



industrial ethernet book

Industrial Ethernet Automation Networking & IIoT

Industri

Special Report

Remote Connectivity Solutions

Page 30

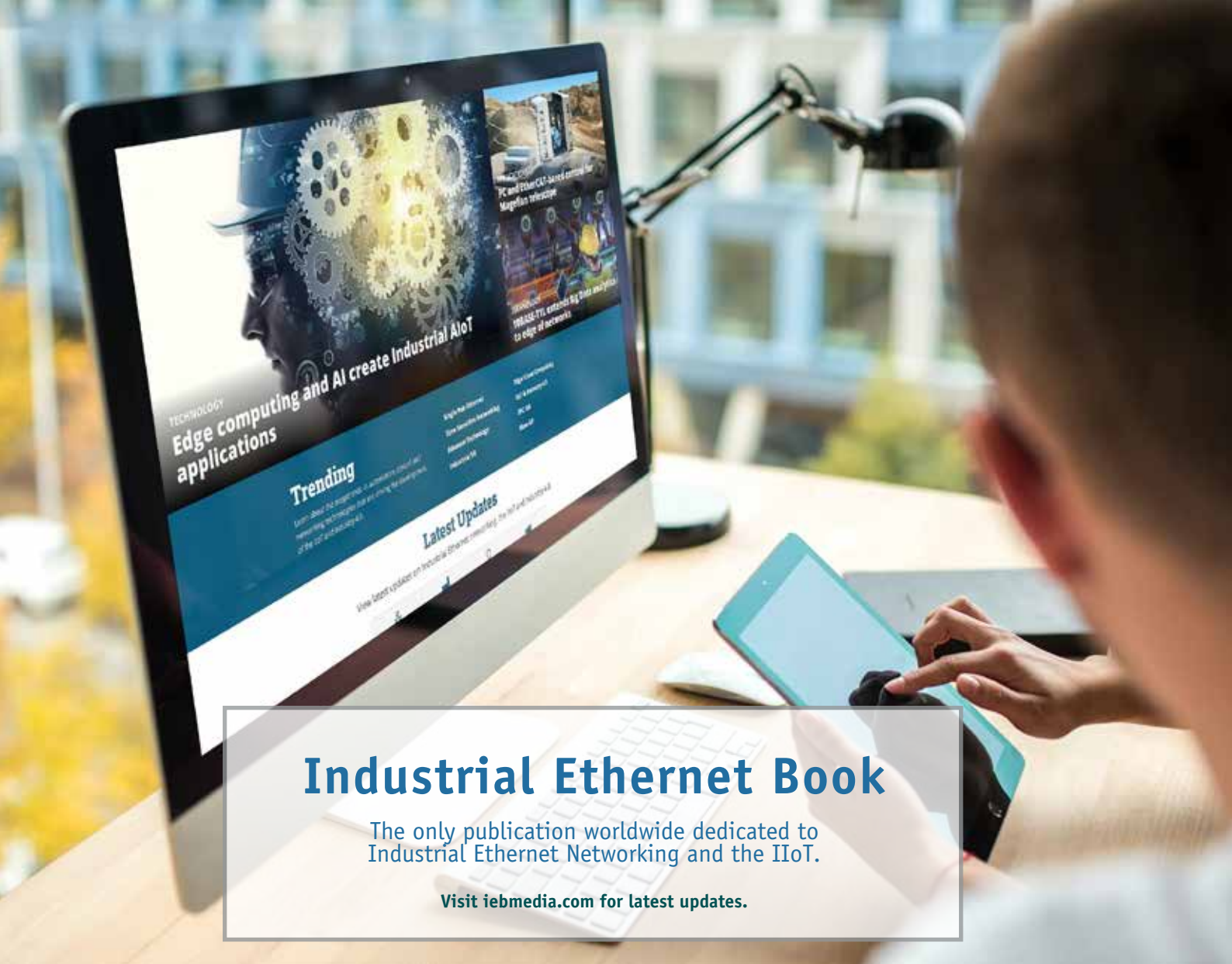
Impact of edge computing on the smart factory 6

Machine monitoring
with edge devices 15

Edge architectures and
cloud in smart factory 20

Current status of AI in
manufacturing 22

Navigating complexities
of Wi-Fi installations 42



Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

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



eBook Archive



Technical Articles



Latest Updates



Trending Topics

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

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

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

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

Industrial Edge and Remote Connectivity solutions

This issue of the Industrial Ethernet Book places the spotlight on two key technological issue: the continuing rise of Industrial Edge Computing and solutions for Remote Connectivity.

Starting on page 6, we present our cover story, "Industrial edge computing rising to the next level", and industry experts who give insight into the current technology trends.

Here is a snapshot look at the topics covered by each of the industry experts interviewed:

AI and machine learning: Data processing on dedicated edge devices is becoming increasingly complex and extensive.

Edge and cloud computing: As data at the edge keeps growing, sending all of it to the cloud isn't practical or affordable

Hyperconnectivity becoming a core requirement: Enabling communication between a wide variety of industrial assets, often spanning different protocols, vendors, and technology generations.

Adoption of cloud and IT technologies: Cloud and IT technologies such as virtualization and containerization are the driving forces behind the rise of industrial edge computing.

Edge computing and cybersecurity: Industrial edge is taking a very prominent role in operational network architecture design.

Software-driven automation: Containerized architectures for flexible software deployment on edge computing equipment, making updates and patch management efficient and scalable.

The bottom line is that industrial edge computing is now in a key role, as the IIoT and Industry 4.0 initiatives continue to grow and AI solutions are moving into the industrial world.

Check out our Special Report starting on page 30, "Industrial remote connectivity solutions" which presents the industry's views on the trends in this key technology area.

Remote connectivity solutions enable quick troubleshooting and maintenance, minimizing production interruptions, and eliminates the need for on-site visits, saving travel expenses and time. Remote access allows personnel to operate and monitor equipment from a safe distance, particularly in hazardous environments.

For this special report, the Industrial Ethernet Book reached out to leading companies involved in developing remote connectivity solutions, asking them to discuss an Industrial Remote Connectivity technology solution they provide, and the specific technical benefits that this approach offers.

Al Presher



Remote Connetivity Solutions: 30



New Products: 46

Contents

Industry news	4
Industrial edge computing rising to the next level	6
Machine monitoring with edge devices	15
Edge architectures and cloud computing impact manufacturing	20
Current status of AI in operational technology	22
Autonomous production with new AI and robotics capabilities	25
Using IO-Link transceiver to manage the data link selection	27
IEB Special Report: industrial remote connectivity solutions	30
Do you actually know... EtherCAT? Part 3	38
Virtualization: the next step in substation evolution	40
Navigating the complexities of Wi-Fi installations	42
Overhead crane performance with advanced AC motor drives	44
New Products	46

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2025**.
Deadline for editorial: September 12, 2025 **Advertising deadline:** September 12, 2025

Editor: Al Presher, editor@iebmedia.com

Advertising: info@iebmedia.com

Tel.: +1 585-598-6627

Free Subscription: iebmedia.com/subscribe

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

Report confirms growing dominance of Industrial Ethernet

After an exceptional surge in 2023, the market experienced a slight slowdown in 2024, with a decrease of approximately 10–11% in newly installed nodes.

HMS NETWORKS HAS RELEASED ITS ANNUAL analysis of the industrial network market, revealing key trends and developments. After an exceptional surge in 2023, the market experienced a slight slowdown in 2024, with a decrease of approximately 10–11% in newly installed nodes. This dip is primarily attributed to a challenging economic environment, uncertainties, and excess production capacity in highly automated sectors such as automotive and manufacturing, particularly in Europe.

Despite the overall slowdown, the study confirms that Industrial Ethernet continues to strengthen its position, while traditional fieldbus technologies are declining at an accelerating pace. During the past two years, shortages in electronic components sustained the demand for serial-based fieldbus solutions as companies turned to any available technology. However, with components now more readily available and economic pressures mounting, the focus has shifted toward more cost-efficient and scalable Ethernet-based communication.

In the 2025 study, HMS concludes that the industrial network market continues to grow, with total market growth over the next five years estimated at +7.7%. Although 2025 is expected to be below this average due to current market conditions, a ramp-up is anticipated in the following years, confirming the continued importance of network connectivity in factories.

Ethernet-based networks now represent 76% of new installations.

The 2025 analysis shows that Ethernet-based industrial networks now account for 76% of new nodes, up from 71% in 2024.

Leading the Ethernet pack:

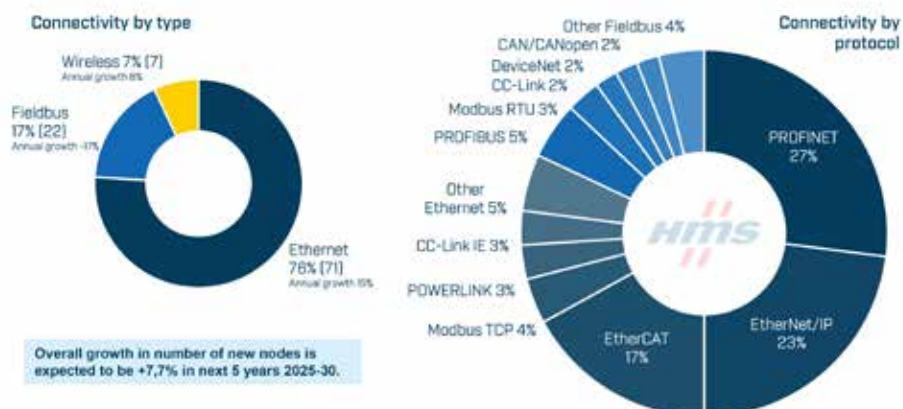
- PROFINET strengthens its lead at 27% (up from 23%)
- EtherNet/IP follows at 23% (up from 21%)
- EtherCAT continues a strong trajectory at 17% (up from 16%)
- Modbus TCP holds steady at 4%
- POWERLINK, CC-Link IE, and other Ethernet networks remain stable, with slight adjustments

Fieldbus technologies now represent just 17% of new nodes, down from 22% in 2024.

Within Fieldbus:

- PROFIBUS remains the largest but drops to 5% (from 7%)

Industrial network market shares 2025



- DeviceNet, CC-Link, and Modbus RTU each decline by 1 percentage point
- CAN/CANopen holds steady at 2%
- Other Fieldbus protocols collectively make up 4%

Wireless remains steady a 7%

Wireless technologies interconnect 7% of new node installations, remaining stable compared to 2024. Wireless continues to be an important complement for non-real-time critical communications, mainly for use cases requiring mobility, flexible networking, or hard-to-reach areas such as in AGVs (automated guided vehicles), mobile industrial equipment, and retrofitting legacy systems. 5G wireless technology, currently implemented for mobile telecom usage, is still experiencing slow adoption in industrial automation. This is due to the complexity of infrastructure management, high implementation costs, and challenges in achieving affordable real-time performance in cellular chips. However, despite these barriers, early industrial deployments, particularly in Asia, are already underway, and the technology holds exciting potential for the future of industrial communication.

Regional insights

Europe: Strong adoption of PROFINET and EtherCAT, with increasing interest in new infrastructure technologies like APL (Advanced Physical Layer) to enable Ethernet communication for process automation applications, and SPE (Single Pair Ethernet) for Ethernet communication up to sensors.

North America: EtherNet/IP remains

the leading protocol in North America, but adoption of smart device-friendly technologies like IO-Link, APL, and SPE is clearly growing, with strong market momentum expected in the coming years.

Asia: PROFINET and EtherCAT are both growing in the Chinese market, while CC-Link IE, the first industrial protocol with TSN mechanism, maintains a strong regional foothold.

HMS Networks' perspective

"This year's data clearly confirms the ongoing shift from traditional fieldbuses to Industrial Ethernet. It's a transition driven by the need for more modern network capabilities in today's automation systems," said Magnus Jansson, VP Marketing at HMS Networks. "While Industrial Ethernet is now well-established, we still see strong growth due to an appetite for more information and the digitalization of the industry. The Ethernet infrastructure also paves the way for further innovation toward gigabit Ethernet, TSN, Single Pair Ethernet, and OT/IT convergence."

The average growth expectation over the coming 5 years is estimated at 7.7%, despite the short-term political and economic uncertainties and upcoming cybersecurity regulations that will force automation companies to rethink the way they connect automation systems.

Magnus Jansson, Vice President of Marketing, Industrial Network Technologies, HMS Networks.

Ultra-compact industrial PCs: Multi-core computing power in IP20 and IP65/67



Measuring just 82 x 82 x 40 mm and with unparalleled mounting flexibility, the C6015 ultra-compact Industrial PC makes optimal use of even the smallest installation spaces. The particularly robust C7015 variant, on the other hand, delivers multi-core computing power directly to the machine to open up even more potential applications. The integrated Intel Atom® CPU with up to 4 cores enables simultaneous automation, visualization, and communication – even in demanding industrial IP65/67 applications. In addition to classic control tasks, both ultra-compact IPCs are particularly well-suited for use as a gateway for networking machines and system parts. Their exceptional computing power means this is even possible with complex pre-processing of large amounts of data. The integrated EtherCAT P connection on the C7015 provides additional flexibility for I/O expansions.

Scan here to see all the benefits
of going ultra-compact



New Automation Technology **BECKHOFF**

Industrial edge computing rising to the next level

Industrial edge computing processes data locally within industrial environments, enabling real-time analytics and machine control. It's used in predictive maintenance, robotics, and quality assurance by reducing latency and enhancing automation.



SOURCE: ISTOCKPHOTO

‘AI-BASED ANALYTICS ON AN EDGE DEVICE CAN DELIVER HIGHLY ACCURATE REPORTS ABOUT THE CONNECTED MACHINE. USE CASES SUCH AS PREDICTIVE MAINTENANCE AND ANOMALY DETECTION CAN BE INSTALLED DIRECTLY ON A MACHINE—EVEN RETROACTIVELY,’ -- DANIEL MANTLER, PRODUCT MANAGER HMI/IPC AT PHOENIX CONTACT GMBH.

FOR THIS REPORT ON THE INDUSTRIAL EDGE, the Industrial Ethernet Book reached out to industry experts to get their perspective on the technologies that are impacting industrial edge computing and its use in the smart factory.

Industrial edge computing solutions involve processing data closer to its source in industrial settings, enabling real-time analytics, automation, and improved decision-making. These solutions typically involve ruggedized edge devices, specialized software, and connectivity options to handle the unique demands of industrial environments while also integrating solutions from the IT world.

Secure and reliable communication between edge devices, the cloud, and other systems is crucial and increasingly involves utilizing industrial communication protocols including as OPC UA, MQTT, and REST APIs.

AI and machine learning

Data processing on dedicated edge devices is becoming increasingly complex and extensive.

According to Daniel Mantler, Product Manager HMI/IPC at Phoenix Contact GmbH & Co. KG, the current megatrends in edge computing applications are 'AI and Machine Learning at the Edge' and 'Containerization and Virtualization'. As AI continues to penetrate edge applications, the data processing on dedicated edge devices is becoming increasingly complex and extensive.

"AI-based analytics on an edge device can deliver highly accurate reports about the connected machine. Use cases such as predictive maintenance and anomaly detection can be installed directly on a machine—even retroactively," Mantler said.

"The great advantage is that, by implementing these analytics on a dedicated device, there is often no need to intervene in the machine or its control program—especially when the edge device, like those from Phoenix Contact, supports all industrial protocols such as Profinet or OPC UA."

All these functions can be easily and rapidly scaled thanks to the second megatrend: the virtualization of the entire edge functionality. For example, the PLCnext control program can be deployed virtually as an OCI container across entire server infrastructures, enabling the execution of highly complex applications and the direct reading and analysis of machine data.

Benefits for smart manufacturing

"Edge computing significantly simplifies the entire workflow. By integrating directly into

the machine, data is collected right at the source. There's no need for complex and secure data transmission paths 'upward' to a cloud or central server. Edge devices typically offer far greater performance than traditional PLCs. Performing analytics—potentially AI-driven—directly at the point of data generation makes perfect sense, especially for retrofitting existing systems,” Mantler said.

He added that the true added value of 'AI on Edge' only partially stems from the edge device itself—software is the key! It requires software that enables any plant operator to extract meaningful insights from their equipment. This calls for a simple app-store-like experience for the edge device. In our case, this is made possible through the PLCnext Store.

Using 'MLnext', a data-driven anomaly model can be created without any prior experience in AI or programming. Through a graphical user interface, MLnext only needs to be fed with data—typically from a time-series database that we've previously installed on the edge device. MLnext learns from collected 'good data' and generates reference curves. The model can then be deployed directly on the edge device to compare live data against the learned patterns, identifying and visualizing anomalies—such as a worn motor shaft—simply and precisely.

“Edge devices are not new—the term has long existed in the industrial sector. What's new and decisive for any edge device today is the software it runs, and how user-friendly it is in enabling data analysis for the operator,” Mantler added.

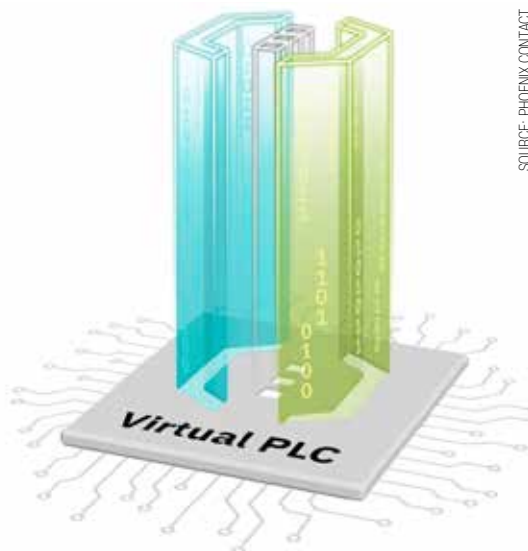
In the case of Phoenix Contact and its new edge device, the 'VL3 UPC 2440 EDGE', the hardware is based on a high-performance industrial PC featuring a QuadCore Atom CPU and 16 GB of RAM. The device runs a user-friendly Ubuntu Pro operating system, allowing software to be extended either natively in Linux or via OCI containers.

Additionally, the device comes pre-installed with Phoenix Contact's virtual controller, 'vPLCnext Control'—a fully functional, real-time-capable PLC. This enables automation solutions to be developed using IEC-61131-3 standards. It also allows direct communication with field-level sensors, actuators, and other controllers via industrial protocols such as Profinet, Modbus, or OPC UA, making data collection seamless.

Software for data analysis and entire pre-defined applications are available through the PLCnext Store, enabling easy expansion of the device's functionality.

Applications and industries

Mantler said that applications range from retrofitted to new installations. Anywhere a



Virtual PLCnext Control offer greater scalability, flexibility, and cost efficiency in automation. As software in an OCI container, it enables seamless integration, combines OT and IT security, and increases the hardware independence of control solutions.

large data stream is generated, an edge device can add value. Even systems that cannot be connected to the internet can benefit. In mechanical engineering, for example, analyzing data can be highly useful for detecting potential failures in advance.

In safety-critical use cases, the edge device can also monitor anomalies within the IT network itself, making it the ideal central interface for data flowing into and out of the system.

Edge devices can also be deployed in small-scale systems, such as an e-mobility charging station, where the edge device handles both control logic and data analysis. In such cases, there's no need for a separate controller in addition to the edge device.

“Edge devices and AI-based analytics on them address a key pain point for plant operators: cybersecurity largely remains under their own control. While analytics via cloud systems are certainly possible, the existing IT infrastructure often does not permit this,” Mantler said.

“High-performance edge devices provide the foundational platform for increasingly complex analytics. To make these advanced mechanisms accessible to a broad range of users, there is a strong focus on offering AI and analytical models in a way that is simple and usable for everyone,” he added.

Edge and cloud computing

As data at the edge keeps growing, sending all of it to the cloud isn't practical or affordable.

According to Dan White, Director of Technical Marketing at Opto 22, it might sound ironic, but cloud computing is what's driving edge

computing.

“As more sensors, controllers, and smart devices come online, the amount of data at the edge keeps growing. Sending all of it to the cloud isn't practical—or affordable. Edge computing lets you clean up, contextualize, and analyze data locally, so you send only what matters for long-term storage or deeper analysis in the cloud,” White told IEB recently.

White said that, as cloud computing expands, cybersecurity is another megatrend shaping edge devices. The more connected your operations become, the more critical it is to protect data in motion. Edge computing gives you a checkpoint at the edge of the network, where you can enforce encryption, authentication, and filtering before anything leaves the plant. At the same time, software-driven automation is changing how systems are built and maintained. Instead of relying only on fixed-function hardware and rigid programming environments, modern automation uses open protocols, scripting, APIs, and containerized applications. That

means more flexibility, faster changes, and easier integration across systems—from the plant floor to business software.

Industrial edge benefits

Industrial edge computing offers a series of specific technical benefits for smart manufacturing, and now advances in AI are factoring into new developments as well.

“You get better data resilience. When network connections fail or cloud services go down, edge systems can keep collecting and storing data locally. That's critical in industries like pharmaceutical and food and beverage, where gaps in data could mean lost product or compliance issues,” White said.

“You also get more control over how and where data flows. Today's edge devices are open enough to support multiple protocols securely. Maybe one system needs MQTT, another polls OPC UA, and a third pulls from a REST API. The edge can serve them all—without middleware or duplicated effort,” he added.

He also said that security has also taken a leap forward. Modern edge platforms support TLS encryption, certificate-based authentication, and firewall rules that let them publish data securely over the public internet, without opening inbound ports. That kind of architecture simplifies remote access for integrators or OEMs while keeping the factory network locked down.

When it comes to AI, the edge currently provides critical support, preparing the data those models need. Clean, contextualized, and consistent data makes upstream AI smarter. No missing units, no mismatched formats—just usable information the model can trust.

SOURCE: PHOENIX CONTACT



SOURCE: ISTOCKPHOTO

“As more sensors, controllers, and smart devices come online, the amount of data at the edge keeps growing. Sending all of it to the cloud isn’t practical—or affordable. Edge computing lets you clean up, contextualize, and analyze data locally, so you send only what matters for long-term storage or deeper analysis in the cloud,” -- Dan White, Director of Technical Marketing, Opto 22.

What makes the newest technologies unique, and how it is different from solutions commonly implemented in the past.

“Modern edge technology is designed for both control engineers and software developers. You’re not locked into one programming language or one way of thinking. Whether you’re building flow logic, writing Python scripts, or connecting to a cloud API, the tools are flexible enough for OT and IT teams to collaborate,” White said.

Security is no longer an afterthought. Today’s edge systems support TLS encryption, client certificates, and strict firewall rules—features expected in IT, but rarely seen on PLCs in the past. Built-in security makes it safer to move data within the factory, across facilities, and into cloud applications.

“Integration has also gotten a lot cleaner. You don’t need layers of middleware to move data anymore. Edge devices can publish directly to brokers, databases, or dashboards, using standard protocols and APIs. And the architecture itself has changed. Instead of pushing everything to a central system, you’re processing and storing data right where it’s created. It’s faster, more resilient, and reduces network load. Maybe most importantly, it’s all open. No vendor lock-in, no black boxes—just tools that talk to each other,” he added.

Industry impact

White said that industries that need reliable, traceable data are seeing the biggest gains from edge technology. In pharmaceutical and life sciences, for example, edge systems can log data locally during network outages, protecting audit trails and maintaining compliance without gaps. That kind of redundancy is critical when product integrity is on the line.

Remote operations are another perfect fit. In sectors like water treatment or energy, where assets are spread out and sometimes hard to reach, edge computing provides real-time monitoring and control even without a persistent connection. Users can process data onsite, push summaries to the cloud, and keep critical systems running no matter what’s happening upstream.

Machine builders are using edge devices to stay connected to the systems they ship. Once a machine leaves the floor, it’s still carrying your brand. Remote diagnostics, usage tracking, and performance feedback help OEMs support customers better and improve designs over time. With enough data, that feedback loop can even shape future AI models.

And across industries, the need for predictive maintenance is growing fast. Whether it’s compressors, pumps, or entire production

lines, edge systems enable condition-based monitoring without adding complexity. Even data centers—where uptime is king—are starting to use edge architectures to keep critical infrastructure in check.

Industrial Edge solutions, the IIoT and Industry 4.0

White told IEB that “edge technology is what makes IIoT and Industry 4.0 real—not just possible, but practical. In brownfield environments, edge devices can pull data from existing systems without touching control logic or disrupting operations. That’s key for plants that can’t afford downtime or don’t want to replace or revalidate equipment just to get data out.”

“But in greenfield designs, the edge can be the control system. Modern platforms combine control, data processing, visualization, and networking into a single device. That means you start with secure, structured, accessible data by default, and you don’t need to add integration layers later,” he said.

“In addition, edge solutions scale cleanly. You can roll it out gradually—one line, one machine, one site at a time—without having to commit to a rigid, top-down architecture. That flexibility makes it easier to move from pilot to production, and from one use case to many.”

Hyperconnectivity becoming a core requirement

Enabling communication between a wide variety of industrial assets, often spanning different protocols, vendors, and technology generations.

Ruth Williams, Product Marketing Manager at Moxa Europe GmbH said that “several megatrends are accelerating the adoption of Industrial Edge Computing including the convergence of IT and OT, the rapid growth of the Industrial Internet of Things (IIoT), and increasing demand for secure, real-time access to operational data. These developments are prompting industries to rethink how they collect, process, and act on information across distributed environments.”

“Hyperconnectivity is emerging as a core requirement, enabling communication between a wide variety of industrial assets, often spanning different protocols, vendors, and technology generations,” Williams said. “Solutions such as smart I/O modules and protocol gateways, including those offered by Moxa, support this evolution by making it easier to bring legacy systems into integrated, data-driven environments without major infrastructure overhauls.”

She said that, at the same time, cybersecurity has become a fundamental consideration in edge deployments. The shift toward adopting

international standards such as IEC 62443 reflects a growing need to secure operational data, particularly as edge computing extends beyond the factory floor to remote or mission-critical sites. Ruggedised, security-aware hardware is increasingly important for ensuring the resilience and integrity of these systems.

Combined with emerging technologies such as 5G and artificial intelligence at the edge, these trends are helping to establish a more intelligent and responsive industrial landscape. Local data processing, real-time decision-making, and machine learning at the edge are enabling new use cases, from predictive maintenance to adaptive process control, while supporting the broader move toward software-defined automation.

Industrial edge technologies

“Software driven automation is reshaping traditional manufacturing by enabling more flexible, responsive, and data centric operations. Industrial edge computing supports this transformation by providing the infrastructure to connect legacy systems with modern control platforms - bringing data processing closer to the source and reducing dependence on centralised systems,” Williams said.

This decentralised model allows for real time data acquisition and analysis, which is

essential for applications such as predictive maintenance, quality control and adaptive process optimisation. Devices such as remote I/O modules, protocol gateways and serial to network converters (common in Moxa’s industrial connectivity portfolio) help manufacturers integrate existing equipment with new software environments, ensuring interoperability across diverse systems.

Advances in artificial intelligence further amplify the potential of edge computing. Running AI algorithms locally enables factories to detect anomalies, optimise energy use and adjust processes dynamically, without relying on constant cloud connectivity. Combined with developments in 5G, which deliver high speed, low latency communication across industrial sites, these technologies are establishing a more intelligent and responsive production environment.

Secure, centralised network management also underpins effective edge deployments. Tools such as Moxa’s MXview software allow operators to monitor distributed assets, manage configurations and ensure secure remote access, ultimately reducing downtime, engineering overhead and lifecycle costs. As more factories adopt cloud integrated, software defined architectures, robust, interoperable edge infrastructure will remain critical for scalability and long-term resilience.

Simplify Machine IP Integration



Skorpion IP Routers ease the integration of new machines into the existing network.

- Reduce installation time
- Eliminate IP address conflicts
- Eliminate site visits with secure remote access

IP Routers

CONTEMPORARY
CONTROLS® **50 years**

Providing Solutions to Your Automation Needs

+1 630-963-7070 • info@ccontrols.com

Learn more at www.ccontrols.com/machine



SOURCE: ISTOCKPHOTO

“Software driven automation is reshaping traditional manufacturing by enabling more flexible, responsive, and data centric operations. Industrial edge computing supports this transformation by providing the infrastructure to connect legacy systems with modern control platforms - bringing data processing closer to the source and reducing dependence on centralised systems,” -- Ruth Williams, Product Marketing Manager, Moxa Europe GmbH.

Breaking away from the past

Williams said that traditional industrial systems have often operated in silos, relying on proprietary protocols and centralised data processing, which limited real-time visibility and flexibility. In contrast, Industrial Edge computing enables smart factories to access fast, secure, and reliable real-time operational insights directly at the edge. This shift supports immediate decision-making and improves responsiveness to changing conditions.

Moxa’s rugged hardware is designed to operate in harsh industrial environments and supports both legacy serial and field protocols alongside secure, scalable integration with modern IT platforms. This hybrid capability allows manufacturers to modernise incrementally without discarding existing infrastructure.

By preprocessing and filtering data locally, edge computing reduces reliance on cloud connectivity, enhancing efficiency and data control. As AI-driven applications such as predictive maintenance and anomaly detection become more prevalent, Moxa’s solutions ensure consistent, protocol-agnostic data flow between machines, gateways, and cloud systems. This unified and cybersecurity-conscious approach enables manufacturers to adopt next-generation automation, unlocking the full

potential of AI and data-driven operations while preserving prior investments.

Applications focus

Williams said that industries that require real-time reliability and distributed operations are well-positioned to benefit from the latest Industrial Edge solutions. In discrete manufacturing, for example, integrating legacy equipment with modern Industry 4.0 platforms is essential for supporting agile production processes. Moxa’s smart I/O modules and protocol gateways facilitate this integration by bridging older serial and fieldbus protocols with Ethernet-based systems.

In the power and energy sector, continuous and secure data transmission from remote substations, solar farms, and wind parks to central control systems is critical. Moxa’s rugged edge devices are designed to operate reliably in harsh environments, providing secure and stable connectivity that supports critical operations.

Critical infrastructure and smart cities depend on consistent edge-level data acquisition for managing intelligent systems and public utilities. Moxa’s modular I/O and protocol converters enable interoperability across diverse device ecosystems, helping to maintain operational efficiency and regulatory compliance.

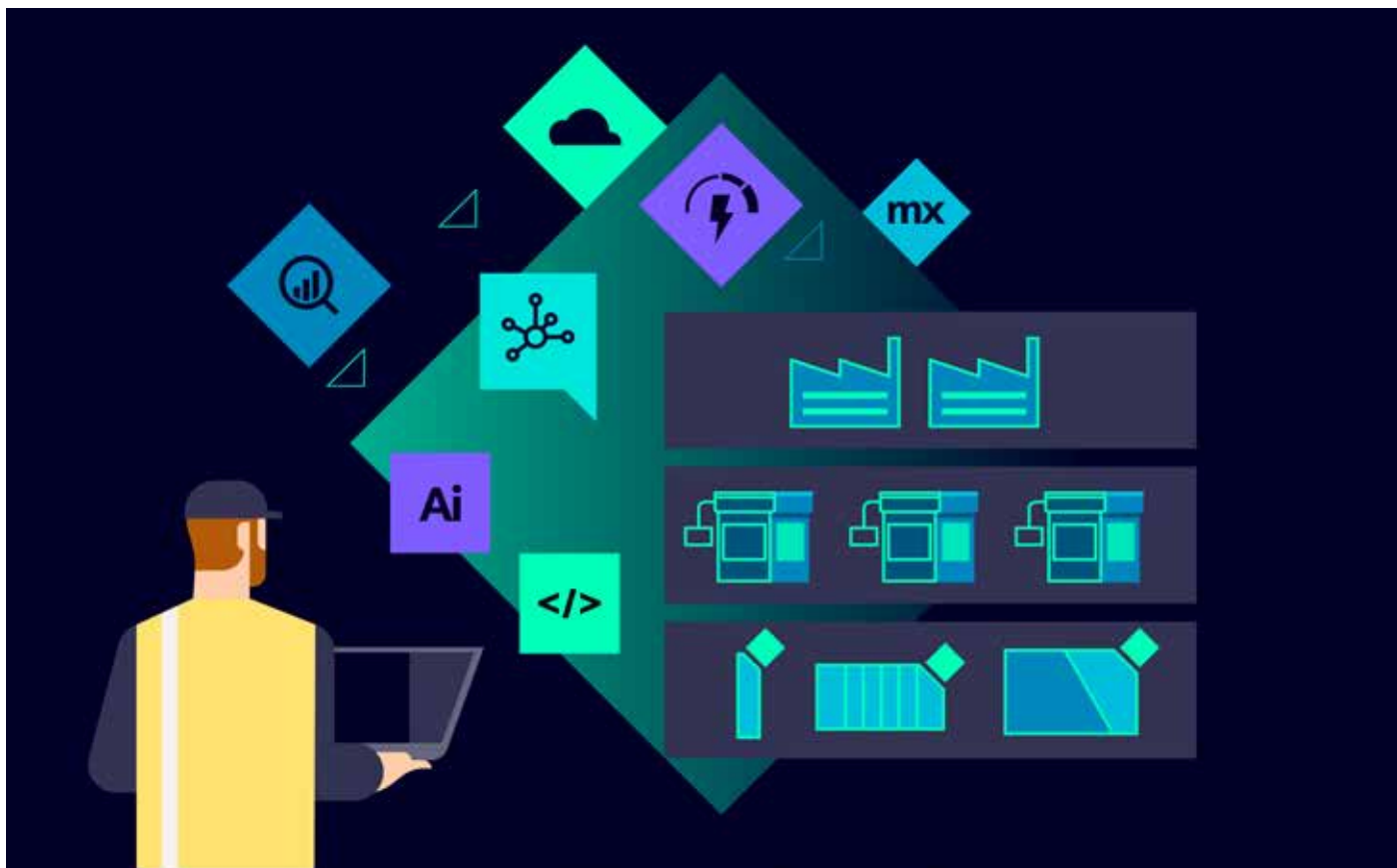
In semiconductor and electronics manufacturing, where yield, traceability, and uptime are paramount, Moxa’s secure gateways and remote I/O solutions support precise monitoring and control, contributing to process optimisation and enhanced data integrity.

Across these industries, Moxa delivers edge connectivity solutions that combine flexibility, resilience, and protocol interoperability, allowing organisations to modernise their operations incrementally while ensuring continuity and security.

IIoT and Industry 4.0 solutions

Moxa contributes to the advancement of IIoT and Industry 4.0 by providing connectivity solutions that help transform standalone machines into networked, intelligent components within industrial systems. Its edge devices facilitate the integration between operational technology (OT) and information technology (IT), enabling secure and reliable data exchange to local human-machine interfaces (HMIs), analytics platforms, and cloud-based applications.

“By emphasising protocol interoperability, network resilience, and cybersecurity, Moxa supports manufacturers in adopting digital transformation in a controlled and compliant manner. Its edge solutions



“Megatrends such as Industrial IoT, IT/OT integration, AI on the shop floor, the adoption of software-defined principles across multiple domains, and, more broadly, the adoption of cloud and IT technologies—such as virtualization and containerization—are the driving forces behind the rise of industrial edge computing,” -- Francisco Javier Franco Espinoza, Strategy and Innovation Manager Factory Automation, Siemens.

enable key Industry 4.0 principles such as decentralisation, transparency, and predictive analytics through support for edge networking, real-time control, and remote diagnostics,” Williams said.

“This approach helps manufacturers shift from reactive maintenance to more proactive, data-driven operations that can scale and adapt over time,” she added.

Adoption of cloud and IT technologies

Cloud and IT technologies such as virtualization and containerization are the driving forces behind the rise of industrial edge computing.

“Megatrends such as Industrial IoT, IT/OT integration, AI on the shop floor, the adoption of software-defined principles across multiple domains, and, more broadly, the adoption of cloud and IT technologies—such as virtualization and containerization—are the driving forces behind the rise of industrial edge computing,” Francisco Javier Franco Espinoza, Strategy and Innovation Manager Factory Automation at Siemens told IEB.

“These same trends are also driving the shift toward software-driven automation—or, as we call it at Siemens, Software-Defined Automation (SDA). SDA is prompting

manufacturers, automation suppliers, and system integrators to rethink every aspect of automation. The goal is to evolve from merely automated production to adaptive production, and ultimately to autonomous production—making every step of the process, from engineering to operations, more efficient and resilient,” he added.

Espinoza said that, at Siemens, we have been working hard over the past few years to equip our customers and partners with the right tools for this journey. Case in point: tools like Siemens Industrial Edge, our edge computing platform and ecosystem; SIMATIC AX, our IT-like engineering environment for PLCs; and the SIMATIC S7-1500V virtual PLC—the first virtualized control system ever used in a real production environment.

Key benefits of Industrial Edge

Espinoza said that key benefits of edge computing include localized data preprocessing, low-latency response, and reduced dependency on cloud and connectivity. A scalable edge computing platform should also allow secure remote management of edge devices and applications, enabling the efficient deployment of production-critical applications across the shop floor, while reducing maintenance and operational costs. This is the case, for example, with Siemens

Industrial Edge, which manufacturers are using to break down data silos in their operations and integrate their IT and OT systems at scale.

Many companies that leverage edge computing in their manufacturing operations do so to implement AI- and ML-supported smart manufacturing use cases—or are planning to do so in the near future. This has been our experience with Siemens Industrial Edge and our Industrial AI portfolio.

“When it comes to generative AI, this technology can help streamline tasks like PLC and SCADA engineering or enhance the way operators interact with and troubleshoot machines. This is exactly what we do with our Siemens Industrial Copilot for Engineering and Industrial Copilot for Operations, respectively. These are just two examples of many possible use cases,” he said.

Impact of new technology

“Automation solutions in the past tended to be monolithic applications, often tied to specific hardware and heavily reliant on proprietary technologies and protocols. This frequently led to vendor lock-in and rigid architectures,” Espinoza said. “Modern technologies stand in contrast to that legacy, emphasizing modularity, openness, and hardware independence. This enables manufacturers to select best-of-breed solutions for each



SOURCE: ISTOCKPHOTO

"The necessity to secure networks from increasingly sophisticated and persistent cyber-attacks combined with the need to have predictable and manageable costs have led to the industrial edge taking a very prominent role in operational network architecture design," -- Dr. Al Beydoun, ODVA President and Executive Director.

task, rather than being locked into a single vendor's portfolio. In addition, there is an increased focus on cybersecurity, scalability, and portability across different platforms."

Applications edge

Espinoza said that industrial edge solutions are gaining rapid traction across sectors such as automotive, food and beverage, pharmaceuticals, and logistics—where real-time data analytics and zero downtime are critical. We have customers in various discrete manufacturing industries using Siemens Industrial Edge to successfully implement and scale AI-supported visual quality inspection, process monitoring, and production analytics. Asset health monitoring and plant optimization are examples of applications successfully implemented by our customers in the process industries.

Edge architectures are particularly valuable where regulatory compliance, fast cycle times, and adaptive production are essential—for example, in pharmaceuticals for batch traceability or in automotive for predictive maintenance. Across these verticals, edge computing empowers manufacturers to realize their digital transformation ambitions while maintaining operational continuity.

A prime example of industrial edge computing in a real-life scenario is the Audi factory in Neckarsulm, Germany, where S7-1500V virtual PLCs control the car body assembly, and advanced AI models run on Siemens Industrial Edge for real-time quality control.

Edge solutions

Espinoza concluded by noting that edge solutions are foundational to the Industrial Internet of Things (IIoT) and Industry 4.0.

"Edge computing forms the connective tissue that merges data from machines, sensors, and business systems in real time. This integration creates the "digital thread" that underpins smart manufacturing," he said.

Siemens' portfolio illustrates how edge computing—through its modular approach, openness and focus on OT environments—enables manufacturers to create value from their data no matter their digital maturity level. This is achieved by implementing new and flexible architectures, breaking down data silos, and deploying analytics and AI at scale in both brownfield and greenfield environments.

"Edge architectures close the loop between the plant floor and the enterprise, unlocking continuous innovation in line with Industry 4.0's vision for fully digitalized factories," Espinoza said.

Edge computing and cybersecurity

Industrial edge is taking a very prominent role in operational network architecture design.

"The necessity to secure networks from increasingly sophisticated and persistent cyber-attacks combined with the need to have predictable and manageable costs have led to

the industrial edge taking a very prominent role in operational network architecture design," Dr. Al Beydoun, ODVA President and Executive Director told IEB recently. "Additionally, the demand for consistent uptime and low latency in operations environments lends to reliance on edge appliances."

His point is that while the cloud offers the benefit of a host environment that is constantly updated with the latest hardware and backbone software, the possibility of misconfigured cloud security combined with the uncertain cost of computing and storage has made the edge a strong consideration for operations environments. Additionally, edge appliances offer the advantage of not having to worry about compromised cloud neighbors leading to unintentional security breaches.

While redundancy is still important, it can be accomplished through back up edge devices located either onsite or split among the local area. Further, virtual controllers can be hosted in edge devices for less critical applications to help manage software updates and reduce hardware reliance in operations facilities. Note that industrial Ethernet networks that support TCP/IP and TLS/DTLS such as EtherNet/IP are well positioned for virtual controller usage.

Industrial edge computing benefits

"Industrial edge computing enables smart manufacturing via usage of data models and algorithms to optimize applications in real time. Data models such as OPC-UA and PA-DIM are supported by leading industrial networks

including EtherNet/IP,” Beydoun said.

For example, the parameters of a solenoid coils response rate or the output measurements of a bottle capping machine can be monitored, and warnings can be issued to ensure quality isn't compromised if the process gets out of specification. This transitions maintenance from a scheduled or reactive activity to a predictive one. Additionally, the inputs for a tensioning machine can be monitored and adjusted as components wear and raw material variances are encountered to ensure that output tolerances are met. The usage of AI combined with industrial edge computing allows not only algorithm optimization for predictive maintenance and loop tuning but can also aid in cybersecurity. AI can help to provide automated initial security alerts to experienced IT security staff based on unusual logins, unexpected elevations of privileges, and other unexpected packet patterns.

Newest solutions

The newest edge, virtual controller, and AI solutions offer the potential to solve existing problems in new ways that can help drive down costs and improve output and quality,” Beydoun added. “Edge appliances include significant computing resources, security patch and OS updatability, and containerization for scalability and flexibility. This enables edge devices to support virtual controllers and AI solutions for low-risk operations applications.”

Virtual controllers are capable of decoupling software from hardware that can help with device maintenance and updating. Additionally, AI can take over tasks that used to require time consuming, custom algorithms and can more flexibly take on new jobs as applications evolve. In the past, devices were limited to being on machine, the software was tied to the hardware provided, and automation required highly specialized engineering. These new edge, virtual controller, and AI solutions provide a greater amount of flexibility to tackle operations challenges both at scale and with fewer resources.

Beydoun said that industrial edge appliances can add value to applications such as quality optimization of pharmaceutical, food and beverage, and consumer goods packaging machines as well as automotive component and final assembly line operations. These types of applications allow for the opportunity to improve quality, throughput, and energy usage via traditional algorithms and AI with an acceptable level of risk. The usage of virtual controllers and edge appliances together can also help to control non-critical systems such as lighting, heating, ventilation, and air conditioning.

Critical national infrastructure such as oil and gas refineries, power plants, and chemical facilities still require traditional onsite physical controllers with redundancy

to help maintain safety and security. It's also important to realize that AI relies on mathematical probability based on real time inputs and models created based on historical data. AI is best leveraged as a powerful tool to enhance and optimize operations, rather than serving as the sole foundation of critical processes.

IIoT and Industry 4.0

“Edge appliances are enabling the promise of IIoT and Industry 4.0 to come to life by providing the computing power and low latency necessary for resource intensive operational technology solutions. An example of this is the usage of digital twins on the factory floor to help workers visualize and replace failed components through augmented reality inclusive of on demand installation and maintenance documentation,” Beydoun said. “The usage of edge appliances also helps to maintain a strong cybersecurity posture, in conjunction with cybersecurity network solutions such as CIP Security for EtherNet/IP, while allowing for the implementation of AI for predictive maintenance.”

He added that edge appliances also allow for greater stability since they aren't at risk of cloud or network cable outages and can keep costs predictable and manageable to enable the ROI needed to scale IIoT and Industry 4.0 solutions. An example of this is an edge device collecting data from external vibration, temperature, and moisture sensors that can serve as an additional warning sign of future failures. Edge appliances can also help manage the control of Autonomous Mobile Robots (AMRs) and Automated Guided Vehicles (AGVs) as well as enable custom engineering tools for onsite workers via onsite Wi-Fi or private 5G networks.

Software-driven automation

Containerized architectures for flexible software deployment on edge computing equipment, making updates and patch management efficient and scalable.

“The industrial landscape is shifting as more operational technology (OT) data is produced and processed at the edge. This trend is fueled by IoT sensors, real-time processing needs, and data security concerns which increase with the rising proficiency of threat actors and sophistication of the tools they employ,” Georg Stöger, Senior Principal Technology Specialist at TTTECH told IEB.

“Software-driven automation is transforming factories with edge applications for real-time decisions, boosted by AI integration. Of course, edge platforms use containerized architectures for flexible software deployment on edge computing equipment, making updates and patch management efficient and

scalable,” Stöger said.

He added that cybersecurity is also crucial, with 80% of CIOs increasing budgets for zero-trust architectures and advanced threat detection at the edge to protect distributed systems. A major challenge is integrating a multitude of legacy OT equipment with little or no cybersecurity capabilities.

As manufacturers face “cloud regret” due to latency and costs, edge computing offers a strategic alternative, with global spending projected to reach \$378 billion by 2028 (Source: IDC's Worldwide Edge Spending Guide), highlighting the importance of processing data where it is created.

Performance benefits

Stöger said that the most immediately obvious benefit of industrial edge computing is performance: Industrial edge computing processes data directly on the factory floor, possibly reducing processing latency and response times to single-digit milliseconds and thus enabling real-time quality control and machine optimization.

AI integration at the edge allows real-time analysis of production data, enabling predictive maintenance that can reduce downtime by up to 50%. These systems use machine learning models that improve continuously.

Another key advantage is data sovereignty: By processing data locally, it can be much easier to ensure compliance with regional regulations and to keep sensitive data within known physical boundaries. Edge computing, properly done, addresses security concerns with role-based access controls and encryption for data that must leave the factory floor. Besides, edge processing also provides resilience against network disruptions, thus increasing robustness and reducing data loss or even downtimes.

Through local processing, edge computing also enhances resource efficiency by massively reducing internet bandwidth consumption, which is a real concern in some situations such as remote locations or sites with limited connectivity.

An example is TTTECH Industrial's IIoT edge platform for machine builders, Nerve, that allows companies to collect, process, and analyze machine data in real-time, as well as manage devices and deploy applications remotely via the online Management System. It forms a secure base with industrial cybersecurity certification according to IEC 62443, to run and maintain (legacy) applications on the edge.

Unique technology

“One major change – at least for OT systems – concerns the handling of software,” Stöger said. “The current software management technology, which is widely used in IT already, is containerization, which packages applications



SOURCE: ISTOCKPHOTO

"the industrial landscape is shifting as more operational technology (OT) data is produced and processed at the edge. This trend is fueled by IoT sensors, real-time processing needs, and data security concerns which increase with the rising proficiency of threat actors and sophistication of the tools they employ,"
Georg Stöger, Senior Principal Technology Specialist at TTTech.

with their dependencies for consistent deployment across different hardware. Unlike past monolithic systems, today's modular edge platforms allow dynamic workload management, letting manufacturers update components without disrupting the entire system. This flexibility of a distributed model brings intelligence directly to data sources."

He added that security has also advanced significantly. Traditional perimeter-based security has been replaced by zero-trust architectures that verify every access attempt, not only by human actors, but also between software services, electronic components, and computing devices. Modern platforms use defense-in-depth strategies, continuous vulnerability monitoring, secure boot processes, and cryptographic verification of workloads.

Data handling has improved, too. Current edge platforms use time-series databases optimized with configurable retention policies to balance analytical needs and storage constraints. This allows to keep relevant parts of data over long time horizons for different types of analyses and applications without needing vast amounts of nonvolatile storage at the edge.

Most importantly, today's edge solutions integrate operational technology with cloud environments, creating hybrid architectures that leverage the strengths of both. This creates a continuous digital thread from the shop floor to enterprise business systems.

Newest Industrial Edge solutions

From TTTECH's perspective, manufacturing is currently leading in industrial edge adoption, using it for predictive maintenance, quality

assurance, and adaptive production. Smart factories process machine vision data for real-time defect detection, achieving high inspection rates with sub-millimeter precision.

Off-highway also shows compelling use cases, for example in smart farming, where autonomous weed control and harvesting systems are harnessing the power of edge-local AI and controls.

The energy sector uses edge computing in generation, transmission, and distribution. For example, wind farms optimize blade pitch based on real-time weather and wind data, optimizing energy output while reducing mechanical stress on the turbine structure. Monitoring of energy consumption and production in industrial sites over time allows to predict future energy flows, enabling cost optimization, peak shaving, and even the trading of flexibilities on energy markets based on AI models.

Process industries like chemical, pharmaceutical, and food production use edge computing for continuous monitoring of critical parameters, detecting subtle deviations that might indicate contamination or quality issues.

Across all these industries, edge computing meets the need for real-time processing, operational resilience, and secure data handling.

Edge solutions: IIoT & Industry 4.0

"By combining computational resources and versatile networking capabilities with state-of-the-art cybersecurity at the industrial site, edge solutions bridge the gap between operational technology and information

technology, driving industrial digitalization," Stöger said.

"Edge computing platforms significantly improve data utilization. Traditional industrial environments generated vast amounts of data that were often untapped due to bandwidth and processing limitations. Edge computing filters, aggregates, and analyzes data locally, sending only select relevant data and actionable insights to higher-level systems or the cloud. This has enabled digital twins that accurately mirror physical assets, supporting simulation and optimization across production lines," he added.

Security in edge platforms addresses the expanded attack surface of connected industrial systems. Modern solutions use defense-in-depth strategies, continuous vulnerability monitoring, and secure communication channels to protect critical infrastructure from sophisticated threats.

Edge computing also supports decentralized decision-making, a key feature of Industry 4.0. By distributing intelligence throughout the production environment, these systems enable autonomous operation of equipment and processes, with local analytics driving real-time adjustments.

"The flexibility of containerized edge applications accelerates innovation cycles, allowing manufacturers to deploy new capabilities without changing hardware," Stöger said. "This agility, combined with the performance benefits of local processing, makes edge computing a cornerstone of industrial transformation."

Al Presher, Editor, Industrial Ethernet Book

Machine monitoring with edge devices

Gaining real-time insights into use of edge devices can help avoid downtime, reduce costs and optimize industrial performance. With today's flexible edge devices, users can create tailored machine monitoring solutions that fit a wide variety of specific business needs.

A CRITICAL MANUFACTURING CONVEYOR BELT at a plant suddenly stops during peak production hours. The entire assembly line grinds to a halt, operators scramble to diagnose the issue, and the company racks up thousands of dollars in lost productivity every hour it's down.

Eventually, a technician discovers the problem: an overheated motor bearing that could have been detected days earlier with proper monitoring.

Keeping machines running smoothly is at the heart of every industrial operation. Machine monitoring helps avoid these downtime scenarios by providing the real-time insights needed to catch problems early and keep equipment working.

Machine monitoring: not just for new machines

Perhaps you've been tasked with an IIoT (industrial internet of things) or digital transformation initiative. The boss wants live production data from existing equipment to improve production visibility, help predict maintenance issues, and keep production operating smoothly.

You might think machine monitoring is only practical or cost-effective for new, high-tech equipment. After all, Industry 4.0 and IIoT platforms are often marketed as solutions for greenfield systems.

But the truth is, the greatest value of machine monitoring lies in improving the equipment you already own—capturing real-time data to optimize performance and prevent unplanned downtime.

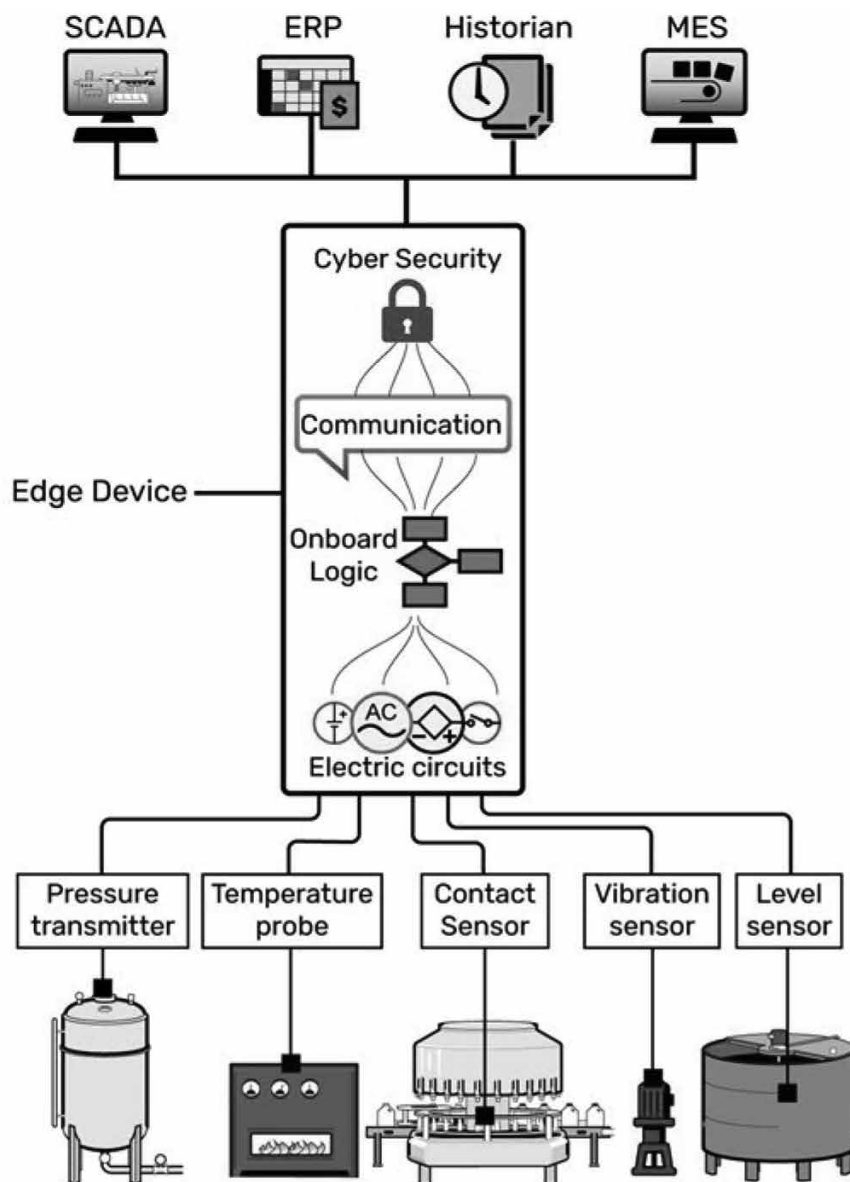
Introducing edge devices

But how can you monitor legacy machines? One solution manufacturers are turning to is edge devices, small-footprint computing devices you can install next to a machine at the edge of your network. Edge devices bridge the gap between your older, non-networked machines and newer smart systems. They collect, process, and transmit data efficiently regardless of the machine's capabilities and without disturbing existing machines or processes.

How do they work?

Edge devices offer a number of unique features and benefits:

Multi-signal support: Modern edge devices



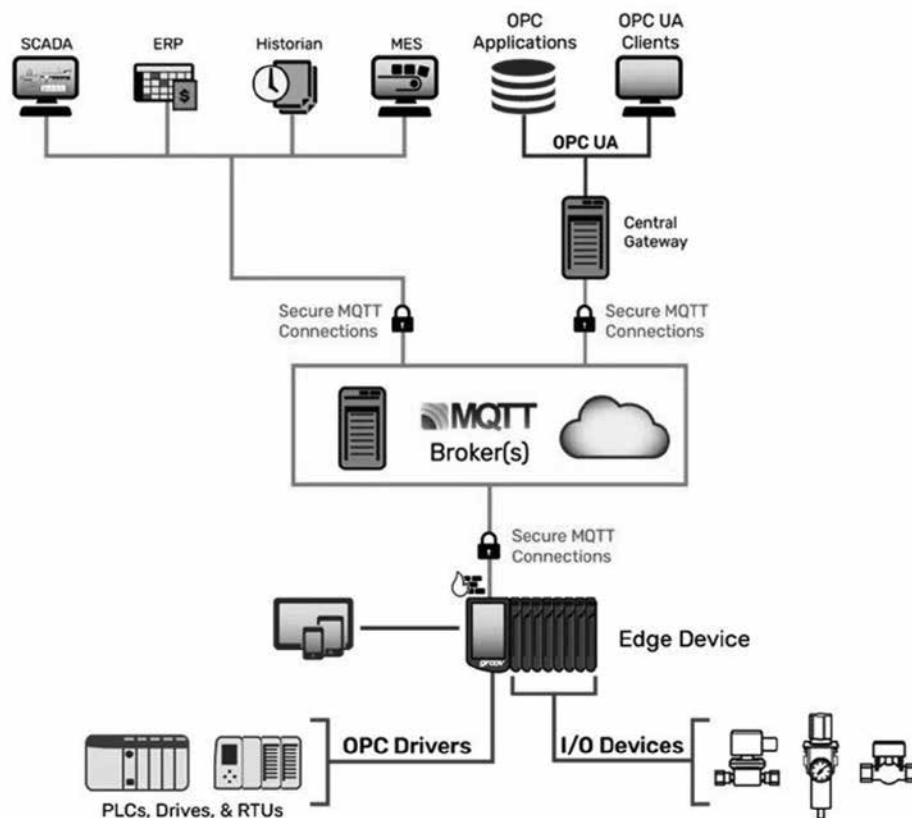
Here is how an edge device can easily integrate with non-networked machines.

connect to common industrial signals from digital and analog inputs, supporting standards such as 0–10 VDC, 4–20 mA, thermocouples, thermistors, and digital pulses for counting applications. You can monitor a wide range of parameters, from temperature and pressure to machine cycles, ensuring compatibility with diverse equipment.

Protocol bridging: Edge devices translate proprietary and legacy protocols into IIoT-ready formats like MQTT Sparkplug® B

or OPC UA®. Whether legacy systems are on Ethernet or serial, edge devices have tools to connect them to modern IT infrastructure.

Local data processing and modeling: Edge devices pre-process data locally, converting raw signals into context-rich formats like user-defined data types (UDTs). Pre-processing reduces the amount of data that is sent and simplifies trend analysis and performance monitoring when the data arrives at its destination.



Leverage OPC drivers on legacy hardware to communicate with MQTT brokers and securely send data to OPC UA clients using edge devices.

Built-in cybersecurity: Today's edge devices are designed with robust security features, including firewalls, SSL/TLS encryption, certificate-based authentication, and zero-trust architecture. They support user authentication with LDAP (Lightweight Directory Access Protocol), VPN tools for secure remote access, and publish/subscribe communication models that prevent inbound port access, reducing vulnerabilities to cyberattacks.

How can you put an edge device to work in your operation? The approach depends on the hardware you're working with.

Different approaches

When considering how you can incorporate edge devices, the approach differs between legacy brownfield equipment (non-networked machines) and newer machines with smart controls (networked machines). Let's explore why.

Non-networked machines

If you're working with older, non-networked machines that don't have built-in connectivity, adding sensors and connecting them to edge devices is a clear-cut and low-cost way to start collecting real-time data.

This straightforward approach unlocks valuable data from even the oldest equipment, without requiring costly upgrades or

modifications.

To get started:

Identify critical data points: Determine the key performance indicators (KPIs) that matter most, such as temperature, vibration, cycle counts, or energy usage. Focus on the metrics that directly impact machine performance, maintenance, and your overall operational goals.

Add sensors: Choose sensors suited to your data points. For example:

- Vibration sensors detect imbalances or wear in rotating machinery.
- Temperature probes monitor heat levels in motors or bearings.
- Flow sensors track the movement of liquid transformers (CTs) measure energy consumption and detect faults.
- Proximity sensors detect the presence, position, or movement of objects, making them ideal for counting parts and monitoring conveyor systems.

Connect sensors to an edge device: Use an edge device with built-in I/O points to read and process sensor data. Then, democratize your data (make it widely available) to your digital infrastructure (SCADA, QMS, OEE, MES, ERP, etc.) via open-standard, IIoT-friendly protocols like MQTT Sparkplug B or OPC UA.

Networked Machines

If your machines have built-in communication

capabilities, existing control systems like PLCs or fieldbuses can provide direct access to data by allowing you to leverage your equipment's built-in communication infrastructure to collect the data that you need.

But if your machines use locked PLC programs or proprietary protocols, edge devices can bridge the gap between closed legacy equipment and modern IT infrastructure, ensuring seamless data access.

Take stock and decide what to do:

First, identify critical data points: Tracking your machine's operating state—idle or in use—helps with utilization and maintenance planning. Monitoring specific alarms and signals, like temperature or vibration, can reveal anomalies indicating potential failures before they occur.

Next, evaluate communication capabilities: Start by identifying the communication protocols your machines support, such as EtherNet/IP, Modbus®/TCP, PROFINET, EtherCAT®, or even older serial networking like RS-232, RS-422, or RS-485. While you can often directly integrate Ethernet-based protocols into modern systems, serial networks may require additional tools, like serial-to-USB or serial-to-Ethernet converters, to make the data usable.

Try to overcome common challenges: Even with Ethernet-based communications, networked machines often have challenges



How a Tier 1 automotive supplier integrated the Opto 22 groov RIO edge device

like locked PLC programs or proprietary protocols. In many cases, you can add third-party software, like an OPC UA server, to help bridge these gaps and translate proprietary protocols into modern IIoT protocols without disrupting operations.

Consider using an edge device to bridge the gap: With common challenges like these, you may find it easier to use an edge device—similar to the approach with non-networked machines. An edge device can tap into existing signals, add new sensors, or leverage onboard OPC UA servers with custom drivers to gather data from proprietary protocols.

And what if your legacy machines are on a serial network? Even older serial protocols can be integrated into modern edge devices using simple and inexpensive serial-to-USB converters. The edge device then converts legacy protocols into cybersecure IIoT standards like MQTT Sparkplug B or OPC UA.

Turning data into action

Whether you're integrating legacy systems or enhancing smart machines, edge devices provide the bridge between your equipment and your Industry 4.0 or IIoT initiatives. Now you can turn your existing equipment into a valuable source of real-time data—without costly overhauls or operational disruptions.

Start small. Add an edge device to a single machine or process, capture critical data, and integrate it into your digital infrastructure. From there, scale as needed, connecting more systems and expanding your monitoring capabilities at your own pace.

Your machines are already working hard—make them work smarter.

Real-world applications

With today's flexible edge devices, you can create tailored machine monitoring solutions that fit your specific business needs. Here's how businesses like yours are leveraging edge devices.

Tier 1 Automotive Supplier

A Tier 1 automotive supplier headquartered in Marysville, Ohio, with six facilities across North America, specializes in plastic injection molding. They faced significant challenges integrating real-time data from their diverse array of machinery. Outdated systems relied on 15-minute manual operator updates, leading to delayed insights, errors, and limited visibility into production performance. As part of their Vision 2030 digital transformation initiative, they sought a scalable, cost-effective solution to unify their

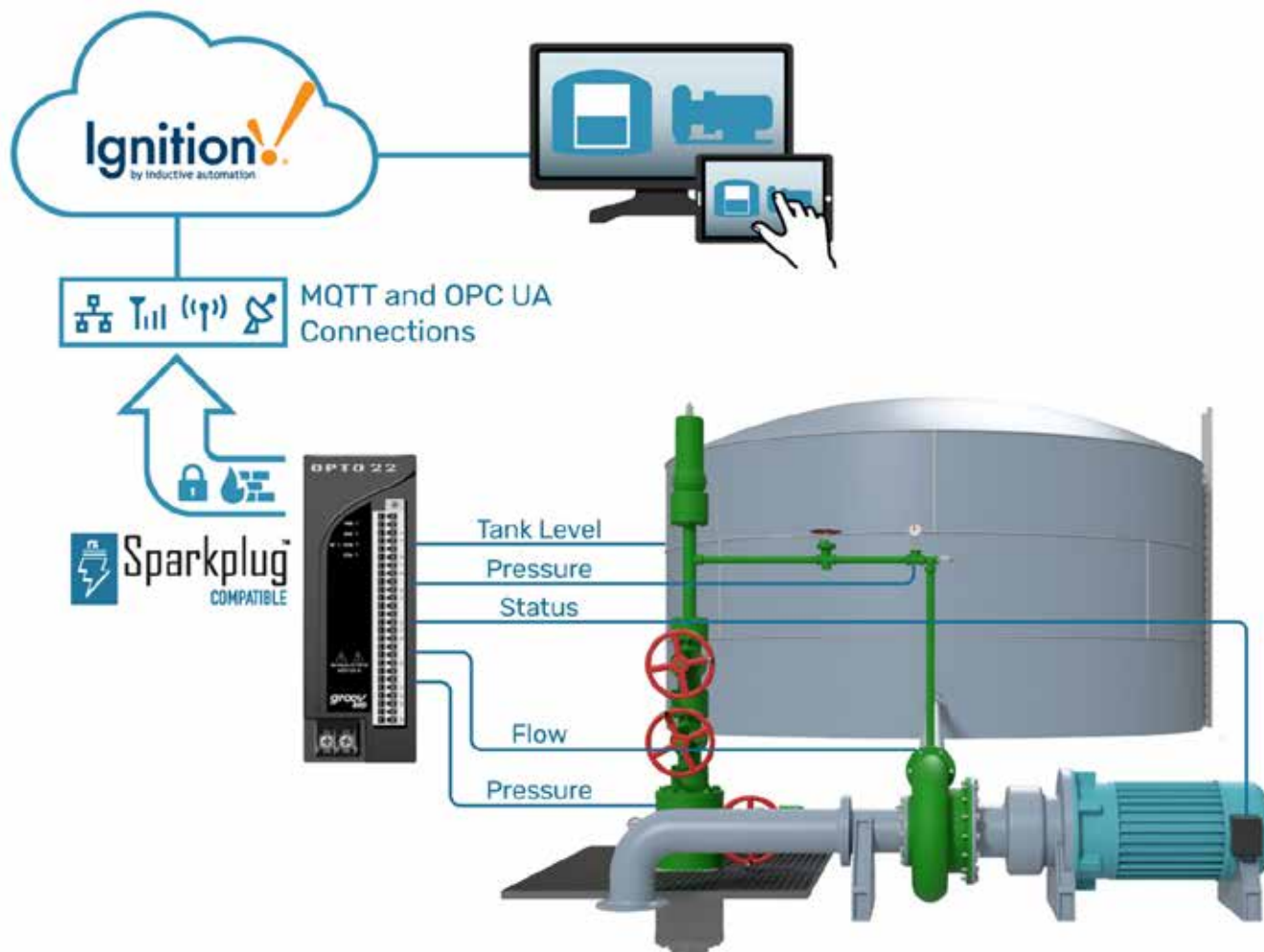
machines, regardless of age or manufacturer. By integrating a compact edge device—Opto 22's groov RIO—they captured critical signals like full-auto status, mold changes, and water flow directly from their injection molding machines.

"groov RIO is simple. You have I/O, plug it in, connect an analog or digital signal, perform some simple configuration, and you are off to the races," their IT specialist explains. Using groov RIO's built-in MQTT Sparkplug B client, they now publish live data into their Unified Namespace (UNS), which runs on Inductive Automation's Ignition SCADA hosted in the cloud.

The initial proof of concept quickly scaled to over 100 machines across multiple facilities, enabling them to track performance and availability in real time. "Now we can develop systems that plug into our UNS and make real-time decisions based on live data down to the second," adds the IT specialist.

Ornamental Plant Grower

One of the world's largest ornamental plant growers, headquartered in Miami, Florida, faced challenges collecting real-time data from diverse equipment like transplanters, robotic systems, conveyors, and irrigation systems. Traditional PLCs required costly software licenses and specialized expertise, making data



SOURCE: OPTO 22

How an oil and gas company integrated the Opto 22 groov RIO edge device.

access difficult. Recognizing that the lack of live data hindered their ability to optimize operations, their automation manager sought a solution that was simple, scalable, and cost-effective.

By integrating a compact edge device—Opto 22's groov RIO—into their existing control systems, they collected data across their machinery, used Node-RED dashboards for real-time visualization, and used SQL nodes to store data in a cloud database on Microsoft® Azure®—leveraging tools like Power BI® for advanced analysis and insights to optimize operations.

"We realized that without accurate, real-time data, we couldn't manage or optimize operations effectively," the automation manager says. "For under \$1,000, copying and pasting code that I already wrote, we can get a new groov RIO deployed in just a few minutes."

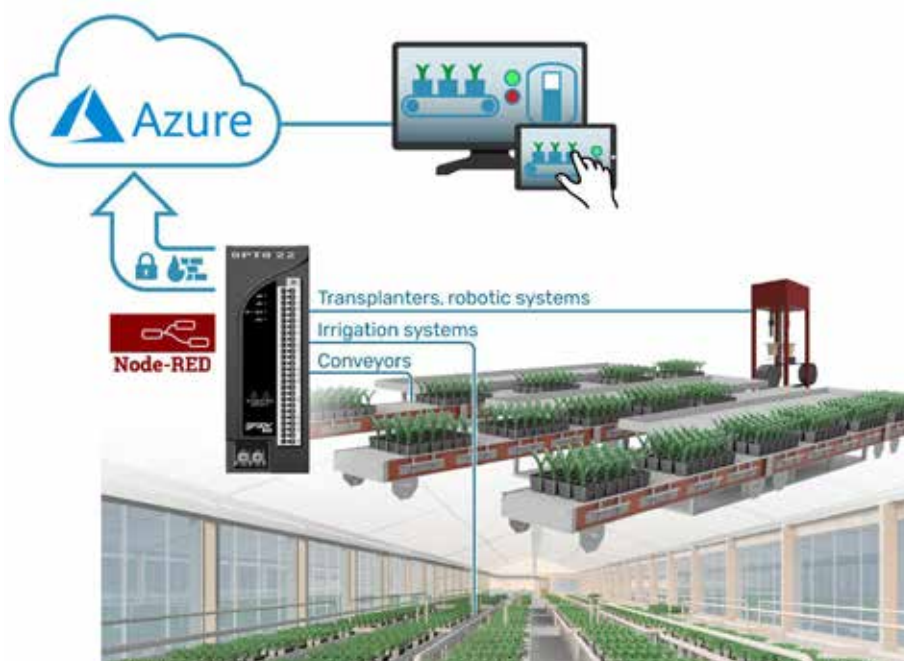
Oil and Gas Company

A Texas-based oil and gas company headquartered in Fort Worth faced challenges with outdated manual systems at their saltwater disposal sites, leading to inaccurate measurements and costly

overflows—at \$200,000 apiece.

Their automation engineer integrated Opto 22's groov RIO edge devices, using both the

RIO's physical I/O connected to level sensors and its built-in Modbus/TCP communication to intelligent pressure sensors.



SOURCE: OPTO 22

How an ornamental plant grower integrated the Opto 22 groov RIO edge device

Describing the edge device as the “Goldilocks solution”—not an expensive panel with unnecessary extras nor a basic PLC lacking the necessary I/O and modern communications—the engineer highlighted its suitability for their IIoT architecture.

Now monitoring tank levels, flow rates, and pump statuses, the groov RIO publishes MQTT Sparkplug B data to their Ignition SCADA system, improving visibility, reducing environmental risks, and saving hundreds of thousands annually.

Water District

An irrigation and drainage district serving over 30,000 acres of farmland in Gila Bend, Arizona, struggled with costly downtime and pump failures, with annual repair costs reaching up to \$400,000. Limited monitoring capabilities forced technicians to rely on frequent site visits, hindering efficiency and timely responses.

To modernize their operations, the district implemented Opto 22’s groov RIO edge devices. Using Node-RED dashboards for real-time visualization and leveraging their FlowFuse™ infrastructure for secure remote management, they automated the collection of data and critical metrics like pump statuses and water levels to improve monitoring.

“This is easily going to pay for itself,” says the district manager, noting reduced pump failures and an estimated \$300,000 in annual savings.

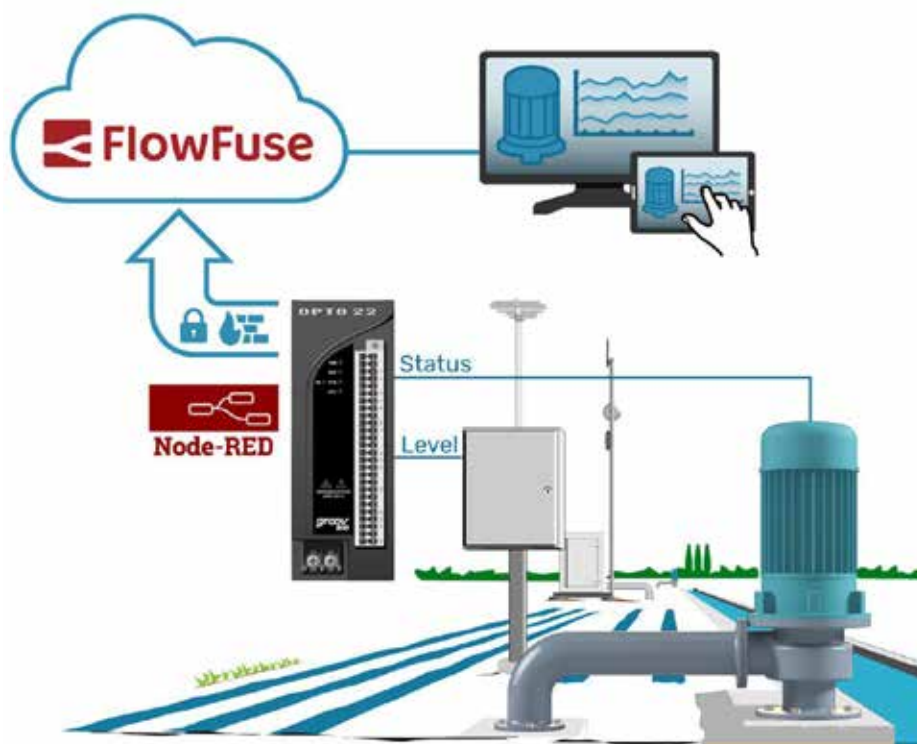
OEM Heat Treatment

An OEM manufacturer of heat treatment systems headquartered in Terre Haute, Indiana, faced challenges in monitoring energy consumption for their high-power furnaces, some of which consume up to 350 kVA per hour. Precise energy tracking was essential to calculate and understand the operational costs of their systems.

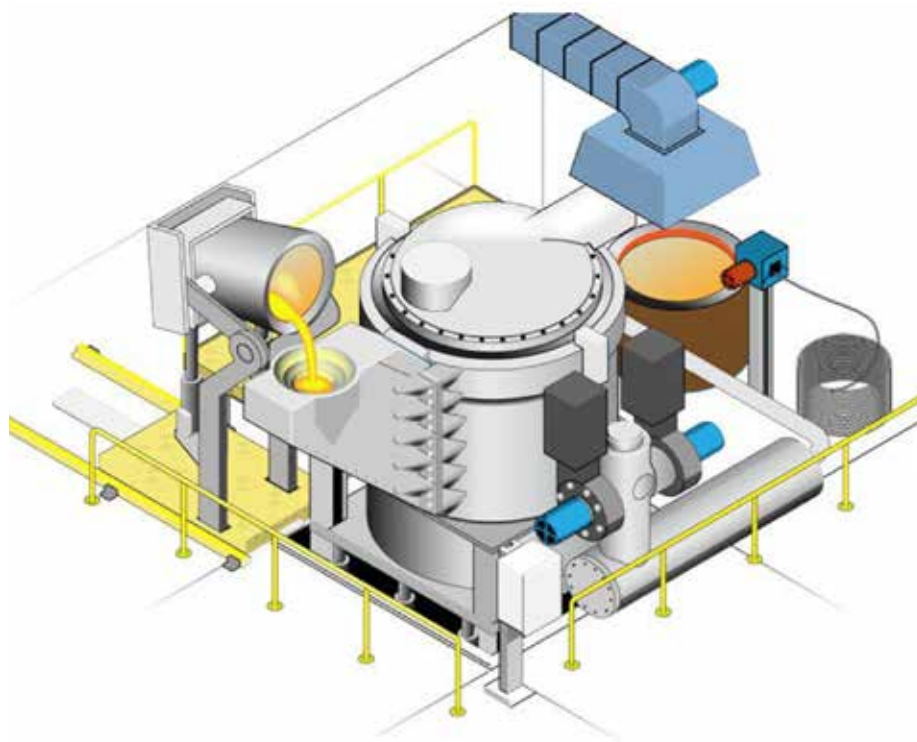
To track energy use, the manufacturer integrated Opto 22’s groov RIO EMU, an IIoT-ready edge device for power and energy monitoring, into their latest furnace designs. The EMU provided real-time energy consumption data, allowing them to calculate the exact energy cost per part produced.

“With energy monitoring, we can calculate in real time how much it costs to heat treat parts, and we can now accurately assign the cost of energy to the production of a particular component,” explains their controls engineer.

This insight enables them to precisely allocate energy costs to specific jobs, refine their pricing models, and identify opportunities to improve furnace efficiency—directly impacting their bottom line.



How a water district integrated the Opto 22 groov RIO edge device.



Furnaces and other high temperature equipment are often the largest energy consumers in a facility.

Conclusion

These companies followed the exact steps outlined in this article: they identified the data they needed, monitored existing signals, added new sensors where necessary, and leveraged existing protocols to collect critical operational data.

Each solution addressed their unique challenges and delivered real results.

So what about you? What data will you capture, and how will you use it to take your operations to the next level? The tools are there—now it’s your move.

Application story by **Opto 22**.

[Visit Website](#)

Edge architectures and cloud computing impact manufacturing

A hybrid cloud computing and edge architecture enables critical, real-time decisions to happen at the edge and strategic, data-intensive analysis in the cloud. Expect to see more edge architectures and cloud computing in manufacturing processes, driving further innovation and efficiency improvements.



SOURCE: ISTOCKPHOTO

In a manufacturing plant, edge architectures involve deploying compute power on the factory floor, co-located with machinery and associated sensors.

MANUFACTURERS ARE RAPIDLY ADOPTING digital technologies to improve efficiency, increase throughput, and control costs. Two important enablers of this digital transformation are edge architectures and cloud computing. When applied effectively, these technologies can significantly enhance Overall Equipment Effectiveness (OEE) by improving product quality, reducing downtime, and maximizing output.

Edge architectures work by processing data close to the machines and sensors that generate it. This reduces the time it takes to detect and respond to issues on the production floor, enabling near real-time decision-making. This is especially valuable in high-speed manufacturing environments where even brief delays can impact productivity or product quality. Keeping data local also reduces the demand on network infrastructure and improves system reliability in areas with unstable connectivity. In addition, processing data at the source helps manufacturers maintain greater control over sensitive information, which can be essential for protecting intellectual property or meeting data privacy requirements.

Cloud computing, on the other hand, offers

a centralized approach. It provides access to scalable computing power and storage that can be shared across multiple facilities, making it easier to implement organization-wide analytics, forecasting, and enterprise applications. By aggregating data from different locations, cloud platforms help identify patterns that may not be visible when looking at individual sites. This enables better decision-making at the management level and supports long-term planning. Cloud platforms also simplify software deployment and updates, allowing manufacturers to roll out new capabilities without investing heavily in on-premise infrastructure. Their built-in redundancy and security features also make cloud systems a dependable backbone for business continuity.

Edge architectures and cloud computing aren't competing technologies—they're complementary. Edge architectures are ideal for tasks that require speed, autonomy, or local control, such as real-time equipment monitoring or safety shutdowns. Meanwhile, cloud solutions excel at coordinating information across the organization, managing large-scale data analysis, and supporting enterprise-wide collaboration. When combined

in a hybrid approach, these technologies offer the best of both worlds: immediate, on-the-ground responsiveness from edge systems and strategic oversight and analysis from cloud-based platforms.

Edge architectures in manufacturing

In a manufacturing plant, edge architectures involve deploying compute power on the factory floor, co-located with machinery and associated sensors. Typical applications of edge architectures include:

Machinery condition monitoring: Increased local compute power enables the real-time monitoring of machinery, supporting predictive maintenance by detecting anomalies and scheduling maintenance activities before failures occur. This approach enhances equipment reliability, minimizes unplanned outages, and lowers maintenance costs.

Real-time quality control: Processing imagery and related data through edge architectures enables manufacturers to detect defects in products as they produce them. Immediate feedback reduces waste and rework, increasing the overall quality of output.

Energy and resource management: Edge

architectures can support energy management more effectively. For example, edge devices can adjust heating and cooling in response to occupancy, plant floor activity, and external weather conditions. Similar edge technology can optimize the use of resources such as water and other raw materials.

One of the significant benefits of edge architectures is the ability to process data closer to its source in real time. This proximity to data enables more rapid decision-making, whether that involves energy consumption, quality control, or machinery maintenance.

The use of edge architectures allows sensitive data to be processed locally, minimizing the need to transmit large volumes of data to centralized cloud servers. This localization of data not only reduces network costs but can also reduce the risk of a data breach. For manufacturers dealing with proprietary processes, recipes, or sensitive client data, this localized data handling is particularly advantageous.

The distributed nature of edge architectures not only minimizes network load; it also enables more efficient resource utilization. It also helps to balance the network load and avoid bottlenecks associated with centralized data processing. Furthermore, for manufacturing plants located in remote areas with unreliable internet connectivity, edge architectures reduce the likelihood of operational outages due to connectivity loss or centralized processing failure. This decentralized approach enhances the overall resilience of the manufacturing process.

Cloud computing in manufacturing

In a manufacturing environment, cloud computing provides centralized, scalable computing resources hosted off-site to support a wide range of operations, from enterprise resource planning (ERP) to advanced analytics and cross-site coordination. Unlike edge architectures, which emphasize localized processing, cloud computing focuses on aggregating, analyzing, and managing data across the enterprise. Typical applications of cloud computing in manufacturing include:

Analytics and machine learning: Data collected from multiple production lines and facilities, centralized in the cloud, is used to identify trends, optimize production schedules, and enhance forecasting. Cloud platforms provide the processing power necessary to train and deploy machine learning models that support quality control, predictive maintenance, and supply chain optimization.

Remote monitoring and diagnostics: Cloud computing enables manufacturers to monitor equipment and operations across geographically distributed plants remotely. This capability allows for centralized support teams to perform diagnostics, analyze performance, and coordinate with on-site



Cloud computing provides manufacturers centralized, scalable computing resources hosted off-site.

staff, thereby reducing the need for physical presence and enhancing responsiveness.

Scalable application deployment and integration: Cloud services facilitate the deployment and integration of new applications, including MES (Manufacturing Execution Systems), digital twins, and industrial IoT platforms. Manufacturers can roll out updates, test new features, and scale solutions without the constraints of on-premise infrastructure.

Two key benefits of cloud computing for manufacturers are scalability and centralized accessibility. Manufacturers can access computing resources without having to invest in or manage extensive on-site infrastructure. This flexibility allows them to scale operations quickly, respond to changing market demands, and improve overall agility.

Cloud computing also provides backup and disaster recovery services. Centralized storage ensures that data is readily accessible in the event of a local hardware failure. These features are particularly beneficial for manufacturers with global operations or those subject to regulatory compliance requirements.

Summary

Edge architectures can provide significant benefits to manufacturers by bringing compute power closer to the data source:

- Reduced latency enables faster response time to machinery and quality issues, resulting in increased throughput, higher quality, and reduced downtime.
- Localized intelligence enables faster decision-making within the organization, facilitating a more agile response to changes in demand.
- Distributed processing increases plant resilience, reduces data security risks associated with transferring data outside the facility, and reduces the costs of centralized infrastructure and

networking.

Cloud computing can provide significant benefits to manufacturers by centralizing data and leveraging scalable, high-performance computing resources:

Enterprise-wide visibility: enables integration of data from multiple plants, suppliers, and systems, supporting advanced analytics, better forecasting, and improved coordination across operations.

Scalable infrastructure: allows manufacturers to deploy new applications, scale workloads, and implement digital transformation initiatives without heavy capital investment in on-site hardware.

Remote accessibility and collaboration: empower teams across departments and locations to access shared data, streamline product development, and coordinate more effectively on production and quality initiatives.

Robust data security and continuity: are supported through cloud providers' built-in cybersecurity measures, automated backups, and disaster recovery capabilities, helping manufacturers maintain business continuity and regulatory compliance.

A hybrid cloud computing and edge architecture enables critical, real-time decisions to happen at the edge and strategic, data-intensive analysis in the cloud. This union of technologies enhances operational efficiency, supports innovation, and allows manufacturers to derive maximum value from their data.

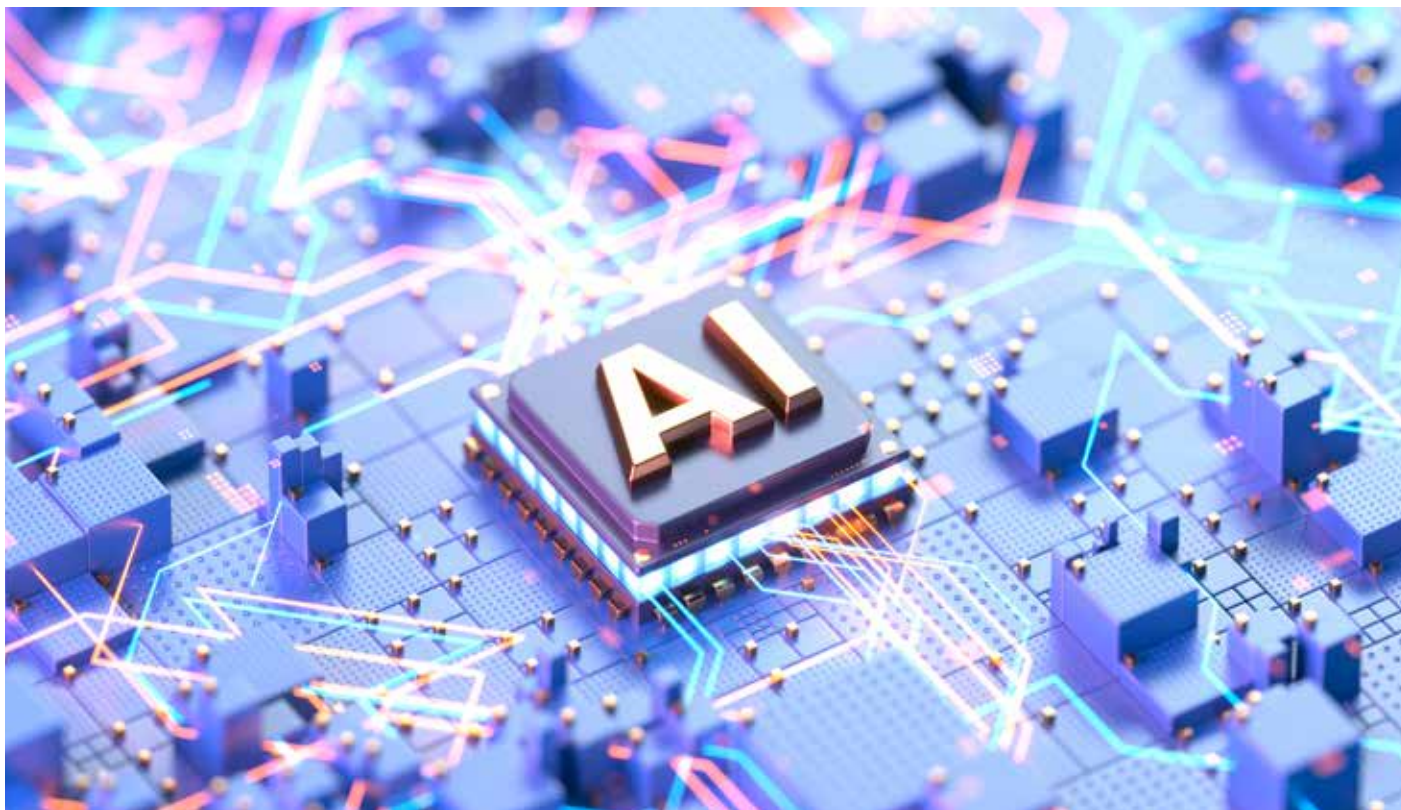
Expect to see more edge architectures and cloud computing in manufacturing processes, driving further innovation and efficiency improvements.

Steve Mustard, president of National Automation, Inc. and former president of the Industrial Society of Automation.

[Visit Website](#)

Current status of AI in operational technology

Rather than expecting a new AI model to help with critical processes, it should first be implemented in non-critical areas or an advisory capacity. For example, AI might first be used to analyze historical data and provide insights without the ability to directly affect operations.



SOURCE: BELDEN

Current AI solutions available are causing organizations to have two main problems: unpredictability of AI outputs and fluctuation in performance.

INTRODUCING AND IMPLEMENTING ARTIFICIAL Intelligence (AI) in Operational Technology (OT) has many benefits. AI-driven analytics are very advanced, enabling higher performance, new data-driven capabilities, lower energy consumption, and provide a way of circumnavigating the upcoming expert shortage by making OT more accessible to non-technical specialists.

However, the current AI solutions available are causing organizations to have two main problems: unpredictability of AI outputs and fluctuation in performance.

Challenges and risks of applying AI in OT

Probabilistic AI vs. Deterministic OT: Industrial AI suffers from the very same shortcomings as publicly available models. Traditional OT control systems (such as PLCs and SCADA) are designed to be deterministic and provide an expected stable behavior to maximize uptime. AI systems, especially

those based on machine learning (like AI agents), are inherently probabilistic. In simple terms, an AI algorithm is (currently) mis-designed for the logic of OT systems.

The Data Dilemma: The main problem is that industrial data is noisy, unstructured, or incomplete. Sensors can drop readings, industrial protocols may provide terse or binary data, and “ground truth” labels for events such as component failures or quality defects are not assured. Feeding AI with this data is not viable for an accurate output. The alternative is training it with high-quality OT data. However, this itself is a challenge and could be a major limitation for companies still struggling with the basics. The Brownfield nature of many OT environments means AI must coexist with legacy systems and protocols. There are no shortcuts to it. Factories must first deal with their digitalization challenges to properly introduce AI.

The Human Factor: The Demand for “Why”:

Another problem is performance fluctuation. This is due to the unique character of AI in industrial processes. The intrinsic value (and a weakness) of industrial AI is that it is designed to mimic an employee. Much like human employees, it takes time to train the AI with the necessary knowledge to avoid errors and biases. When an AI system flags an anomaly, or recommends adjusting a process parameter, engineers will demand to know why. Unlike a traditional algorithm with a clear logical rule, a machine learning model’s reasoning can be logically flawed.

Overall, there are many challenges with integrating AI into OT systems. These range from technical issues (unpredictable behavior, data issues, lack of computational power, integrating into legacy systems) to human and organizational factors (trust, skills gaps, regulatory compliance). Fortunately, we are already seeing companies gaining relevant experience and building a set of best practices to deal with these

issues. In the next section, we look at some of the existing strategies that can mitigate the risks and streamline the adoption of AI in industrial environments.

Strategies to mitigate AI risks in industrial environments

It is always best to start small and safe when implementing new mitigation strategies. Rather than expecting a new AI model to help with critical processes, it should first be implemented in non-critical areas or an advisory capacity. For example, AI might first be used to analyze historical data and provide insights (e.g. suggesting maintenance windows or flagging inefficiencies) without the ability to directly affect operations.

This allows experienced operators who continuously oversee the outputs to provide feedback and optimize the model. Only when the AI has proven to be sufficiently reliable in this read-only role should it be gradually introduced into closed-loop controls.

Pilot projects in a testbed or sandbox environment, utilizing either digital twins or other simulation environments, are a must. By the time the AI is controlling something in production, it should have gone through multiple stages:

1. offline analysis
2. decision support
3. supervised automation
4. autonomous control for select and well-understood tasks

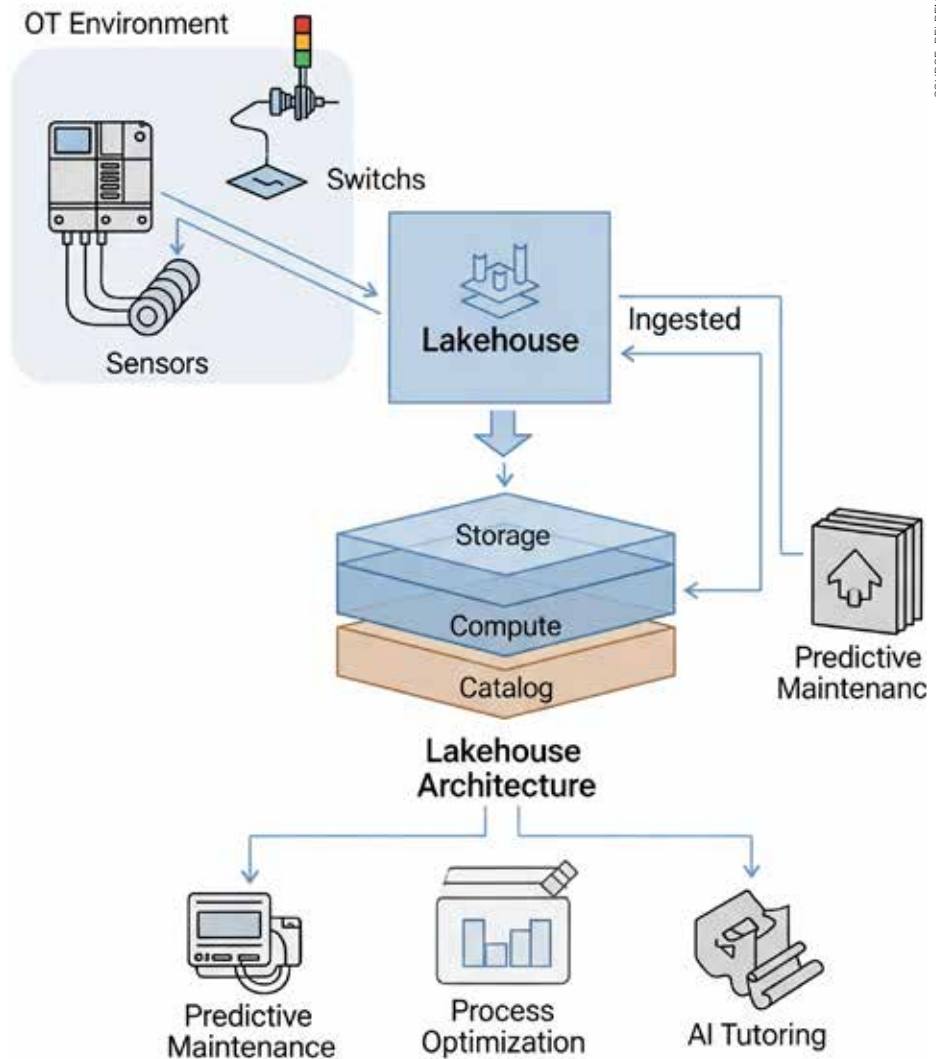
Effective use of AI in OT therefore calls for eXplainable AI (XAI) techniques, where AI decisions should be accompanied by human rationale. For example, an AI-based “industrial agent” that identifies a network fault should be able to explain its conclusion by pointing to specific anomalous metrics or error patterns, much like an experienced human technician would. By providing context, e.g. “Switch 3’s traffic is outside normal VLAN parameters, which likely caused the device to disconnect”), the AI’s actions become transparent, allowing operators to reliably verify it. This continuous improvement loop is analogous to preventive maintenance for machines, except it is for the algorithms.

Data architecture at the core of it – the lakehouse

Another key area of discussion is unified data ingestion & storage architecture. Lakehouse Data Architecture is currently the most suitable model for effective implementation of industrial AI.

The Lakehouse combines three important building blocks:

- a storage layer for managing data persistence,
- a compute layer for handling queries and processing tasks,



The Lakehouse Data Architecture is currently the most suitable model for effective implementation of industrial AI.

- a catalog that controls metadata and schema definitions.

The Lakehouse model combines capabilities that usually require multiple data lakes to perform into a single workflow that enables organizations to perform both analytical and AI-driven workloads against a single source of truth.

Lakehouse architecture stores large amounts of data on cloud platforms like S3, Azure Data Lake Storage, or Google Cloud Storage. Costing around \$20-23 per terabyte per month, this is much cheaper than the price of traditional storage systems. In complex network monitoring scenarios such as capturing detailed telemetry from thousands of switches, routers, and optical equipment terabytes worth of data can be captured and stored each year. Lakehouse now provides a way of storing multiple years of performance metric data efficiently and cheaply so that organizations can perform more accurate analyses and experience better long-term results.

There is also the schema evolution to talk about. This uses open table formats such as Delta Lake, Apache Iceberg, or Apache Hudi, and can adapt without interruption when new metric and data points are received. This enables users to integrate them and other AI contextual inputs without downtime or migration.

Lakehouse architecture is also based on open standards, so there are no vendor lock-in issues. By storing data in widely supported formats, such as Parquet or ORC, and employing standard APIs like S3, organizations have the freedom to choose from several compute engines (Spark, Trino, and DuckDB) based on their unique requirements. However, one of the biggest advantages for teams building AI-driven applications is the unified data access offered by Lakehouse. Engineers and operators can effortlessly analyze multiple data types using standard SQL queries or Python DataFrames, and built-in features like “time travel” make revisiting historical baselines or investigating past anomalies straightforward.



SOURCE: ISTOCKPHOTO

- **Risk Assessment:** There is an 87% likelihood of receiver failure within the next 45 days, prior to the subsequent scheduled maintenance."

Process optimization

AI is also increasingly used to fine-tune industrial processes to achieve optimal performance. For example, AI might discover that a slight adjustment in oven temperature and conveyor speed in a furnace process yields a higher output with lower energy per unit under certain humidity conditions. An automotive plant also used AI to analyze its assembly line and found that rearranging some tools and parts (e.g. moving a component bin closer to a workstation) could save each worker a few seconds, adding up to significant productivity gains over time.

AI tutoring

Another emerging use case is AI tutoring. AI can collect information on the knowledge and experience gained by seasoned engineers and store the data so that newcomers can learn from the engineers without them being directly present. With many industries facing the generation exchange, AI tools can help mitigate the negative impacts.

For example, an "AI agent" could observe how an expert troubleshoots a particular machine over time, through either recorded data or natural language explanations, and learn to replicate that diagnostic process. Later, a less experienced technician could query the AI: "Why is Machine A producing off-spec product?" and the AI might respond with a reasoning similar to what the expert would have done. The outcome is a workforce that can onboard faster (since newbies have an AI tutor to consult) and more experienced professionals can focus on high-value activities with greater care.

The above examples demonstrate that, when thoughtfully implemented, AI can significantly enhance industrial operations, from reducing downtime and waste to improving safety and worker efficiency. Companies at the forefront of Industry 4.0 are treating AI as a key tool in the automation toolbox, complementing classical control systems and human expertise.

As explainable AI (XAI) techniques mature and data architectures become more unified, the journey from supervised AI to trusted autonomous control will accelerate. For industrial organizations, the essential first step remains the same: building the foundational data and networking infrastructure today to support the intelligent operations of tomorrow.

Dr. Ashwani Singh, Director Architecture & Technology, Belden.

[Visit Website](#)

Another emerging use case is AI tutoring. AI can collect information on the knowledge and experience gained by seasoned engineers and store the data so that newcomers can benefit.

Use cases: AI in industrial automation

Despite the challenges, we can already see the first emerging use cases of AI in automation. The most mature and widely adopted AI use cases in OT are those that augment human decision-making.

Predictive maintenance:

One of the most common AI applications in OT is in predictive maintenance. AI is used to predict equipment failures before the fault physically occurs. From motors in conveyor belts to valves and switches on the production line, there are many areas where AI systems can monitor the performance and degradation of components to spot excessive wear and highlight impending failures with operators being alerted to any potential issues weeks or even months in advance.

An example below shows how an AI agent monitors network hardware (such as the optical transceivers in industrial switches) and notices a gradual signal strength decay. The conversation with the AI after this potential issue had been identified is as follows:

AI Agent: "After reviewing the network telemetry, I advise replacing the optical receivers in Switch-Core-3. I've noticed a steady decline in signal strength by approximately 0.3 dBm over the last month, without any associated link-down events. This type of degradation typically points to component aging rather than physical connection problems."

Network Admin: "That's going to cost around \$15,000. How confident are you in this recommendation?"

AI Agent: "My confidence level is high—approximately 90%. The degradation follows a consistent, linear trend, unlike fiber contamination which usually appears as abrupt signal fluctuations during reconnection events. Historical records from 18 comparable switches indicate a similar pattern predicted optical receiver failures within 60 days at an accuracy rate of 87%. Additionally, maintenance logs do not report any fiber cleaning or reconnections during this period."

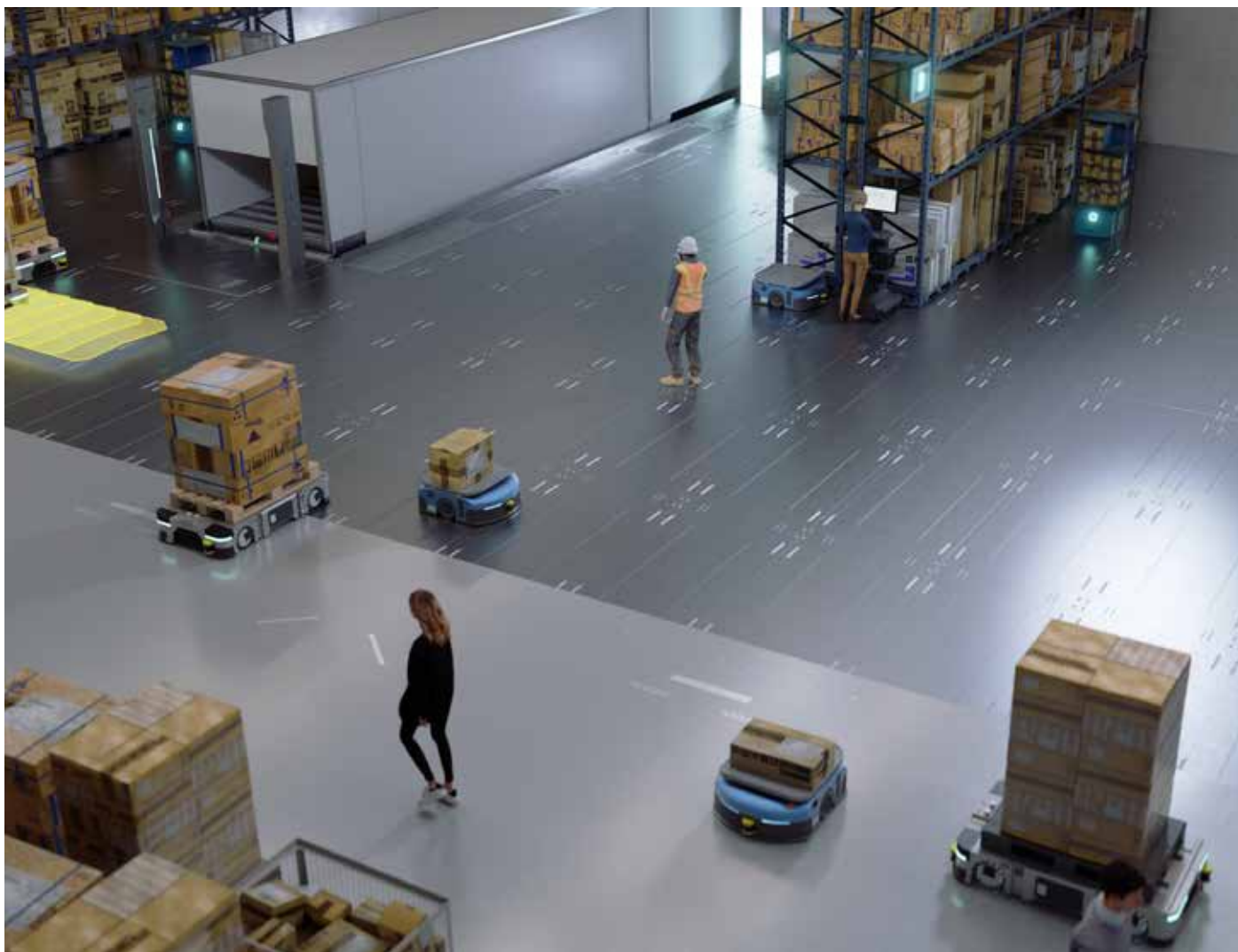
Network Admin: "Can you display the trend analysis and provide similar cases for reference?"

AI Agent: "Certainly. Here's the detailed analysis:

- **Signal Strength Trend:** Over the past 30 days, signal strength has steadily dropped from -2.1 dBm to -2.4 dBm.
- **Link-Down Events:** No link-down occurrences recorded in maintenance logs during this time.
- **Historical Comparison:** Of 18 previous similar situations, 16 resulted in optical receiver failures within a 60-day timeframe.
- **Potential Impact:** Estimated downtime costs approximately \$50,000 per hour if failure occurs.
- **Optimal Maintenance Window:** Next scheduled maintenance is planned for next weekend.

Autonomous production with new AI and robotics capabilities

Through an agent-based interface, users will be able to configure autonomous mobile robots (AMRs) and automated guided vehicles (AGVs), assigning them tasks like transporting materials and goods across the shop floor. This is yet another building block for automating automation in a factory with the help of generative AI.



SOURCE: SIEMENS

Innovation includes expansion of the Operations Copilot with AI agents for autonomous transport systems.

SIEMENS HAS ADVANCED AUTONOMOUS production with new AI and robotics capabilities for automated guided vehicles.

- Operations Copilot to interact with physical AI agents
- Vision: Multi-agent systems with physical and virtual AI agents for autonomous transport systems and mobile robots
- New software-based safety solution Safe Velocity

At the automatica trade show in June, Siemens announced plans to integrate its Operations Copilot into driverless transport systems and

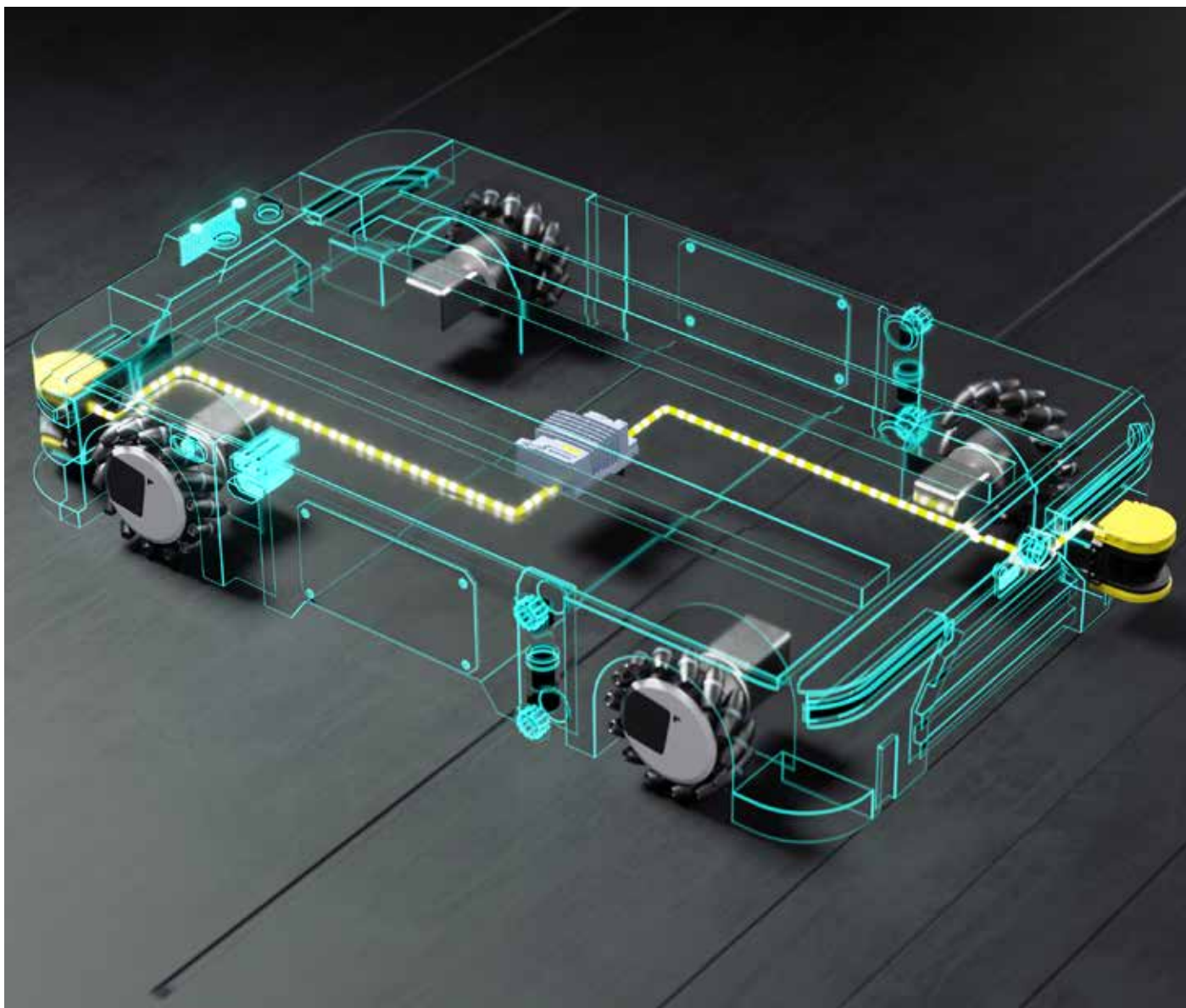
mobile robots. The Operations Copilot is an industrial copilot for machine operation and maintenance. As mobile transport robots increasingly operate as autonomous physical agents powered by artificial intelligence (AI), the Operations Copilot will serve as a user interface for humans.

Through this agent-based interface, users will be able to configure autonomous mobile robots (AMRs) and automated guided vehicles (AGVs), assigning them tasks like transporting materials and goods across the shop floor. This is yet another building block for automating

automation in a factory with the help of generative AI.

Operations Copilot enhanced with agents for AMRs and AGVs

In a next step, Siemens plans to expand the capabilities of the Operations Copilot by introducing AI agents specifically developed for use with AMRs and AGVs. These agents support both the commissioning and operation of individual vehicles and entire fleets. *Commissioning in particular is a complex and time-intensive process:* AGVs need to be



Safe Velocity software enables fail-safe speed monitoring of autonomous vehicles.

integrated into the factory's existing IT and OT infrastructure and configured for specific conditions like routes and transfer stations. To streamline this task, engineers can rely on the *Operations Copilot*: It leverages AGV sensors and cameras to generate a detailed understanding of their environment. The Operations Copilot can access all relevant technical documentation of the installed components and retrieve real-time system data through its agent interface. This enables commissioning engineers and operators to work more efficiently, resolve issues faster, and ensure rapid deployment.

"By integrating both physical and virtual AI agents into our Operations Copilot, we're unlocking a new dimension of interaction between humans, robotics, and AI," said Rainer Brehm, CEO of Factory Automation at Siemens. "This enables our customers to deploy autonomous transport systems more quickly, operate them efficiently, and enhance

safety – bringing us one step closer to a fully autonomous factory."

New Safe Velocity software enhances safety on the shop floor

AGVs are equipped with navigation and sensor technologies, that allow them to move safely and reliably through production and intralogistics environments – with no direct human intervention. When people or objects appear in their path, AGVs automatically slow down, stop, or navigate around these obstacles. Siemens' new software solution, Safe Velocity, enables the fail-safe monitoring of vehicle speed, which permits the protective fields of safety laser scanners to be dynamically adjusted in real time.

The TÜV-certified software is compatible with the hardware and software from a variety of AGV manufacturers and enhances existing safety systems to meet stringent industrial safety standards. Safe Velocity reduces the

need for additional safety hardware. This simplifies system architecture, saves valuable vehicle space, lowers engineering complexity, and minimizes cabling requirements – without compromising functional safety.

In the future, the Operations Copilot will interact with AI agents such as Safe Velocity to analyze targeted data from safety laser scanners and monitor the speed of AGVs. The virtual Safe Velocity agent supervises autonomous vehicles and can cooperate with other agents designed for AGV and AMR applications. This way, Siemens is building a multi-agent system where the Operations Copilot orchestrates both physical and virtual AI agents, enabling seamless interactions and deeper integration between the real and the digital worlds.

*Technology article by **Siemens**.*

Visit Website

Using IO-Link transceiver to manage the data link selection

The requirement for microcontrollers to manage multiple tasks simultaneously means they can struggle to meet the timing specifications for IO-Link data communications. Some manufacturers have been left with using a second microcontroller to manage the IO-Link stack, but now this is no longer necessary.

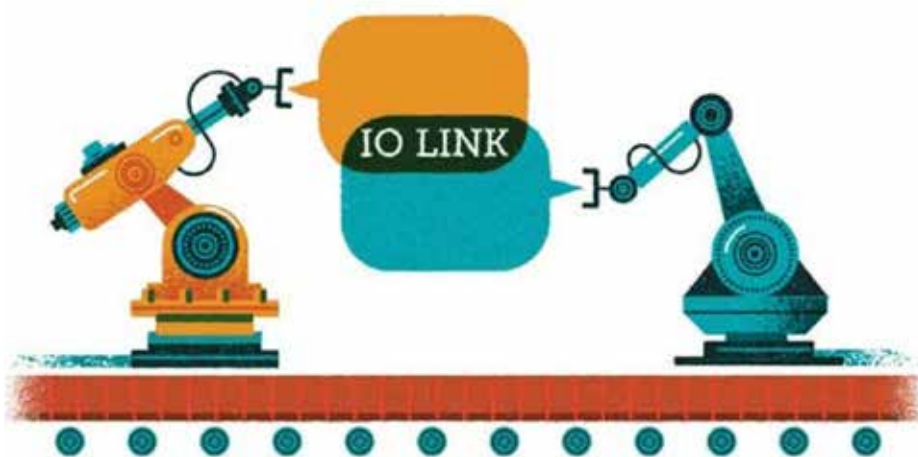
HOW CAN IO-LINK DEVICE MICROCONTROLLERS overcome the challenges associated with adhering to the timing requirements specified in the IO-Link standard?

Answer

An IO-link device microcontroller is expected to perform multiple tasks simultaneously, which can cause difficulty in responding to a request within the acceptable specified time window.

This is especially true if performing a task from which the microcontroller cannot be interrupted. A typical solution for this timing challenge is to use a second microcontroller to manage the IO-Link stack, thereby maintaining a more constant response time interval between the IO-Link device and the IO-Link master.

However, this is a highly inefficient approach because it uses more power and requires a much larger PCB and therefore a larger sensor enclosure. A superior alternative is to use a transceiver capable of managing both the data link and physical layers in the communication pathway. By unburdening this task from the device microcontroller, this transceiver enables the design of even smaller, more complex, higher functioning, and cost-effective industrial field instruments.



SOURCE: ANALOG DEVICES

Innovation includes expansion of the Operations Copilot with AI agents for autonomous transport systems.

Introduction

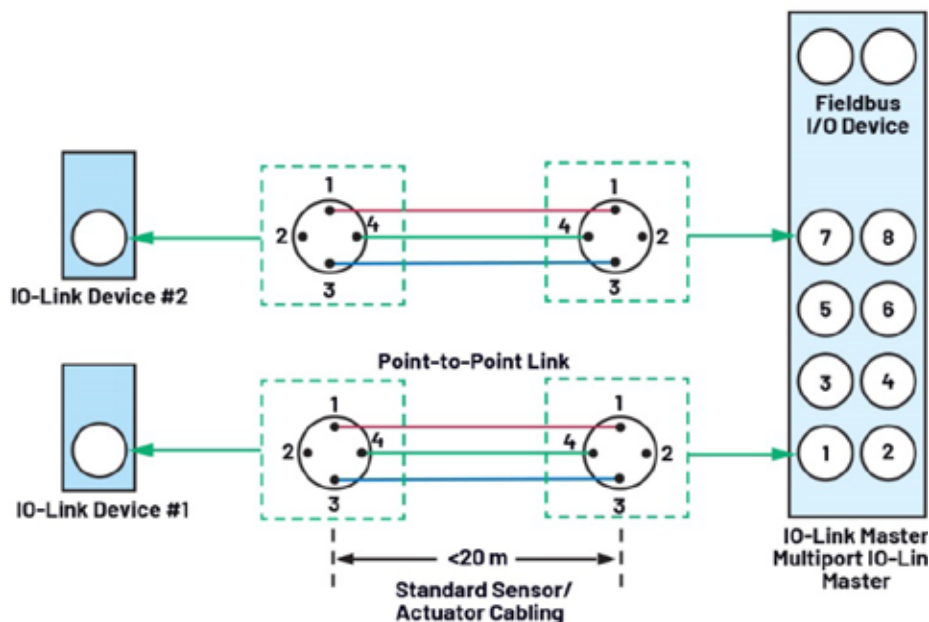
“To do two things at once is to do nothing”—while this take on multitasking by the Latin writer Publilius Syrus might be extreme, there are some circumstances where multitasking can lead to tasks not being performed in the way they were initially intended or on time.

As industrial processes become more complex, field instruments like sensors and actuators have evolved to perform several different tasks simultaneously, including maintaining regular communication with a process controller. This imposes additional overhead on the device microcontroller that must be carefully managed or process data can be lost, leading to production downtime (the very thing that modern industrial communication protocols are supposed to reduce).

IO-Link Timing

IO-Link is a 24 V, 3-wire industrial communications standard that enables point-to-point communication between industrial devices and an IO-Link master that, in turn, communicates with higher level process control networks.

In IO-Link applications, a transceiver acts as the physical layer interface between a microcontroller running a data link layer protocol (stack) and the 24 V IO-Link signal line. IO-Link communication involves several types of transmission, including process data, value status, device data, and events. These allow industrial devices to be quickly identified, traced, and attended to if an error occurs, helping to reduce downtime. IO-Link enables remote configuration; for example, if the threshold for a process alarm to be triggered



SOURCE: ANALOG DEVICES

Figure 1. IO-Link master/device communication interface.

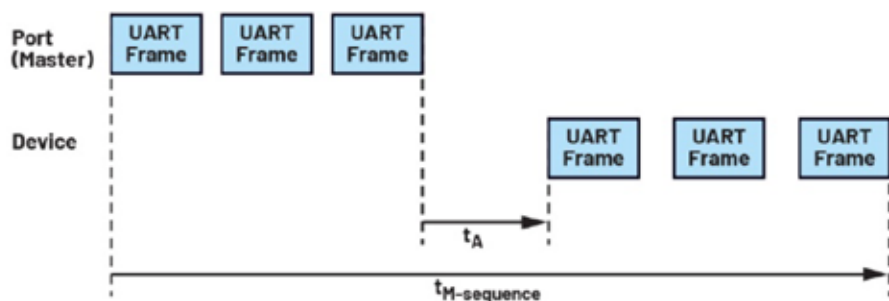


Figure 2. M-sequence timing in IO-Link communication.

needs adjusting, this can be done by sending the updated threshold to the device over the IO-Link connection without the need for a technician to visit the factory floor.

Communication between an IO-Link master port and a device is subject to several timing

constraints and takes place in a fixed schedule called M-sequence time. An M-sequence message includes a command or request sent from the IO-Link master to a device and the reply message from the device. Figure 2 illustrates the timing parameters in an

M-sequence consisting of a message between an IO-Link master port and a device message. The device must respond to the master within the response time of the device, t_A , which ranges from 1 Tbit to 10 Tbit (Tbit = bit times). For a COM3 baud rate, t_A should be between 4.3 μ s and 43 μ s. If the response time is outside of this range, a communications failure occurs.

When punctuality slips

An IO-link device microcontroller is expected to perform multiple tasks simultaneously, which can cause difficulty in responding to a request within the acceptable time window specified for t_A . This is especially true if performing a task from which it cannot be interrupted—this type of task is often referred to as a nonmaskable interrupt (NMI). If the device microcontroller does not respond within the specified time

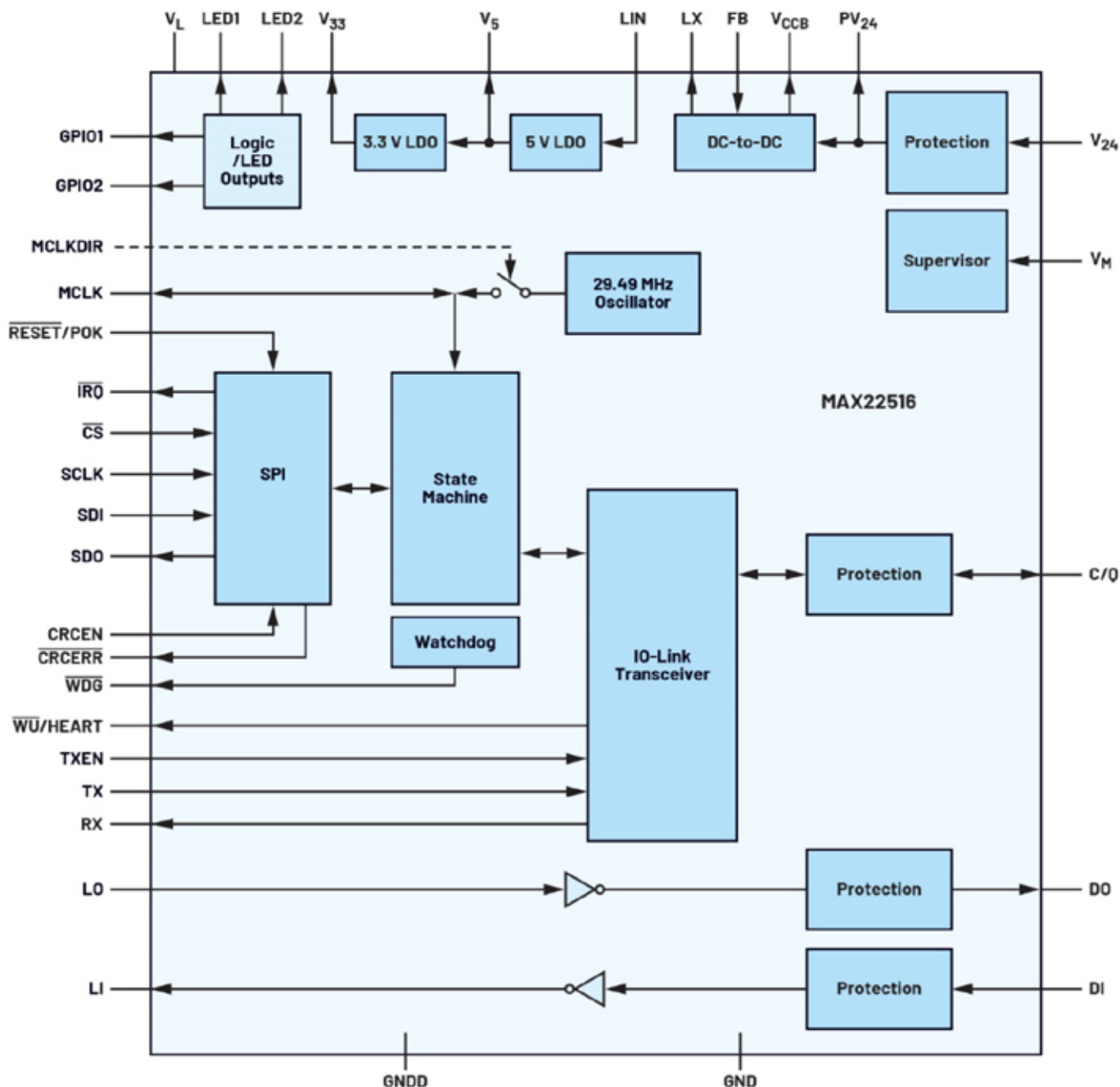


Figure 3. MAX22516 IO-Link state machine with transceiver and integrated DC-to-DC converter.

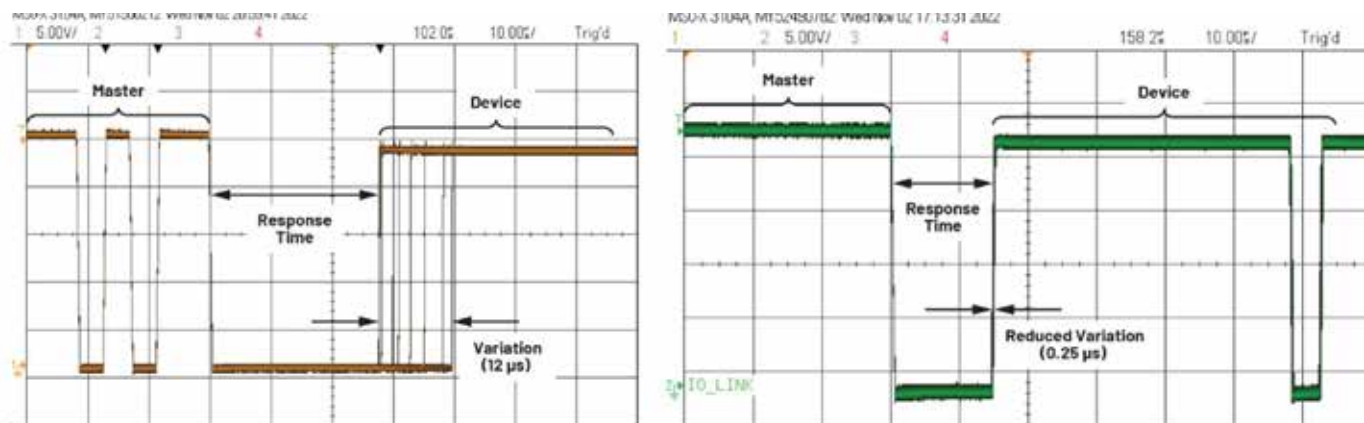


Figure 4. Comparing the response time of an application using a single microcontroller (left) and the MAX22516 (right) to manage IO-Link communication.

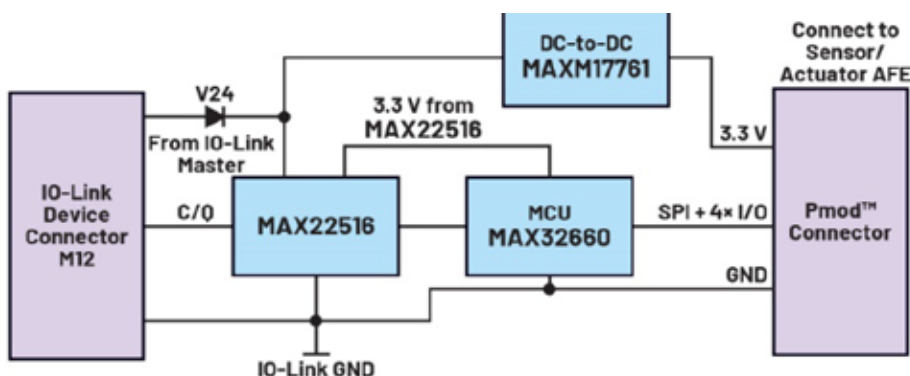


Figure 5. MAXREFDES281 IO-Link device reference design.

window, communication breaks down and must be reinitiated.

For example, in the case of an ultrasonic distance sensor, some of the many tasks that the microcontroller is expected to perform include:

- Send ultrasonic bursts
- Process the intrinsic line from the last burst, then calculate the distance
- Measure ambient temperature to compensate for the speed of sound
- Manage sensor background tasks (for example, power management)
- Reply to IO-Link cyclic requests
- Reply to IO-Link acyclic requests

Continuously processing data samples leaves little time for a microcontroller to manage the data link layer communication tasks, leading to considerable variations in the device response time. In extreme cases, it may not be possible to meet the timing requirement for t_A .

Timing issues caused by NMIs cannot be addressed by simply using a faster microcontroller with more features. A typical solution for this timing problem is to use a second microcontroller to manage the IO-Link stack, thereby maintaining a more constant response time interval between the device and the IO-Link master. However, this is a highly inefficient approach because it uses more power

and requires a much larger PCB and therefore a larger sensor enclosure.

Managing the data link

A superior alternative is to use a transceiver to manage both the data link and physical layers in the communication pathway. The MAX22516 IO-Link state machine (Figure 3) integrates all the functionality commonly found in IO-Link device transceivers, including the 24 V C/Q, an integrated step-down DC-to-DC converter, and 5 V and 3.3 V linear regulators.

This device is the first transceiver to include a full-feature state machine to fully manage the timing of IO-Link data communication. It autonomously handles communication with the IO-Link master for requests such as configuration and maintenance requests, as well as process data transfers using data written to registers and FIFOs by the microcontroller. A major benefit of using this transceiver is that it affords more options when selecting a microcontroller for the sensor, because the device microcontroller is not required to manage the task of communicating with the IO-Link master.

The MAX22516 monitors incoming messages from the IO-Link master. Once a complete indexed service data unit (ISDU) configuration or maintenance request is received, it

automatically sends ISDU BUSY messages to the IO-Link master and notifies the device microcontroller that communication has been successfully completed. The microcontroller can load on-demand data into the ISDU FIFO, a task that typically requires many cycles to perform, as time permits. Input process data (PDIn) and output process data (PDOut) are managed by the transceiver using data in the PDIn and PDOut FIFOs, allowing the microcontroller to write data to the PDIn FIFO and read from the PDOut FIFO without any time constraints. Integrated buffers ensure that data in the FIFOs is not lost or overwritten before being processed.

Figure 4 shows how using this transceiver dramatically reduces the time it takes for a device to respond to an IO-Link master compared to an application using a single microcontroller. The device response time is reduced by more than 50%, while the variability is also reduced considerably from 12 μ s to 0.25 μ s.

The MAXREFDES281 IO-Link device reference design (Figure 5) features the MAX22516 and can be used to verify the timing performance of different types of IO-Link sensors.

Conclusion

The requirement for microcontrollers to manage multiple tasks simultaneously means they sometimes struggle to meet the timing specifications for IO-Link data communications. Some equipment manufacturers are left with the unpalatable alternative of using a second microcontroller to manage the IO-Link stack. This two-microcontroller approach is now no longer necessary because the MAX22516 IO-Link transceiver integrates a state machine that can manage all IO-Link communication, freeing up the main device microcontroller to perform other time-critical tasks.

Brian Condell, digital marketing engineer, Analog Devices.

Visit Website

IEB Special Report: industrial remote connectivity solutions

Industrial remote connectivity solutions enable machine builders and users to securely access industrial equipment from any location. These solutions facilitate seamless and secure Industrial Internet of Things (IIoT) functionality, allowing for remote maintenance, troubleshooting, and machine data visualization.



SOURCE: ISTOCKPHOTO

"The latest solutions for Industrial Remote Connectivity are driven by innovations that focus on simplifying infrastructure, enhancing security, and enabling centralized management, especially as there is exponential growth in new industrial assets coming online. Cisco industrial routers exemplify these trends by providing a modular, secure, all-in-one platform that consolidates multiple networking functions into a single device,"

-- Emily Kasman, Industrial Security Product Marketing Specialist, Cisco.

INDUSTRIAL REMOTE CONNECTIVITY SOLUTIONS enable secure access and management of industrial equipment and operations from remote locations, enhancing efficiency, reducing downtime, and improving safety.

Remote access enables quick troubleshooting and maintenance, minimizing production interruptions, and eliminates the need for on-site visits, saving travel expenses and time. Remote access allows personnel to operate and monitor equipment from a safe distance, particularly in hazardous environments.

For this special report, the Industrial Ethernet Book reached out to leading companies involved in developing remote connectivity solutions, asking them to discuss an Industrial Remote Connectivity technology solution they provide, and the specific technical benefits that this approach offers.

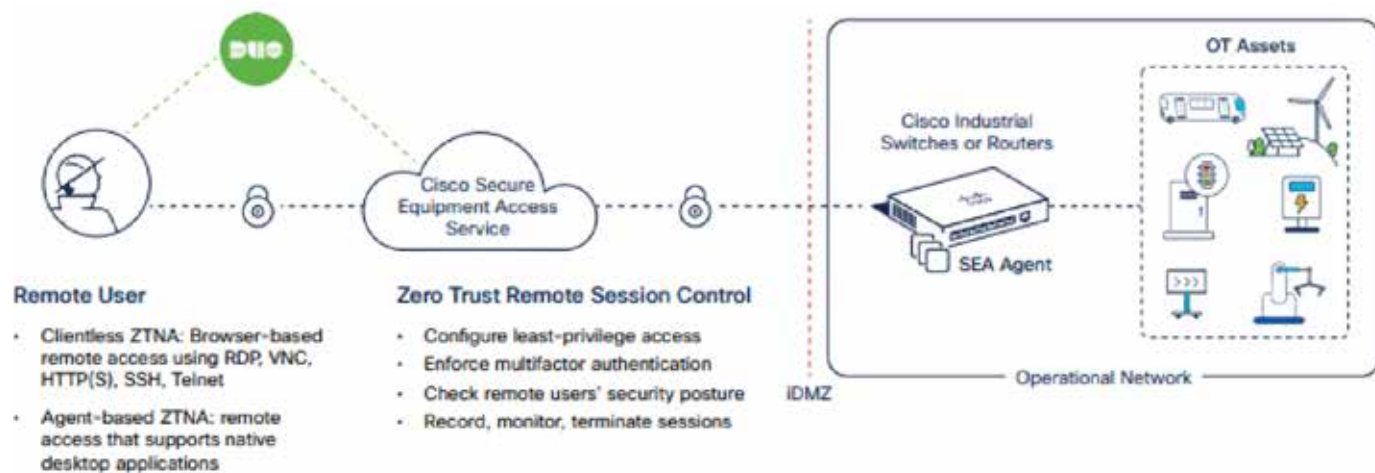
Reliable connectivity solutions

Robust industrial routing addresses evolving needs of modern industries.

"One key advantage of Cisco's industrial routers is their modular design, featuring pluggable modules that allow businesses to adapt to varying connectivity requirements," Emily Kasman, Industrial Security Product Marketing Specialist at Cisco told IEB recently. "Whether a location relies on 4G, 5G, fiber, or other technologies, Cisco's portfolio provides the flexibility to support diverse backhaul options. Moreover, these backhaul options can be changed or upgraded over time without replacing the entire router, ensuring the ability to meet evolving needs and technology changes with unmatched long-term cost efficiency."

Kasman added that Cisco's industrial routers also serve as a unified platform, for both connectivity and cybersecurity. They embed comprehensive security capability including next generation firewalls (NGFW), OT visibility, ZTNA remote access and more, eliminating the need to source dedicated products for each function, simplifying deployments and reducing operational complexity. Combined with Cisco's SD-WAN solution, organizations can centralize management, automate configurations, and enforce consistent security policies across the network.

"With these capabilities, Cisco delivers WAN infrastructure that is easy to manage, evolves with business needs, and supports a wide variety of connectivity scenarios, enabling cyber-resilient and efficient operations across industrial environments," Kasman said.



Cisco is a global leader in IT networking, offering purpose-built rugged hardware specifically designed for the unique demands of Operational Technology (OT) environments. Cisco delivers secure, high-performance networking that withstands extreme conditions while enabling seamless IT and OT integration. Cisco's industrial switches and routers are trusted worldwide for their reliability, advanced security features, and comprehensive management capabilities. Cisco's industrial remote connectivity solution leverages its robust industrial routing portfolio to address the evolving needs of modern industries. Field assets in remote or challenging locations require reliable and secure connectivity, and Cisco's routers are designed to meet this demand while simplifying network management.

Technology trends

Kasman said that the latest solutions for Industrial Remote Connectivity are driven by innovations that focus on simplifying infrastructure, enhancing security, and enabling centralized management, especially as there is exponential growth in new industrial assets coming online. Cisco industrial routers exemplify these trends by providing a modular, secure, all-in-one platform that consolidates multiple networking functions into a single device. This eliminates the need to source and deploy separate products for each function, saving costs and valuable space in industrial environments.

"With embedded cyber resilience and modular, future-ready connectivity, Cisco industrial routers enable you to connect and manage all your remote industrial assets and build a secure WAN infrastructure, even in harsh environments. Because they use the same technologies and management platform than Cisco's enterprise networking solutions, they allow organizations to use existing skills and unify networking and security across IT and OT environments," she added.

As industries generate massive amounts of

data at remote sites and production facilities, the need for edge computing has never been greater. Processing data closer to its source reduces latency, minimizes bandwidth usage, and enables faster, smarter decision-making where it matters most. Cisco addresses this need with Edge Intelligence running on its industrial routers, allowing businesses to securely collect, process, and act on data at the edge in real time. Beyond Edge Intelligence, Cisco's industrial routers support a wide range of applications, including remote asset management, threat detection, and secure connectivity, empowering organizations to optimize operations and drive innovation across their industrial environments.

Technology innovations

Kasman said that Cisco industrial routers offer unparalleled functionality in a single, compact device. Unlike traditional solutions that require multiple products to handle various networking needs, Cisco industrial routers integrate advanced networking, modular capabilities, and advanced security into one platform. This streamlined approach not only reduces hardware costs and deployment complexity but also saves valuable space in industrial environments.

With Cisco's SD-WAN Manager, businesses can centralize management and automate deployment and configuration tasks. Security policies are unified, meaning they are created in one location and automatically applied across the entire network, leaving no gaps and ensuring consistent protection everywhere.

Cisco industrial routers embed zero-trust network access (ZTNA) capabilities, enabling organizations to gain secure remote access to connected assets, for configuring and troubleshooting devices without dispatching technicians. Because ZTNA capabilities are built into the routers, there is no need to deploy additional hardware. This helps reduce costs and simplifies deployment, especially in remote locations where small cabinets might not have the space for additional hardware

appliances.

"Using the same SD-WAN console, businesses can configure their networks and deploy security policies, creating a streamlined, cost-effective solution. Cisco Industrial Routers deliver efficiency, security, and scalability in a single solution, making them an invaluable asset for modern industrial networks," Kasman said. "This is especially valuable for industries with widely distributed assets, as it eliminates the need for on-site visits, reducing operational expenses and downtime. This combination of security, flexibility, and centralized management makes Cisco industrial routers a standout choice for modern industrial networks."

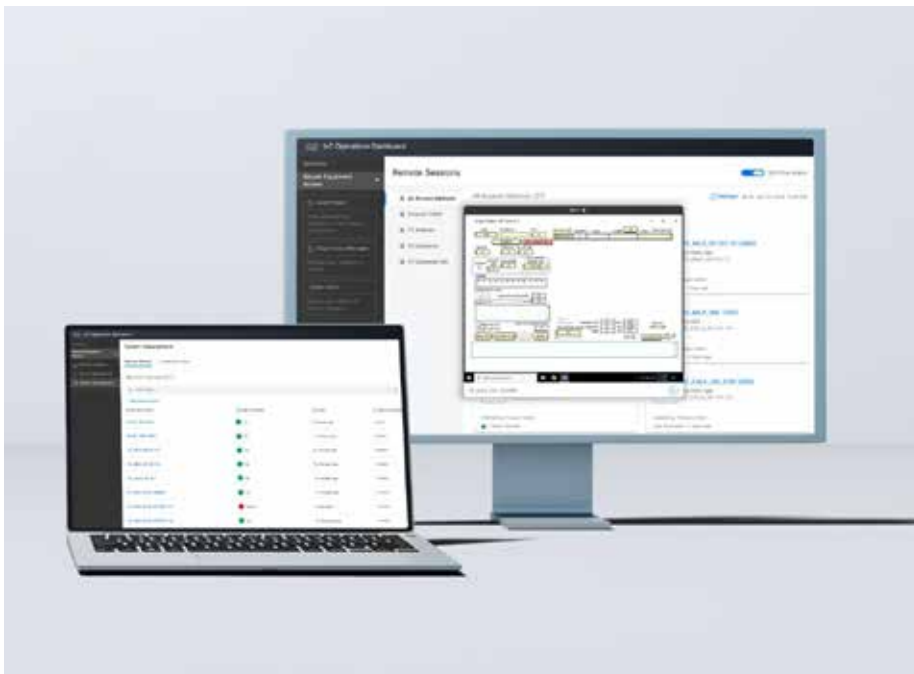
Remote connectivity solutions

Cisco Secure Equipment Access is designed to address the evolving needs of organizations across a variety of sectors by providing secure, seamless, and efficient remote connectivity to critical equipment and systems. In today's increasingly connected world, these solutions are essential for supporting operations, reducing on-site visits, and enabling timely responses to system issues—all while maintaining robust security standards.

Kasman said that key applications include not only remote monitoring, troubleshooting, and configuration, but also secure firmware upgrades, software patch management, and real-time diagnostics of field devices.

Industries such as manufacturing, roadways infrastructure, public transportation, renewable energy, oil and gas, water utilities, and EV charging stations all benefit from these capabilities. For instance, in manufacturing, remote connectivity supports predictive maintenance and minimizes unplanned downtime. In energy and utilities, it allows operators to manage geographically dispersed assets and respond rapidly to outages or anomalies.

By delivering these advanced security features and connectivity options, Cisco Secure Equipment Access not only protects



SOURCE: CISCO

data collection, reducing on-site service and speeding up troubleshooting.

According to Daniel Korte, Technology management PLCnext Technology, Phoenix Contact Electronics GmbH, “Security functions such as encrypted communication, firewall protection and role-based access ensure reliable operation. The PLCnext Control platform enables real-time on-site data processing through edge computing and cloud services. Thanks to support for open source software and standard IT protocols, the platform is interoperable, flexible and ideal for modern industrial environments. It supports containerized applications and secure data exchange.”

Technology trends

“Key trends driving industrial remote connectivity include the convergence of IT and OT, edge computing and the adoption of cloud-native technologies. Innovations such as containerization, 5G and AI-driven analytics are changing the way remote systems are managed,” Korte said. “At Phoenix Contact, we see an increasing demand for platforms like PLCnext Technology that support open standards and enable integration with third-party tools and services. Cybersecurity is also a key focus, with secure booting, encrypted communications and identity management becoming standard. In addition, with the rise of the digital twin and predictive maintenance, the need for reliable remote access to machine data in real time is increasing. Together, these trends improve operational efficiency, reduce costs and enable new business models.”

What makes this technology unique?

Korte said that PLCnext Technology is characterized by its openness, flexibility and the integration of IT functions into industry automation. Unlike conventional PLCs, PLCnext supports high-level languages such as C++, Python and Java as well as IEC 61131-3 and allows developers to use familiar tools. The Linux-based architecture enables containerized applications and seamless cloud connectivity to any cloud, including Proficloud.io. This hybrid approach bridges the gap between automation and digitalization, allowing users to implement advanced analytics, AI and remote services directly at the edge. The platform's cybersecurity features, including secure boot and encrypted communication, ensure secure remote operations. This unique combination of openness, security and scalability makes PLCnext Technology the ideal solution for future-proof industrial connectivity.

Focus of remote connectivity solutions

Korte said that remote connectivity solutions are essential in industries such as

Secure Equipment Access (SEA) directly addresses challenges by offering a secure, purpose-built remote access solution tailored for OT. Unlike traditional VPNs, SEA enables fine-grained, role-based access control, ensuring users only connect to the specific devices they are authorized to manage.

operational technology environments but also supports regulatory compliance, enhances productivity, and facilitates safe, scalable remote workforces. These benefits are indispensable for industries that rely on secure, always-available access to distributed or remote assets.

Addressing engineering challenges

“New Remote Connectivity solutions are designed to address several key engineering challenges faced by modern industrial organizations as they strive to maintain secure and efficient operations. Industrial enterprises increasingly rely on remote experts, contractors, and OEM partners to configure, troubleshoot, and support critical assets across geographically dispersed sites,” Kasman said. Traditional VPN solutions, however, are not ideal for OT environments. VPNs often provide broad, always-on access to the entire network, making it difficult to enforce least-privilege access policies. Managing granular permissions with VPNs is complex and often beyond the capabilities of most OT teams, especially at the scale required for industrial operations.”

Cisco Secure Equipment Access (SEA) directly addresses these challenges by offering a secure, purpose-built remote access solution tailored for OT. Unlike traditional VPNs, SEA enables fine-grained, role-based access control, ensuring users only connect to the specific devices they are authorized to manage. This supports operational needs while dramatically reducing cybersecurity risks. Furthermore, SEA empowers OT engineers with a self-service portal that allows them to

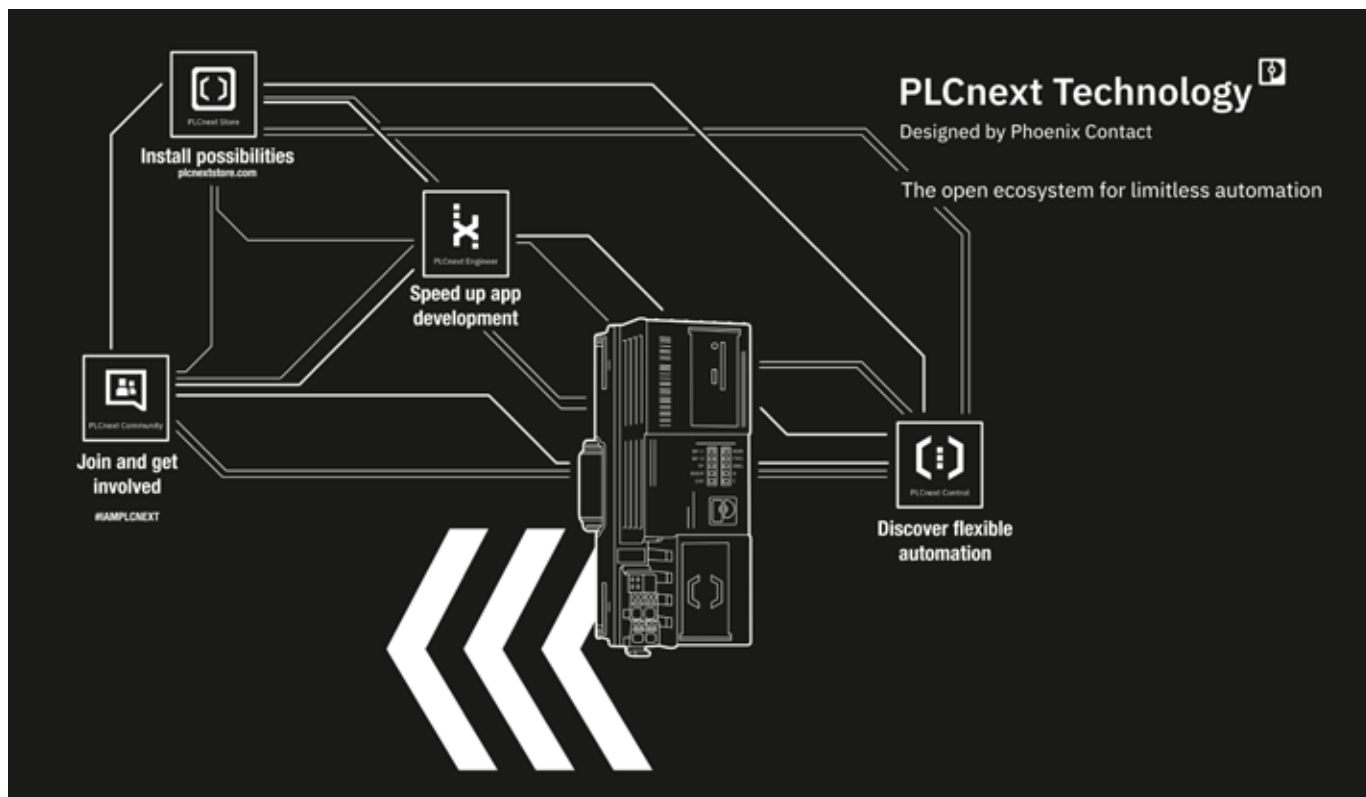
grant, monitor, and revoke remote access as needed—without requiring specialized IT expertise.

“This approach not only simplifies remote support and maintenance but also helps maintain high levels of uptime and operational continuity in critical industrial environments,” Kasman added. “SEA provides a single portal to manage access policies for all sites, making it simple to scale and empowering OT teams to independently manage users and assets, all while ensuring compliance with policies and controls defined by IT. By solving these engineering challenges, Cisco Secure Equipment Access empowers organizations to achieve secure, productive, and scalable remote connectivity while proactively mitigating risks in today's evolving threat environment.”

PLCnext technology

Robust remote connectivity options such as Proficloud.io is cloud agnostic using integrated MQTT and other communication technologies.

The PLCnext Technology Ecosystem from Phoenix Contact offers a comprehensive solution for industrial IoT applications. It combines robust remote connectivity options such as Proficloud.io, is cloud agnostic through integrated MQTT and other communication technologies and can be extended via the PLCnext Store with various remote connectivity options that provide secure VPN access to PLCnext controllers. These tools support remote diagnostics, programming and



"Key trends driving industrial remote connectivity include the convergence of IT and OT, edge computing and the adoption of cloud-native technologies. Innovations such as containerization, 5G and AI-driven analytics are changing the way remote systems are managed," -- Daniel Korte, Technology management PLCnext Technology, Phoenix Contact Electronics GmbH.

manufacturing, energy, water/wastewater and transportation. Applications include remote monitoring of decentralized systems, predictive maintenance and centralized control of decentralized systems.

In the renewable energy sector, for example, operators use PLCnext Technology to monitor wind turbines and solar farms from central locations. In water management, remote access enables real-time control of pumping stations and wastewater treatment plants. OEMs benefit by offering remote diagnostics and updates for their machines, reducing service costs and increasing customer satisfaction. These solutions are particularly valuable in geographically dispersed or hazardous environments where on-site access is limited or costly.

"Modern solutions for remote connectivity face several technical challenges: secure data transmission, interoperability, scalability and real-time responsiveness. Traditional systems often lacked flexibility and required proprietary tools. PLCnext Technology overcomes this problem by supporting open standards and IT protocols that enable seamless integration into existing infrastructure," Korte said.

He added that cybersecurity is a major concern, and the Phoenix Contact platform includes a secure launch, encrypted communications and user authentication to protect against threats. Another challenge is managing large amounts of data at the edge -

PLCnext Technology enables local processing to reduce latency and bandwidth usage. Finally, remote updates and diagnostics reduce downtime and maintenance costs, addressing the need for efficient lifecycle management in industrial environments.

Encrypted tunnels

Utilizing dual Ethernet network interfaces, zero-trust user authentication, OpenVPN client and granular firewall control.

"Opto 22's groov devices—groov EPIC and groov RIO—are designed from the ground up for secure, reliable remote connectivity. With dual Ethernet network interfaces, zero-trust user authentication, a built-in OpenVPN client, and granular firewall control, they let engineers connect to remote systems over encrypted tunnels without exposing the control network to the public internet," Dan White, Director of Technical Marketing at Opto 22 told IEB.

White said that, with tight, built-in firewall controls, users choose which services are exposed. In many cases they don't need to open any ports at all, because groov devices can publish data outbound using MQTT with Sparkplug. This publish/subscribe model avoids polling and sends updates only when something changes. With TLS encryption and client-authenticated certificates, it's a secure,

efficient way to move data across networks without exposing the system.

For diagnostics and visualization, there are options. Browser-based HMI software groov View is built in for control, trending, and status screens, and is accessible from any device with proper credentials. If user standardize on Inductive Automation's Ignition, groov devices also support Ignition Edge to provide tag access, alarming, and mobile-friendly visualization.

"And because groov devices combine control, I/O, networking, and data services in one platform, there's no need for separate gateways or PCs to enable remote support. It's all built-in. This setup reduces complexity, improves security, and gives engineers practical tools to monitor and support systems from wherever they are," White said.

Technology trends

White said that one of the biggest shifts is the adoption of MQTT Sparkplug B. It's changed how industrial systems move data by replacing the traditional poll-response model with a publish-subscribe approach that's faster, more efficient, and firewall-friendly. Devices push updates only when something changes, reducing bandwidth and simplifying connectivity across networks.

"Security is no longer something you have to add—it's baked in. Modern systems include built-in VPN clients, use TLS encryption



SOURCE: ISTOCKPHOTO

"One of the biggest shifts is the adoption of MQTT Sparkplug B. It's changed how industrial systems move data by replacing the traditional poll-response model with a publish-subscribe approach that's faster, more efficient, and firewall-friendly. Devices push updates only when something changes, reducing bandwidth and simplifying connectivity across networks," -- Dan White, Director of Technical Marketing, Opto 22.

by default, and support certificate-based authentication. Many are designed with outbound-only communication in mind, so there's no need to open inbound ports. That aligns well with IT security policies and makes deployment much easier in remote or cloud-connected applications," White said.

He added that cloud integration is another major trend. Edge devices can now publish data safely and securely to cloud platforms for monitoring, analytics, and long-term storage—without middleware or external gateways.

"Scalability is a major differentiator. Remote connectivity today isn't limited to large, centralized systems. It can start with a single device in the field and scale to hundreds across multiple sites, all managed with consistent tools, protocols, and security policies," White added.

Traditional industrial systems have been isolated or hard to integrate. Now, edge devices are designed to speak both OT and IT languages: Modbus/TCP, serial RS232/485, OPC UA, analog, and digital I/O on one side; MQTT Sparkplug B, REST API, and SSL/TLS security on the other. That makes it easier to move data securely among machines, cloud platforms, and enterprise systems.

These platforms are also self-contained.

Instead of piecing together PLCs, gateways, and third-party VPN appliances, everything you need for control, visualization, remote access, and data communication is in one small box.

Applications solutions

"Remote connectivity is a natural fit for industries with widely distributed assets or critical infrastructure," White said.

In water, wastewater, and utility systems, remote access reduces the need for site visits and allows operators to monitor tanks, pumps, and generators across large service areas. It's essential for catching issues early and reducing response time.

Oil and gas, along with broader energy markets, rely on remote systems to manage wellheads, substations, and other unmanned locations. With secure access to live data, teams can make informed decisions without having to be on-site, or to wait for someone who is.

Machine builders and OEMs benefit from staying connected to the systems they ship. Remote diagnostics help them support customers in the field, track equipment usage, and even push updates after deployment. It's a huge win for uptime and customer satisfaction.

Building automation and smart facility

applications also depend on remote connectivity—especially when managing HVAC, lighting, and power systems across multiple buildings, campuses, or regions.

Engineering challenges

White added that security has always been one of the biggest barriers to remote access. Older systems often required opening inbound ports or punching through firewalls—something most IT teams rightly pushed back on. Modern solutions are designed with outbound-only communication, TLS encryption, and certificate-based authentication, making secure access possible without compromising the network.

Complexity in older setups was another challenge. Engineers used to need a mix of PLCs, modems, remote desktop software, and custom scripts just to access a remote site. New platforms integrate all of that—control, networking, remote access, and visualization—in one box.

Data loss was also common in remote systems. If the network went down, data just disappeared. Today's solutions buffer and store data locally, then publish it when the connection is restored. You keep a complete record, even across outages.

Finally, updates used to be painful. Making



"As industries become increasingly digitized, three trends are shaping the transformation of remote connectivity: stronger cybersecurity requirements, hybrid infrastructure integration (legacy and Ethernet-based devices), and the need for scalable, resilient remote access," -- Philipp Jauch, Integrated Marketing Manager, Moxa Europe GmbH.

changes to logic, firmware, or configuration meant being on-site or walking someone else through it. Now, secure remote updates are built-in, so engineers can support systems across sites or time zones without leaving their desks.

Remote Connect

Securely bridge field devices, service engineers and application servers over the internet.

According to Philipp Jauch, Integrated Marketing Manager, Moxa Europe GmbH, Moxa's Remote Connectivity solution is designed to securely bridge field devices, service engineers, and application servers over the internet. At the heart of this solution is Moxa Remote Connect (MRC), a platform that

offers an easy-to-deploy, cybersecure approach to industrial remote access.

The solution combines three key components: the MRC Server, MRC Gateway, and MRC Client. The MRC Server acts as a centralized connection management platform that defines relationships between gateways and clients. The MRC Gateway connects Ethernet-ready devices at remote sites to the internet securely, while the MRC Client, installed on an engineer's laptop, provides intuitive access to remote devices.

Administrators can define access schedules and set permissions through the MRC Server, offering full control over when and how devices are accessed remotely. To further simplify deployment, MRC Quick Link, a Moxa-hosted remote connection service, minimizes maintenance overhead by handling the setup

and connection process for users.

Latest remote connectivity solutions

"As industries become increasingly digitized, three trends are shaping the transformation of remote connectivity: stronger cybersecurity requirements, hybrid infrastructure integration (legacy and Ethernet-based devices), and the need for scalable, resilient remote access," Jauch said. "With cybersecurity taking center stage, regulatory initiatives such as the EU Cyber Resilience Act (CRA) are setting the bar for mandatory product-level security. In parallel, technical standards like IEC 62443 provide a structured framework for securing industrial systems, from development to deployment. Together, these pressures are prompting manufacturers and operators to reassess how they manage secure remote



Moxa Remote Connect (MRC) provides a secure, cloud-based platform for remote access.



"The increasing demand for IoT and IIoT devices necessitates robust connectivity solutions for seamless integration. The latest AI and machine learning technologies enable predictive maintenance and process optimization, while software-defined networking (SDN) allows flexible, centralized network management, enhancing scalability and adaptability in industrial environments," -- Lars Walpurgis, Product Owner - Sinema Remote Connect, Siemens.

access to field equipment. Meanwhile, digital transformation initiatives are expanding the number and diversity of connected devices, requiring both compatibility and manageability."

In this context, Jauch said that industrial connectivity solutions must deliver secure-by-design architectures, support for both brownfield and greenfield deployments, and fail-safe network performance in increasingly remote and unmanned environments.

Moxa's OnCell G4300 Series cellular routers were developed with these exact challenges in mind. Built in compliance with IEC 62443-4-2 and developed under IEC 62443-4-1 secure development practices, the series offers future-ready security alongside flexible networking options. The routers also support legacy serial devices and modern Ethernet-based systems, enabling a smoother transition for operators modernizing their infrastructure.

Cellular routers

Moxa's OnCell G4300 Series cellular routers combine advanced cybersecurity, reliable connectivity, and broad interoperability, making them uniquely suited for industrial remote access.

Security features include Secure Boot, which ensures only authenticated firmware and software are executed during startup, and Deep Packet Inspection (DPI), which inspects

OT protocol traffic to control exactly which devices are allowed to read or write data. An integrated firewall provides granular control over services and ports, reducing the attack surface of connected systems.

To support both modern and legacy infrastructure, the routers include built-in RS-232/422/485 ports, enabling secure connectivity to older serial devices without additional hardware. For Ethernet-based setups, a model with an integrated 8-port Ethernet switch simplifies network deployment at remote sites.

Connectivity stability is enhanced through GuaranLink, which continuously monitors link status and triggers automatic failover or reconnection mechanisms when needed. The feature is highly configurable, allowing adaptation to diverse use cases and environments.

Finally, with global LTE band support, a single device model can be used across multiple regions, streamlining logistics, reducing the bill of materials, and simplifying international deployments.

Applications and industries

"Industrial remote connectivity solutions are essential across various sectors—unified by the need to connect and manage equipment in the field. These applications often involve machines with long life cycles (~15 years),

deployed in remote areas, where sending service engineers on-site is costly and time-consuming," Jauch said.

Jauch said that factory automation is a prime use case, where machine builders often provide service contracts that require fast response times in the event of downtime. However, restrictive IT policies at manufacturing sites can complicate remote access. By using Moxa's remote connectivity solution, machine builders retain secure, direct access to their machines without depending on third-party IT configurations.

In oil and gas, the need for explosion-proof and certified equipment is critical. The OnCell G4300 Series meets international standards including IECEx, ATEX, and CID2, enabling secure remote monitoring of pipelines and other critical assets.

The rise of electric vehicle (EV) infrastructure also demands scalable and robust connectivity solutions. Harsh outdoor environments, a high volume of deployed charging stations, and the risk of communication loss all necessitate a solution that can maintain reliable and secure connections over long distances.

Engineering challenges

"Managing a growing number of remote connections across globally deployed machines and applications poses significant challenges. Engineers need secure, scalable, and easy-to-

deploy connectivity—especially as regulatory expectations increase,” Jauch said.

New regulations such as the EU Radio Equipment Directive Delegated Act (RED-DA) aim to improve cybersecurity for wireless and internet-connected products. While not yet in force, it is already shaping design priorities by encouraging manufacturers to implement more secure communication practices from the start.

In parallel, initiatives like the Cyber Resilience Act (CRA) and standards such as IEC 62443 highlight the importance of secure development lifecycles and device-level protections.

Moxa addresses these needs by offering industrial connectivity products that are easy to deploy and comply with modern security expectations. Our solutions can also be integrated with MXview One, Moxa’s network management software, which simplifies device monitoring, visualises bandwidth usage, alerts engineers to unusual activity or rogue devices, and accelerates documentation processes.

Sinema remote connect

Server application facilitates simple, secure remote access to widely distributed machinery and plants, such as remote maintenance.

Siemens offers the SCALANCE M series of industrial routers, which provide secure remote access to machines and plants. This solution supports VPNs, 5G, firewall functionalities, and various mobile and broadband connections, ensuring reliable and secure communication. Key benefits include reduced downtime, efficient maintenance, and enhanced data security.

According to Lars Walpurgis, Product Owner Sinema Remote Connect at Siemens, SINEMA Remote Connect, the Siemens management platform for remote networks, is a server application which facilitates simple, secure remote access to widely distributed machinery and plants, such as remote maintenance. SINEMA Remote Connect ensures the secure administration of VPN tunnel connections between the control centers, the service engineers, and the installed systems. Secure remote maintenance can then be carried out via the TIA Portal, for example.

“This avoids direct access to the corporate network in which the machine to be maintained is integrated,” Walpurgis said. “The stations that are to communicate with one another ‘meet’ at a neutral location, the SINEMA Remote Connect Server, also known as a rendezvous server. This then verifies the identity of the individual stations by an exchange of certificates before access to the machine via the corporate network or cellular network, and the dedicated SCALANCE industrial router becomes possible.”



SINEMA Remote Connect enables remote access for teleservice and remote maintenance conveniently and securely, even if they're integrated into other networks.

Trends and innovations

“The latest solutions for industrial remote connectivity are driven by several key technology trends. For instance, 5G integration offers high bandwidth and low latency for real-time data transfer,” Walpurgis added. “Edge computing brings processing power closer to data sources, reducing latency and improving efficiency. Also, advanced cybersecurity measures ensure data integrity and secure remote operations. A key for that is a unified Identity and Access Management (IAM) to securely authenticate and maintain users and machines.”

Walpurgis added that the increasing demand for IoT and IIoT devices necessitates robust connectivity solutions for seamless integration. The latest AI and machine learning technologies enable predictive maintenance and process optimization, while software-defined networking (SDN) allows flexible, centralized network management, enhancing scalability and adaptability in industrial environments.

“Industrial remote connectivity technology is unique due to its comprehensive security measures, such as advanced encryption and multi-layer firewall protection, which ensure data integrity and secure remote operations,” Walpurgis said. “Its high reliability and seamless integration with various existing systems and network protocols make it adaptable and versatile for different industrial needs. In that sense, SINEMA Remote Connect is an easy-to-use tool for Operational

Technology (OT) on the shop floor.”

He said that remote connectivity solutions are predominantly focused on industries like manufacturing, process industries, energy, and public infrastructure. These solutions are critical for applications such as remote monitoring, which allows for the observation of industrial processes from a distance; predictive maintenance, which uses data analytics to predict equipment failures and schedule timely maintenance; decentralized control systems, which distribute control functions across various devices for increased reliability and efficiency; and real-time data processing, which enables immediate analysis and response to data collected from industrial operations.

“Automation engineers face several challenges, including ensuring secure remote access to sensitive industrial systems, managing the complexity of network configurations, and minimizing system downtime,” Walpurgis said. “Particularly for OT remote connectivity Layer-2 access is a challenge. Modern remote connectivity solutions address these challenges by providing secure and encrypted communication channels that protect against unauthorized access and cyber threats. They also offer user-friendly configuration tools that simplify network management and setup. Upcoming European security regulations like Cyber Resilience Act (CRA) and NIS-2 are additional challenges.”

Al Presher, Editor, *Industrial Ethernet Book*

Do you actually know... EtherCAT? Part 3

EtherCAT is recognized as an international standard and is standardized in IEC 61158 and IEC 61784. The first two parts of this series dealt with the technical features of EtherCAT. This third part deals with the structure and work of the EtherCAT Technology Group (ETG) and the services it provides to its members.



SOURCE: ETHERCAT TECHNOLOGY GROUP

Figure 1: The international team of the EtherCAT Technology Group supports ETG members all over the world.

ETHERCAT HAS ESTABLISHED ITSELF AS A powerful real-time Ethernet fieldbus system in industrial communication. The first two parts of this series dealt with the technical features of EtherCAT. This third part deals with the structure and work of the EtherCAT Technology Group (ETG) and the services it provides to its members.

The EtherCAT Technology Group is the user organization that deals with the development and distribution of EtherCAT. It was founded in 2003 and is now the largest fieldbus user organization in the world with over 8000 members from 76 countries. ETG members include suppliers and users of EtherCAT devices, users of EtherCAT technology as well as research institutes and universities.

The ETG forms the ecosystem around EtherCAT technology. To this end, it works on the further development of the technology, promotes the interoperability of EtherCAT devices from different manufacturers and actively supports companies in their implementation.

Technological development and standardization

The technical development of EtherCAT takes place in working groups, the so-called Technical Working Groups (TWGs). These groups are made up of experts from the member companies and deal with various aspects of the technology, such as specification extensions, development of device profiles or the definition of standardized implementation guidelines.

A central principle is the downward compatibility of the EtherCAT specification. There is a single technology version that is supplemented by extensions instead of new, modified versions being published regularly. This ensures that devices in old systems can be replaced by current devices without having to pay attention to version differences and keep track of historical firmware and hardware versions. Long-term stability and interoperability are among the advantages of EtherCAT.

EtherCAT is recognized as an international

standard and is standardized in IEC 61158 and IEC 61784. There are further standardizations for specific industries, for example in the semiconductor industry through SEMI (E54.20).

Interoperability and conformance assurance

To ensure that EtherCAT devices from different manufacturers can communicate with each other without any problems, the ETG requires the use of the official EtherCAT Conformance Test Tool (CTT). The CTT software tests the devices for compliance with the EtherCAT specification and also checks the EtherCAT SubDevice Information (ESI) file for valid values.

There are also device-specific protocol tests, for example for the CiA 402 drive profile. The test results are saved for analysis and documentation purposes. The CTT is continuously maintained and expanded with new test cases; its use is already helpful during the development phase in order to



Figure 2: The EtherCAT Plug Fests are a pragmatic approach to testing the interoperability of EtherCAT devices from different manufacturers under real conditions. (in the picture: EtherCAT Plug Fest at ETG member Panasonic)

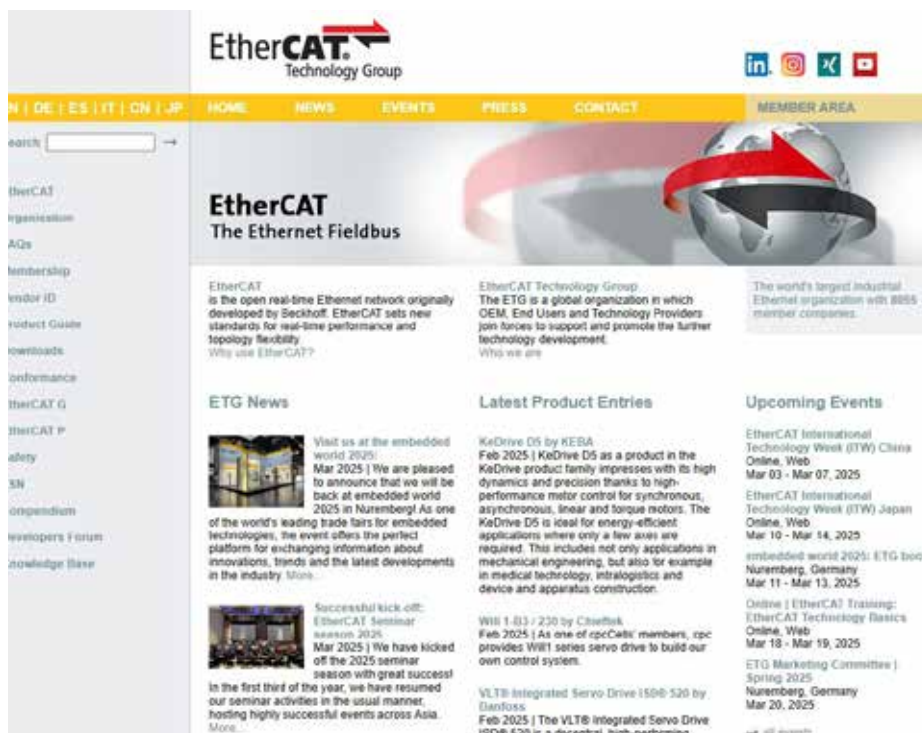


Figure 3: The EtherCAT Technology Group website gives members access to a wide range of EtherCAT-related offers and services.

detect errors in the interface implementation at an early stage. The test procedure and test content are defined and further developed by a corresponding working group within the ETG, the Technical Working Group Conformance.

In addition to the mandatory in-house tests with the EtherCAT Conformance Test Tool, manufacturers can have their devices tested in

EtherCAT Test Centers (ETC) accredited by the ETG. Comprehensive tests are carried out there that go beyond the automatic protocol test. A successful test in an ETC is confirmed with an EtherCAT Conformance Tested certificate. For safety-critical applications, there are special tests for Safety over EtherCAT (FSoE), which are carried out by independent testing

organizations such as TÜV.

In addition, the ETG offers further measures for conformity testing. These include the EtherCAT Plug Fests, regular developer meetings at which manufacturers can test their EtherCAT devices in a shared test environment. Possible interoperability problems are identified and resolved at an early stage. These events take place several times a year in Europe, Asia and North America.

Support for members

In addition to the above-mentioned offers and tools, the EtherCAT Technology Group provides its members with various other services, including technical documentation and specifications in several languages, software stacks and development tools, training courses and workshops as well as support for the implementation of EtherCAT from the five regional ETG offices in Europe, Asia and America.

In addition, the ETG organizes numerous events such as trade fairs, seminars and webinars every year to disseminate information about EtherCAT.

Through its comprehensive support services, strict conformity tests and continuous further development, the EtherCAT Technology Group contributes significantly to the worldwide dissemination and future-proofing of EtherCAT.

Christiane Hammel, *EtherCAT Technology Group.*

[Learn More](#)

Virtualization: the next step in substation evolution

Advanced software platforms can support the development of virtualized operations. With comprehensive support for IEC 61850 and advanced features including seamless redundancy, automated engineering and role-based access control, software solutions are simplifying the transition to software-defined substations.



Virtualization decouples software applications from the underlying hardware using virtual machines (VMs) managed by a hypervisor. A single server can host multiple VMs, each dedicated to specific functions. This approach not only reduces the physical hardware footprint but also simplifies maintenance and upgrades, making substations more agile and resilient.

THE ENERGY INDUSTRY IS RAPIDLY evolving to meet the demands of a digital, decentralized, and decarbonized future. Among these advancements, virtualization in substations can transform traditional systems into dynamic, flexible, and software-defined environments. Here, Jurgen Resch, Industry Manager for Energy at automation supplier COPA-DATA, explores the concept of virtual substations, the benefits and challenges of virtualization in PAC, and how software supports transformation.

A virtual substation represents the next evolution of digital substations, where all Protection, Automation, and Control (PAC) functions are executed in a software

environment. Traditional Intelligent Electronic Devices (IEDs) are replaced by virtualized counterparts running on central servers. Key functions, including cybersecurity, switches, and firewalls, are centralized and managed dynamically through software platforms. Virtual substations enable utilities to consolidate hardware, enhance operational flexibility, and reduce costs.

Virtualization decouples software applications from the underlying hardware using virtual machines (VMs) managed by a hypervisor. A single server can host multiple VMs, each dedicated to specific functions. This approach not only reduces

the physical hardware footprint but also simplifies maintenance and upgrades, making substations more agile and resilient.

Drivers for virtualization

The push toward virtualization is driven by several factors. Complexity is increasing with the integration of Distributed Energy Resources (DERs) like solar and wind into traditional grids. These resources are intermittent and place additional pressure onto grids, and as such demand advanced control and protection solutions, and virtual substations offer the flexibility and scalability to adapt to these evolving needs.

What's more, virtualization brings



The zenon Energy Edition from COPA-DATA is a complement for any PAC (protection, automation and control) installation. This substation automation system is suited for various tasks in the substation domain, such as: Digital Substation for local as well as remote operation; Control Room (SCADA) applications, for advanced supervision of cross-regional substation infrastructure or in conjunction with 3rd party systems; and Protocol Gateway, to flexibly interface with higher-level control systems.

cost efficiency by reducing expenditure through hardware consolidation and lowering operational costs by streamlining maintenance processes. Meeting sustainability goals is another driver, as smarter energy management and reduced reliance on resource-intensive physical infrastructure contribute to these objectives. Standards like IEC 61850 also provide the interoperability and integration required for virtualized PAC systems, further encouraging the shift to virtualization.

Virtualized PAC systems offer significant benefits. By replacing multiple IEDs with software-defined solutions, utilities can reduce their dependence on vendor-specific hardware. As already stated these systems are also highly scalable and flexible, enabling easy adaptation to changing grid requirements.

Enhanced resilience is another advantage, as virtualized environments support failover mechanisms and improve overall system reliability. Centralized data collection within virtual substations facilitates better decision-making across areas like power quality management, fault detection, and energy optimization.

Challenges in virtualization

While virtualization offers numerous advantages, it also introduces distinct challenges, particularly concerning availability and reliability. In a physical substation with IEDs, the failure of a

single device typically affects only a small portion of the system, as each IED operates independently. By contrast, a virtual substation relies on a smaller number of redundant hardware components – often just two servers – making it appear less robust from a purely hardware-centric perspective.

However, the functional components of a virtual Substation can be distributed into virtual machines (VMs) and containers, with each representing the functionality of a physical IED. This approach allows it to achieve a level of availability and reliability comparable to a physical Substation when designed with appropriate redundancy and fault-tolerance mechanisms. Transitioning to this model requires a shift in mindset – from thinking in terms of hardware components to focusing on virtualized resources like VMs and containers.

The IEC 61850 standard is key in the virtualization of PAC systems. By defining protocols for communication and data exchange, IEC 61850 ensures interoperability between devices and systems from different vendors. Its support for sampled values (SV) and Generic Object-Oriented Substation Event (GOOSE) messaging is particularly significant in enabling real-time data communication in virtual substations.

The future of substation automation

Advanced software platforms can support the development of virtualized operations, and COPA-DATA's zenon Energy Edition is

an effective automation tool for substation virtualization. With comprehensive support for IEC 61850 and advanced features including seamless redundancy, automated engineering, and role-based access control, zenon simplifies the transition to software-defined substations. zenon's vendor-agnostic architecture supports diverse protocols and hardware, allowing flexible integration across a wide range of systems.

Preconfigured templates and object-oriented design streamline project complexity and reduce errors, while real-time visualization and control enhance situational awareness. Additionally, zenon facilitates the deployment of PAC functions in virtual environments, ensuring reliable and secure operation.

As utilities prepare for the large-scale deployment of virtual substations over the next decade, the focus will be on validating technology, ensuring compliance, and adapting operational practices. Virtualization represents a transformative opportunity to modernize substations, meet sustainability goals, and build a resilient, future-ready grid. COPA-DATA's zenon can support the energy industry in this process, bridging the gap between traditional systems and the next generation of software-defined substations.

Article by **COPA-DATA**.

[Visit Website](#)

Navigating the complexities of Wi-Fi installations

Wireless applications come with unique challenges. Knowing what to look for during the design phase can help avoid issues during the installation and operation of connected devices. By carefully planning and understanding potential obstacles, installers can avoid common pitfalls.



SOURCE: ANTAIRA

While wireless solutions can be convenient, even the simplest application of a wireless networking standard can come with challenges that need careful planning and troubleshooting.

WIRELESS INSTALLATIONS ARE OFTEN SEEN AS an easy replacement for cables, particularly in situations where running wires or fiber optics is impractical or too costly. While wireless solutions can be convenient, even the simplest application of a wireless networking standard can come with challenges that need careful planning and troubleshooting. Below are some ways to help navigate the installation of a wireless network.

Site survey and spectrum analysis

Before beginning any wireless installation, conducting a thorough site survey and spectrum analysis is essential. A site survey allows installers to measure actual signal strength, identify dead spots, and detect sources of interference throughout the area. Spectrum analysis can reveal existing wireless networks and other sources of radio frequency (RF) noise that may compete for bandwidth. By understanding these environmental factors, installers can plan more effectively, especially in congested areas where multiple networks may already be operating. This preemptive approach helps prevent performance issues and ensures a more reliable setup from the start.



Site survey measures actual signal strength, identifies dead spots, and detects sources of interference throughout the area.

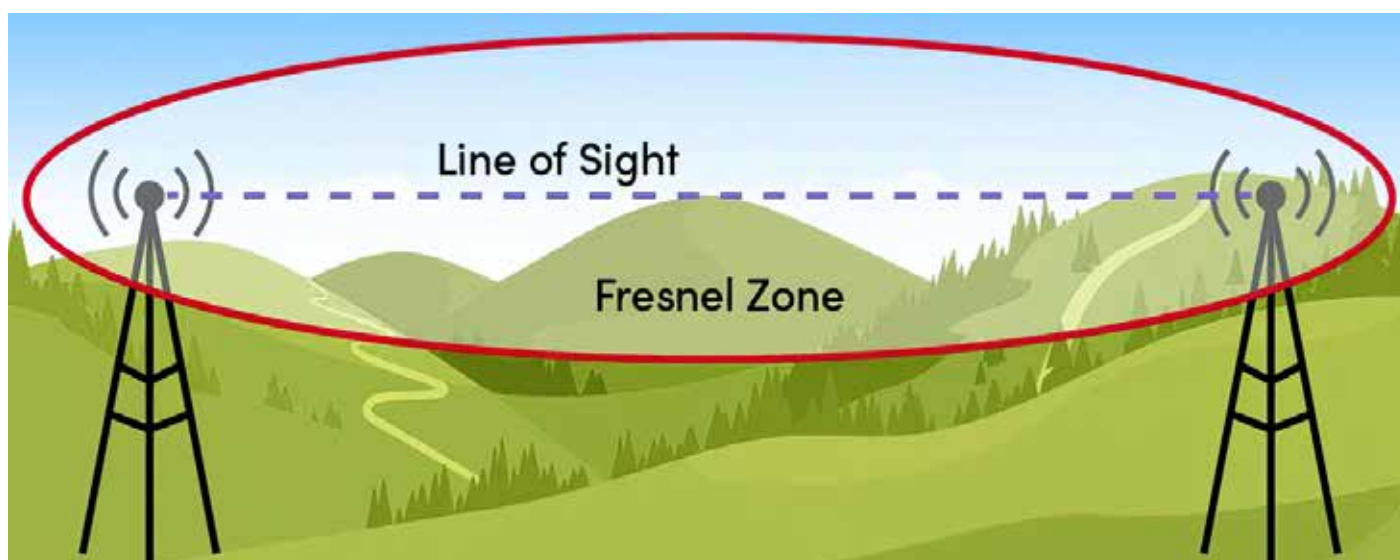
Overcoming environmental challenges

Wireless networks are particularly appealing in industrial settings, where it's challenging to run cables, whether twisted pair or fiber

optic, through complex environments. Take a machine shop as an example, where a wireless network was used to install a surveillance system. Over the weekend, the wireless network itself was installed and tested, and everything seemed to be working perfectly. But on Monday morning, when the shop workers arrived and began operating machinery, the whole wireless access network stopped working. What happened?

Before jumping to solutions, it's essential to consider potential troubleshooting methods. For instance, checking for interference sources like high-power motors, testing network stability at different times, and measuring wireless signal strength around machinery could help identify the problem. In this case, it's likely that many of the machines in the shop use high-power electrical motors, which often emit electromagnetic interference (EMI) or RF noise. This RF noise can disrupt Wi-Fi signals by creating interference within the wireless frequency range, especially if the equipment is unshielded.

To address this, you could use directional antennas to focus the signal and power through the interference. Alternatively, try guiding the signal around problematic areas



Without physical barriers blocking the direct path between WiFi antennas, the network can maximize signal strength, reduce latency, and improve data transfer rates.

with known sources of RF noise. In some cases, shielding certain motors or repositioning equipment may also be options.

Line of Sight and the Fresnel Zone

"Line of sight" is a common term used when deciding if a wireless connection is feasible. However, it's one of the most misunderstood terms in wireless installations. A clear visual path between two points doesn't necessarily guarantee a stable wireless connection. For example, if you're setting up a wireless access point or a wireless bridge to connect wireless devices between two buildings and can see the far building from the near one, you might assume line of sight is established, and the wireless access point connection can be made. However, this may not always be the case.

This is where the Fresnel zone concept becomes important. The Fresnel zone is a football-shaped area between two antennas, and any obstruction within this zone can cause interference. The frequency in use (2.4 GHz, 5 GHz, 6 GHz, 60 GHz) affects the size and shape of the Fresnel zone, but the concept remains the same: the clearer this zone is, the less signal interference and stronger the signal. This is one reason why placing antennas higher up can improve signal quality—the lower half of the Fresnel zone avoids being obstructed by the ground.

It's also important to remember that line-of-sight conditions can change over time. For instance, trees may lose their leaves in fall but fill out in summer, potentially blocking signals. New structures or other objects might be placed in the path that was once clear. Asking about future plans and assessing the likelihood of seasonal changes can prevent unexpected disruptions.

Echoes and reflections

In industrial environments, certain building materials can interfere with wireless signals.

For instance, many industrial buildings use corrugated steel siding for cost efficiency and durability. Unfortunately for wireless security, this material can cause a reflective, echoing effect, which confuses the wireless receivers.

This problem often occurs when an antenna, especially an omnidirectional one, is mounted flat against corrugated steel. The effect is somewhat more obvious with omnidirectional antennas, but even directional antennas like panel antennas can experience similar issues. Panel antennas have multiple radiation patterns called "lobes". The main lobe points in the direction of the desired connection. However, side lobes can bounce back when mounted against steel, creating interference. Mounting the antenna a few feet away from the wall can often mitigate this issue.

Metal walls aren't always as obvious as corrugated steel; sometimes, metal mesh inside walls or even certain types of insulation can cause issues. Asking about wall materials can provide helpful insight before installation begins.

Latency requirements

When implementing wireless networks for latency-sensitive applications—such as real-time monitoring or automated machinery—it's crucial to consider potential challenges. Wireless signals can experience latency and jitter due to interference, signal reflection, and congestion, impacting performance.

Advancements in Wi-Fi technology, particularly Wi-Fi 6 and Wi-Fi 7, have introduced features designed to address these issues. Wi-Fi 6 incorporates Orthogonal Frequency-Division Multiple Access (OFDMA) and Target Wake Time (TWT), which enhance network efficiency and reduce latency by allowing more devices to communicate simultaneously and scheduling transmissions

to minimize contention. Wired connections are generally preferred for applications requiring the highest reliability and lowest latency. If a wireless setup is essential, it should be carefully evaluated to ensure it meets the performance requirements of these demanding applications.

Planning for coexisting networks

Before installing a new wireless network or connecting devices, assess the environment thoroughly to understand existing wireless setups and potential sources of interference. This is especially important when using the 2.4 GHz band, as only three non-overlapping channels are available. While adding a new 2.4 GHz link might still be possible, switching to a 5 GHz or 60 GHz frequency is often advisable if other devices' open networks or data traffic may already occupy this band.

Another important consideration is the presence of other wireless signals that may overlap or jam the frequencies of mobile devices you plan on using. High-density areas are more prone to frequency congestion, while remote areas are typically less impacted by interference.

Avoiding common pitfalls

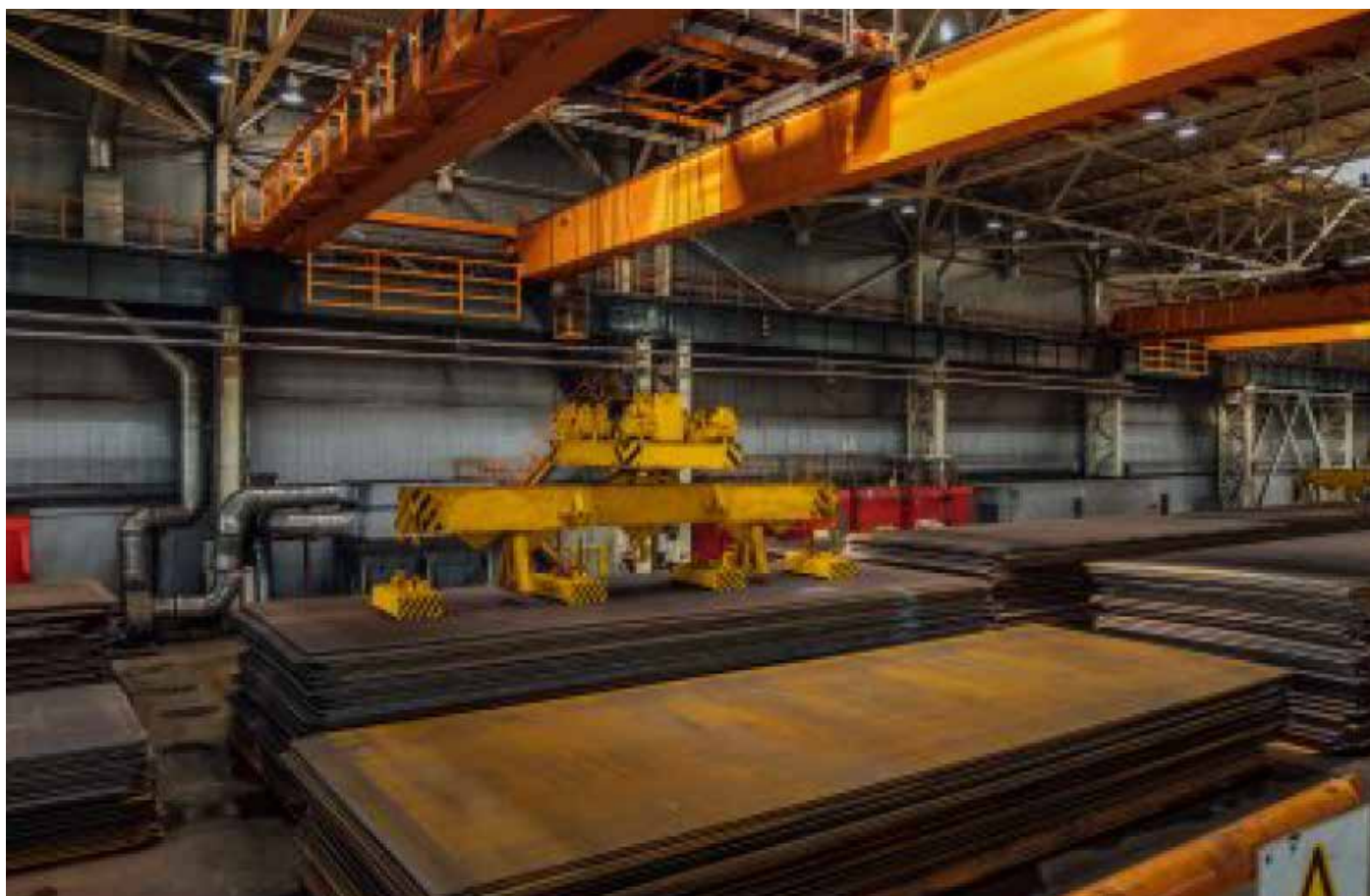
Wireless applications, though often perceived as straightforward, come with unique challenges. Knowing what to look for during the design phase can help avoid issues during the installation and operation of connected devices. By carefully planning and understanding potential obstacles, installers can avoid common pitfalls, ensuring a more prosperous and reliable Wi-Fi security setup.

Henry Martel, Field Application Engineer, Antara Technologies.

[Visit Website](#)

Overhead crane performance with advanced AC motor drives

In the overhead crane market, precision and reliability are critical due to the demanding nature of heavy-duty applications. The collaboration between Delta and Elektro-Mak has set a new benchmark, demonstrating the immense potential of integrating advanced motor control systems in industrial applications.



SOURCE: DELTA

The future of manufacturing is connected, intelligent, and remarkably efficient. Embracing IIoT is not just a technological advancement; it's a strategic imperative for achieving long-term competitiveness and success.

OVERHEAD CRANES REQUIRE ADVANCED motor control systems to ensure smooth, efficient, and safe operations, particularly in lifting and transporting heavy loads. The complexity of these operations demands high-performance drives that can manage constant torque, minimize load oscillations, and provide reliable braking sequences.

Addressing these unique requirements, Delta's innovative AC motor drive solutions have been successfully adapted to enhance the performance and reliability of overhead crane solutions provided by Elektro-Mak Crane Systems Ltd., a leading manufacturer of overhead cranes in Turkey. This collaboration has showcased Delta's strong market position and demonstrated its commitment to enhancing operational

efficiency in the crane industry.

Established in 1989 in Izmir, Turkey, Elektro-Mak Crane Systems Ltd. is renowned for its expertise in producing overhead cranes with capacities ranging from 250 kg to 200 tons and bridge openings below 45 meters. Operating from a state-of-the-art plant in Manisa covering 6,000 m², Elektro-Mak is a prominent player in the Turkish crane market. The company's dedication to quality and innovation has positioned it as a trusted partner for heavy-duty crane solutions.

Overcoming challenges and achieving seamless integration

The collaboration between Delta and Elektro-Mak began with the goal of enhancing the performance of overhead

cranes using Delta's advanced AC motor drives. Elektro-Mak adopted Delta's C2000+ AC Motor Drives for hoisting, ME300 AC Motor Drives for long travel, and trolley operations. These drives were selected for their high-level motor control performance, competitive pricing, and robust technical support.

Delta's AC motor drives were integrated into Elektro-Mak's overhead cranes, addressing the company's need for a cost-competitive solution with an anti-sway function using open-loop control. The entire testing and commissioning process, completed in just two days, required extensive support from Delta's R&D and product management teams, particularly for parameter adjustments and overcoming tough environmental conditions.

The integration process faced challenges, particularly with the anti-sway function without an encoder. However, through persistent testing and parameterization on-site, Delta's team successfully implemented a solution that met Elektro-Mak's stringent requirements.

Remarkable results and enhanced production efficiency

The results of this collaboration were outstanding. Elektro-Mak experienced a significant improvement in crane performance, with the anti-sway function and reliable braking sequence enhancing safety and operational efficiency. The ease of integration and robust performance of Delta's AC motor drives allowed Elektro-Mak to meet its production goals effectively in less time.

This project is a testament to Delta's commitment to providing innovative, cost-effective automation solutions tailored to meet specific customer needs. The success story of Elektro-Mak underscores the importance of close collaboration and a thorough understanding of customer requirements.

In the words of Martien Heesterbeek, Product Manager at Industrial Automation Business Group, Delta EMEA, "This project with Elektro-Mak not only showcases our capabilities in delivering advanced automation solutions but also reinforces our commitment to customer satisfaction and innovation. We are proud to have supported Elektro-Mak in achieving

significant improvements in their production processes."

Sükrü Terzi, General Manager at Elektro-Mak shared his thoughts on the collaboration: "Partnering with Delta has been a transformative experience for us. The integration of their AC motor drives into our crane systems has not only boosted our production reliability and efficiency

but also underscored our commitment to adopting cutting-edge technologies. Delta's support throughout the project has been excellent, and we look forward to continuing this successful partnership."

Outlook and future plans

The collaboration between Delta and Elektro-Mak has set a new benchmark in the overhead crane industry, demonstrating the immense potential of integrating advanced motor control systems in industrial applications. As Delta continues to innovate and expand its product offerings, the company remains committed to providing reliable and efficient solutions, including both small and high-power AC drive that meet the evolving needs of the market.

Delta's dedication to problem-solving and customer support, combined with Elektro-Mak's operational excellence and strategic insights, has forged a formidable partnership. This collaboration stands as a beacon of success in the automation industry, providing a model for others seeking superior solutions in overhead crane manufacturing.

By leveraging Delta's cutting-edge automation solutions, Elektro-Mak has set a new benchmark in the overhead crane industry, demonstrating the immense potential of integrating advanced motor control systems in industrial applications.

Application case study by **Delta Electronics**.

[Learn More](#)



Integration of AC motor drives into crane systems has boosted production reliability and efficiency.



Delta AC motor drives integrated into the overhead cranes addressed the need for a cost-competitive solution by offering an anti-sway function using open-loop control.

Plug 'n' Play Network Extender

Solution enables Ethernet data transmission of distances up to 1 km network range via any 2-wire Single Pair Ethernet (SPE) technology solution.

Network specialist W&T is offering a new network Extender SPE that enables the transmission of Ethernet data over distances of up to 1 km and more, based on the new Single Pair Ethernet (SPE) technology.

The converter set can be used to connect any Ethernet devices over long distances. The connection can be implemented using any two-conductor cable, with maximum length depending on the cable used. SPE can bridge distances of up to 1000m, with two extender sets even further.

The Network Extender SPE is designed for industrial use and supports applications in areas such as building automation, manufacturing and traffic engineering. Thanks to the Power-over-Ethernet (PoE) supply, the device allows both data transmission and power supply via a single cable.

Commissioning is quick and easy via Plug & Play and without the need for IP configuration. The device features high immunity to interference and complies with the applicable standards for industrial use.

Article no. 55608 is now available to commercial customers for a net price of EUR



SOURCE: W&T

498.00 and can be tested free of charge for 30 days. More information at wut.de/55608 or +49 202-26 80 110.

Wiesemann & Theis GmbH was founded in 1979 by Reinhard Wiesemann and Rüdiger Theis. With 50 employees, the company produces microcomputer and network technology at its Wuppertal site. With the

Web-IO 4.0 product line, the Wuppertal-based network specialist has long since succeeded in bridging the gap between classic automation technology and Industry 4.0 / IoT.

W&T

[Learn More](#)

5G Slice for the water industry

Siemens and O2 Telefónica partner to develop solutions based on 5G network slicing.

The new connectivity solution "5G Slice for the Water Industry" allows water utilities to monitor and control their entire system of automation technology over a virtual 5G network using 5G network slicing technology. These networks are optimized to reliably deliver defined Quality of Service (QoS) for automation applications. This is critical for processes like pressure control, flow measurement, and automated emergency response at water utilities' mostly distributed sites.

5G network slicing is a technology that divides O2 Telefónica Germany's physical 5G mobile network into customized virtual networks called slices. These 5G slices are regionally limited and optimized for individual use cases in terms of their speed, response time, and security. The two partners worked together to develop and test a solution consisting of 5G routers from Siemens and 5G slices from O2 Telefónica to fulfill the high communication requirements of automation protocols. Thanks to the end-to-end separation of data traffic from the public Internet, the solution ensures a high level of cybersecurity



SOURCE: SIEMENS

and data protection for water companies which are subject to critical infrastructure regulations.

"By working with O2 Telefónica Germany, we can offer our customers in the water industry a secure and reliable communication solution for their distributed applications. The combination of Siemens hardware and

5G network slicing delivers the necessary quality, reliability and security for demanding automation applications," said Axel Lorenz, CEO Process Automation at Siemens.

Siemens

[Learn More](#)

Siemens Xcelerator

New Xcelerator portfolio from Siemens offers up to 20 percent in energy savings with Drivetrain Analyzer Cloud thanks to AI-based drive optimization.

- Siemens Xcelerator portfolio offers powerful drive optimization for industrial customers
- Drivetrain Analyzer Cloud: Continuous monitoring and AI algorithms generate specific efficiency measures
- Cloud-based approach enables optimization of energy efficiency of drives across multiple sites
- Siemens Industrial Copilot for operations: Drive train support for users

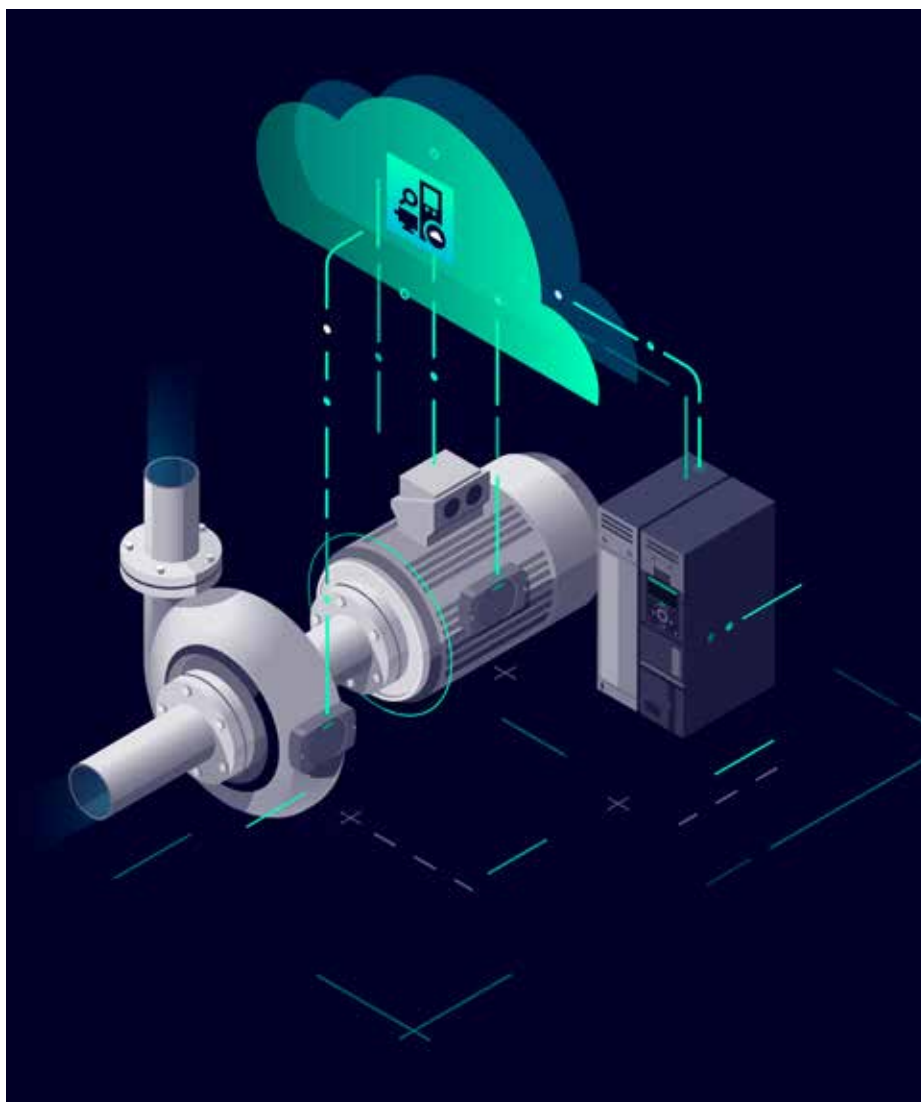
Industrial companies are under increasing pressure to improve their energy efficiency and reduce their carbon footprint. A major energy consumer in industry is the drive train, which consists of variable speed drives, motors, pumps, and other components. Drivetrain Analyzer Cloud, a powerful solution from the Siemens Xcelerator portfolio, helps companies significantly reduce the energy consumption of their drive systems through energy-based maintenance.

Continuous monitoring, AI-based optimization for energy efficiency

The Connection Module IOT collects extensive data from the drive train and transmits it to the Drivetrain Analyzer Cloud. There, relevant operating data such as load, electrical power consumption and energy consumption of the drives are continuously calculated and displayed. Drivetrain Analyzer Cloud also helps to save energy by using advanced AI-based analysis algorithms to accurately detect deviations from the optimal operating point, monitor energy consumption, CO2 emissions, and costs, and generate optimization suggestions.

Thanks to its data-driven approach, it even precisely calculates the return on investment (ROI) so that future investments can be allocated as accurately as possible. This allows users to take targeted actions to increase energy efficiency: for example, adjusting the engine control, maintenance intervals, and load distribution. Drivetrain Analyzer Cloud also detects when an engine is operating inefficiently and automatically recommends a more efficient alternative. Using Drivetrain Analyzer Cloud can reduce the energy consumption of a drive system by 10 to 20 percent.

The cloud-based approach also makes it possible to share results across sites and optimize the efficiency of the entire manufacturing infrastructure. In addition,



Drivetrain Analyzer Cloud, a powerful solution from the Siemens Xcelerator portfolio, helps companies significantly reduce the energy consumption of their drive systems through energy-based maintenance.

the Drivetrain Analyzer Cloud insights can be integrated into higher-level energy management systems.

Siemens Industrial Copilot for operations

To make it even easier to use in the future and to address the shortage of specialists, users are now supported by an integrated Siemens Industrial Copilot for operations. With the GenAI-based chatbot, users can communicate in their native language to ask specific questions and get critical assistance with interpreting data and information.

This takes the efficiency and value of Drivetrain Analyzer Cloud to a new level.

With the Siemens Industrial Copilot Siemens is revolutionizing the industry by enabling customers to leverage this technology across the entire value chain – from design and planning to engineering, operations, and services.

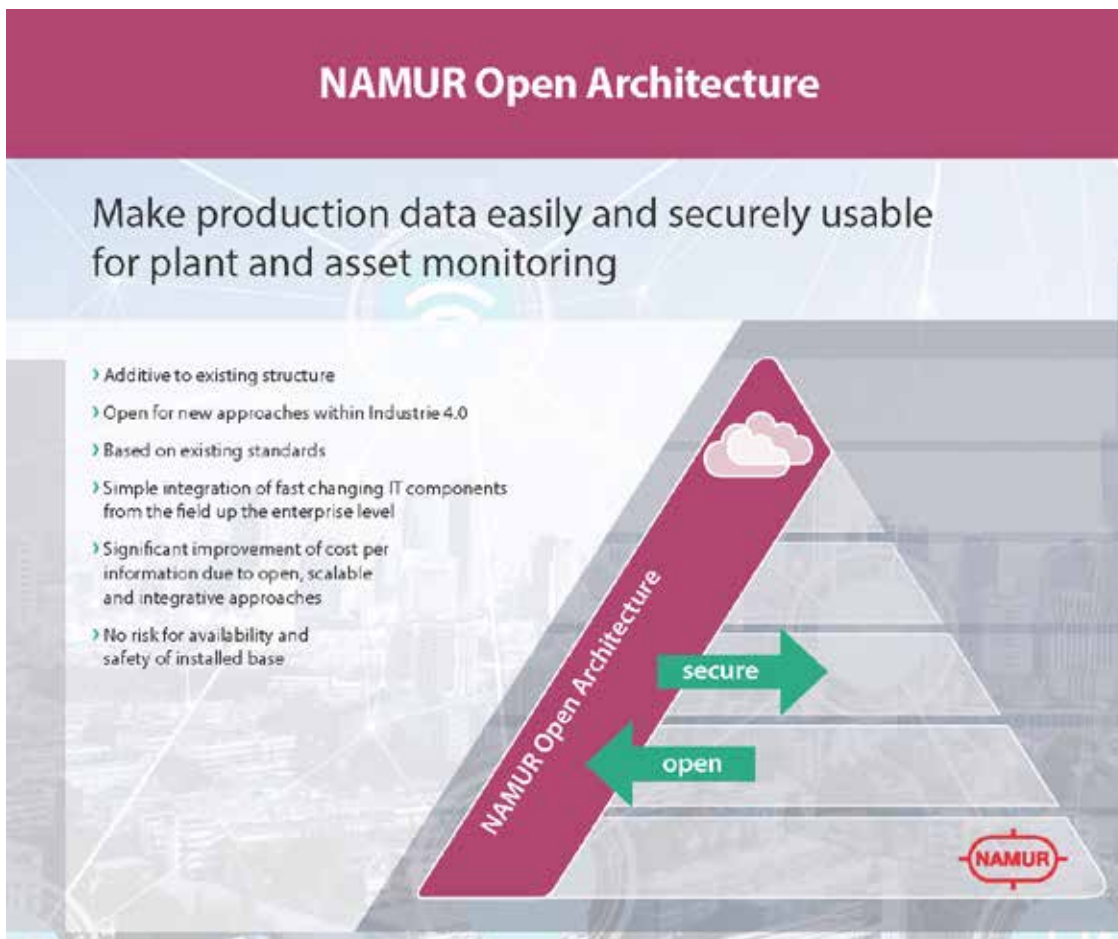
Drivetrain Analyzer Cloud is part of the Siemens Xcelerator portfolio. Industrial companies can take advantage of Drivetrain Analyzer Cloud to significantly improve their energy efficiency and sustainability. This is an important step toward achieving their sustainability goals.

Siemens

[Learn More](#)

NOA cooperation kicks off

The goal is to prepare and deliver NOA (Namur Open Architecture), an open standard for efficient and secure vertical communication at process automation production plants



In this context, the Steering Committee decided to optimize the practical suitability of provisions with the aid of a pilot plant as soon as work on the specification begins. The implementations currently available are based on the requirements and implementation hints specified in the NAMUR recommendations, making them an excellent foundation for further work. They also show that the technology is available and can now be scaled in a large number of plants so urgently needed savings potential can also be realized in short order. The pilot plant provides practical infrastructure similar to a Plug Fest into which additional new implementations are to be integrated on a continual basis. Both this approach and plant testing under real-world conditions have already proven themselves in the cooperative efforts

The goal of NOA is increasing the productivity of process plants. At a joint workshop attended by experts of the cooperating partners, the members of the Steering Committee have evaluated the use cases described in the NAMUR recommendations for relevance and urgency. Crucial topics have been defined, and the priorities and necessary steps for the work to come have been specified.

Karlsruhe, Germany on March 06, 2025:

In June last year, the cooperation between NAMUR, ZVEI and PI (PROFIBUS & PROFINET International) was officially sealed. The goal is to prepare and deliver NOA (Namur Open Architecture), an open standard for efficient and secure vertical communication at process automation production plants.

Feedback-free transmission

The task is to define NOA as a standardized channel for the feedback-free transmission of required digital data to a parallel second channel from the field for the purposes of monitoring, process optimization and predictive maintenance. The work in the cooperation has now begun and is bearing its first fruits.

Utilizing previously developed use cases as a basis, and with the support

of available test plants for determining the degree of interoperability of NOA implementations in different applications, valuable experience revealing achievable potential savings—which in turn can point out the possibility of cost reductions—is being gained. This is all taking place with the aim of achieving a long-lasting interoperable standard. To this end, the cooperating partners have already started agreements within the framework of the established NOA Steering Committee.

At a joint workshop attended by experts of the cooperating partners, the members of the Steering Committee have evaluated the use cases described in the NAMUR recommendations for relevance and urgency. Crucial topics have been defined, and the priorities and necessary steps for the work to come have been specified.

of NAMUR and ZVEI over the past few years.

Utilizing findings from the pilot applications, test scenarios are being created which in turn substantially contribute to the evaluation of specification document quality and the quality of implementation in interoperable NOA products—and they do it early in the process of creating the specification. These test scenarios then form the basis for the establishment of certification testing and provision of the required tools in the following step.

The Steering Committee will establish Joint Working Groups to carry out specification work, define quality assurance measures and implement marketing projects.

NAMUR, ZVEI and PI

New cellular routers and switches

New product introductions from Phoenix Contact include a new line-up of industrial outdoor cellular routers and 19-inch rackmount managed switches for industry.

Phoenix Contact is extending its remote communication portfolio to include industrial outdoor cellular routers. The Cellulink product family connects network-capable devices to the cellular network worldwide and is certified in accordance with IEC 62443-4-2.

Routers and antennas are combined in compact devices and can thus be mounted on the control cabinet, on a wall, or on a mast. The devices are supplied with Power over Ethernet, enabling quick and easy installation with just one Ethernet cable. The all-in-one concept saves costs for additional cellular antennas and antenna cables, as well as space in the control cabinet and installation time. The products have numerous cybersecurity functions as well as certification in accordance with IEC 62443-4-2. They are therefore optimally prepared for the Cyber Resilience Act.

Each device supports dual SIM and provider fallback as well as GNSS (Global Navigation Satellite System) for precise positioning and time synchronization. Configuration and firmware updates are carried out conveniently via web-based management, a REST API, and comprehensive device and update management. The Cellulink product family is divided into three device classes, which differ only in terms of their technological and performance capabilities:

With a European LTE CAT1 module, the 2000 series offers affordable and reliable entry-level cellular connectivity, with sufficient data throughput for most smaller-scale applications.

The 4000 series is equipped with a global LTE CAT4 module and covers all common LTE applications. These devices can be used internationally and provide mid-range data throughput.

With a global 5G module, the 6000 series represents the highest performance class. These devices are optimized for very high data throughput and low latencies and can be used in both private and public 5G networks worldwide.

New 19-inch rackmount managed switches for industry

Phoenix Contact also presented a new portfolio of managed switches in 19-inch format at the Hannover Messe 2025. Featuring up to four 10 Gigabit ports, the FL Switch 5900 series switches offer high data performance, comprehensive security functions, and modern TSN mechanisms.

The five product versions supplement



SOURCE: PHOENIX CONTACT

The Cellulink product family connects network-capable devices to the cellular network worldwide and is certified in accordance with IEC 62443-4-2.



The FL Switch 5900 series switches offer high data performance, comprehensive security, and modern TSN mechanisms.

the well-established FL Switch 2000 series and provide a similar range of functions for optimum compatibility. With up to four 10 Gbps uplinks (SFP+) and 24 Gigabit ports, the rackmount switches combine high performance with a high degree of flexibility. Combo ports and SFP ports also provide flexible connection options for copper and fiberglass communication.

In addition, the 19-inch switches include a complete range of TSN functions for use in time-critical applications. An optional redundant power supply enhances failsafe performance.

Phoenix Contact

[Learn More](#)

Generative AI Assistant

New smart co-pilot developed specifically for connected production and maintenance.

Software maker Augmentir has developed a new smart co-pilot developed specifically for connected production and maintenance. Augie uses generative AI to provide targeted support for skilled workers in their work. This involves much more than just questions and answers.

Augie starts with the digitalization of standard operating procedures (SOPs). In doing so, he converts paper-based or digital content directly into structured work instructions. Now, all users have to do is take a photo of a notice with safety instructions to turn it into an interactive checklist.

Existing Word, Excel, PDF or JPG files are automatically converted into dynamic content that guides industrial workers at their workplace. Initial practical applications show that SOPs can be digitized 85 percent faster this way.

The effort required for onboarding new employees also decreases significantly, by up to 72 percent according to Augmentir. This is because Augie can create interactive training modules with tests and solutions in a matter of seconds. To do this, it uses content from manuals, videos or existing tests. This



SOURCE: AUGMENTIR

also helps with further training: based on integrated skill management, the system tailors the content precisely to the user's level of knowledge and practical experience.

Augie also comes into its own during operation. If, for example, a specialist notices a problem with a system, the assistant analyzes relevant documents in a matter of seconds. It

then provides precise explanations, including instructions for troubleshooting. In practice, this has led to an average of one-third more productivity.

Augmentir

[Learn More](#)

PMIC for industrial computing

Microchip's MCP16701 integrates buck converters, Low Dropout Voltage Regulators (LDOs) and controller.

The rapid integration of AI into industrial, computing and data center applications is fueling demand for more efficient and advanced power management solutions. Microchip has announced the MCP16701, a Power Management Integrated Circuit (PMIC) designed to meet the needs of high-performance MPU and FPGA designers. The MCP16701 integrates eight 1.5A buck converters that can be paralleled, four 300 mA internal Low Dropout Voltage Regulators (LDOs) and a controller to drive external MOSFETs.

This highly integrated device can result in a 48% area reduction with less than 60% of the component count of a discrete solution. The MCP16701 is in a small-form-factor 8 mm × 8 mm VQFN package to offer a compact and flexible power management solution for space-constrained applications. The MCP16701 meets diverse power needs and supports Microchip's PIC64-GX MPU and PolarFire® FPGAs with a configurable feature set.

"With the introduction of the MCP16701, Microchip is setting a new standard in PMIC technology by offering an unprecedented level of integration and flexibility," said



SOURCE: MICROCHIP

Rudy Jaramillo, vice president of Microchip's analog power and interface division. "This advanced PMIC is designed specifically for high-performance applications, enabling our customers to streamline their design process."

The MCP16701 features an I2C communication interface to simply and enhance communication efficiency between

the PMIC and other system components. The device operates within a temperature range of TJ -40°C to +105°C for reliable performance in diverse environmental conditions.

Microchip

[Learn More](#)

Kubernetes Manager for dev teams

Efficient Kubernetes management is a strategic element in cloud computing.

An infrastructure-agnostic solution by mogenius simplifies onboarding, enhances transparency, and boosts efficiency through an intuitive self-service approach. Its next-generation Kubernetes Manager, specifically designed for DevOps engineers and application developers. The tool delivers an intuitive Developer Experience (DevEX) and provides detailed insights into Kubernetes operations for teams of all experience levels—from beginners to experts. Within the Kubernetes workspaces, resources and objects can be grouped and assigned to specific teams for monitoring and management. Teams gain valuable insights into multiple Kubernetes clusters and can take action with comprehensive self-service features for incident management.

Simplicity and cognitive load are key factors for the success of Kubernetes in enterprises. Developers and DevOps teams often spend over 60% of their time on infrastructure and administrative tasks. The reasons are usually straightforward: too many tools, information overload, and the challenge of managing appropriate access rights.

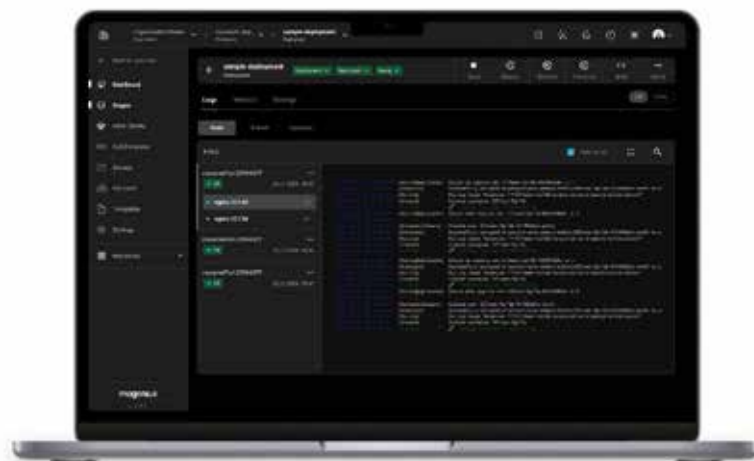
The Kubernetes Manager extends the Kubernetes API with the mogenius operator and custom resource definitions. Once the

operator is installed, workloads, resources, and access rights can be organized in workspaces, simplifying complex structures and filtering relevant information. Enhanced role-based access control ensures that developers can securely access essential metrics, logs, and the status of all resources within their workspaces without

needing direct cluster access. Developers can view critical data with a single login, simplifying workflows and saving valuable time.

Mogenius

[Visit Website](#)



Wi-Fi 6, Wi-Fi 6e and Wi-Fi 7 antennas

Pasternack's latest indoor/outdoor line of antennas covers bands from 2.4 to 6 GHz.

Pasternack, an Infinite Electronics brand and a provider of RF, microwave and millimeter-wave products, has announced the launch of its new Wi-Fi 6, Wi-Fi 6e and Wi-Fi 7 antennas. The new product family includes rubber ducks, omnidirectional and flat-panel antennas. It is designed to deliver high performance for the latest wireless communication standards.

The antennas operate across the 2.4, 4.9, 5, 5.8 and 6 GHz bands, ensuring broad compatibility and superior connectivity for a variety of applications. They are available in multiple configurations, including four, six or eight ports, which offers 4x4, 6x6 or 8x8 MIMO capabilities.

This range of options supports high-bandwidth, low-latency and multi-user gigabit networking, making them ideal for both indoor and outdoor deployments, including large venues. For flexibility and easy installation, the antennas are equipped with a variety of connectors, such as N female, N male, RP-SMA male and RP-TNC male.

Key features include the ability to cover

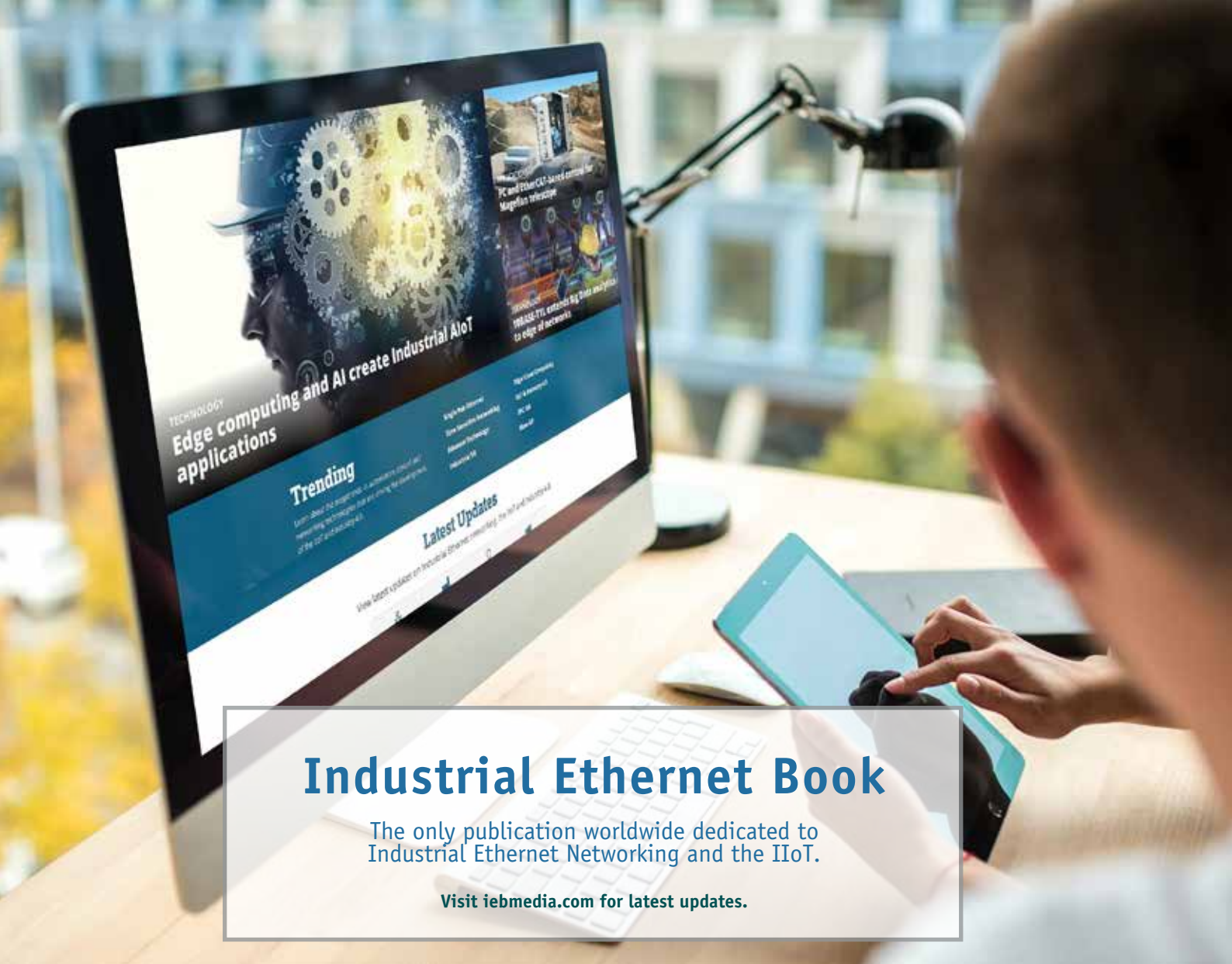
the latest frequency bands of Wi-Fi 6e and unlicensed 6 GHz bands, tilt-and-swivel rubber duck options, and multi-port omnidirectional and flat-panel designs. They deliver 1.2 GHz more spectrum than previous Wi-Fi antennas, which translates to enhanced performance and future-proofing for the latest devices released in 2021 and beyond.

"This new line provides reliable, high-performance solutions that support the latest wireless technologies," said Senior Product Manager Kevin Hietpas.

Pasternack

[Learn More](#)





Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

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



eBook Archive



Technical Articles



Latest Updates



Trending Topics

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

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

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

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