for a specific application and operate independently. These slices can be more efficient by being tailored to exactly what they need to accomplish. Network slicing can divide up a network in a way similar to Virtual Local Area Networks (VLANs).

Today, 5G offers the ability to enable IT/OT collaboration as a direct connection from added sensors or existing machine diagnostics to higher level systems such as Supervisory Control and Data Acquisition (SCADA), Computerized Maintenance Management Systems (CMMS), Enterprise Resource Planning (ERP), and cloud environments for data evaluation and response. While many of today's 5G enabled applications are currently supplements to existing automation network infrastructure, that is likely to change as further technology enhancements to adapt 5G to industrial automation take place and additional successful use cases are proven.

Given the challenges of IT-OT convergence from a technology perspective, what is your personal view of the importance of this issue for your customers and plans currently in progress.

Bhargava: Most of our customers recognize the importance of bridging the gap between these traditionally separate domains due to the increasing adoption of digital transformation, Industry 4.0, and the Industrial Internet of Things (IIoT). However, not everyone is where they need to be. Technology certainly helps.

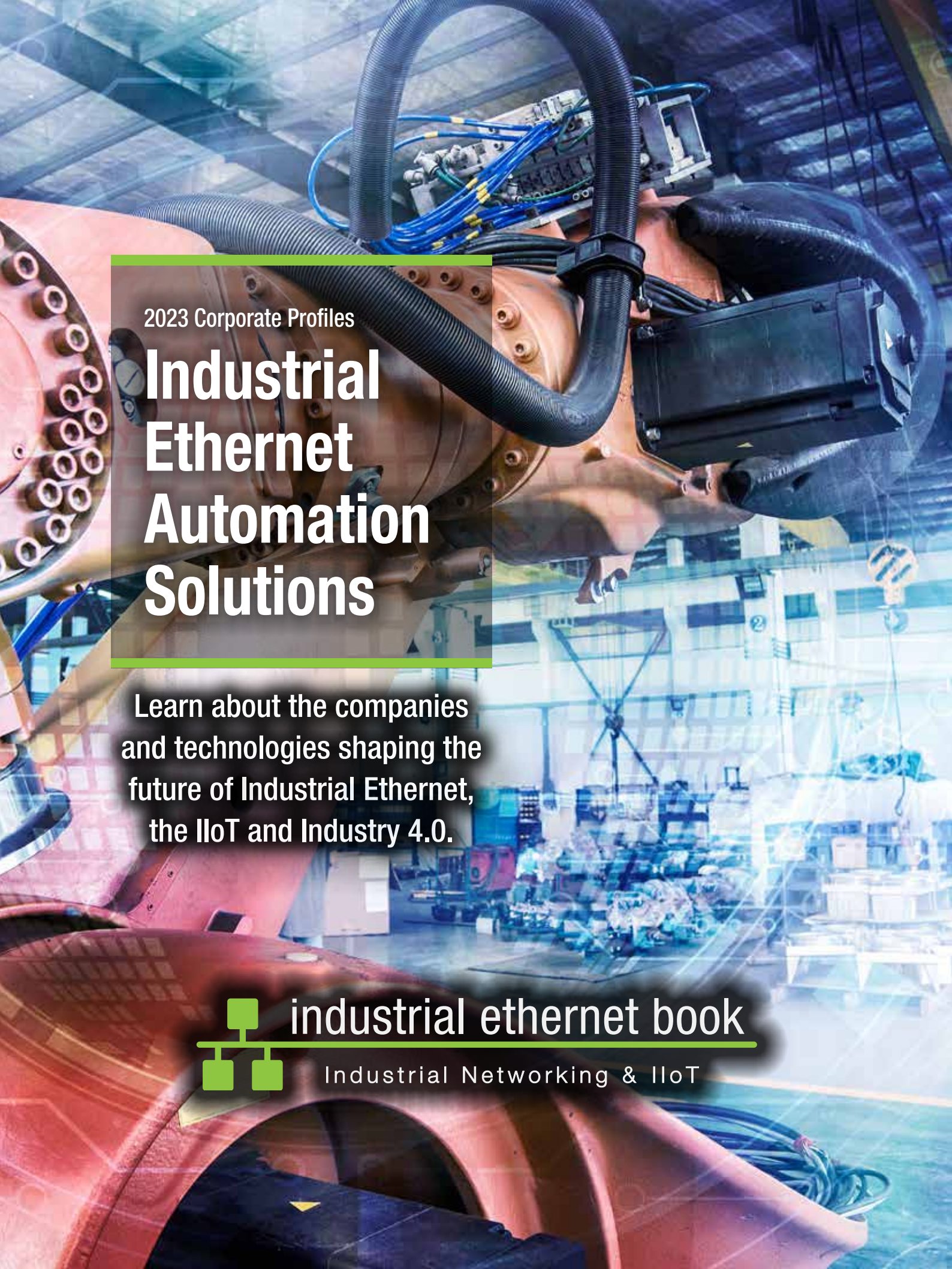
For example, Unilin Group, part of Mohawk industries, and maker of flooring, MDF boards, and insulation panels, adopted Industry 4.0. IT quickly realized that they needed visibility, segmentation, and control. This realization spurred the IT team to standardize on Cisco Catalyst IE3400 switches at scale and run Cyber Vision for visibility and to define segmentation policies. But because the budget was owned by OT, IT demonstrated to them the value, benefits, and potential savings to make the case for change, partnered with the OT team, and together they defined and enforced security policies that do not disrupt production. *Read the Unilin case study.*

Another customer that comes to mind is Gwinnett County DOT in Georgia, USA. To effectively manage traffic across a network of 2650 miles (about the width of the United States) of roads and 750 traffic signals, their OT teamed up with IT to digitize their vast network with Cisco Catalyst IE3400, Cisco Catalyst IE3300 and other switches. They decided early on that the DOT network would not be in a bubble, and that it would be tied to their IT network, which would give them the flexibility to access it from anywhere in the county. *Read the Gwinnett County DOT story.*

Several other customers have similar projects in progress, and we hope to report on their achievements in due course.

Beydoun: Public 5G networks offer lower cost and convenience through sharing the costs of a pre-configured standard network with others. However, Private 5G networks are ideal for industrial use by ensuring higher potential levels of application customization, security, and reliability. Private 5G networks for automation are in the process of being deployed now. In fact, the EtherNet/IP industrial network has been shown to be ready to use with 5G through a proof-of-concept test between Ericsson, Qualcomm, and Rockwell Automation.

A test plan was developed and executed to show reliable EtherNet/IP and CIP Safety communication with the goal of zero faults. The test cases were run from a Rockwell GuardLogix area controller over 5G (3GPP Release-15, NSA, on-premise, mmWave spectrum) to Rockwell FLEX 5000 I/O devices across 12 different areas with a range of requested packet interval (RPI) settings. RPI is the rate at which the controller and the I/O exchange data. The test was successful and shows that a private 5G network can support default EtherNet/IP and CIP Safety RPI settings as a result of low latency and jitter. The supported RPI settings will allow for wireless industrial applications such as stationary (static, nomadic, rotating parts) skids, machines or equipment that use EtherNet/IP standard and safety I/O communications.



2023 Corporate Profiles

Industrial Ethernet Automation Solutions

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

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. Our 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

- 2022 global sales: €1.515 billion (+28%)
- Headquarters: Verl, Germany
- Managing owner: Hans Beckhoff
- Employees worldwide: 6,000
- Engineers: 2,200
- Subsidiaries/representative offices worldwide: 40
- Sales offices in Germany: 24
- 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, however, not a typical semiconductor company. It pushes the boundaries of silicon technology, investing heavily in software, systems expertise, and domain knowledge within its 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 its 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 Chronous™, Analog Devices´ family 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 10BASE-T1L concepts for robust field instrument connectivity in process control – our market-leading Ethernet portfolio of combined software and hardware solutions are scalable and timed to perfection.

ADI Chronous encompasses 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 Chronous 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 Chronous 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 and rich industrial expertise and system design knowledge coupled with advanced technologies 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.

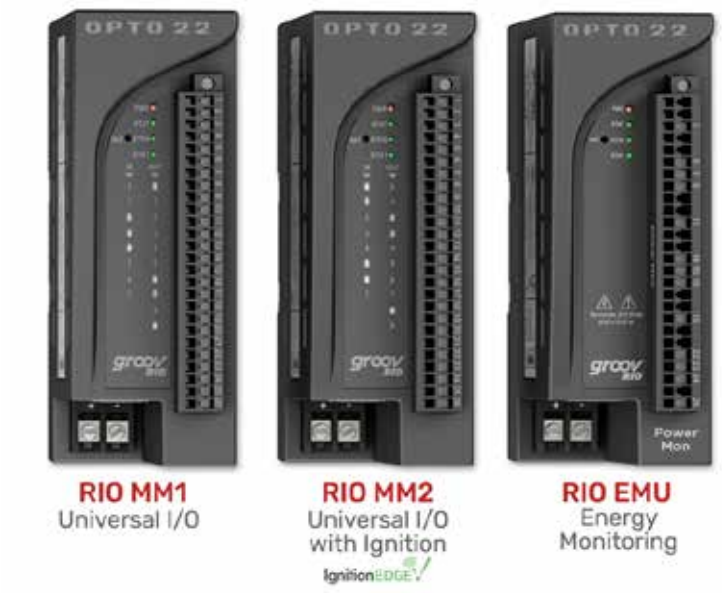
SOURCE: OPTO 22

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.

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



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.

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.

Opto 22
www.opto22.com

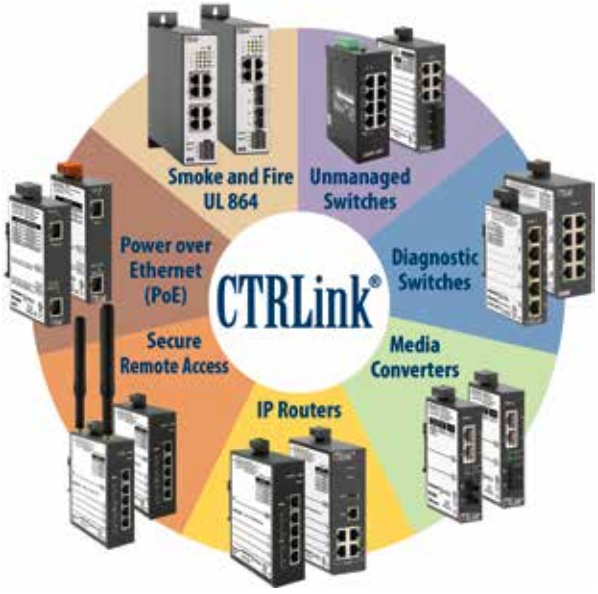
Visit Website

Contemporary Controls: Your Trusted Partner

Providing innovative and reliable solutions to the industrial automation industry for more than 48 years, Contemporary Controls has been a leader in innovative solutions for industrial automation.

WITH MORE THAN 48 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.



SOURCE: CONTEMPORARY CONTROLS

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.

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

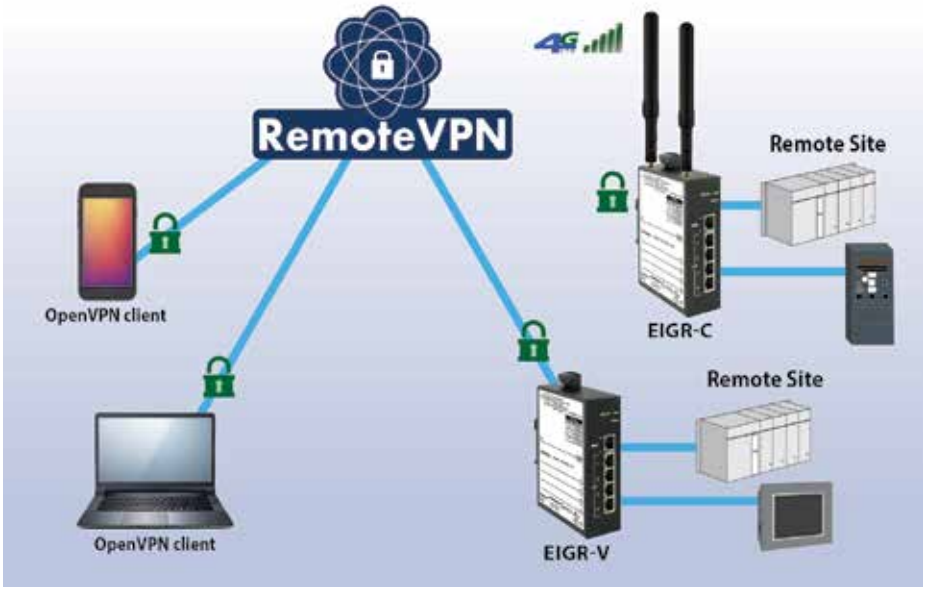
Contemporary Controls' Skorpion series of IP routers ease the integration of new machines into the existing network. Each machine consisting of multiple IP devices connects to the LAN side while keeping the same IP settings for the devices and the application, lowering installation cost and eliminating 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.



The RemoteVPN service provides secure remote access.

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

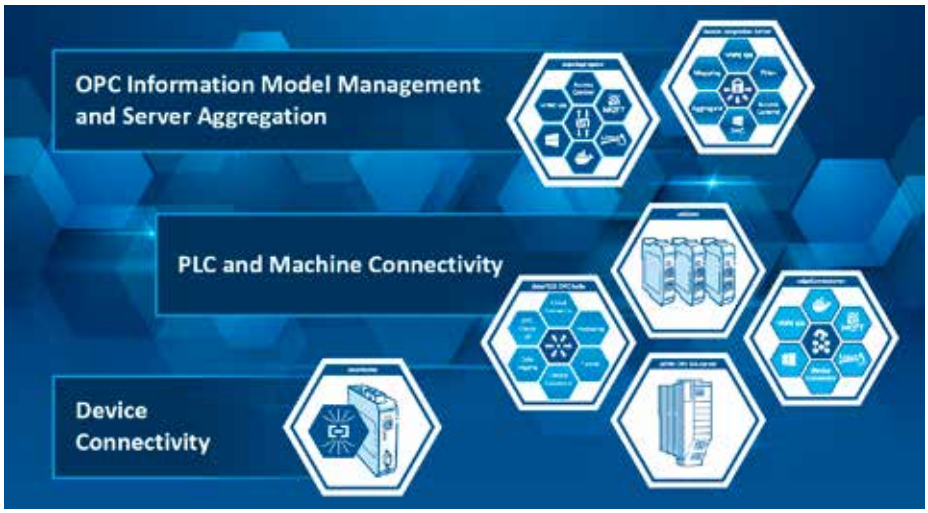
Visit Website

Softing Industrial: Data Integration for Industrial IoT

Designing OT/IT integration and cloud connectivity in a secure and flexible way.

THE CONNECTIVITY OF MACHINES IS A central component of the digital factory. IoT applications, monitoring, and data analysis can only be implemented flexibly and securely if devices and systems are networked end-to-end.

As a recognized expert in digital data exchange in industrial applications, Softing Industrial can support you in bridging technological gaps and flexibly and securely designing smooth data exchange between machines and plants, OT/IT integration, and cloud connectivity.



SOURCE: SOFTING INDUSTRIAL

Softing products ensure seamless data exchange between machines and plants, OT/IT integration, and cloud connectivity.

Machine Connectivity

Our machine connectivity products help to improve scalability and reduce the operating cost of your solution in both brownfield and greenfield projects. The Docker-based **edgeConnectors** provide access to process data in Siemens and Modbus controllers. The integrated software solution **dataFEED OPC Suite** serves as a complete package for OPC communication and cloud connectivity, providing access to the controllers of leading manufacturers and to IoT devices. The products improve connectivity at the interface of OT and IT and facilitate the use of standard IT management and monitoring solutions.

Device Connectivity

Digital plant asset management helps plant managers to improve their operation, commissioning, maintenance, and diagnostics processes. The software and hardware solutions **smartLink SW** and **smartLink HW** from Softing Industrial help to unlock HART, PROFIBUS, and other device data for plant asset management applications to support secure and innovative solution architectures.

SOURCE: SOFTING INDUSTRIAL

IT/OT integration up to edge and cloud applications leads to optimized processes.

Server Aggregation

OPC UA has turned into a de facto communication standard for IT/OT integration, supported by many devices. Softing Industrial offers solutions to connect such devices efficiently, add an additional layer of security, and leverage the full potential of OPC UA information models. The **Secure Integration Server (SIS)** acts as an aggregator, providing the required address space filtering, access control, and semantic extraction functions via OPC UA, and serves as a central OPC UA server. SIS combines all mechanisms for the management, regulation, and monitoring of data access in one central location. This allows you to control the interface between OT and IT at a single point and manage it easily and securely. The **edgeAggregator** from Softing Industrial provides OPC UA server aggregation capabilities as well as additional security for OPC UA-based data integration.

Softing Industrial Automation GmbH

info.automation@softing.com

Visit Website

Cisco Industrial IoT

Cisco Industrial IoT (IIoT) transforms critical industries and improves lives by bringing IT to the physical world to increase business resiliency and employee safety.

SOURCE: CISCO

Figure 1: Cisco industrial networking portfolio.

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

Industrial network connectivity

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 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.

Industrial network security

Organizations around the world are connecting their industrial environments to enterprise networks to automate production and gain operational advantages. Organizations are deploying IoT technologies to migrate to Industry 4.0, optimize production, and build new generations of products and services. This 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. 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.

Figure 2: Cisco industrial cybersecurity starts with deep visibility.

Strategic partnerships

Cisco has built and tested joint architectures with leading Industrial Automation and Control Systems vendors such as Rockwell Automation and Schneider Electric, making it easy for customers to implement a complete solution while minimizing risks.

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

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.

SOURCE: MOORE 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 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.

SOURCE: MOORE INDUSTRIES

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 50 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. *Watch the video>*

Moore Industries Worldwide

www.miinet.com
Email: info@miinet.com

Visit Website

Phoenix Contact: celebrating 100th anniversary

In the anniversary year 2023 – Phoenix Contact is celebrating the 100th anniversary of the company's founding.

SOURCE: PHOENIX CONTACT

A CENTURY OF PASSION FOR TECHNOLOGY AND innovation: In 100 years, the family-owned company Phoenix Contact developed from a commercial agency for industrial products into a global manufacturing company.

"Together, we have achieved a great deal over these years, remaining true to the values and culture of our family business despite growth and further development. This anniversary is a special moment for us. We have built the foundation on which we can now continue on our path into the future. Together with our customers and business partners, we will drive forward solutions for the energy revolution that are the basis for a sustainable world," says Frank Stührenberg, CEO Phoenix Contact, describing the significance of the 100th anniversary.

Connections of people and technologies

Good connections are not only elementary in Phoenix Contact's products they have also given rise to a globally active industrial company from the idea of businessman Hugo Knümann. With the founding of Phönix Elektro- und Industrie-Bedarfsgesellschaft in Essen in 1923, the company initially started out as a pure sales company. In 1928, the business connection with RWE led to the invention of the first terminal block on a DIN rail. In 1949, Knümann met Josef Eisert, a development engineer at Siemens, who took over the company in 1953 after Knümann's death.

From Blomberg to the world

A pure sales company becomes a company with its own production. At the location in Blomberg, to which the company had to be relocated during the war, tool shop, plastics production, screwdriver shop, assembly, locksmith's shop, warehouse and shipping department were soon established. With the innovative fieldbus system Interbus, the basis for industrial networking follows in 1987. After the foundation of the first foreign subsidiary in the USA in 1981, more than 50 subsidiaries follow all over the world.

Together for the future

Today, Phoenix Contact employs around 22,000 people and has generated sales of 3.6 billion euros in 2022. Worldwide, production is carried out in a manufacturing network in 11 countries with varying degrees of vertical integration. Together with customers and partners, Phoenix Contact develops solutions for the world of tomorrow with trend-setting connection and automation technology. The holistic concepts including engineering and services are used, for example, in transportation infrastructure, e-mobility, clean water, regenerative energies and intelligent supply networks or in energy-efficient machine building and systems manufacturing.

Social responsibility

Phoenix Contact is committed to paving the way for the "All Electric Society," a future in which energy from renewable resources is available everywhere in sufficient quantities in an economical and sustainable manner. Furthermore, reducing overall energy demand through efficiency measures and creating intelligent and networked systems through sector coupling is key to this sustainable future.

Phoenix Contact GmbH & Co. KG
Email: info@phoenixcontact.com
Phone: +49 52 35 300
www.phoenixcontact.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.

SOURCE: CLPA

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.

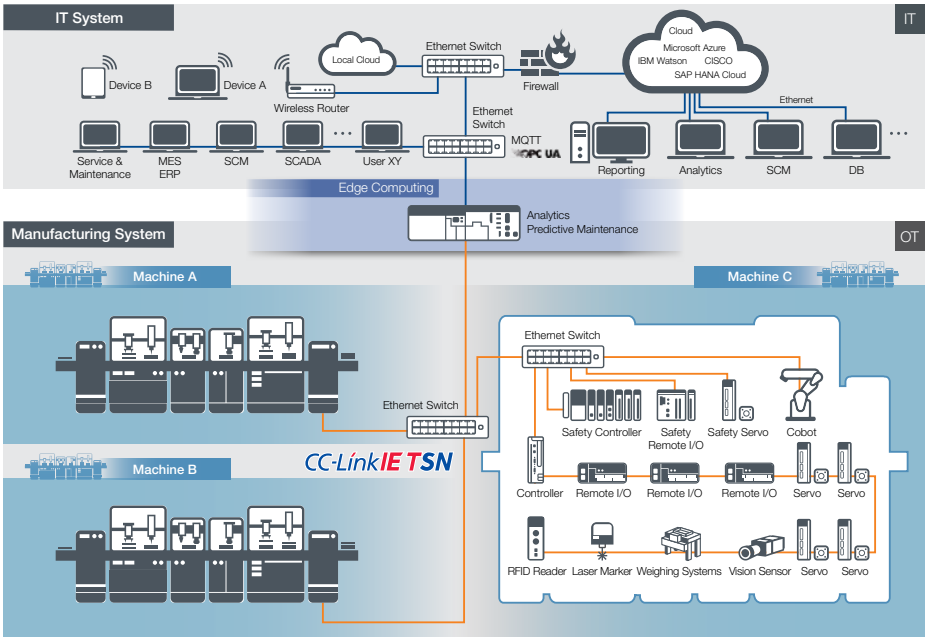
In order to meet demanding productivity and quality targets, current production trends demand cost effectiveness, better process insights, the shortest cycle times and the management of large amounts of process data. Complying to IEEE 802.1 standards, CC-Link IE TSN provides this capability by combining gigabit performance with the integration of control, safety and motion data along with general TCP/IP traffic **on a 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 4,200 member companies worldwide, and more than 2,800 certified products available from over 380 manufacturers. Together, these form a global installed base of about 40 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.



SOURCE: CLPA

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

Forward-thinking Industrial Network Specialists

Hilscher facilitates both powerful and secure industrial networks, systems integrations and device manufacturing through advanced, quality-engineered product offerings.

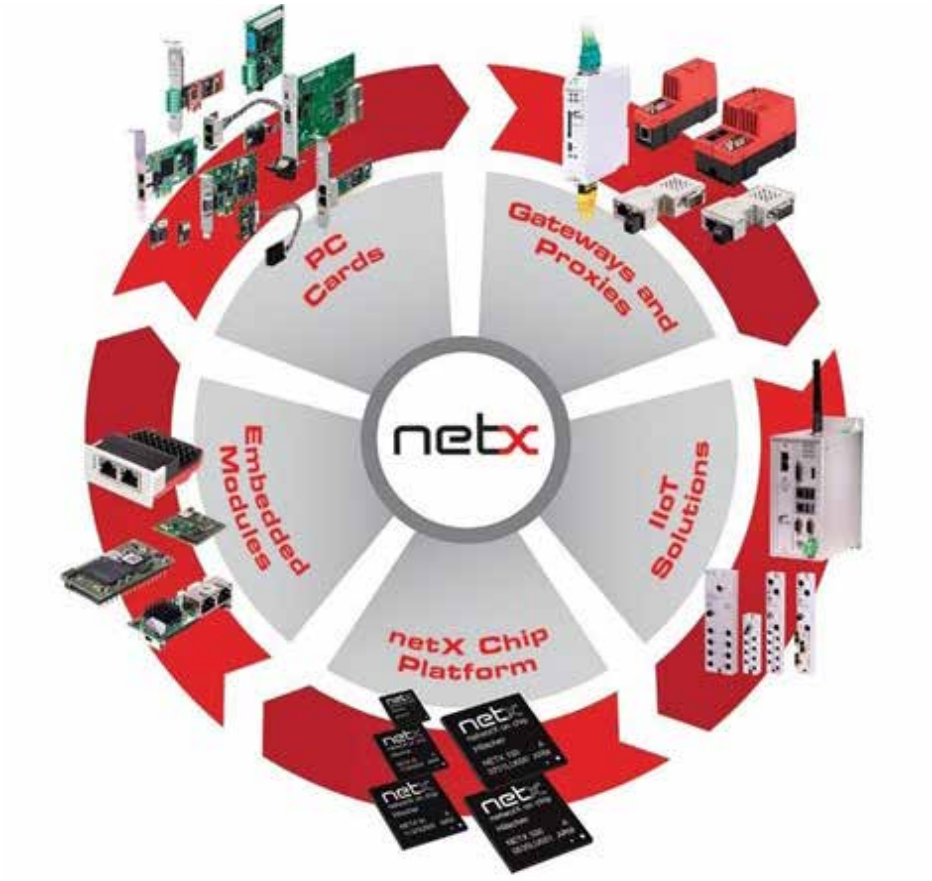
HILSCHER IS A GLOBAL SPECIALIST IN NETWORK connectivity solutions for device makers, OEMs, system integrators and end-user manufacturers. Founded in 1986 with locations worldwide, Hilscher's communications products span single-chip ASICS, embedded modules, PC cards, gateways, proxies, protocol converters and IIoT solutions.

Advanced and Robust Controllers

At the heart of every product is Hilscher's own netX network controller ASIC. netX is a game-changer because it allows "best-in-class" network choice for any application. The netX-based solutions support industrial communications protocols, including fieldbuses (DeviceNet, Modbus, CC-Link, PROFIBUS and more); real-time Ethernet (EtherNet/IP, EtherCAT, PROFINET, Modbus TCP, CC-Link IE, POWERLINK, Sercos III and TSN) and IIoT protocols (OPC UA and MQTT), with universal master and/or slave connections.

Streamline Security Development

For device makers and OEMs, netX chips and embedded solutions allow any industrial communications protocols to be designed into your products with built-in security, using one chip family and a common set of software tools. This helps "future-proof" your designs while minimizing costs and development time.



SOURCE: HILSCHER

The netX network controller ASIC allows "best-in-class" network choice for any application.

Simple Systems Integration

The primary concern for end-users and system integrators is how to interconnect all the different automation networks found across their manufacturing facilities. Hilscher's netX-based products for these challenges include gateways, proxies, PC cards and supporting software stacks that make it easy to connect one network to another for improved dataflow.

Hilscher's netFIELD portfolio is a platform for simplifying IIoT deployment. It includes sensorEDGE devices and gateways; netFIELD Edge Gateways; netFIELD Cloud, with a Software-as-a-Service Platform and Portal; and netFIELD Applications to configure and connect to automation protocols and commercial clouds.

Hilscher
Email: info@hilscher.us
Phone: 630-505-5301

Visit Website

Nucor subsidiary POK brings foundry to Industry 4.0

New factory saves initial and recurring costs, improves products with groov EPIC and Ignition solutions. The challenge was how, at a reasonable cost, to aggregate all process information from equipment and PLCs and then successfully exchange that information with corporate SCADA and ERP systems.

SOURCE: OPTO 22

Steel pouring process at POK.

MOVING TO INDUSTRY 4.0 TAKES TIME AND determination, especially for an established company in a heavy industry. Castings Foundry POK in Guadalajara, Jalisco, Mexico, was founded in 1894 and in 2018 became a subsidiary of the Nucor Corporation, the largest steel producer in the United States.

A fully integrated precision castings company, POK has moved toward "POK 4.0" in a series of steps over several years, changing from manual to automated systems and integrating those systems for more available, immediate, and reliable data. Their goal is a plant that predicts and prevents defects, communicates the whole process of casting and machining in real time, and where equipment self-regulates based on current circumstances. One of their first steps toward this vision was in 2012, when they developed an enterprise resource planning (ERP) system in response to a customer request for individual serial number traceability. When put in place, ERP data input was still manual. But it was a start.

POK casts parts for oil & gas producers, mining, sugar mills, and other industries, making pumps, pipes, valves, rotors, impellers, drill heads and pieces, and industrial components.

The company produces several alloys such as high-strength steel, stainless steel, low-alloy steel, carbon steel, and other specialty alloys such as Inconel. They offer two types of casting:

SOURCE: OPTO 22

Ing. Giorgio Moreno of POK (right) and Ing. Miguel Cuevas of IC22 (left).

- No-Bake Sand castings, which are generally reserved for larger parts, up to 8,000 lbs.
- Investment casting, which uses the traditional lost wax method or their own proprietary "soluble molding" technique, producing pieces from a few ounces up to 1000 pounds.

In addition, POK offers melting, state-of-the-art vacuum induction melting (VIM), heat treating, CNC machining, a conventional machine shop, and a pattern shop for designs in a variety of materials. Information from all these processes and equipment would need to be integrated.

Focus on customers

In business for more than 125 years, POK has long-standing relationships with customers and focuses on maintaining those relationships. They custom design products for clients and work with them to design products that improve their processes or reduce production costs. Clients often ask POK's design team for help in making a product to slightly different specifications, for example, a harder material or a less expensive design

that serves the same purpose.

With increasing business, the company decided to build a new facility to double its production capacity. Giorgio Moreno, Special Projects Coordinator, was tapped to design POK Acatlan. Giorgio had worked in POK Santa Anita for more than ten years, where he was part of the ERP development and saw the challenges of getting accurate data from disparate equipment and systems. Giorgio was determined to design the new facility with Industry 4.0 in mind.

The challenge

The question was how to do that at a reasonable cost: how to aggregate all process information from their equipment and PLCs and then exchange that information with corporate SCADA and ERP systems. While these systems were currently on premises, Giorgio wanted to leave open the possibility of cloud-based software and services later on.

But integrating all their processes into a single automation system was a non-starter. POK uses equipment from manufacturers all over the world, which may be supplied with PLCs from Rockwell Automation, Siemens, or several others. For the new foundry, they wanted to use the best equipment and processes for their needs, regardless of where it came from or the controller it used. A closed system from a single supplier would limit their options and increase costs dramatically.

Giorgio obtained quotes from system integrators, but the vendors making proposals for the new plant quoted turnkey systems that he knew were more expensive than what they could create for themselves.

"Every equipment vendor wanted to sell us their systems, with their individual monitoring systems that were not compatible with our other machines," he says. "We wanted to develop the new factory internally to save costs and avoid recurring costs such as licensing. The main challenge was to communicate with all our equipment without voiding any warranties."

SOURCE: OPTO 22

The groov EPIC system (center right) offers a wide -20 to 70 ºC operating temperature range.

SOURCE: OPTO 22

Ignition Perspective HMI screens in the main control room.

Working in POK Santa Anita had introduced Giorgio to Opto 22 SNAP PAC products, which he found to be easy to program, simple to use, and highly reliable. When he saw the IoT capabilities in Opto 22's new groov EPIC (edge programmable industrial controller) and its direct integration with Inductive Automation's Ignition SCADA software, he could see the way forward. EPIC and Ignition could integrate data from all possible equipment and processes they might need to use.

Implementation

The 14 groov EPIC systems POK, led by Giorgio Moreno, installed at the edge of the foundry's network serve multiple purposes: local control, connectivity with PLCs in the separate systems, data acquisition, and secure communications with Ignition.

Each EPIC system consists of an industrial processor and I/O on an 8-module chassis, all UL Hazardous Locations Class 1 Div 2 approved and ATEX compliant. The sturdy stainless-steel construction of the system and its wide -20 to 70 °C operating temperature range fit right into the foundry's needs.

SOURCE: OPTO 22

KUKA Robot controlled via groov EPIC for Shelling process.

EPIC processors can be programmed with either Opto 22's flowchart-based PAC Control or with any IEC 61131-3 compliant language using the CODESYS Development System. For this implementation, Giorgio chose CODESYS for programming.

"The digital inputs indicate position switches of the equipment and its moving parts; the digital outputs are for driving solenoids and for lamps to indicate system status to the operator. The thermocouples are for temperature, the 4-20 mA inputs for temperature and pressure sensors, and the 4-20 outputs for some control loops, especially to regulate temperature," explains Miguel Cuevas, Gerente Comercial at Opto 22's distributor in Mexico, Instrumentación y Control 22 (IC22). IC22 provided both the Opto 22 and Inductive Automation products.

In addition to local control, the EPIC processors are used for supervisory control, for example, to run batch processes. And unlike a standard PLC, they also connect directly to PLCs and other automation equipment: variable speed drives, KUKA robots, induction ovens, compressors, and much more. The EPICs consolidate data from all these and exchange it via Ignition with the ERP and SCADA systems.

A groov EPIC system can run either Ignition EDGE or Ignition FULL on its processor, but in this case, Giorgio chose to run Ignition on a separate server. He uses Ignition Tag Historian, Alarm Notification, Perspective, Sequential Function Charts (SFC), and OPC UA. Postgres, an open-source SQL database, provides the database for Ignition Historian. The flexible ERP is Odoo.

The company uses the Perspective Module's scripting function to directly control some processes in specialized equipment. They also use Ignition to directly monitor power meters, gas meters, resin meters, and sand level meters, some of their largest recurring production costs.

HMIs

Giorgio has taken full advantage of the opportunities for operator interfaces (HMIs), using both Ignition Perspective and the groov View software built into groov EPIC.

"We now have a mission control in the center of our factory where all pertinent Perspective screens display every active part of our process," says Giorgio.

"Perspective has allowed us to add an HMI to any of our equipment, including those that don't even have a physical HMI. All of our operators, with the appropriate credentials, can view the HMI of any machine using tablets at the machine or even with their mobile device."

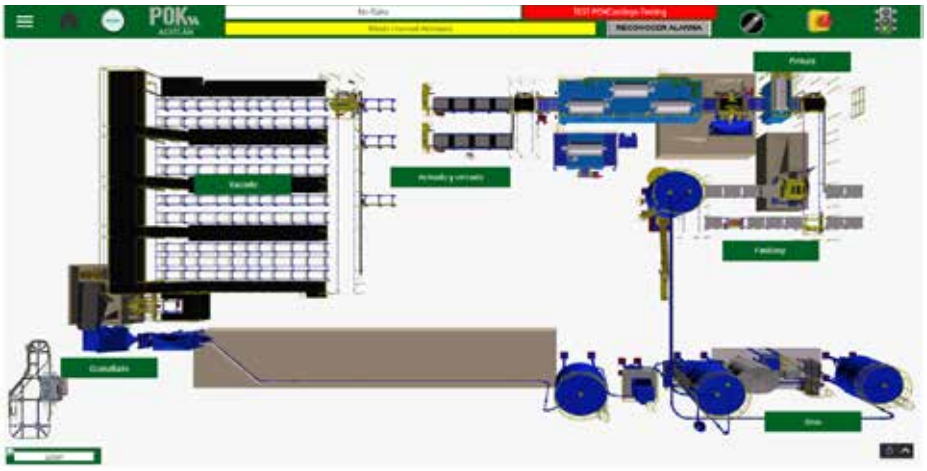
At the same time, the groov View HMI gives Giorgio local access to systems.

"We were able to use both groov View's HMI and groov View HMI screens give local access on mobile devices.

Perspective simultaneously, and that allows us to have local HMI control should our network connection to the edge ever fail. This was great for us to find out, as we used these double HMIs for our processes that are

SOURCE: OPTO 22

groov View HMI screens give local access on mobile devices.



Perspective HMI Screens: Top View for No Bake (top) and Silos for No Bake (bottom)

Perspective HMI screen: Kuka Robot Control for Shelling.

of critical importance."

"I have an integrated HMI and I can take advantage of organizing my factory into zones depending on their proximity to a nearby EPIC. I can integrate all independent processes—shelling, inductive furnace, heat treatment, etc.—and have a local HMI that allows me to control it, with no added costs," he says.

In addition, they can freely and easily create and generate new reports and trends in groov View.

Results

POK is delighted with the results of the work. Manufacturing now is fully automated, from order entry into the ERP system, to manufacturing the product, to updating finished goods in the same ERP.

Operators find that historical reports, process tracking, and tracking production make their jobs easier. Every engineer can monitor any part of the plant from their mobile phone, a local tablet, or from mission control at the center of the plant.

SOURCE: BECKHOFF

The company estimates it is saving money in many ways: initial outlay, lower recurring costs, improved product quality through tracking, faster new product production with automated orders in the ERP system, and even labor costs.

"We estimate to have saved over 60% of the cost of this had we purchased a turnkey system from our vendors. We don't have to pay any recurring licensing costs for any of our software. We are not limited by users, devices, tags, screens, etc. Ignition allowed us to use the licenses that we had already purchased for our equipment from our first plant into this second plant with ease," says Giorgio.

They look forward to upgrading POK Santa Anita using the same licenses and physical servers used for POK Acatlan. "With EPIC, I can talk to any PLC that I purchase: Rockwell, Siemens, Mueller I/O. We can add new machines, new processes, new operators, new software, new visualizations, and our only cost is the time to make the modifications in Ignition," he notes.

Labor costs are significantly less than with a large closed system, too, Giorgio says. "Because EPIC, CODESYS, and Ignition are so easy to use, we were able to hire recent college graduates to do much of the programming and HMI screens. For example, engineers can transfer skills in any IEC 61131-3 language to CODESYS. You can have two people with experience and everyone else can be less experienced."

Future plans

At this point POK2 Acatlan is 80% operational, and the company is looking forward to applying a similar tech stack with groov EPIC and Ignition in POK Santa Anita.

"We chose Opto for its simplicity in the development and implementation of projects, because there are no recurring license costs, and because the support is free. The cost/benefit ratio is excellent," says Giorgio. "Working with Opto was wonderful, both with local support from the Opto 22 distributor in Mexico and directly from Temecula, California."

As Miguel from IC22 summarizes, "The remarkable thing about this project was that we exploited the capacity of the IIoT concept, because the EPIC took information from field sensors, made control loops and control logic like any ordinary PLC, with the plus that it communicated with Allen-Bradley drivers, with a KUKA robot that speaks EtherNet/IP, and more. In addition to all this, it shares information with the SCADA Ignition and finally with the ERP Oodo."

POK 4.0 has arrived.

*Application article by **Opto 22**.*

Learn More

Reduce industrial CO_2 emissions via increased motion efficiency

There is a great need to reduce industrial CO_2 emissions. But the path to net zero will also create new opportunities for industrial manufacturing companies to embrace new technologies to accelerate lower carbon manufacturing. Increased industrial activity will also double the number of deployed motors in use by 2040.

CONSUMERS TODAY ARE LOOKING FOR LOWER carbon products and services. Governments around the world are increasing regulations to reduce carbon emissions to meet their net zero greenhouse gas emissions targets.

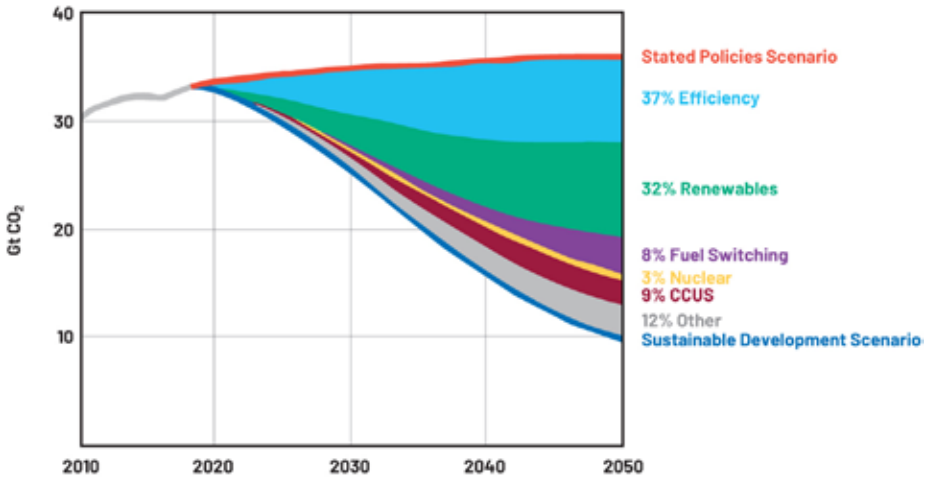
Navigating the path to net zero will create new opportunities for industrial manufacturing companies to embrace new technologies to accelerate lower carbon manufacturing. This article will delve into two essential focal points to improve CO_2 reduction in the industrial sector:

- Increased energy efficiency through increased deployment of motor drives
- The impact of digital transformation strategies to deliver increased manufacturing efficiency

The Paris Agreement in 2015 set out a plan to limit global warming to 1.5°C by 2050. Meeting the 1.5°C target in 2050 requires a >80% reduction in current CO_2 emissions. The current trajectory is toward global warming of 1.9°C to 2.9°C, which will lead to a significant reduction in global GDP, displace up to 33% of the world population, and cost trillions of dollars in annual disaster-related losses.

The world has warmed by 1.1°C and experts say that it is likely to breach 1.5°C in the 2030s. The challenge to meet the 1.5°C target is significant. It will require a shift in investment away from fossil fuels and toward energy efficiency, renewables, and nuclear power generation as well as carbon capture, utilization, and storage (CCUS) along with other low carbon areas. Figure 1 outlines a path to the 1.5°C target by reducing CO_2 emissions to 6 Gt CO_2, as covered in World Energy Outlook 2019. This study includes two major sections: the Stated Policies Scenario and the Sustainable Development Scenario.

The Stated Policies Scenario considers only specific policy initiatives that have already been announced. The Sustainable Development Scenario describes a pathway that enables the world to meet climate, energy access, and air quality goals, and is fully compliant with the Paris Agreement. At the same time, it maintains a strong focus on the reliability and affordability of energy for a growing global population. The largest reduction in CO_2 emission identified as part of the Paris Agreement is efficiency at 37%. Global energy-related CO_2 emissions grew by 0.9% in 2022, reaching a new high of over 36.8 Gt. Emissions



SOURCE: ANALOG DEVICES

Figure 1. CO_2 emissions reductions by measure in the Sustainable Development Scenario relative to the Stated Policies Scenario.

from industry declined by 1.7% to 9.2 Gt in 2022. With 25% of CO_2 emissions coming from industry in 2022, accelerating industrial energy efficiency investments will be a key part of the path to net zero emissions in 2050.

Higher efficiency motors can reduce industrial CO_2 emissions

The global electricity supply in 2022 was 28,642 terawatt-hours, contributing 13.6 Gt of carbon emissions (36% of global CO_2 emissions in 2022). Industry consumes 30% of global electricity, with electric motors making up 69% of power consumption. With ~450 Mu of motors installed in the industry and ~52 Mu new motors installed in 2022 (split between brownfield upgrades and greenfield developments), higher efficiency motion assets are reducing electricity consumption and CO_2 emissions. Motors are used across industrial applications to drive pumps, fans, compressed air systems, material handling, processing systems, and more. It is estimated that if all deployed motor driven systems were operated at maximum efficiency, it would reduce global electricity demand by 10% and remove 2490 Mt of CO_2 emission in 2030.

Increased energy efficiency with deployment of motor drives

The most basic and lowest efficiency motion solutions are based on a grid-connected or AC-powered, 3-phase motor that uses a switchgear to provide on/off control and protection circuitry. These basic motion solutions run at a relatively fixed speed, independent of any load variation.

Adjustments in output variables (such as fluid flow in pumps and fans) are implemented with mechanical controls such as throttles, dampers, and valves, and significant speed changes are implemented with gears. It is estimated that 70-80% of all deployed motors today are grid connected and would benefit from being connected to an inverter or variable speed drive to reduce energy consumption.

The addition of a rectifier, DC bus, and a 3-phase inverter stage creates an inverter with variable frequency and variable voltage output that is applied to the motor to enable variable speed control. This inverter driven motor significantly reduces energy consumption by running the motor at the optimum speed for the load and application. Examples include higher efficiency pumps and fans. When added to the existing motor of a pump, fan, or compressor, an inverter can typically reduce power consumption by ~25%.

For higher performance motion control applications, a VSD enables accurate torque, velocity, and position control. To achieve this, current and position measurement are added into the basic open-loop inverter drive. Conveyors, winding, printing, and extrusion machinery are typical examples of these applications. It is estimated that between 20% and 30% of all deployed motors in industry are inverter driven or connected to a

Figure 2. Industrial motors key statistics.

VSD. By moving more deployed motion assets from grid-connected motors to inverter driven or VSDs, we can significantly reduce the energy consumption and CO_2 emissions of the ~450 Mu of motors deployed in industry.

The important role of motor energy regulations

Intelligent motion control solutions are delivering and will continue to deliver significant reductions in energy consumption by moving more applications from fixed speed motors to high efficiency motors and VSDs, in part driven by energy efficiency regulations.

This reduction in energy consumption will enable more sustainable manufacturing with reduced CO_2 emissions. To accelerate the deployment of higher efficiency motor driven systems, the International Electrotechnical Commission (IEC) has contributed to the definition of energy-efficient electric motor standards. This includes the IEC 60034-2-1 test standard for electric motors and the IEC 60034-30-1 classification scheme comprised of four levels of motor efficiency (IE1 through IE4). These standards have made it easier to compare efficiency levels between motor manufacturers. They also provide a reference for governments to specify the efficiency levels for their minimum energy performance standards (MEPS), helping countries to meet their energy efficiency and carbon dioxide emissions targets.

IEC 60034-1 Efficiency Classes:

- IE1 Standard Efficiency
- IE2 High Efficiency
- IE3 Premium Efficiency
- IE4 Super Premium Efficiency

Significant progress has been made by governments worldwide to set MEPS for motors. Since 2020, countries consuming 76% of global electric motor system electricity have introduced MEPS for motors at either the IE2 or IE3 level, contributing to reduced industrial electricity consumption. In the EU, since July 1, 2021, a minimum efficiency class of IE3 (Premium Efficiency) is required for motors from 0.75 kW to 1000 kW. A minimum of IE2 (High Efficiency) is required for smaller motors from 0.12 kW to 0.75 kW. Starting July 1, 2023, the MEPS will increase to IE4 (Super Premium Efficiency) for motors between 75 kW and 200 kW in the EU.

When we look at the total cost of ownership of a motor driven system over the life of its deployment, 70% of the total cost is electricity compared to 5% for the purchase of the motor and 20% for the maintenance of the motors. Therefore, by deploying more efficient motion driven systems, we can significantly reduce the operation cost of industrial motors while also reducing CO_2 emissions.

Digital transformation strategies deliver manufacturing efficiencies

VSDs use data from voltages, currents, position, temperature, power, and energy consumption combined with external sensors for monitoring vibration, and other process variables. With a converged information technology/operating technology (IT/OT) Ethernet network, motion applications are networked together communicating data and motion insights to cloud-based data storage or on-premises storage.

Motion data and insights are more accessible and can be analyzed by powerful cloud computing and artificial intelligence to optimize manufacturing flows, reducing the energy consumption and CO_2 emissions created in manufacturing. Access to motion insights extends equipment lifespans, improves manufacturing quality, and reduces unplanned downtime and material wastage while increasing safety in plants.

Motor driven systems are now integrating advanced sensing, signal processing, edge AI, and connectivity solutions to create motion data and insights at the Intelligent Edge. These new insights are communicated to the manufacturing execution system (MES). The MES can then identify deployed motors that are being operated significantly below their nominal rated output, resulting in underutilization and increased electricity consumption. Another critical capability is identifying deployed motors that operate too near to or slightly above their rated output, which also results in increased electricity consumption and potential lifetime issues. In a large manufacturing installation with several hundred to several thousand motors deployed, digital transformation strategies are especially crucial to reducing electricity consumption and CO_2.

World Economic Forum—Sustainable Lighthouse Network

The World Economic Forum's Shaping the Future of Advanced Manufacturing and Value Chains platform has set up the Global Lighthouse Network, which recognizes top leaders in manufacturing as lighthouses. The World Economic Forum's Global Lighthouse Network showcases real-world examples of how digital transformation strategies are accelerating the reduction of CO_2 emissions in industry. It is a community of manufacturers using advanced technologies to drive new innovations in smart manufacturing to increase productivity and sustainability. As of January 2023, the Global Lighthouse Network comprises 132 manufacturing sites worldwide, including 13 sustainability lighthouses. Schneider Electric's Le Vaudreuil factory is one of the sustainability lighthouses at the forefront of digital transformation. The Le Vaudreuil facility has demonstrated the impact of data-driven insights to catalyze more sustainable manufacturing by:

- Reducing power use by 25%
- Reducing material waste by 17%
- Reducing CO_2 emissions by 25%

Conclusion

The path to net zero will create new opportunities for industrial manufacturing companies to embrace new technologies to accelerate lower carbon manufacturing. Increased industrial activity (almost half of which occurs in China and India) will double the number of deployed motors in use by 2040.

Therefore, the CO_2 reduction impact and the business opportunity size for new higher efficiency motor driven systems will increase significantly. At Analog Devices, we are fully dedicated to driving automation toward a more sustainable and efficient future. Our advanced technologies and solutions are designed to support the next generation of manufacturing systems, focusing on improving every level of efficiency from precise motion control and seamless connectivity to enhanced insights and analytics at the edge.

Maurice O'Brien, Strategic Marketing Manager, Industrial Automation, ***Analog Devices.***

Learn More

SCADA is dead, or is it?

Industry 4.0 is changing the way manufacturers operate, but it is also transforming how SCADA systems work, and what businesses should expect from them. Long gone are the days when straightforward data capture is enough. To fulfil Industry 4.0 goals, SCADA systems must be much more advanced.

SOURCE: COPA-DATA

To fulfil Industry 4.0 goals, SCADA systems must be much more advanced.

DATA PLAYS A VITAL ROLE IN DIGITALIZATION of industrial facilities. But, as industry's digitalization goals become more ambitious, and our expectations of facility data increases, how is technology for data capture and analysis changing?

Let's get this straight: SCADA as we knew it is gone. The traditional automation pyramid has collapsed, and IT/OT convergence is on the rise. The next generation of solutions has arrived and is paving the way for advanced manufacturing.

We are in the age of industrial digitalization, and control and monitoring software has never been so ubiquitous. Before we can understand the purpose of SCADA in Industry 4.0 journeys, we need to understand how the technology is changing. The technology has shifted from a tool for monitoring and data capture, to the technology shaping the smart factories of the future. One of the crucial ways this is achieved is the use platforms with open system architecture.

Open system architecture

Open system architecture describes the elimination of vendor dependence that is often associated with early and proprietary SCADA systems. In practice, an open system is not limited to operating with one original equipment manufacturers (OEMs) products, or a limited number of communication protocols.

This level of flexibility is key to ensuring modern systems are fit for purpose in modern factories. Moreover, providers of futureproof SCADA systems must be willing to continually adopt and embrace new standards to keep up with the growing scale of Industrial Internet of Things (IIoT) device networks. When specifying a software platform, guaranteed updates are one the one hand a necessity, however vendors do also need to ensure Long-term support (LTS) for up to ten years.

IT and OT convergence

Another consideration is the integration of Information Technology (IT). Some modern platforms are capable of integrating data sets that were previously limited to the IT space. For instance, capturing data from Enterprise Resource Management (ERP) or Manufacturing Execution Systems (MES) systems for consideration alongside Operational Technology (OT) data from the factory floor.

Data collected by IT systems can be used to streamline production processes, fix critical issues faster and make better informed decisions — but only if it is collected, transmitted and processed effectively and securely. The most effective systems will

SOURCE: ISTOCK

IT/OT convergence is on the rise, and the next generation of solutions has arrived and is paving the way for advanced manufacturing.

be able to operate across both of these technology spheres. In addition, a software platform doesn't only gather data from different hardware and IT systems but do also need to provide data in an open format and accessible for third parties, e.g. through a REST API. Modern SCADA can operate like a data hub or, as you could also name it, as an OTIL (Operation Technology Integration Layer).

Applying SCADA for Industry 4.0

Now we understand the potential of modern SCADA systems — how do engineers use this technology in their digitalization journey? On its most basic level, a SCADA system lets an operator verify that its machinery is operating correctly. However, modern systems should enable an operator to use SCADA data to determine how to make improvements or adjustments to equipment to maximize productivity or efficiency.

At the beginning of any digitalization project, a manufacturer should consider its data sets and use them to determine smart goals. Is achieving better energy efficiency a key company goal? The platform should be capable of identifying areas of high energy usage, and this is where that organization should start their process. Is improved capacity to produce customized projects a goal? In this case, data on equipment availability will be key. In order for the company to make informed decisions on digitalization, having access to a full facility of data sets is key.

Without having clear visualization of all the data produced from a facility — whether this is related to energy usage, productivity, downtime or something else — it is impossible to embark on an informed Industry 4.0 journey. In fact, proper investment in data collection technology should come before any other smart factory investment — including any hardware.

Challenges of SCADA upgrades

A common challenge faced by engineers when updating their SCADA system is setting up new automation projects. Overhauling aging SCADA systems can leave engineers with a significant programming burden. This is particularly challenging as the industry continues to struggle with skills shortages. However, good systems are capable of removing the need for complex programming.

The product philosophy of COPA-DATA's zenon, as an example, is to set parameters instead of programming. In practice, this means an extensive library of pre-designed static and dynamic elements and symbols. This means that no prior knowledge of programming is needed and projects can be created via clicking instead of coding — in comparison to an engineer having to write tens of thousands of lines of code. This can result in significantly less downtime for a manufacturer switching its system and crucially, a reduced need for investment, recruitment and training resources for the engineering team.

This ease-of-use is crucial for a next generation SCADA to be implemented in an Industry 4.0 project. Frankly, the only good digital tools you will invest in, are the ones you will actually use.

SCADA for Industry 4.0

There is no doubt that Industry 4.0 is transforming the way manufacturers operate, but it is also transforming how SCADA systems work, and what businesses should expect from them. Long gone are the days when straightforward data capture is enough. To fulfil Industry 4.0 goals, SCADA systems must be much more advanced.

At COPA-DATA, we took the decision to move away from using heavily the terminology SCADA for our solutions approximately five years ago. The zenon software platform had developed into a far more advanced tool for data capture, visualization, analysis and reporting. For manufacturers with Industry 4.0 goals, a platform with this level of comprehension is necessary.

Stefan Reuther, member of the executive board at industrial software specialist, ***COPA-DATA.***

Learn More

What is digital twin technology and impact for manufacturers?

Digital and virtual twins are quickly becoming the staple within many industries thanks to the number of benefits they bring to each company. Manufacturing and logistics in particular can benefit from the technologies, thanks to vastly reduced lead times and help when it comes to planning efficiently.

DIGITAL TWIN TECHNOLOGY HAS QUICKLY become a staple with many of the largest manufacturers in the automotive and industrial engineering sector around the world thanks to its ability to provide huge amounts of value in saving time and optimizing plant effectiveness.

Digital twin | virtual twin technology

Digital twin technology allows manufacturers to gain a digital representation of a real-world system – the digital twin mirrors the software or model to gain data and insight that can update. Digital twin is actually an executable model of a physical system. The physical system can be a factory or a plant or a mine or resource any of them. Which brings in learning and experiences from the physical part, so that you can continuously update your distribution model. The next step up from digital twin is virtual twins, which provide a far more dynamic look factory systems. Virtual twins provide businesses with the ability to visualize models and simulate sophisticated experiences—whereas digital twin solutions are static. Virtual twin essentially shows manufacturers exactly what can be executed and implemented in the real world, it's primary focus is to give actionable solutions to improve efficiencies.

In fact, Virtual Twin technology helps us visualize a model not only of the product, but manufacturing and operations as well. When thinking about the capabilities of digital twins, they operate in a closed loop of "ability to ability", but virtual twin goes beyond that. It provides the opportunity where you can control the real world with the virtual world with this closed loop ability and we can bring innovation to expand on that. Virtual Twin solutions can be beneficial for almost any manufacturing organization, both small and large. It empowers workforce of the future, and considering current conditions, it's like bringing in new resiliency while people are working in the new or next normal due to this pandemic.

Industries that can benefit

Digital twins initially found their way into a select few industries where businesses could easily see value and return on investment. The automotive & industrial equipment sectors were the two main areas that invested in digital twin technology initially, along with oil and gas. These industries had a clear need for the insights provided by digital twins to streamline processes and provide extra efficiency.

SOURCE: DELMIA

Virtual twins provide businesses an ability to visualize models and simulate sophisticated experiences.

In more recent times, manufacturing and life sciences are beginning to really catch up on the benefits that are brought about by digital twins as they're really relying on the twins ability to provide sophisticated models that can be acted upon. In manufacturing and the operations industries, the overall goal for most businesses is to achieve greater profitability in a safe and sustainable way.

The length and breadth of industries that can adopt this type of technology stretches far and wide, and the same can be said about virtual twin technology, as this is essentially a step further than the insights offer by digital twins.

Why important for manufacturers?

There are benefits to having digital or virtual twins integrated into your workflow as a manufacturing business, though the most pertinent are time, cost and resource savings, increased levels of safety for all employees. In recent years, there's been an increased focused on sustainable manufacturing and a 'circular economy', with real emphasis being placed on improving the overall productivity and safety of processes. Alongside this, there's been a real shift in manufacturing bosses looking for more control over production, whilst also minimizing costs. All of this is covered by digital/virtual twins, as they give manufacturers access to important information about cutting costs whilst maintaining, and improving, workflows.

Whilst manufacturing and operations industries are becoming ever more complex due to the digitalization and innovation within each sector, it's important that things are made as simple as possible. Operation lead times can begin to become longer and longer if inefficiencies in the new workflow aren't ironed out, and that's where digital and virtual twin technology comes in to play. Having insight and agility to make changes in manufacturing is exceptionally important, especially with supply chain issues that are currently facing the vast majority of manufacturers.

To really emphasize the effectiveness of virtual twin technology in particular, in one case study, DELMIA saw plant effectiveness increase by 250% after the installation of a virtual twin. The twin provided an in-depth analysis of inefficiencies and provided the manufacturer with simulation models that would help to combat those inefficiencies. Alongside this, employee safety and fulfillment rose by 5% in time savings.

In a separate case study, DELMIA saw another company increase on-time deliveries by 50% thanks to better planning techniques and technologies. There was a 50% reduction in lead times, enabling the company to maintain high levels of orders, while shipping a higher percentage out on-time to consumers.

Thomas Prashanth Mysore, Strategic Business Development and Industry Marketing Director, ***DELMIA.***

Learn More

Using IP routers for machine control

The Skorpion series of IP routers simplify machine integration into an existing IP network.

SOURCE: CONTEMPORARY CONTROLS

The Skorpion series of IP routers can help resolve network conflicts between the IT department and operations technology (OT).

MODERN FACTORIES ARE COMPRISED OF complex equipment and subsystems that communicate via IP–the backbone of the Internet. The integration of new machines or subsystems can be compromised if they have a fixed range of IP addresses that conflict with other existing plant addresses or the overall addressing policy dictated by the IT department, which often puts restrictions on IP usage. Contemporary Controls' Skorpion series of IP routers can resolve network conflicts between the IT department and operations technology (OT).

IP routers

Skorpion IP routers connect two IP networks together—passing appropriate traffic while blocking all other traffic using either a wired or wireless connection. Either Ethernet-to-Ethernet (LAN-LAN) or Ethernet-to-modem (LAN-WAN) routing is possible with external DSL or cable modems. A stateful firewall makes a WAN connection as secure as possible.

Each machine or subsystem (which consists of multiple IP devices) connects to the LAN side of the router while keeping their same IP settings for the devices and the application, thus lowering installation costs and eliminating troubleshooting.

The IP address for the WAN port on the IP router is the only setting that requires modification to join the factory network, allowing rapid integration and multiple machines to reuse the same configuration on the LAN side. The various machine subsystems are presented as one device to the plant network but can be easily accessed individually by using various features of the IP router, such as Port Forwarding, Port Range Forwarding, and Network Address Translation (NAT).

The Skorpion IP routers allow the machine builder to retain the same configuration used during factory acceptance testing when installing at the customer site. Models are available to support variety of networking and OT requirements. The EIPR series of IP routers have a 10/100Mbps Ethernet WAN port and a built-in 4-port LAN switch. The EIGR series add Gigabit ports for faster speeds and higher data throughput. The EICR series include a built-in cellular modem that links cellular to 10/100/1000 IP networks. Cellular models are also available for European customers.

The routers are also used to isolate traffic and to gain secure access to machines remotely. Some models support Virtual Private Network (VPN) functionality. This can be enabled to allow secure remote access to the machine at the site for remote diagnostics and troubleshooting. This allows remote access to the machine over the internet and through the plant network for servicing. Plant data can be pushed to the cloud for further analysis for process optimization and/or predictive maintenance.

Skorpion IP routers have been successfully used in robotics, automated guided vehicles (AGVs), packaging, scientific equipment, and more. Skorpion IP routers reduce installation time, eliminate IP conflicts, and easily comply with your customer's IP requirements.

Contemporary Controls

Visit Website

Ethernet-APL is ready to use

Endress+Hauser's load test of a realistic setup claims to confirm the new technology's performance.

EXPECTATIONS IN THE PROCESS INDUSTRY FOR the new physical layer are enormous. Now, Ethernet-APL has shown that it can meet these expectations according to testing by Endress+Hauser.

The instrumentation manufacturer Endress+Hauser says they have successfully conducted two load tests of a realistic Ethernet-APL setup with components from various manufacturers. The results confirm the new technology's reputation as a significant development in industrial communication.

The load tests were designed according to customer specifications to prove that components from different manufacturers can be combined to create a reliable and robust system based on Ethernet-APL. The global chemical company BASF defined the requirements from the customers' point of view. On the hardware suppliers' side, Endress+Hauser stood next to Pepperl+Fuchs, Honeywell and ABB. Their components were confirmed to work together effectively.

SOURCE: ENDRESS+HAUSER

Ethernet-APL offers potential bandwidth and speed that could lift field data transmission to a new level.

Ethernet-APL-ready flowmeter. Proline Promass F gives fast process insights. Digital, highly accurate signal processing starts right at the sensor and is the basis for a robust multi-parameter measuring device.

Successful load tests prove market readiness of Ethernet-APL

The first test was set up with nearly 240 Endress+Hauser measuring devices, including flow, pressure, temperature and level sensors. They were integrated into a system with Pepperl+Fuchs' field switches and a Honeywell control system, all using Ethernet-APL and PROFINET. For the second test ABB provided the control system and was tested along with the previous field switches and measuring devices. The test results were deemed to be conclusive. Ethernet-APL can be used under realistic circumstances. The test cases were carried out with maximum network layout, and the scalability and fault tolerance were successfully verified. All relevant requirements like total netload or redundancy switch-over times were met or exceeded.

Open Integration partner program enabled and supported tests

The Endress+Hauser Open Integration partner program unites more than a dozen manufacturers that want to ensure the streamlined interaction of their complementary products. The partners test and document the integration of their offerings and how digitalization may be fully utilized within typical process automation applications.

According to Jörg Reinkensmeier, head of the Open Integration partner program at Endress+Hauser, "The load tests proved that Ethernet-APL can be used for real. The components from various manufacturers work together smoothly, and the systems run reliably. We are proud that the close cooperation with our Open Integration partners made it possible to validate this technology. We have reached a milestone of bringing Ethernet to the field level of process automation."

Ethernet-APL opens new possibilities for data use

Ethernet-APL enables the use of Ethernet at the field level of process plants. The 2-wire technology with power and communication over the same wire pair meets the requirements of even harsh process environments. Fast and digital data transmission with high bandwidth is now possible over long distances and in explosive atmospheres. Easy access to data from field instruments can lift process automation to a new level of efficiency and professionalism.

With the success of the load test, BASF, Endress+Hauser, Pepperl+Fuchs, Honeywell and ABB have taken a significant step towards a technological infrastructure that is open, future-proof and ready for the Industrial Internet of Things (IIoT).

Endress+Hauser is soon launching a full portfolio of Ethernet-APL measuring devices that transmit data via the PROFINET protocol.

Endress+Hauser

Visit Website

Future-proof networking solution

Future-proof networks with Moxa's EDS-2000 and EDS-4000 Industrial Ethernet switches from Impulse Embedded.

MOXA'S EDS-2000 AND EDS-4000 INDUSTRIAL Ethernet Switches are available now from Impulse Embedded providing systems integrators with networking tools that play a pivotal role in connecting multiple devices within a Local Area Network (LAN). Acting as intermediaries, these switches facilitate the seamless transfer of data packets between connected devices, such as computers, Wi-Fi access points, servers, and IoT devices.

Effective industrial Ethernet switches must be durable to maintain seamless, uninterrupted network connectivity and make the most of their capabilities. Moxa's EDS-2000 and EDS-4000 ranges meet all the requirements of industrial network environments.

EDS-2000 and EDS-4000 differences and benefits

- Extended operating temperature range for harsh environments
- Easy access DIP-switch to enable Quality of Service (QoS), and Broadcast storm protection (BSP) and more
- Small footprint frees up space inside cabinets for more device connections
- EDS-4000 is the first IEC 62443-4-2 compliant industrial Ethernet switch

The core main difference between the EDS-2000 range and the EDS-4000 range is their manageability. EDS-4000 Ethernet switches are managed, which provides a higher level of control, security and performance optimisation, making them ideal for medium to large-scale networks that require higher levels of customisation and monitoring.

EDS-2000 Ethernet switches are unmanaged, which means that these switches function out-of-the-box and will work the moment they're plugged in. These switches are simple and easy to use and are a cost-effective choice for simple network environments that will not require much configuration.

EDS-2000 feature highlights

- 5 or 8 Ethernet port options.
- SC/ST fibre models are available for the EDS-2008-EL Series.
- Full Gigabit ports for the EDS-G2000-EL/ELP Series.
- Supports 12/24/48 VDC input.
- Microsecond-level latency.
- High EMC resistance.

When network data travels through an Ethernet Switch, there is no priority over which device takes precedence when entering or leaving. Ethernet Packets or Ethernet Frames arrive on an Ethernet Port and are directed through the switch based on the network table.

SOURCE: IMPULSE EMBEDDED / MOXA

The EDS-4000 range is an IEC 62443-4-2 compliant industrial Ethernet switch, making it an optimal choice for cybersecurity and safeguarding against malicious activity.

Quality of Service is a unique feature for unmanaged switches that addresses this challenge. Devices can assign priority to the traffic they are sending, and the unmanaged EDS-2000 switch can interpret and apply appropriate priority to the network packets being transmitted through the switch.

Broadcast Storm Protection is another essential feature for maintaining consistent network connectivity in the EDS-2000 range. Broadcast Storms can take place for any number of reasons; when a Broadcast Storm occurs, the network is overwhelmed with network traffic in a short period of time, overwhelming its capacity.

The struggle to process this high number of broadcast packets can bring an Ethernet network to a standstill. Network throughput is either greatly reduced, or the network can crash. To maintain network stability and safeguard against these issues, Broadcast Storm Protection is crucial in any network setup, especially an Industrial Automation Ethernet network.

In addition, the EDS-2000 is a cost-effective option in a compact size, freeing up space inside cabinets for more device connections. Despite its form factor, this model doesn't compromise on features and boasts easy data control and durability for harsh environments, including a wide operating temperature range. The EDS-2000 also features remarkably low power consumption figures, which not only leads to reduced energy costs but also aligns with today's growing emphasis on environmentally conscious technology solutions.

EDS-4000 managed switches

The EDS-4000 range is the first IEC 62443-4-2 compliant industrial Ethernet switch, making it an optimal choice for cybersecurity and safeguarding against malicious activity. With 10/100Mbps Fast Ethernet, and 10/100/1000Mbps Gigabit Ethernet in the G4000 series, these switches boast incredible networking speed while your data packets are kept secure in a fully controlled network infrastructure.

A unique feature of Moxa's EDS-4000/G4000 range is its modular power design, allowing the power unit to easily be removed and replaced in the event of a failure. This also makes Moxa's Ethernet switches a seamlessly adaptable choice for varying power demands and redundancy requirements.

Impulse Embedded / Moxa

Visit Website

Secure routers leverage IEC 62443-4-2

Secure cellular routers offer all-round data protection to bolster network security of critical infrastructure.

MOXA HAS INTRODUCED A NEW FLAGSHIP MODEL to its OnCell Series of next-generation secure cellular routers, the OnCell G4302-LTE4. These advanced-level secure cellular routers have new security software that complies with IEC 62443-4-2 standards, improving performance and speeding up vulnerability fixes. Also, their alignment with global wireless approvals enables secure communication for different industrial applications.

The 2022 Industrial Cybersecurity Report by Trend Micro stated cyberattacks had affected 89% of organizations in the manufacturing, electric, and oil and gas industries. Among these industries, the oil and gas sector suffered the most significant financial damages, with an average cost of around USD 2.8 million. These findings highlight the pressing need for robust cybersecurity measures and protocols to safeguard critical infrastructure and protect against financial losses. For example, the famous ransomware attack on Colonial Pipeline in 2021, a turbulent history of cybersecurity and the largest on oil infrastructure in the U.S., shows the importance of strong cybersecurity defenses in OT environments to protect critical operations from cyberattacks.

"Moxa is devoted to developing a comprehensive networking solution with built-in security features for our customers. The OnCell G4300 Series, with its rugged design and industry certificates, ensures Moxa customers' critical systems remain running, and the cellular secure routers always stay at the forefront, protecting Industrial IoT applications from cyberthreats," said Li Peng, head of Moxa Industrial Network Security Business.

The OnCell G4302-LTE4 integrates MXsecurity software, providing centralized security and network management functions to configure and monitor devices remotely. Real-time alerts and notifications help enterprises quickly identify and troubleshoot issues. IEC 62443-4-2 compliance and advanced features like Secure Boot, Virtual Private Network (VPN) and Network Address Translations (NAT) protect data and networks from cyberthreats.

With built-in WAN redundancy and GuaranaLink technology, the OnCell G4302-LTE4 helps recover connection quickly, reducing downtime and minimizing interruptions to operations. Offering industrial-grade reliability, the OnCell G4302-LTE4's rugged hardware is suitable for hazardous locations and has CCCEx, IECEx, ATEX, and Class 1 Division 2 certifications. Its wide temperature range from -30°C to 70°C ensures reliability, even in harsh environments. Furthermore, the OnCell G4302-LTE4 also has the EN50121-4, NEMA TS2, and E-mark E1 certifications to meet the needs of vertical applications.

SOURCE: MOXA

Ethernet-APL offers potential bandwidth and speed that could lift field data transmission to a new level.

Network security based on IEC 62443-4-2

The OnCell G4302-LTE4 comes with GuaranLink support for continuous and reliable cellular connectivity. It restores cellular connections before these issues lead to complete network failure. With the ability to connect via WAN, the WAN Redundancy function detects any loss of WAN connection. It seamlessly switches to the cellular interface when the Ethernet interface is down and automatically switches back when it recovers.

Furthermore, Secure Boot, a built-in security mechanism, ensures edge computers boot only from a validated and authorized bootloader and operating system. All these features ensure the comprehensive protection of cellular routers from most types of threats. However, updates of the OnCell G4302-LTE4 security features will continue to stay ahead of the curve and fend off cyberattacks.

Network management software

The OnCell G4302-LTE4 secure cellular routers, alongside the MXsecurity industrial security management software, provide real-time visibility of cyberthreats with alerts and event notifications. The map view of the status of all cellular routers allows users to monitor distributed devices at a glance, enabling actionable management for better detection and reaction against cyberthreats.

Connecting every device through MRC Quick Link, users can remotely access devices quickly, reducing maintenance costs, and saving time. It helps OT and IT managers arrange resources accordingly for those cellular routers in unmanaged areas. The OnCell G4302-LTE4 not only builds up a security shield for network protection but also supports enterprises by managing all devices globally.

To experience the newest OnCell G4302-LTE4, users can contact Moxa's regional office to join an early-bird program that runs from August 2023 to March 2024. The program has limited openings and will be available on a first-come, first-served basis.

OnCell G4302-LTE4 highlights:

- Global cellular bands support for Europe, Australia, the U.S., Japan, and Asia-Pacific
- Certification approvals by NEMA TS2, E-Mark E1, EN 50121-4, CID2, ATEX, CCCEx, and IECEx
- IEC 62443-4-2 based design for cybersecurity protection with Secure Boot and future software feature updates
- Built-in central management software supported by MXview One, MXconfig, MXsecurity, MRC Quick Link
- Uninterrupted connection technology supported by GuaranLink and WAN redundancy
- Industrial-grade hardware for harsh environments with a wide operating temperature range of -30 to 70°C.

Moxa

Visit Website

Enhanced remote I/O solution

Opto 22's *groov* RIO firmware version 3.5 adds real-time control to remote I/O.

Opto 22 announces the latest firmware version 3.5 for *groov* RIO edge I/O. This latest release includes the CODESYS runtime engine, allowing the groov RIO to now function as a real-time controller coupled with software-configurable I/O.

This latest firmware update offers a CODESYS programming option along with enhancements for performance and security.

The new firmware for *groov* RIO delivers a compact, configurable, and secure PLC for end-user or OEM engineers, technicians, and developers with smaller industrial control applications.

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

groov RIO was introduced to the market in 2020. With this new free firmware update, all current *groov* RIO customers can update their existing RIOs to this latest version and gain these new capabilities.

groov RIO as a PLC

Security, control programming, and software-configurable I/O are now in the same compact *groov* RIO edge device. The on-board CODESYS runtime engine fully supports

IEC-61131-3 control programs written in the programming language of your choice: structured text, ladder logic diagram, functional block diagram, and continuous or sequential function chart.

In previous firmware versions of *groov* RIO, control options relied on Python or Node-RED programming software. The CODESYS control engine now brings an additional programming option for industrial automation applications requiring more low-level control.

To use this new CODESYS runtime engine, users first download and install the free CODESYS Development System from the US CODESYS Store. Next, they download and install version 3.1.0.0 or later of the free Opto 22 Library Package for the CODESYS Development System from Opto 22. They can then create an application and download it to *groov* RIO, making RIO a compact, self-sufficient, and secure PLC—great for machine-building where space is at a premium or where local I/O needs a small footprint.

The CODESYS runtime engine license (product number GROOV-LIC-CRE-RIO) is available for separate purchase from the Opto 22 website for a list price of $100 USD. Once purchased, the activation process generates a CODESYS license key, which is applied to the appropriate *groov* RIO device through the CODESYS Development System.

SOURCE: OPTO 22

This latest firmware update offers a CODESYS programming option along with enhancements for performance and security and support for Sparkplug compatibility.

Other features added to *groov* RIO firmware version 3.5:

- *Sparkplug 3 compatibility*. The RIO 3.5 firmware now includes Sparkplug 3.0 protocol certification. *groov* RIO products now bear the "Sparkplug Compatible" label, ensuring that the Sparkplug specification has been verified and the product provides the highest level of compatibility.
- *Upgraded Node-RED software*. This release also includes an update to Node-RED version 3.0, which offers enhancements like an improved context menu, debug path tooltips, and the ability to search all Node-RED flows continually.
- *Other notable features*. End users will appreciate the additional User Interface options for I/O batch operations, MMP streaming, and Modbus.

For the *groov* RIO model GRV-R7-MM2001-10, version 3.5 firmware also includes an embedded software upgrade to Inductive Automation's Ignition Edge version 8.1.21, improving security and performance.

For complete information on new features and bug fixes, see the ***groov* RIO Release Notes**.

Availability

groov RIO 3.5 firmware is available now as a free download from Opto 22. This free update is available for all three *groov* RIO models: the universal I/O models GRV-R7-MM1001-10 and GRV-R7-MM2001-10, and the power and energy monitoring model GRV-R7-I1VAPM-3.

Opto 22

Visit Website

5GHz wireless AP/client bridge

New 5GHz wireless AP/Client Bridge simplifies point-to-point/multipoint applications.

A secure, cost-effective way to extend wireless networks is the goal of the AMY-5133-AC-PD Wireless Access Point/Client Bridge. Supporting net data rates up to 867Mbps, its semi-industrial radio broadcasts 5GHz, 802.11A/N/AC signals for use in point-to-point and point-to-multipoint wireless data applications, facilitating high-density transmissions between buildings and large areas without the complexity of Ethernet cables.

The AMY-5133-AC-PD can be purchased for $199 (USD). It is also available as a kit (AMY-5133-AC-PD-KIT) comprised of two pre-configured units for those customers looking for simple "out of the box" installations. The kit's pre-configured bridges will automatically locate their peer to create a secure, long-range wireless network link. Pre-configured settings can be changed via the web interface on either side of the network.

The AMY-5133-AC-PD combines a rugged yet compact plastic housing with an integrated high-gain, 14dBi MIMO directional panel antenna and is powered by a Qualcomm™ 802.11AC chipset featuring MU-MIMO technology. These features decrease the time each device must wait for a signal and dramatically speed up the network, improving the transmitting and receiving of multiple data streams even in RF-congested sites. The 128MB of RAM and an additional 16MB of flash memory makes the AMY-5133-AC-PD suited for applications demanding higher capacities.

SOURCE: ANTAIRA

The AMY-5133-AC-PD is engineered for flexible installation. It can be powered by either Gigabit Ethernet IEEE 802.3af/at (PoE, PoE+) via its two RJ45 auto-sensing ports or an external 12VDC power supply. Depending on the application, it can be wall- or pole-mounted mounted in temperature ranges as diverse as -30° to 45° C (-22° to 113° F).

Antaira

Learn More

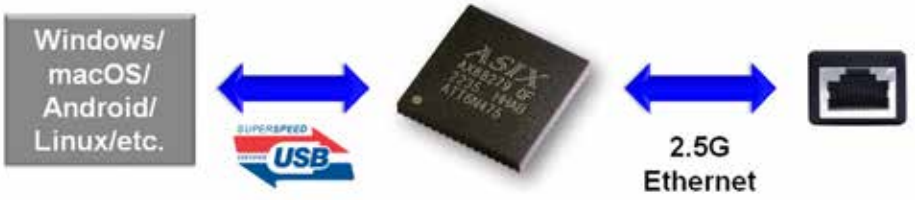
USB 3.2 to 2.5G Ethernet controller

New controller technology provides 2.5G Ethernet performance using new AX88279 USB Chip.

The ASIX AX88279 USB 3.2 to 2.5G Ethernet Controller supports advanced driverless and plug-and-play features by supporting in-box network drivers on different platforms such as macOS, Windows 11/10/8.x, Linux/Android/Chrome OS and Nintendo Switch, etc.

As wireless network technology becomes more ubiquitous, today's laptops and smart mobile devices are commonly equipped with wireless network connectivity to meet the needs of portability, thin & light design, energy efficiency, and cost-effectiveness in the smart world. In this swiftly evolving era of network technology, the demand for rapid and reliable network connections is becoming ever more critical.

Therefore, wired network technology can continue to maintain its pivotal role in the network market by offering high reliability, high-speed transmission, low latency, and robust security network communication. In response to this market's demand for portable, high-speed, and reliable wired network connectivity, ASIX launches the latest AX88279 USB 3.2 to 2.5G Ethernet Controller, which is equipped with an integrated 2.5G/1G/100M Base-T Ethernet PHY and provides maximum network throughput up to 2.34Gbps. In addition, AX88279 supports advanced Precision Time Protocol (PTP) feature for those specific applications requiring precise time synchronization capabilities.



SOURCE: ASIX

In response to this market's demand for portable, high-speed, and reliable wired network connectivity, ASIX launches the latest AX88279 USB 3.2 to 2.5G Ethernet Controller

The AX88279 boasts exceptional cross-platform compatibility, supporting inbox network drivers on major operating systems, including Windows 11/10/8.x, Linux/Android/Chrome OS and Nintendo Switch, etc., and also compatible to the native CDC-NCM driver of macOS and Linux operating systems. This characteristic of driverless installation on different platforms enables users to effortlessly achieve a good plug-and-play networking experience.

The AX88279 is a high-integrated, easy-design and cost-efficient USB Ethernet controller solution. It is suitable for various smart home and office network applications, which require establishing 2.5G Ethernet network connectivity through the USB 3.2 interface, such as laptops, USB Ethernet dongles, docking stations, smart mobile device cradles, POS terminals, game consoles, smart cameras, set-top boxes, 5G/LTE router, and embedded systems with USB 3.2 interface.

ASIX

Learn More

dataFEED OPC Suite

OPC UA tunnel increases security for OPC Classic communication, adds support for InFluxDB databases.

Version 5.30 of dataFEED OPC Suite from Softing Industrial offers two new features: an OPC UA tunnel to increase security for OPC Classic communication plus support for InfluxDB databases.

The dataFEED OPC UA Tunnel is a new component of Softing Industrial's dataFEED OPC Suite. It enables easy and secure access to OPC Classic servers across network boundaries and firewalls. A DCOM configuration is no longer required.

Configuration of the two tunnel ends is quick and easy using Export/Import. The security mechanisms of the OPC UA standard, which include authentication of users by means of certificates as well as signing and encryption of data, ensure maximum protection. The suite currently supports up to 50 OPC UA tunnel connections.

SOURCE: SOFTING

Process data storage in Influx DB databases

With version 5.30 dataFEED OPC Suite offers the possibility to store process data in an InfluxDB for subsequent processing and analysis. InfluxDB is one of the most widely used NoSQL databases. It ensures extensive scalability, high availability as well as fast writing and reading.

All-in-one data integration solution

dataFEED OPC Suite Extended is a complete package for OPC communication and cloud connectivity, providing access to the controllers of leading manufacturers and to IoT devices.

The suite acts as a gateway between the two OPC standards, allowing the integration of existing OPC Classic components and applications into modern Industry 4.0 OPC UA solutions.

Softing

Visit Website

Industrial Ethernet PoE++ switches

New series of ruggedized Industrial Ethernet switches with PoE++ for power hungry devices.

The IE220 Series of industrial-grade switches are ruggedized for enduring performance in harsh environments such as those found in OT networks and outdoor installations. These switches are hardened to withstand difficult environmental conditions, such as electromagnetic noise, wide-ranging temperatures, high humidity, and vibration.

The IE220 Series is designed for many vertical markets and related applications, such as:

- *Building automation:* Facility management including security and access control, fire protection, energy management, heating/ventilation/air-conditioning, and lighting control.
- *Smart cities:* Public space and urban infrastructure that provides safety and security, parking management, environmental metering, lighting, and information kiosks.
- *Roadway transportation:* Adaptive traffic control, telematics, and preventive maintenance.

IE220 Series switches deliver high-performance Gigabit connectivity to IIoT devices without compromising performance or throughput, thanks to dual 10 Gigabit fibre uplinks and PoE++ Gigabit interfaces.

SOURCE: ALLIED TELESIS

High power

The PoE++ Gigabit interfaces offer up to 95W per port. Along with a generous power budget, this makes the IE220 Series the ideal companion for surveillance cameras, monitors, point of sale, access systems, PoE lighting and other devices that require over 30W to operate.

Allied Telesis

Learn More

Skycloud for managing field data

Solution provides capabilities for monitoring, analyzing and controlling field data.

Digi SkyCloud is a solution for monitoring, analyzing and controlling field data. The 23.5 update of SkyCloud introduces a range of new features, giving users systems integrations with remote monitoring and control solutions — delivering flexibility and optimal efficiency, making it well-suited for industrial, agricultural and environmental industries.

Company administrators can now better manage their deployment and user base. At the forefront of this release are the introduction of REST APIs and the ability to deploy device configurations across groups of devices. Additional key highlights from the latest SkyCloud release include an intuitive user interface and improved user experience. With a modern look and feel, SkyCloud now offers improved search and filter functionality, a quick view tile page with user-organized device status, and user roles management for company administrators.

This latest cloud update emphasizes Digi's long-standing dedication to delivering comprehensive solutions for industrial monitoring and control across various sectors, including water management, precision agriculture and environmental compliance.

SOURCE: DIGI INTERNATIONAL

Introduced in early 2023, Digi Connect Sensor+ coupled with SkyCloud provides companies with seamless data collection and visualization capabilities for remote field data. Within minutes, organizations can configure sensors, establish threshold alarms, and gain valuable visual insights, enabling the rapid deployment of Industrial Internet of Things (IIoT) capabilities in just a matter of days.

Digi International took ownership of the SkyCloud platform as part of its acquisition of Ctek in 2021.

Digi International

Learn More

Efficiency through energy transparency

Energy, power and phase angle can be recorded directly at the machine.

With the EE 121-1 from the S-DIAS series energy, power and phase angle can be recorded directly at the machine. The compact DIN rail module supports the user in predictive maintenance and can also be used to monitor costs.

The voltages from the 3 input phases (L1, L2 and L3) are measured and up to 12 currents are recorded which can be assigned to any phase. The voltage, as well as current inputs have a 16-bit resolution. The measuring range of the UL/CSA verified module is 0-520 V AC and 0-2 A AC.

In addition to current and voltage sequences, the EE 121-1 can be used to measure and monitor the phase position and frequency. It enables the calculation of Ueff and Ieff for each channel, as well as the energy consumption since the first activation. The module can also detect power disruptions or a phase drop and registers the 0 crossing point for the application.

The main power synchronization is also possible with the S-DIAS modul. A timestamp function is hereby provided for the zero voltage crossing points. Therefore, when using several energy recording modules, the time offset of the voltage zero crossing points of two main voltages can be determined.

SOURCE: SIGMATEK

Voltages from the 3 input phases (L1, L2 and L3) are measured and up to 12 currents are recorded which can be assigned to any phase. The voltage, as well as current inputs have a 16-bit resolution.

Technical data:

- Dimensions: 25 x 104 x 98 mm
- 3 voltage inputs (0-520 V AC)
- 12 current inputs (0-2 A AC)
- UL/CSA verified

Sigmatek

Learn More

Safety logic solver and alarm

New SLA Multiloop and Multifunctional Safety Logic Solver and Alarm from Moore Industries.

To meet demand for Industry 4.0 factory automation solutions keeps across the United Kingdom, a new partnership was created between UK's industrial automation distributor Routeco, and global wireless industrial automation solution provider CoreTigo.

The two companies agreed on pursuing a joint effort, leaping industrial automation forward and creating numerous new applications and capabilities. By doing so, Routeco is expending the spread of IO-Link Wireless communication in its territories, shifting machines to wireless communication, and unbinding their full capabilities.

IO-Link Wireless provides essential characteristics for advanced industrial manufacturing. From a 5 Msec low latency and deterministic nature, through scalability reliability and coexistence capabilities, it portrays must have abilities for a competitive market. IO-Link Wireless presents reliability of 1 e-9 Packet Error Rate (PER), which compared to everyday wireless communications protocols such as Wi-Fi, Zigbee and BLE (Bluetooth low energy), is 1 million times better (1e6).

Complementing Routeco's portfolio, some of CoreTigo's main solutions target challenges in the Packaging, Automotive, Pharmaceuticals and Metal Works. Enabling for the first time real-time control and monitoring on industrial rotating devices, IO-Link Wireless enhances and opens the door for new capabilities with Rotary Tables & Carousels, Transport Tracks, Smart Machine Tooling, Robotic End-of-Arm, Condition Monitoring and many others.

SOURCE: MOORE INDUSTRIES

IO-Link Wireless is a deterministic, low latency (5 msec), highly-reliable and scalable universal wireless communication protocol. Based on the IO-Link IEC 61131-9 standard, it is designed for factory automation, coexisting with both wired and wireless networks.

Moore Industries

View Data Sheet

Fully managed Ethernet switches

Rockwell Automation offers more functionality on the plant floor by releasing new, fully managed switches.

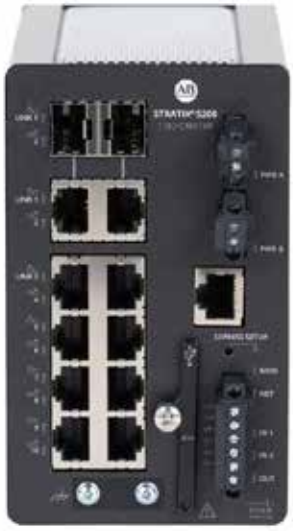
Stratix® 5200 fully managed Ethernet switches from Rockwell Automation have higher port speed options, all gig ports and still offer redundant and resilient system features, including DLR and PRP. The Stratix switches are easier to set up, configure and offer enhanced security features.

New Allen-Bradley® Stratix 5200 fully managed switches offer various hardware configurations and features. These options give machine builders more value and flexibility.

Key features include:

- Expansion of higher port speed options with all gig SKUs
- Redundant and resilient architecture options that support fully managed and high performance switch tiers
- Simplified portfolio and switch selection that is streamlined for fully managed and high performance

Stratix 5200 managed switches are based on the Cisco® IOS® XE platform that includes a new graphical web user interface for improved performance, enhanced troubleshooting tools, fundamental disaster recovery features and customizable dashboards. They also align with Cisco Cyber Vision Sensor options and tie into Cisco TrustSec software for a defined segmentation approach. In addition, they offer fundamental protection against counterfeit hardware and software risks and additional encryption options.



SOURCE: ROCKWELL

The switches include a robust set of switching features to support a wide range of architectures and complies with international standards, such as IEC 62443-4-2 for cybersecurity, offers port security, and access control lists.

Rockwell Automation

Learn More