July/August 2024 143
ISSN 1470-5745

industrial ethernet book

Industrial Ethernet Automation Networking & IIoT

Special Report

Remote Connectivity Update

Page 30

Megatrends Shaping the Industrial Edge 6

groov EPIC

Your Digital Transformation-ready Edge Platform

groov RIO

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

All the tools you need, included.

CODESYS
groov MANAGE
Ignition EDGE INCLUDED
PAC Control
groov VIEW
MQTT
Linux
Node-RED
Sparkplug COMPATIBLE
ssh
OPENVPN
OPC UA SERVER

Learn more today at www.opto22.com.

50 Anniversary

OPTO 22
Your Edge in Automation.™

GET CONNECTED…

Visit our new website at: www.iebmedia.com

The next wave of Generative AI at the edge

The next-generation high performance, energy efficient Edge AI accelerator addresses the latest Generative AI solutions at the edge from vision to billions of parameters large language models.

EdgeCortix® Inc., a leading fabless semiconductor company specializing in energy-efficient AI processing at the edge, has unveiled its next-generation SAKURA-II Edge AI accelerator.

This state-of-the-art platform, paired with EdgeCortix's innovative second generation Dynamic Neural Accelerator (DNA) architecture, is engineered to tackle the most challenging Generative AI tasks in the industry. Designed for flexibility and power efficiency, SAKURA-II empowers users to seamlessly manage a wide range of complex tasks including Large Language Models (LLMs), Large Vision Models (LVMs), and multi-modal transformer-based applications, even within the stringent environmental constraints at the edge. Featuring low latency, best-in-class memory bandwidth, high accuracy, and compact form factors, SAKURA-II delivers unparalleled performance and cost-efficiency across the diverse spectrum of edge AI applications.

Well-suited for numerous use cases across the manufacturing, industry 4.0, security, robotics, aerospace, and telecommunications industries, SAKURA-II features EdgeCortix's latest generation runtime reconfigurable neural processing engine, DNA-II. Leveraging this highly configurable intellectual property block, SAKURA-II delivers power efficiency and real-time processing capabilities while simultaneously executing multiple deep neural network models with low latency. SAKURA-II can deliver up to 60 trillion operations per second (TOPS) of effective 8-bit integer performance and 30 trillion 16-bit brain floating-point operations per second (TFLOPS), while also supporting built-in mixed precision for handling the rigorous demands of next-generation AI tasks.

The SAKURA-II platform, with its sophisticated MERA software suite, features a heterogeneous compiler platform, advanced quantization, and model calibration capabilities. This software suite includes native support for leading development frameworks such as PyTorch, TensorFlow Lite, and ONNX. MERA's flexible host-to-accelerator unified runtime is adept at scaling across single, multi-chip, and multi-card systems at the edge, significantly streamlining AI inferencing and shortening deployment times for data scientists.

AI has a bright future for use in smart manufacturing applications, and is just in its infancy in terms of product development.

Al Presher

Private 5G Communications: 17

New Products: 53

Contents

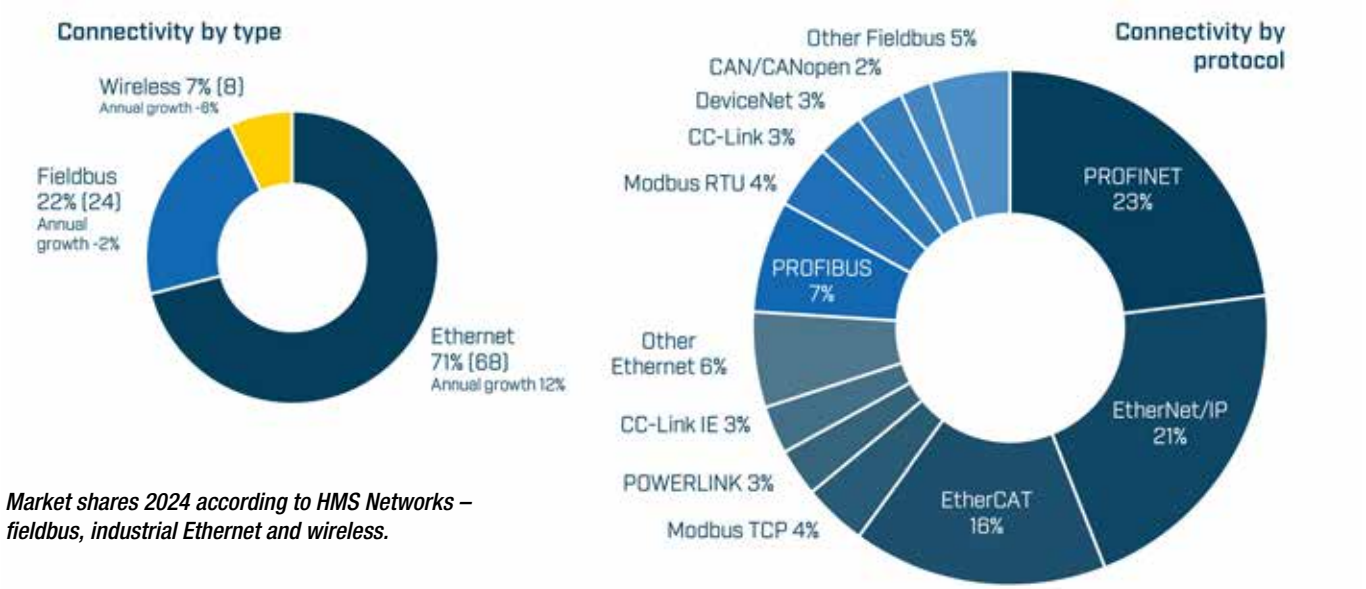
Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2024.**
Deadline for editorial: September 12, 2024 **Advertising deadline:** September 12, 2024

Editor: Al Presher, editor@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +1 585-598-6627
Free Subscription: iebmedia.com/subscribe
Published by IEB Media Corp., 1247 Anthony Beach Rd., Penn Yan, NY, 14527 USA ISSN 1470-5745

Industrial Ethernet 71% of all newly installed network nodes

Annual analysis reveals steady growth in industrial network market, and industrial network market shares for 2024 according to HMS Networks.



SOURCE: HMS NETWORKS

Market shares 2024 according to HMS Networks – fieldbus, industrial Ethernet and wireless.

EVERY YEAR, HMS NETWORKS CONDUCTS A comprehensive analysis of the industrial network market, aiming to estimate the distribution of new connected nodes by type and protocol within factory automation. The latest study indicates that the industrial network market continues to expand, with an anticipated 7% growth in 2024.

Industrial Ethernet dominance

Notably, Industrial Ethernet remains the dominant player, representing a substantial 71% of all newly installed nodes (compared to 68% last year). Meanwhile, fieldbuses have declined to 22% (from 24%), and wireless technologies have seen a slight dip from 8% to 7%. Among the top contenders, PROFINET account for 23% of newly installed nodes, followed closely by EtherNet/IP at 21%, and EtherCAT now stands at 16%.

Each year, HMS Networks presents their analysis of the industrial network market, focusing on newly installed nodes within factory automation globally. As an independent supplier of solutions within Industrial ICT (Information and Communication Technology), HMS has substantial insight into the industrial network market. The 2024 study includes estimated market shares and growth rates for fieldbuses, industrial Ethernet, and wireless technologies.

In the 2024 study, HMS concludes that the industrial network market continues to grow, with total market growth in 2024 expected to be +7%, confirming the continued importance of network connectivity in factories.

Industrial Ethernet shows steady growth

Growing by 12%, Industrial Ethernet accelerates its growth and continues to capture market share. Industrial Ethernet now accounts for 71% of the global market for newly installed nodes in factory automation (compared to 68% last year). PROFINET is the largest protocol, with a market share of 23%, surpassing EtherNet/IP, which accounts for 21% of new nodes. The popularity of EtherCAT remains strong and is now securely in third place with a 16% market share.

Fieldbuses experience expected decline

Traditional serial fieldbus installations continue to lose momentum. While fieldbus installations still constitute a significant portion of new nodes added, annual growth is expected to drop by -2% in 2024. PROFIBUS leads the fieldbus rankings with a 7% market share, followed by an even distribution among other well-known fieldbus protocols. Together, fieldbuses account for 22% of the market in 2024. Despite the decline in new fieldbus nodes, many devices, machines, and factories will continue to rely on these well-functioning and proven fieldbuses for years to come.

Wireless technologies maintain steady presence

Wireless technologies have seen steady growth in recent years, although the pace of growth is now reported to have slightly decreased. Wireless solutions still comprise a robust 7% of the total share by type. The market continues to introduce more products with support for industrial wireless, and acceptance of wireless solutions in factory settings is on the rise. Typical use cases include cable replacement applications, wireless machine access, and connectivity to mobile industrial equipment.

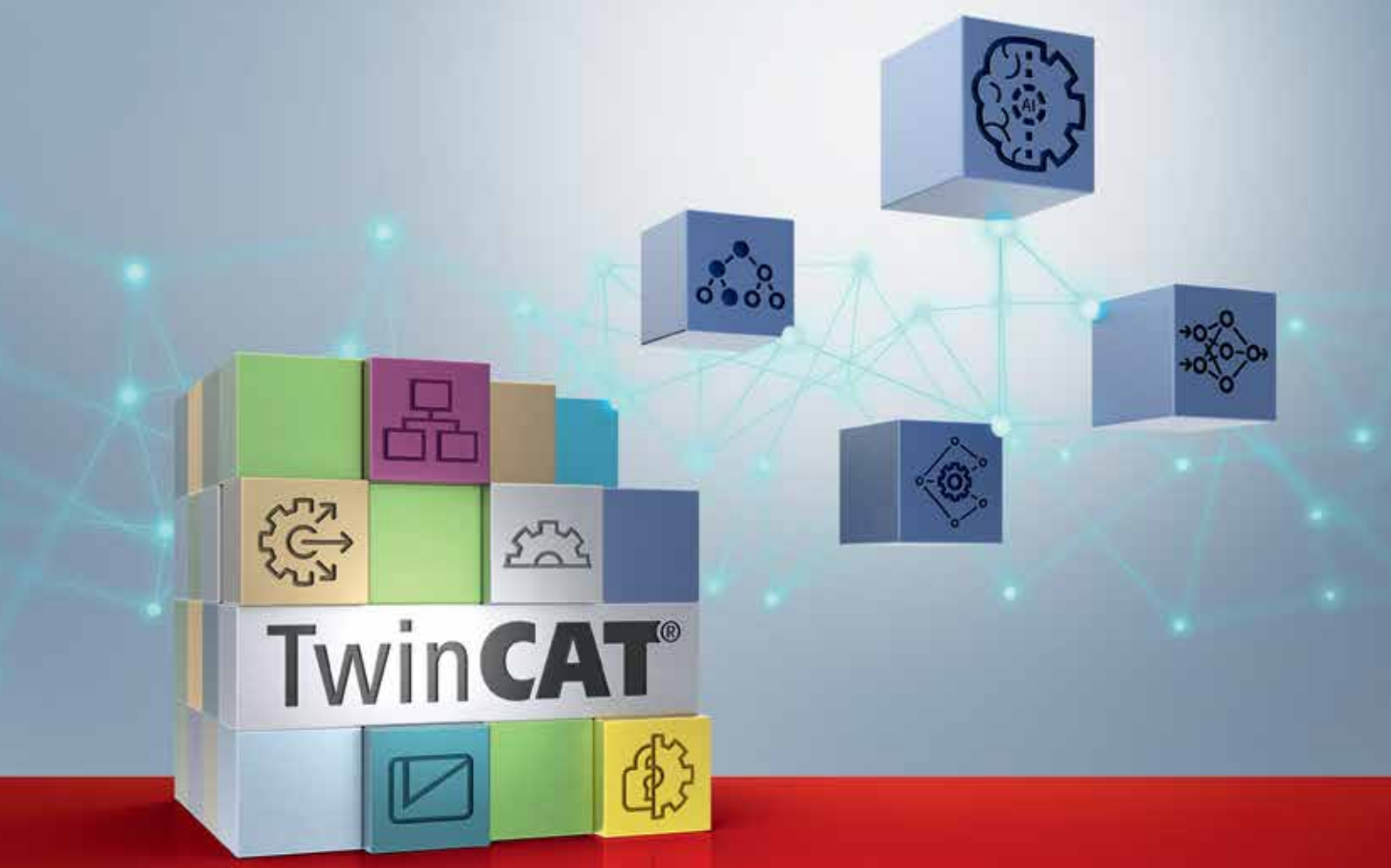
Industrial networking key for productivity and sustainability

"Connectivity is now standard in factory automation, with Industrial Ethernet leading the way. However, as we look ahead, we anticipate a dynamic landscape with emerging trends and technologies. While Industrial Ethernet currently dominates, we'll witness exciting changes and innovations that will shape the future of industrial networking." – Magnus Jansson, Product Marketing Director at HMS Networks, Business Unit Anybus.

The study includes HMS' estimation for 2024 based on number of new installed nodes within Factory Automation. A node is defined as a machine or device connected to an industrial field network.

*News report by **HMS Networks**.*

Machine learning for all automation sectors



TwinCAT Machine Learning: AI is simply integrated into the control level

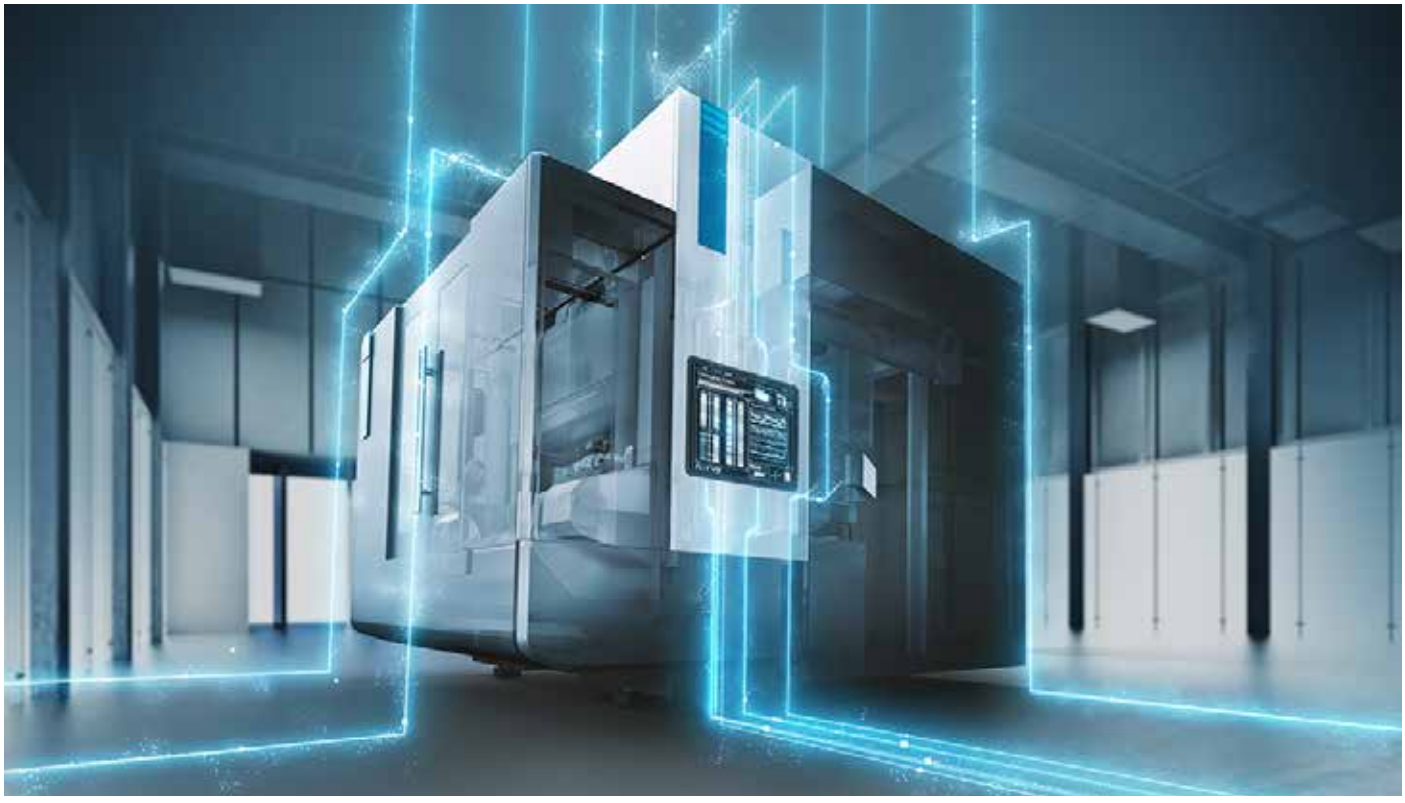
- AI models as a function block in the PLC: AI as a component of the control code
- real-time execution on the standard control IPC: in sync with motion, sequential logic, vision, and much more
- acceleration of complex AI models: Beckhoff IPC with NVIDIA GPU and interface from the PLC
- automated training of AI models: AI model creation that doesn't require AI expertise
- open interface for trained AI models (ONNX): trained AI with interoperability
- AI model lifecycle management: model updates without compilation, stop, and restart

Find out more about machine learning

New Automation Technology **BECKHOFF**

Industrial Edge computing megatrends special report

Industrial Edge and Cloud Computing are among the most exciting areas of technology development for smart manufacturing. This special report provides the perspective of nine industry experts as they share their shared vision for the future of the Industrial Edge and the megatrends that are pushing initiatives forward.



SOURCE: TTTECH INDUSTRIAL

"Edge computing plays a crucial role for localized data processing with reduced latency and improved security and privacy. Software technologies driving these advancements include containerization with Docker and orchestration with Kubernetes, and edge AI frameworks that can work with resource constrained hardware platforms," Georg Stöger, Director Training and Consulting at TTTech Industrial.

INDUSTRIAL EDGE AND CLOUD COMPUTING has a bright future. With all the latest advancements in artificial intelligence, cloud computing and data management, the next generation of industry will be more secure and intelligent than ever before.

What makes edge-computing unique and different is how networking devices are now being mobilized as compute nodes, replacing dedicated hardware resources that were commonly implemented for the purpose in industrial networks.

For this update on the Industrial Edge, we reached out to a series ofindustry experts to get their perspective on the technologies that are shaping the present and future developments with the Industrial Edge. Each provides a unique view of its potential impact on smart manufacturing, and how companies can leverage this unique ability to bring data processing closer to the plant floor.

Real-time data generation and preprocessing

Localized data processing with reduced latency and improved security and privacy.

"Technology trends that make more complex and powerful Industrial Edge and IIoT solutions possible include widespread sensor deployment for real-time data generation and data preprocessing at the edge; wired and wireless high-speed, low-latency networks for interconnecting more I/O and processing units locally at the edge; and AI for predictive maintenance and enhanced decision-making," said Georg Stöger, Director Training and Consulting at TTTech Industrial.

"Edge computing plays a crucial role for localized data processing with reduced latency and improved security and privacy. Software technologies driving these advancements include containerization with Docker and orchestration with Kubernetes, and edge AI frameworks that can work with resource constrained hardware platforms. Federated learning has come up more than once as an AI technology trend; this technology can address resource constraints, privacy concerns, and scalability in edge-centric applications of various verticals including industrial automation," Stöger said.

Stögeradded that cybersecurity remains an overarching key topic for edge, cloud, and IIoT systems, especially in the EU, where the NIS2 directive is going to take full effect by the fourth quarter of 2024.

Why it matters

Stöger said that edge computing brings data processing closer to the source, reducing latency and bandwidth usage, which is essential for real-time decision-making and rapid response to operational changes.

AUTBUS –

THE NEW **MULTIDROP** DATA COMMUNICATION BUS READY FOR RAILWAY APPLICATIONS

InnoTrans

Come visit us!

24 - 27 Sep 2024
Berlin, Germany
Hall 4.1 Stand 405

ABN300 Series

The AUTBUS Converters to Ethernet/CAN/RS485

The new AUTBUS data bus technology, standardised by the IEC, offers a simple, cost-effective and cable-reducing installation solution through multi-drop data networking of end devices, with maximum availability ensured by ring redundancy. AUTBUS represents an alternative solution for communication technology in demanding environments, such as those encountered in railway applications. AUTBUS data technology, based on 2-wire twisted pair data cables, supports up to 254 multidrop device connections with a data bandwidth of 100 Mbps and a maximum cable length of 500 m. Another key feature is the multi-protocol capability for transparent (tunneling) transmission of data protocols such as Ethernet-based protocols or CAN bus.

This integration leads to improved safety, reliability, and operating efficiency, making AUTBUS an optimal data transmission technology for new and modernized railway systems.

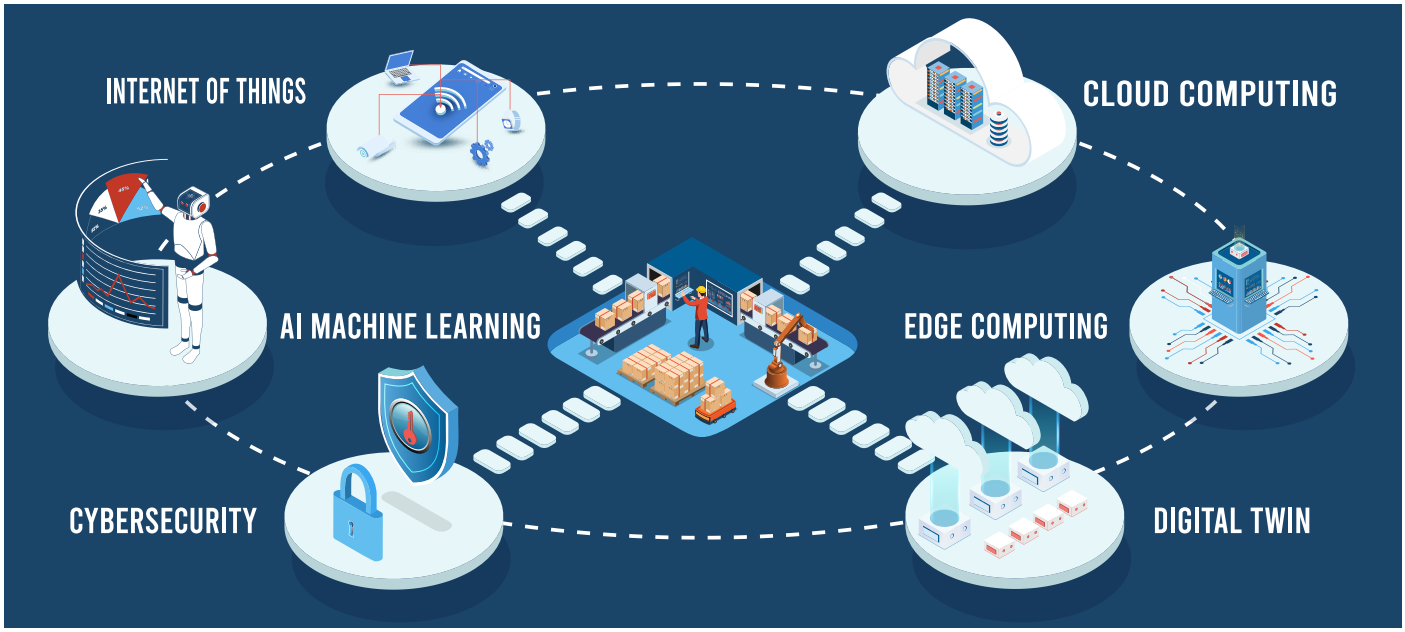
- *Up to 254 multidrop nodes*
- *2 wire twisted pair cable*
- *100 Mbps high data bandwidth*
- *Up to 500 m distance*
- *Real-time deterministics*
- *Bus & Ring topology*
- *Multibus protocol tunneling*
- *Compatible with SPE cables & connectors*

Learn **AUTBUS**

Try **ABN300**

KLG SMARTEC

www.klgsmartec.com | autbus@klgsmartec.com



SOURCE: ISTOCKPHOTO

The industrial edge encompasses networking technologies that are at the cutting edge of innovations in smart manufacturing.

Localized processing improves reliability and security by minimizing the transmission of sensitive data over networks.

Cloud computing provides scalable storage and computational power, allowing manufacturers to handle large volumes of data and complex analytics without hardware constraints. Also, cloud computing can perform analyses and optimizations based on a global view of process data from multiple assets, which is not available at each edge device.

"The combination of edge and cloud computing enables seamless integration of IoT device data collection, advanced analytics, and AI/ML models, leading to a more connected and intelligent manufacturing environment," Stöger said.

By leveraging these technologies appropriately, manufacturers can achieve higher levels of automation and operational efficiency. The integration of industrial edge and cloud computing transforms manufacturing into a more agile, data-driven, and intelligent industry, paving the way for innovations and more sustainable manufacturing practices.

Uniqueness of technology solutions

According to Stöger, industrial edge and cloud computing bridge the gap between IT and OT infrastructure; they integrate real-time data processing and advanced analytics with control infrastructure that used to operate in isolation due to technical constraints and security concerns. Unlike past solutions that relied heavily on centralized computing, a hybrid edge/cloud infrastructure can utilize containerization technologies like Docker and Kubernetes which orchestrate and distribute computational tasks across the edge and the cloud.

Edge devices often provide substantial computational resources, allowing them to perform data acquisition, data (pre)processing, AI inference, and decision-making locally on a single device, possibly combined with local HMI functions. This results in significantly reduced processing latency and more cost- effective infrastructure. The use of and orchestration tools such as Kubernetes facilitates the development, deployment, and management of applications across diverse environments, ensuring consistency and scalability.

Past implementations often struggled with scalability and flexibility due to hardware limitations and rigid infrastructure. The new approach leverages the cloud for its storage and processing power. The integration of robust cybersecurity measures also marks a significant improvement, as contemporary solutions should be designed based on a comprehensive cybersecurity framework which systematically protects distributed networks and data flows.

Focus on innovation

"Machine builders and energy management systems are among the industries which can benefit substantially from these solutions," Stöger said.

"In industrial automation, edge/cloud computing can create highly responsive and adaptable production lines. Real-time monitoring and control enabled by edge computing allow for immediate diagnostics and adjustments of machinery, enhancing productivity and quality and reducing downtime. For machine builders, this means the ability to offer more sophisticated and reliable equipment, equipped with predictive maintenance capabilities that anticipate failures before they occur," he said.

Stöger added that energy management for industrial production systems benefits from real-time data analytics that optimize energy consumption and distribution, improving efficiency and reducing costs. These systems can help to predict and even dynamically adjust energy flows in response to demand fluctuations, leading to more sustainable and efficient operations.

Advances in artificial intelligence, particularly federated learning, are playing a crucial role in these developments. Federated learning allows AI models to be trained across multiple decentralized devices or servers holding local data samples, without exchanging the data itself. This is particularly beneficial for systems where sensitive data privacy and security are paramount. By deploying federated learning, system builders can develop and refine AI models directly on the edge devices, ensuring that the models are continuously learning and improving from local data while maintaining data privacy. This decentralized approach not only enhances data security but also reduces the latency and bandwidth required for continuous data transfer to the cloud.

Looking to the future

"As edge computing continues to evolve, it will incorporate more advanced AI and machine learning applications directly at the point of data generation, enabling real-time analytics and decision-making capabilities. This localized processing will reduce latency, increase reliability, and enhance data privacy, driving more efficient and responsive industrial systems," Stöger said.

"Looking at one technology in particular, we believe the integration of federated learning will allow for continuous improvement of AI models while maintaining data security, facilitating smarter and more adaptive industrial processes. As these technologies become more widely available and their potential is better understood, they will drive

further innovation in predictive maintenance, energy management, and automated quality control, leading to an even more interconnected, intelligent, and efficient industrial landscape," Stöger said.

Industrial Edge megatrends

Focus on security and flexible choices among programming platforms.

Dan White, Director of Technical Marketing at Opto 22 said that "it's the security features on today's edge devices that enable secure data transfer to the cloud, which in turn enables advanced cloud computing. Publish/subscribe communication technologies like MQTT Sparkplug, a new international standard, publish data only when changes occur, reducing unnecessary data flow and network traffic. Support for SSL/TLS certificates ensures that those connections are securely authenticated and encrypted. Outbound connections from your edge devices means no inbound ports are open—significantly reducing cyber attack vectors. IT departments can enjoy user authentication that supports lightweight access directory protocol (LDAP), the same tools used on every PC in your plant."

Flexible programming platforms

White said that flexible programming platforms on edge devices are another key cloud enabler. With open-source friendly software tools, developers can work with languages and protocols they prefer. Tools like user defined data types (UDTs) can add context to raw data, so when it arrives in the cloud, it already has meaning and context—rather than clumps of raw data that muddy the waters.

"On the cloud, software technologies like artificial intelligence and machine learning, which require vast amounts of storage and processing capability, enable data scientists to perform powerful analysis to improve future operations. Using commonly understood programming tools like structured query language (SQL), cloud computing makes it easy to work with enormous data tables. This simply can't be done at the edge with limited computing resources," White said.

White added that edge technology is the lifeblood of operational technology. After all, you can't rely exclusively on cloud platforms like AWS and Snowflake to run a machine on the plant floor—it's just not practical. A simple network outage would cripple your operations. Neither can you rely on edge computing devices to analyze large swaths of data to gain better insight into your operations—edge devices aren't built with that kind of computing power.

"Design your edge and cloud architectures with each other in mind. Choose edge devices that support the technologies that the cloud relies upon. Ethernet protocols that are standard, like REST APIs, MQTT Sparkplug, OPC UA, and even legacy protocols like Modbus and Ethernet/IP all play important roles in the technology stack from the plant floor to the cloud," White said.

SOURCE: ISTOCKPHOTO

" It's the security features on today's edge devices that enable secure data transfer to the cloud, which in turn enables advanced cloud computing. Publish/subscribe communication technologies like MQTT Sparkplug, a new international standard, publish data only when changes occur, reducing unnecessary data flow and network traffic," Dan White, Director of Technical Marketing at Opto 22.

He added that the impact of a cohesive edge-to-cloud architecture is substantial and used a car analogy. Edge devices are new modern EVs that are sending all their data to the cloud to improve self-driving and safety algorithms. The algorithms are regenerated periodically with the best and most current data, then they get sent down to the vehicle in the form of a firmware update. After each update, the vehicle operates more safely and drives better than ever before. The EV never relied upon the cloud for real time driving control, but the better driving algorithm would not be possible without cloud computing power to process data from millions of cars worldwide. Not to mention the global visibility—the car manufacturer can anticipate potential safety, maintenance, or service issues before the driver.

Unique technology solutions

White said that "the newest technology is universal, not proprietary" For example, a PLC with its own REST API would have been a completely foreign concept just a few years ago, but now there are a number of them available on the market. In fact, some PLCs now come equipped with REST APIs, OPC UA servers, and MQTT clients/servers—along with legacy protocol support like Modbus, ProfiNET, and Ethernet/IP.

'Engineers and designers are tired of being locked into closed, proprietary systems versus a system that uses an architecture built on open standards. In the past, most edge devices were part of closed systems—like a PLC with a dedicated HMI and a proprietary Ethernet protocol for communications. What was once the status quo has quickly become an antiquated architecture," White said.

"And don't confuse open standards and open source friendly communications with vulnerability. We're talking about the same types of communication and security methodologies that people use every day for online banking, private healthcare data, and sensitive corporate communications," he added.

As management demands that more operational data be available, legacy proprietary systems have proven to be a bottleneck for valuable plant floor data. In contrast, IT professionals who are looking to get data from modern edge devices have no trouble understanding the standard communications onboard.

Applications focus

OEM machine builders and service companies have a lot to gain from the latest edge and cloud solutions. In the past, machine builders would deploy their machine to a customer site and walk away. Typically they'd get a phone call or email for service when the machine failed. The service model was purely reactive. It often left the customer with costly downtime situations and hurt the reputation of the machine builder.

Machine builders who are taking advantage of modern edge-to-cloud architectures can benefit immensely. Machines deployed in the field are continuously providing key data—and with cloud computing power—machine learning and AI algorithms can improve designs for the machine of the future.

And even more importantly, OEMs can monitor their machines in real time and get alerts, often learning of a potential failure or downtime situation before the customer.

SOURCE: ISTOCKPHOTO

"Industrial manufacturing is highly programmed and full of automation, but the future of smart manufacturing requires more autonomy. Building autonomous systems for manufacturing will require new datasets of clean and trusted data, machine learning applied on top of first principles, and ways to manage scaled deployment to distributed automation systems," Oliver Haya, business manager and Adam Gregory, software platform manager at Rockwell Automation.

With this kind of knowledge, the OEM can provide better service at a lower cost than ever before—a win-win scenario.

Looking ahead

"Software containerization is emerging as a new tool on industrial edge solutions. Software containerization is a method of packaging an application and its dependencies together so it can run reliably on any computing environment. Containers make custom software deployment on edge devices simple and consistent," White said.

By reducing conflicts and dependencies, software containerization enables rapid, scaleable updates. Containers can be added or removed quickly based on current needs, allowing flexible resource management, which is crucial for handling varying workloads on edge devices. Plus, containers are lightweight, optimizing the limited computing resources available on edge devices.

"With software containers, you can apply new versions or fixes quickly without significant downtime, ensuring that edge devices remain up-to-date and efficient. This adaptability and efficiency are vital for advancing IIoT and Industry 4.0," White concluded.

Emergence of Containers and Clusters

Unlocking new value propositions for security, collaboration, and scalability.

According to Oliver Haya, business manager, and Adam Gregory, software platform manager at Rockwell Automation technology megatrends are enabling new levels of Industrial Edge and Cloud Computing solutions.

"Cloud computing has been growing steadily for years across every industrial vertical. However, the use cases were limited by the costs of applications in the cloud, the challenges of large-scale data from manufacturing, and network security through the plant operations. Many applications that moved to the cloud started as a lift-and-shift of existing on-premises software, significantly limiting the cost benefits and functional value of what the cloud can offer.," Haya and Gregory told the Industrial Ethernet Book recently.

"New applications are taking advantage of containerization and clusters, making them more portable across cloud and edge and easier to scale. These new solutions also become more affordable with cloud-native and edge-native designs, and unlock new value propositions for security, collaboration, and scalability. As modern security models proliferate into the industrial market, it will become easier not only to bring data from edge to cloud, but also to send data, applications, and AI models from cloud to edge."

Benefits of new technology

Haya and Gregory went on to discuss the benefits of this technology and how these megatrends are impacting smart manufacturing.

Today, industrial manufacturing is highly programmed and full of automation, but the future of smart manufacturing requires more autonomy. Building autonomous systems for manufacturing will require new datasets of clean and trusted data, machine learning applied on top of first principles, and ways to manage scaled deployment to distributed automation systems. Data contextualization at the manufacturing edge enables better datasets that can be made more meaningful by merging with engineering data from the cloud.

As the data is used to make better design decisions, new code and models need to deploy securely back to the edge for low latency execution. Who's going to do this? Subject matter experts today are already overloaded, and new engineers often take time to onboard into traditional automation programming tools. Using SaaS can reduce their non-value-added time with automatic software management, seamless onboarding, and GenAI copilots to simplify their life and give them room to innovate toward autonomous operations.

Breaking from the past

"Designing for edge-native and cloud-native applications optimizes in many ways. One of the best aspects of containerized microservices and compute clusters is the ability to scale usage quickly. This makes it easier to get new users and sites running, while also making the adoption more elastic – downsize as you need. Having access across the right users makes it easier to have features that emphasize human collaboration, like SaaS for automation system design that integrates git-based version control and CI/CD pipelines," Haya and Gregory said.

"The evolution of security to support multi-user and multi-device systems, like zero-trust architectures will ensure only the right actors can engage with the control systems and data systems. As the data systems evolve, new AI paradigms will revolutionize access to data for decision making. Putting all of these together is essential to centrally managing distributed automation systems."

Applications and industries

Haya and Gregory said that the first prerequisite to benefiting from edge and cloud solutions is a robust network architecture – without standard IT/OT security measures and enough network bandwidth, the value of edge and cloud may not be fully realized. Across industries, companies that have geographically separated facilities can benefit from cloud, as can small companies without extensive IT support staff.

AI-enabled tools that are designed to run at the edge for better latency and lower cost of compute will enable better prescriptive maintenance and improved process control. Mixing edge and cloud will have benefits for reducing carbon intensity per product and controlling energy costs by optimizing production plans with real time data from equipment, utilities, and weather. Connecting data from the edge with cloud-based digital twins will enable better decision making. Along with digital twins, generative AI co-pilots, enabled by SaaS in the cloud, will have widespread adoption throughout the automation lifecycle.

SOURCE: ISTOCKPHOTO

"Wringing the most possible value out of data is becoming crucial if a company wants to be leading edge. The largest companies in the world were mere startups 25 years ago. Harnessing data propelled their astronomical growth. Data and extracting maximum value from it are now essential for nearly all companies," Dave Eifert, Senior Business Development Manager – IIoT, Phoenix Contact USA.

Future of industrial edge solutions

"While automation has been traditionally comfortable with on-premises computing and enterprise data centers, the emergence of edge and cloud are blurring the lines between these – this will continue to create more hybrid deployments," Haya and Gregory said.

"The fluidity of applications, to be managed from a centralized interface in the cloud while being deployed across many sites, creates a future of software-defined architectures. This will expand the use cases that span edge and cloud to include more design software, more HMI, more MES, more analytics, and more AI/ML deployments. Coordinating versions of PLC code, HMI projects, recipes, and machine learning models from every site into a global corporate discipline will reinforce the learnings and share best practices more easily. Critical to this expansion will be standards-based development, including tools like OPC UA companion specifications and the newly announced Margo Initiative for edge interoperability."

More power at the Edge

Harnessing data can provide impetus and opportunities for growth.

According to Dave Eifert, Senior Business Development Manager – IIoT, Phoenix Contact USA, "more compute power (whether GPUs or enhanced CPUs) provides much more power at the edge. AI models, in some cases, can be trained at the edge, and in most OT-related use cases, can be run at the edge. AI software that is designed for the Edge is changing the paradigm, allowing ML and AI to avoid the latency and cost of making a round trip to an offsite cloud. The nearly limitless power of the Cloud can be harnessed for particularly demanding AI and ML model training. It also can be leveraged for multi-tenant applications or to serve an enterprise that is geographically dispersed."

"Wringing the most possible value out of data is becoming crucial if a company wants to be leading edge. The largest companies in the world were mere startups 25 years ago. Harnessing data propelled their astronomical growth. Data and extracting maximum value from it are now essential for nearly all companies," Eifert added.

He added that, from a technical standpoint, Edge and Cloud computing can be thought of as a way to flatten the communications architecture to a publish-subscribe topology. Data can then be normalized and shared with appropriate applications and people. For example, energy data can be captured and can be synced with production data. It is easy to then see when energy is still being used (wasted) or when production isn't running.

Very importantly, all this same data can then be used to train ML models that can then be run to find anomalies that the human eye cannot detect. This information can lead to effective preventive maintenance and avoid downtime.

Technology innovations

Eifert said that today's Edge and cloud-based systems start with the premise that the data is as important as simply controlling the process. The biggest difference is a streamlining of how to get data from the process to all the places it needs to go to help the operation (business) fully flourish.

"From a technical standpoint, that means going from the hierarchical automation pyramid where the bottom layer is comprised of "dumb" sensors and actuators, up to the PLC level where control occurs. The next layer up is the supervisory (or SCADA) level," Eifert said.

Above this is the Manufacturing Execution System level, and finally the top of the pyramid holds the Enterprise Resource Planning system. In this architecture it is difficult to get data from layer to layer, and to move it horizontally across the layers. The new topology – Publisher-Subscriber allows data producing devices to publish data to a central software hub called a broker. Other devices and applications can subscribe to the broker, creating two-way communications. In this way, the cyber-secure, free flow of data can be established.

Prime applications/industries

Eifert said that all industries are ripe for modernization to digitalization including Edge and cloud solutions. As he stated earlier, data's effective use has tremendous potential value. Not harnessing it is like throwing away valuable currency. This is true of harnessing data's value in real time. Logged data can provide additional usefulness when fed into machine learning models that can provide additional insights that humans cannot identify without the assist given by ML.

"Generative AI can be used in powerful ways, for example, to enable a non-programmer to simply ask or command a machine to give some

SOURCE: ISTOCKPHOTO

"Industrial edge computing focuses on processing data locally close to the source such as machines, sensors, and control systems. This allows for faster decision-making. Cloud computing on the other hand runs applications located in data centers and is well suited for tasks that require extensive data analysis," Vivek Bhargava, Product Marketing Manager at Cisco.

information or perform some action, much as when we interact with our iPhones through Siri," Eifert said.

The future for industrial edge solutions will also contribute to further developments of the IIoT and Industry 4.0.

"Think of the billions of people carrying powerful computers around in their pockets. Most could not program these smart phones, but they can derive benefits through using them in intuitive ways," Eifert said. "The future of Edge and cloud solutions will similarly allow the operator and executive to interact with the machine, the plant, or the enterprise in similarly intuitive ways. Further, machine-to-machine coordination will become mainstream, eliminating human intercession before acting. We'll be wise to walk that path slowly, and eliminate risks and unintended consequences, but we will move in this direction."

Industrial Edge and Cloud

Distinct but complimentary technologies create megatrends by driving innovation.

According to Vivek Bhargava, Product Marketing Manager at Cisco, industrial edge and cloud computing are two distinct but complementary approaches to data processing in industrial environments such as manufacturing plants, or any other location where large amounts of data are generated.

"Industrial edge computing focuses on processing data locally close to the source such as machines, sensors, and control systems. This allows for faster decision-making. Cloud computing on the other hand runs applications located in data centers and is well suited for tasks that require extensive data analysis," Bhargava said.

"As industries look to adopt new technologies to evolve their operations, increase connectivity, derive real-time insights, improve security, and use AI/ML algorithms to improve efficiency, both edge and cloud computing are becoming increasingly important. Both technologies together allow industries to leverage the benefits of both localized processing and large-scale cloud resources," Bhargava said.

He added that software technologies such as Kubernetes and Docker provide containerization allowing for easy portability and scalability across diverse computing environments. Management and orchestration systems enable easy deployment, configuration, monitoring, and lifecycle management of such applications across edge devices. AI/ML aided industrial analytics software operates on large datasets and provides deeper insights for more efficient operations.

Impact on smart manufacturing

"By combining the strengths of both edge and cloud computing, industrial facilities can achieve significant technical advantages. In fact, edge computing may be used to extract production data, transform this data so it's normalized and ready to be consumed, and transport them to cloud resources for a deeper analysis and correlation," Bhargava said.

Another set of technical advantages comes from the ability to reuse your industrial networking devices as compute resources. Although you could deploy server appliances and span network traffic to them for extracting and processing data, it is much more efficient to embed that processing within the network switches and routers that transport the data. By building your industrial network with equipment that can run custom applications, you can increase scalability and achieve simpler architectures by eliminating the need for standalone appliances.

"Industrial edge and cloud computing are transforming manufacturing into a smarter, more data-driven industry. Some of the common benefits include predictive and preventive maintenance by analyzing sensor data, improved quality control with continuous process monitoring, optimized production processes with AI/ML algorithms, and increased sustainability by monitoring and controlling energy usage," Bhargava added.

Bhargava said that what makes edge-computing unique and different is how networking devices are now being mobilized as compute nodes, replacing dedicated hardware resources that were commonly implemented for the purpose in industrial networks. By leveraging switches and routers for computing, you not only avoid dedicated resources, but also make your architecture more scalable and

simpler, and by removing the need for SPAN networks to send traffic to those resources you also reduce your OpEx.

"Today's edge and cloud computing are actively playing a role in making industries smarter. Edge and cloud work together, with edge nodes handling real-time processing and initial analysis, while the cloud provides vast storage, advanced analytics, and machine learning capabilities. For example, data can be preprocessed and filtered at the edge before sending it to the cloud, reducing bandwidth requirements and enabling AI applications," he said.

For example, Cisco provides Cyber Vision, an application that can be loaded into Cisco industrial switches and routers which identifies all connected assets, map communication activities, and assess vulnerabilities through deep-packet inspection (DPI) and active discovery methods. It also continuously monitors assets for any changes in their behavior that could indicate presence of malware. Data from this application can be sent to a cloud portal for further analysis, visualization, correlation, and to determine response.

Another Cisco application allows zero-trust network access (ZTNA) for enforce security policies when remote teams log into industrial assets for configuration, maintenance, or troubleshooting purposes. This is especially useful for geographically dispersed operations.

Industrial Edge and Cloud solutions

Bhargava said that industries across the board can benefit from edge and cloud solutions. The manufacturing sector, for example, can predict failures before they happen and take preventive actions. Real-time decision making can help operations such as autonomous vehicles and robots. Industries like oil and gas or utilities can remotely monitor power generation facilities like wind and solar farms, oil wells, etc.

Cybersecurity is one critical requirement across all industries that stands to greatly benefit from edge and cloud computing. Security applications can now be built into the networking devices, which are in the best position to analyze transiting traffic and derive insights, as explained above.

"Advances in AI can be quite the game changer for many industries. AI algorithms are used to analyze the vast amounts of data generated by IoT devices. Machine learning models can identify patterns and anomalies, enabling predictive maintenance and real-time decision-making. Similarly, AI-powered image recognition is used in quality control processes in manufacturing, as well as in surveillance and security applications in various industries. Natural language processing enables chatbots and virtual assistants to provide human-like interactions," Bhargava said.

SOURCE: ISTOCKPHOTO

"Artificial Intelligence (AI) is set to transform how things get done in almost every area of business and industrial automation will be a key part of this revolution. While the elevated level of excitement surrounding AI may lead to some short-term disappointment in the initial results, the long-term expectations, if anything, are not high enough," Steve Fales, Director of Marketing, ODVA.

IIoT and Industry 4.0

Bhargava said that "industrial edge and cloud solutions are poised to power the next phase of Industrial IoT and Industry 4.0. For example, edge computing will become more deeply integrated with IIoT devices allowing for faster processing and action on the data generated by sensors and machines, leading to more efficient and responsive manufacturing processes."

"As connectivity between machines becomes ubiquitous and networks are updated to transport the vastly increasing amounts of data reliably from edge to the cloud in real-time, it will trigger the development of more complex cloud-based solutions that act with physical processes in real time," he added.

Impact of Artificial Intelligence

Powerful ability to leverage mathematical and programming models.

Steve Fales, Director of Marketing at ODVA said that "artificial Intelligence (AI) is set to transform how things get done in almost every area of business and industrial automation will be a key part of this revolution. While the elevated level of excitement surrounding AI may lead to some short-term disappointment in the initial results, the long-term expectations, if anything, are not high enough. The emergence of large language models like ChatGPT, that can, in essence, guess with an extremely high degree of accuracy what the appropriate grammar and words should be to answer questions for a chat bot application or to create highly accurate language translations, have proven to be the initial 'killer app' showing everyone the value that AI can bring to the table."

Fales said that one of the key drivers behind AI is that the mathematical and programming models that underpin the technology have been built using open-source libraries and easy to use programming languages like Python. This is enabling AI, machine learning, and deep learning to propagate much faster than would otherwise be possible.

"A data scientist can readily take advantage of the technology to build custom models based on the available open-source libraries that can then be trained either on an open source or a custom data set, that can also be proprietary. Large and small companies alike are racing ahead quickly to create solutions that range from generic tools that allow non-data scientists to use AI to custom built solutions for specific applications," Fales added.

Technology benefits

Fales said that industrial automation has been leveraging huge amounts of data at very fast speeds to provide responsive and accurate real time application solutions for many decades now. The control algorithms aren't

SOURCE: SPE

"The future of industrial edge solutions is promising. With all the latest advancements in AI, cloud computing, and data management, the next generation of industry will be more secure and intelligent than ever before," Collin Brown, Field Application Engineer at Red Lion Control.

likely to drastically change any time soon as the loop tuning and controller programs have been optimized over the years by highly skilled engineers. What will change is that the high-level relationships between different devices, machines, applications, and plants can now be better monitored, analyzed, and understood to find opportunities for process improvement. In other words, while micro-level optimization has been done well for some time, macro-level optimization is the new opportunity frontier.

To understand the big picture of a plant, Fales said that it is imperative to look at data differently. While a fast update of data that gets discarded quickly is best for loop tuning, plant wide optimizations will require greater update time intervals and broader sources of data. AI requires large data sets over significant periods of time to identify trends that can then be compared to the current application data to determine both correlation and causality. Additionally, data from seemingly unrelated sources such as the weather, and other time series data that can be scraped from the web, can also provide insights into what is taking place and why. AI models can determine what relationships exist between data from many different sources to help create more accurate predictions. Using large amounts of data from many different sources is referred to as Big Data, which requires using computing capabilities from open-source solutions, such as Hadoop or Apache Spark, to allow the resource intensive calculations to be split up and done across thousands or even millions of servers.

AI creating possibilities

"Processing power and connectivity are the key difference between what is possible today with AI versus in the past," Fales said. You can now have compute resources spread out over the entire internet and be able to get data from the factory floor to the cloud and back fast enough to allow for near real time optimization."

An example is that you can now attach vibration, temperature, and sounds sensors to machinery that will allow an AI model to combine this information with other data such as throughput and quality to predict failure. This can help to replace some of the collective knowledge that takes many years to develop but can also be lost very quickly to retirement.

Additionally, industrial communication networks, such as EtherNet/IP, are adopting solutions such as the Process Automation Device Information Model (PA-DIM) and the OPC UA information model to make sure that data from the factory floor can be easily understood and used by cloud applications. The new pathways from the automation device to the edge, cloud, and back also create new security risks. This has led to device level security solutions such as CIP Security for EtherNet/IP, which allows for data encryption and integrity, device authentication, role-based access, device level firewalls, and more.

Newest Industrial Edge and Cloud solutions

"The hardest, costliest, and most dangerous problems are prime opportunities for AI to solve. Machines that breaking down in the middle of the night when support isn't available, chemical plants where failures can result in environmental disasters, or automotive plant shutdowns that cost millions present compelling business cases to invest the resources to come up with automated models that can help to monitor and proactively solve issues," Fales said.

One of the limitations of AI today is that it is a complicated art and a science. Data scientists must understand data analytics and programming; however, they also need to understand that the choice of model(s) employed, type of data included in the model, the training data used, and the parameters of the model can be the difference between success and failure. For example, having the right data context and metadata to understand how to best use the information in a model is critical.

Fales said that a lot of pre-work needs to be done to make sure that the data is the most useful. This pre-work can involve tried and true database tools such as SQL, which can be easily connected to industrial networks like EtherNet/IP via solutions from ODVA Member Softing. There isn't a clear right or wrong answer because there are many methods to creating a successful AI model. Tomorrow, AI models might not be as sensitive to the design considerations as AI may be able to help build the model itself or there may be significant learnings that take place in the future. However, today, AI requires that a custom model be built for a specific application to generate the precise and accurate results

needed. Once a model is successfully built and deployed though, it can be used indefinitely.

Looking to the future

"The future for AI on the industrial edge will be realized through embedded AI chipsets and models. As more powerful AI chips are developed and the production costs go down the threshold, the return on investment will lower and allow for increased output and quality," Fales said.

Additionally, models over time will become less dependent on designer skill, which will lower the cost of implementing AI and thereby increase the usage rate. Furthermore, when AI models become powerful enough to not only be able to handle new situations and data based on an existing model, but to update the model itself based on the new information then we will see a new era of AI in automation and beyond. While we might have to wait some time for self-designing AI to become possible, there are plenty of amazing solutions available today.

For example, new ODVA Member Elementary uses machine learning and EtherNet/IP data to identify quality issues before a product is shipped. The usage of machine learning allows for new issues to be identified that weren't specifically outlined in an algorithm. In this way, the best of people and machines can be combined, allowing for novel situations to be handled with relative ease while allowing for a production line to go faster than a person could ever handle. With data being analyzed in quantities and at speeds never before possible via AI, resulting in the identification of new trends and information, significant productivity improvements are on the horizon that are poised to pave the way for a new era of prosperity.

Importance of MQTT technology

More streamlined data collection and method for effective interface to the cloud.

According to Collin Brown, Field Application Engineer at Red Lion Control, technology megatrends such as use of MQTT is enabling Industrial Edge and Cloud Computing innovations.

"From a Red Lion perspective, MQTT has been one of the most widely adopted technologies in the cloud computing space. MQTT is a lightweight publish-subscribe, machine to machine network protocol for message queueing. This technology has allowed for more streamlined data collection and provided a simple and affordable method of getting one's data to the cloud," Brown said.

"Industries who harness vital data can use MQTT to safely transmit data back to the cloud where it can be stored, interpreted, and visualized. Having all this data in the cloud allows for better predictive maintenance, improved decision-making, and enhanced safety/hazard detection. The introduction of 5G has been essential for the development of these new cloud technologies. 5G offers high bandwidth and low latency, enabling faster data processing and response times. 5G is not just faster than 4G, there is much more to consider. 5G can handle more devices by offering a high capacity for connectivity. With 4G, the connection played as a "one size fits all," whereas with 5G, depending on the needs of the device, the network energy consumption can be "throttled" for a more efficient output."

Industrial Edge technology benefits

Brown said that "utilizing an industrial edge in your application simplifies the collection, handling, and analysis of data from industrial devices. This will not only allow insightful decision-making, but also keep IT efforts and costs at a moderate level. Data being computed in the cloud allows for real time information, better record keeping, centralized device management, and remote visibility."

He added that a well-designed cloud system that monitors itself adds convenience, comfort, and peace of mind. Cloud computing offers several benefits over traditional computing. To start, integrating cloud computing into your application adds scalability. Since there is no longer a need for hardware, companies can expand their IT infrastructure by simply setting up virtual servers. This provides secondary advantages, such as cost reductions, increased flexibility, and improved mobility. Given that cloud computing centralizes assets, collaboration becomes easier for people who may only be able to remotely access data. Utilizing this technology also decreases a company's carbon footprint since physical servers are no longer necessary.

"One unique modern-day technology that drives cloud computing is virtualization. Virtualization is a technology that creates virtual representations of physical machines, such as servers, storage, and networks, using software that simulates hardware functions. These virtual assets require less construction, less physical materials, and can be created anywhere with an internet connection. In the past, to add machines to your application, you would need to buy a new dedicated device," Brown said.

This pattern leads to many complications such as device license management, device compatibility, and additional power requirements. With the integration of virtual assets, these headaches quickly go away. These now "software defined" appliances can run on the same platform, taking advantage of the hardware we already own. These virtual assets can be containerized, further adding security to one's application. If one of the assets needs to be updated, rather than shutting down the entire system, you can simply stop that specific container and proceed with the update process. Moving toward virtualized systems helps keep convenience and security high without sacrificing functionality.

Prime applications/industries

"Industries in remote locations have begun to gain value by making use of cloud solutions. Data that was once stranded locally can now be safely backed up off site. Specifically, the oil and gas industry have strict regulations they must abide by in order to continue operations. With new cloud technology, this indispensable data can now be protected from local memory corruption or loss of connectivity. AI is playing a significant role in the development of new industrial cloud solutions by enabling advanced capabilities that enhance efficiency, productivity, and decision-making," Brown said.

He added that predictive maintenance has seen huge benefits using AI algorithms to analyze data from industrial equipment, predicting maintenance needs before they occur. Difficult tasks such as energy management can even use AI to analyze consumption and optimize usage. With sustainability being one of the big three facets of Industry 5.0, this technology will speed up meeting sustainability goals without the need for additional manpower. Lastly, AI can be a powerful cyber security tool. Using AI to detect anomalies in real-time leads to faster response times and will overall enhance the cybersecurity of an application.

"The future of industrial edge solutions is promising. With all the latest advancements in AI, cloud computing, and data management, the next generation of industry will be more secure and intelligent than ever before," Brown said. "Industry 4.0 at its core is based around connectivity. As more industrial edge solutions make their way into applications, industry 4.0 tech will become easier and more affordable for companies to integrate into their day-to-day operations. As the industrial edge evolves, it continues to focus on these key factors that can be the make-or-break for companies who chose to add this tech to their systems."

As we start to see this tech work successfully, there will be more demand. More demand leads to more money and time invested in moving this technology forward, resulting in better cybersecurity and resource management.

"All these factors come together to create an industrial edge that helps companies not only collect data from their applications, but also get the most use from it. Data is no longer trapped at the ground level, with these new advancements, we will start to see data being further accessed, connected, and visualized," he added.

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

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.

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 ethernet book

Industrial Networking & IIoT

Enabling smart manufacturing with private 5G communications

As smart manufacturing continues towards Industry 4.0, the role of private 5G networks becomes increasingly pivotal. Moxa's contributions in mitigating pain points and providing robust solutions position the company as a key player in shaping the future of connectivity in smart manufacturing.

SOURCE: MOXA

Private 5G not only enables wireless connectivity but also paves the way for a smarter, more agile, and secure industrial ecosystem. The unique benefits of private 5G, such as dedicated network frequencies, enhanced stability, and secure local data storage, align seamlessly with the specific requirements of smart manufacturing applications.

THE EMERGING WORLD OF SMART manufacturing has been made possible by the tremendous amount of data that can be transmitted and processed today. As real-time monitoring and control increase efficiency and return on investment, the Industrial Internet of Things (IIoT)-enabled factory floor can also embrace large-scale, cost-effective customization at short notice, delivering a competitive edge for many industries.

To build truly automated, intelligent, and robust industrial applications, communication capabilities must meet a set of stringent requirements. 5G networks, boasting unprecedented speeds, check all the boxes. With extensive capabilities, private 5G is perfect for building robust connectivity in manufacturing applications.

Not only does a private 5G network architecture offer smart manufacturing all the benefits of a 5G cellular network, such as high bandwidth, low latency, and extensive IIoT capabilities, it also features dedicated network frequencies to avoid interference from other cellular signals. As a result, private 5G networks offer improved stability and security, allowing data to be stored locally and privately, rather than on a shared public network.

This article discusses the industry trend towards adopting wireless networks in manufacturing, how smart manufacturing can benefit from private 5G, the specific pain points of implementing private 5G in the industrial context, and how the latest private 5G solutions on the market help overcome these challenges.

Industry is going wireless

With the manufacturing industry moving towards Industry 4.0 and Lighthouse Factories, the amount of data transmitted using wireless technology is increasing annually and "going wireless" has become a topic of discussion in the automation industry. Therefore, in key regions promoting smart manufacturing, local governments have already designated dedicated frequencies for 5G private networks, including the United States (n48), Germany (n77), Australia (n77), Japan (n79), South Korea (n79), and Taiwan (n79). These frequencies are reserved for specific regional use and prevent wireless instability caused by interference from public network frequencies. In addition, some regions, such as China, also leverage frequencies from telecom providers for private 5G networks.

According to the Private 5G Network Market Size, Share & Trends Analysis Report (2023), the private 5G network market size accounts for US$2 billion and is expected to grow to US$36 billion by 2030, achieving a compound annual growth rate (CAGR) of 51%. These projections show a positive outlook and substantial market potential for private networks that warrants more investment.

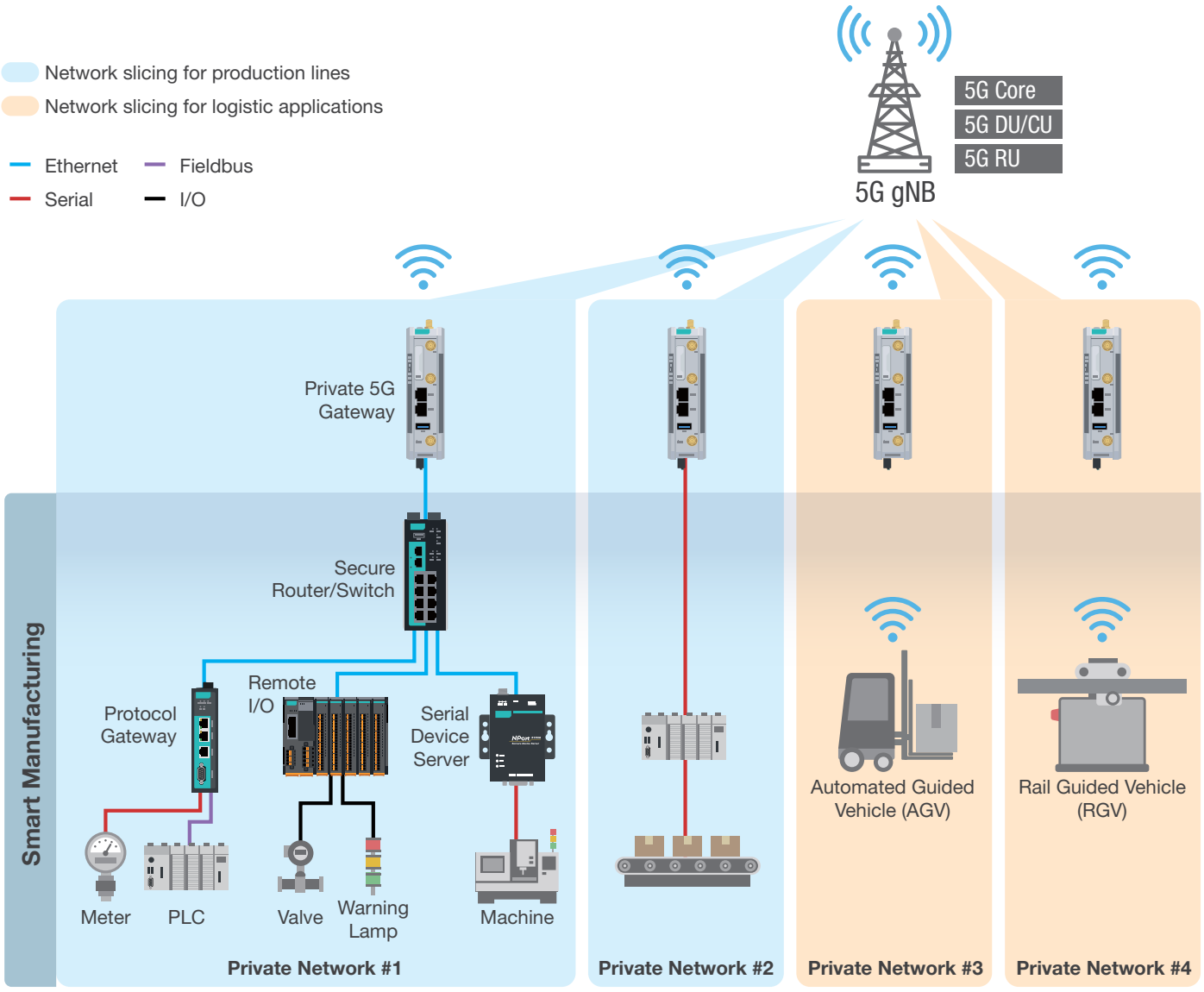


Figure 1: Private 5G networks in smart manufacturing applications.

Well-known electronic device brands and manufacturers worldwide are already developing their own 5G dedicated equipment, such as central units (CU), distributed units (DU), and radio units (RU) in the Open Radio Access Network (ORAN) framework. This trend is driven by the recognition of the extensive applications of 5G in the market and the development of its architecture. One of the primary applications is private 5G.

Private 5G benefits for smart manufacturing

Smart manufacturing has unique security and stability requirements that can benefit substantially from private 5G architecture. Private 5G provides dedicated network frequencies to ensure stable signal performance without interference from other public frequencies. It also offers a customized network environment to provide the most suitable connectivity and security for specific areas. Importantly, it ensures that all data is stored locally, rather than on a public network that can be easily compromised. For example, hackers could intercept data transmitted over a public network, or infiltrate a vulnerable network and gain unauthorized access to sensitive data.

Examples of current private 5G applications in smart manufacturing include fixed-point programmable logic controllers (PLC) as well as mobile transportation carriers, such as automated guided vehicles (AGV), automated mobile robots (AMR), and rail guided vehicles (RGV).

Industrial 5G gateways on the market often emphasize support for multiple interfaces for versatility, leading to more complex equipment architectures and bulky sizes. However, this emphasis overlooks manufacturing customers' need for compact 5G equipment with low power consumption.

Through decades of experience in industrial automation and networking, Moxa has identified key pain points and requirements for overcoming the technical challenges of implementing private 5G networks used in smart manufacturing.

Private 5G pain points

The first major obstacle to successfully deploying a private 5G network for smart manufacturing is reconciling information technology (IT) and operational technology (OT) priorities. These two domains are often at odds as IT emphasizes high security whereas OT prioritizes high availability. For example, in OT systems, production capacity and occupational safety take precedence over cybersecurity. Manufacturers cannot afford the impact of strict cybersecurity measures on production line operations, which can lead to a decrease in production capacity. Therefore, it's important to perform an on-site analysis to gain in-depth insights into the manufacturing processes and OT network architecture and take stock of production line assets. This requires understanding the genuine needs of

SOURCE: MOXA

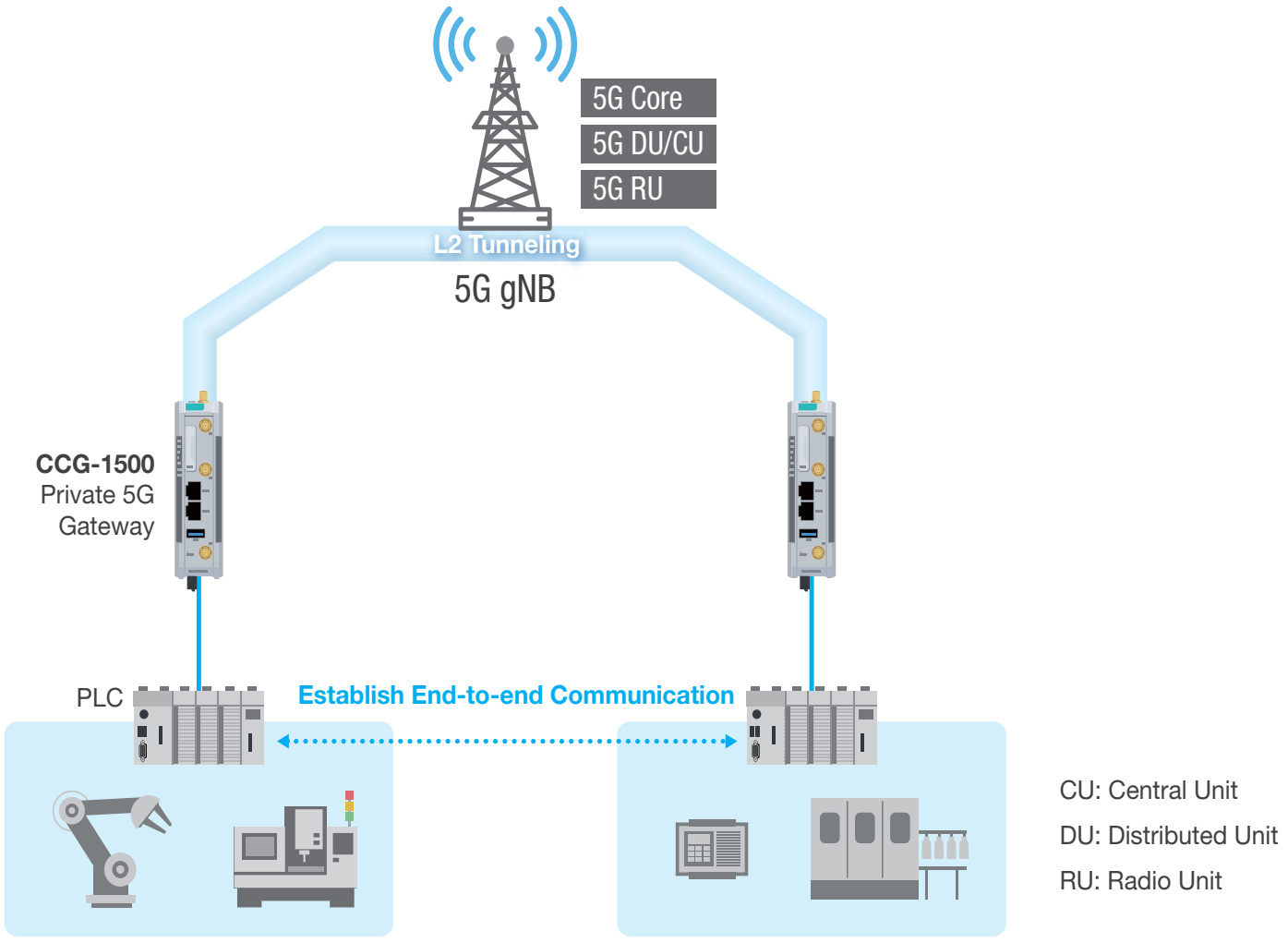


Figure 2: Layer 2 tunneling for end-to-end communication over a private 5G network.

customers on the OT side and translating them into a language that IT can process, with the goal of establishing an intelligent system that combines efficiency and security.

However, understanding the differences between OT and IT is only the first step. System integrators still need to overcome several challenges to implement industrial private 5G, including infrastructure deployment, device and endpoint management, and integration with existing systems.

1. Infrastructure deployment: To use private 5G, integrators will need to construct the necessary infrastructure, including 5G gateways, base stations, 5G core networks, and Multi-access Edge Computing (MEC). These devices are costly and have a high technical threshold that requires experienced professionals to deploy. Because all 5G deployments are unique, each site requires a customized configuration that cannot be easily copied to other sites.

2. Device and endpoint management: Managing various devices and endpoints within a private 5G network is complex. This often involves using customized software to manage all 5G devices, handling tasks such as authentication, firmware updates, status monitoring, and viewing historical messages.

3. Integration with existing systems: Communication protocols used by industrial equipment predominantly operate at the Layer 2 level, whereas 5G architecture works in Layer 3 and above with IP functionality. Therefore, IT professionals face the challenge of enabling 5G communication to support Layer 2 packet pass-through.

Moxa solutions

Whether building a 5G network for smart industry or implementing other OT/IT convergence projects, system operators are looking for the most efficient way to overcome pain points while lowering deployment costs.

When integrating diverse OT devices, factory engineers can leverage Moxa's vast portfolio of serial communication products to connect a wide range of field devices. For many years, Moxa has specialized in establishing industrial communications for OT equipment, such as terminal PLCs, meters, and sensors using a wide range of protocol gateways, remote I/Os, and serial converters. Fully embracing the new 5G era, Moxa is now helping simplify the integration and transmission of data communications from these OT devices to 5G cellular networks through Moxa's private 5G gateways.

Compact and energy-efficient

Moxa's CCG-1500 Series private 5G cellular gateways pack powerful performance in a compact form factor, measuring only 100 x 125 x 35 mm. Featuring customizable network settings and built-in redundancy with automatic SIM card switching, the CCG-1500 Series delivers outstanding field performance and stable network connectivity.

Moreover, the CCG-1500 Series' low power consumption (average 8 W) allows for better battery life and fewer power inputs, reducing maintenance and operating costs over the product's lifetime. These features are especially important for remote deployments where power efficiency is key.

IIoT compatibility and performance

Designed as both a media and a protocol converter, the CCG-1500 Series is ideal for IIoT applications. Its 5G-to-Ethernet and 5G-to-serial conversion capabilities support both public and private networks and streamline

SOURCE: MOXA

Private 5G not only enables wireless connectivity but also paves the way for a smarter, more agile, and secure industrial ecosystem. The unique benefits of private 5G, such as dedicated network frequencies, enhanced stability, and secure loc Moxa's CCG-1500 Series al data storage, align seamlessly with the specific requirements of smart manufacturing applications.

OT (Ethernet and serial) to private 5G data transmissions. Dual-SIM redundancy offers industrial-grade reliability for uninterrupted connectivity. Wide temperature models are available for extended temperature applications. All CCG-1500 Series models are thoroughly tested in a testing chamber to ensure reliable 5G performance in wide-temperature environments.

Ethernet frame tunneling with Layer 2 data packets

Moxa's private 5G solutions enable Ethernet frame tunneling services, making it possible for Layer 2 data packets to be transmitted over the 5G network as end-to-end (E2E) communication between two or more terminal devices. Seamless E2E communication allows data packets from the central control to reach end devices securely over a private 5G network, saving time and resources otherwise spent managing devices on-site.

Accessories to boost performance

Prior to the official launch of the CCG-1500 Series, Moxa conducted proof-of-concept (PoC) verifications with several major customers and found that many factories often ignore the potential signal interference caused by operational equipment or metal partitions when deploying their private 5G infrastructure. This oversight can result in poor signal quality and attenuation, as well as additional costs by having to deploy more radio units (RUs) to maintain signal quality.

Moxa offers additional accessories to optimize the performance of the CCG-1500 Series private 5G gateways. The LNA-1000 Series low-noise amplifiers (LNA) strengthen reception quality and support 5G cellular bands. Meanwhile, the BST-1000 Series signal boosters enhance signal output power and support the n48 and n78 bands.

Moxa's CCG-1500 Series

Moxa's BST-1000 Series is the first signal amplifier on the market to support TDD Duplex mode. The BST-1000 Series can enhance the signal strength and signal transmission distance of CCG-1500 Series 5G gateways by up to 50%. In environments with heavy signal interference, the BST-1000 Series helps enhance the signal to ensure a stable connection to the cellular base station.

Network oversight and management software

A private 5G network needs to be constantly monitored and maintained for optimal performance. Moxa's Device Lifecycle Management (DLM) software allows trained IT and OT operators to perform device management. With support for the Open Mobile Alliance (OMA) LwM2M protocol, DLM makes it easy for administrators to have a centralized view of the network and identify potential issues quickly. With DLM, users can perform secure software updates, monitor the network status, access logs, troubleshoot, and perform other network management functions all in one place.

Summary

As smart manufacturing continues towards Industry 4.0, the role of private 5G networks becomes increasingly pivotal. Moxa's contributions in mitigating pain points and providing robust solutions position the company as a key player in shaping the future of connectivity in smart manufacturing.

Private 5G not only enables wireless connectivity but also paves the way for a smarter, more agile, and secure industrial ecosystem. The unique benefits of private 5G, such as dedicated network frequencies, enhanced stability, and secure local data storage, align seamlessly with the specific requirements of smart manufacturing applications.

Moxa, with its comprehensive suite of products and decades of expertise, addresses the 5G migration challenges by offering compact and energy-efficient solutions like the CCG-1500 Series private 5G gateway.

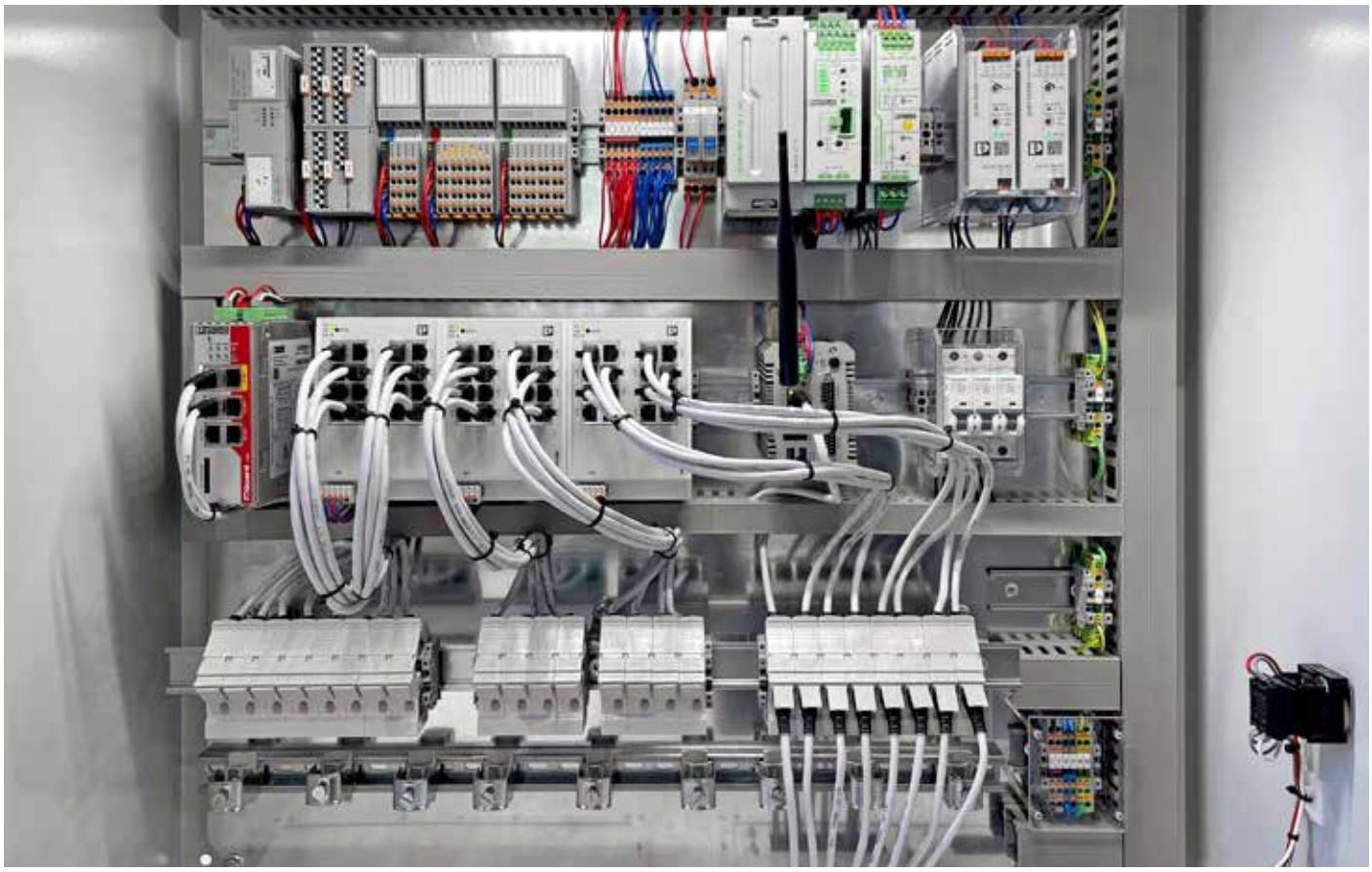
The inclusion of features such as Ethernet frame tunneling for end-to-end communication, signal booster and low-noise amplifier accessories, and network oversight and management software show Moxa's commitment to providing reliable and tailored 5G solutions for the industrial sector.

Jun CH Wang, Product Manager Industrial Wireless Division, ***Moxa Inc.***

Learn More

Smart edge computing: optimizing the entire value chain

Edge devices based on PLCnext Technology combine the robustness of proven industrial PCs with an open automation platform and intelligent IoT edge concepts can be built with this approach. By using edge devices to process and analyze the growing volumes of data, the entire value chain can be optimized.



SOURCE: PHOENIX CONTACT

The edge device sorts large volumes of data without major delays and close to the point of origin.

THE TERM EDGE COMPUTING IS INEXTRICABLY linked to the term cloud computing. While cloud computing – i.e., the connection of systems to the Internet – has been gaining in importance for several years as part of the future-oriented Industry 4.0 project, edge computing seems to be a relatively new technology. The possibilities of this approach will be demonstrated using the EPC 1502 edge device.

An Internet connection to link the system to a cloud is often necessary when data volumes need to be evaluated and stored. In many applications, however, the data must be collected, checked, and fed back into the process in very short cycles. Whenever this is the case, a public cloud solution is not suitable – simply because of the latency times on the Internet. Edge computing is therefore increasingly being used for such smart applications. The edge devices from Phoenix Contact, which are based on the PLCnext Technology ecosystem, combine the robustness of proven industrial PCs with the open automation platform. Intelligent IoT edge concepts can be built with this approach. By using edge devices to process and analyze the growing volumes of data, the entire value chain can be optimized.

Easy to integrate box for collecting local data

The range of applications for edge devices is broad, as potential applications can be found wherever data needs to be analyzed or is already being analyzed in the cloud. At the beginning of the development of every edge application, the user always asks the same question: how can the data be accumulated centrally?

Developing autonomous vehicles, a traffic light system, or intelligent thermostats that would benefit from the power and responsiveness of an edge computer can be a complex undertaking. Above all, the edge device used must be flexible. In addition, a large amount of system data, which is usually provided by numerous different sensors from various manufacturers, must be collected. Furthermore, the field devices communicate via a wide range of industry protocols. And what is more, the data is often analog, which cannot be accumulated easily.

The tailor-made Edge Collection Box from Phoenix Contact is therefore ideal for collecting local data. The switchgear and controlgear assembly collects digital, analog, and temperature signals via the connected sensors. The box can be easily integrated into an existing production environment. The data is captured in parallel so that, for example, the CE marking of the machines is not invalidated. The main component of the Data Collection

SOURCE: PHOENIX CONTACT

The Data Collection Box from Phoenix Contact for easy data collection in existing systems without jeopardizing the CE marking of the machines.

Box is the EPC 1502 PLCnext Control with an IIoT framework. Energy and process data can be collected easily via the framework based on the familiar industry-standard communication protocols.

SOURCE: PHOENIX CONTACT

The EPC 1502 edge computer from Phoenix Contact with a large data storage system, high-performance hardware, and unconventional interfaces compared to a traditional PLC.

Secure Data Box as a secure interface to higher-level IT systems

Once the data has been collected and analyzed locally via the edge device, the device then often serves as an intermediate layer to the cloud. While collecting data in existing systems may already be difficult, potentially there is an even greater task to be solved: how can the summarized data, evaluated alarms, and edge device analyses be transferred securely to the cloud?

This is where another integration-capable solution from Phoenix Contact comes in: the Secure Data Box is designed for use in combination with the Data Collection Box switchgear and controlgear assembly. It establishes the secure interface between the production network and higher-level IT networks, external service providers, and cloud systems. Unauthorized access is blocked by the firewall of the integrated FL mGuard security router. The firewall only allows the necessary data traffic, ensuring optimum protection of the segmented network. Optionally, the EPC 1502 edge device can also be accessed directly via the mGuard Secure Cloud app. With this approach, the user receives all information regarding remote maintenance.

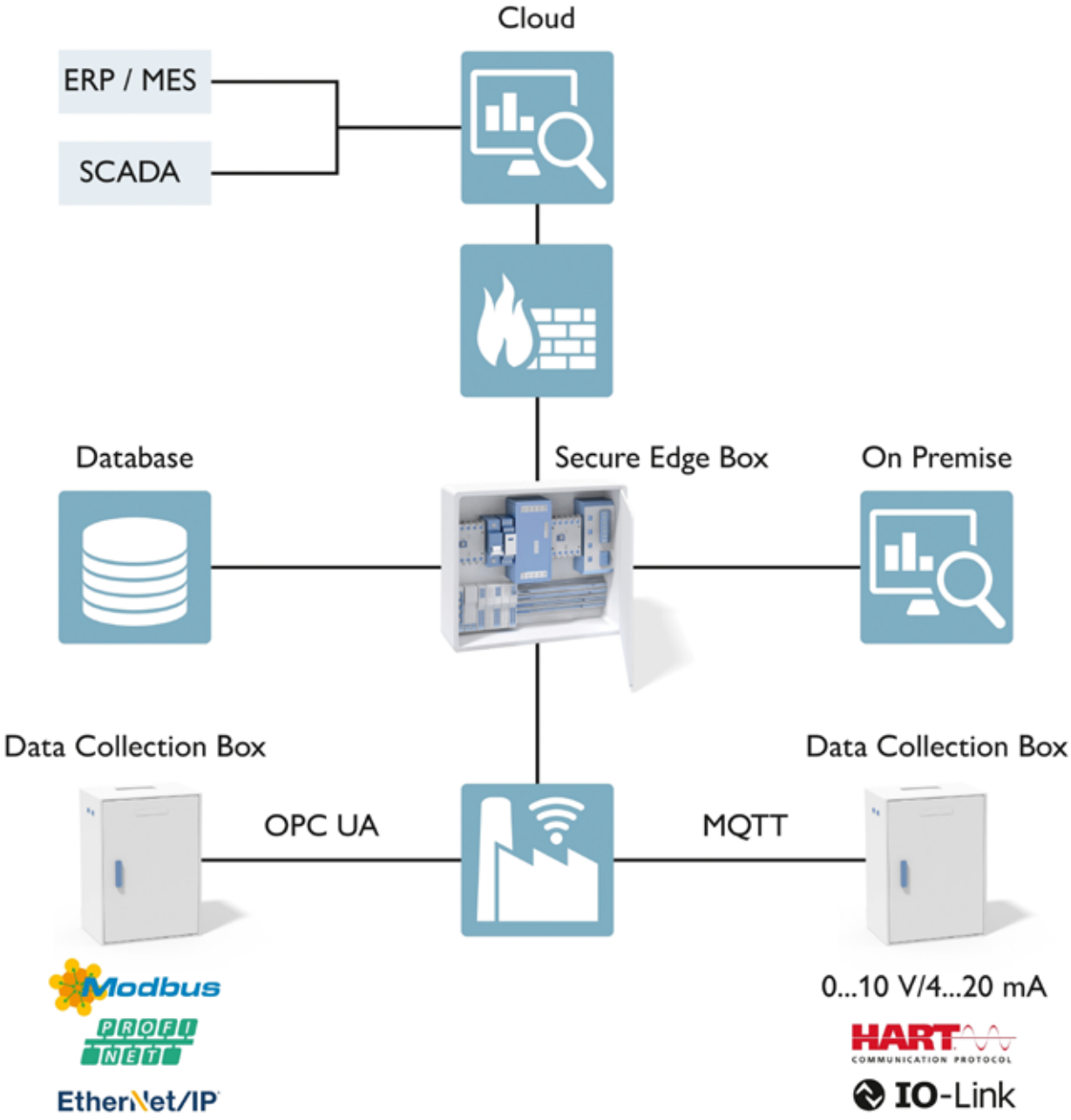
Reliable operation of automated guided vehicle systems

Back to the application examples cited: what added value would the use of the edge device in an automated guided vehicle system (AGVS) bring, for example? The openness of the edge device bridges the gap between classic control functions and AGVS navigation. A quick connection to existing navigation solutions can be realized with a plug-and-play interface for the Robot Operating System (ROS). With support for high-level language programming, the ROS interface, and Docker software, users can also implement their own approaches directly on the edge device. The PLCnext Technology online store includes a wide range of apps that enable the edge device to send firmware and application updates to all other controllers as well.

The device installed at the "edge" of the network thus provides a simple and secure entry point for remote maintenance of the entire system. The collected data can be displayed locally via dashboards. Artificial intelligence and its algorithms analyze data points to detect anomalies. This creates the basis for predictive maintenance, as the solution warns of failing drive shafts or motors at an early stage.

This enables immediate repair, which in turn minimizes production downtime. With the atypical interfaces, which are not usually

SOURCE: PHOENIX CONTACT



Interaction between the Data Collection Box and Secure Edge Box for securely visualizing data locally and sending it to the cloud via a VPN tunnel.

provided by a traditional control system, data can be forwarded directly via WLAN, which saves on laying cables. The large internal data storage system means that data can be stored locally over a longer period of time. Edge devices are therefore often essential for the reliable operation of automated guided vehicle systems and the associated efficiency and flexibility.

Wide range of possible uses in large and small applications

Edge computing can be utilized in different ways in different individual applications. The combination of ready-to-install edge boxes can significantly simplify the implementation of large systems with considerable amounts of data that need to be collected using different protocols. Existing systems can be converted to edge computing easily with the integration-capable solutions that are installed outside the machines, meaning that they retain their CE marking. In smaller systems, the edge device must bring benefits with many supported protocols and apps for functional extension so that the user receives added value with simple installation.

Scalable solutions from single source

In addition to a device with sufficient computing power and connectivity, system manufacturers who do not yet have an in-house solution for realizing an edge application also need the right software environment. With the combination of hardware and software in a ready-to-install product, the EPC 1502 is tailored to the essential requirements of an edge application. The device can also be extended with additional apps.

For existing systems, easy-to-use tailored solutions are required to generate added value from the analysis of the data without losing the CE marking during the necessary conversion.

Phoenix Contact provides scalable solutions, from the high-performance VL3 UPC industrial PC and the EPC 1502 edge computer, through to ready-to-install data boxes for easily collecting data and transferring it securely to cloud systems. By processing the resulting data directly at the point of origin, every application benefits.

Daniel Mantler, Product Management HMI/IPC, ***Phoenix Contact****.*

Visit Website

Operational virtualization a challenge for industrial networks

Breaking down information and data silos by combining information technology (IT) and operational technology (OT) helps companies significantly increase their performance, productivity, flexibility, and sustainability.

SOURCE: SIEMENS

Secure communication and data exchange between Information Technology (IT) and Operational Technology (OT) are the backbone of digitalization.

IT/OT CONVERGENCE MEANS THAT THE REAL world of automation merges with the digital world of IT. However, it is important to note that industrial networks in OT and office networks in IT have very specific requirements that must be taken into account when connecting the two worlds to ensure a reliable data exchange.

This also applies to new trends such as virtualization. In recent years, the virtualization of servers has established itself as the standard in the IT environment. Companies have realized that by consolidating servers, they can increase their efficiency and reduce costs.

Now a similar trend is emerging in OT, in which not only servers, but also programmable logic controllers (PLCs) and industrial PCs are to be virtualized. But what does the network architecture look like that is to form the basis for meeting the requirements of this technology?

Server virtualization is basically a technology that allows the setup and operation of multiple virtual servers on a single physical server. This ensures the efficient utilization of hardware resources by abstracting the underlying physical infrastructure and enabling the dynamic allocation of computing power, memory, and storage to virtual machines (VMs). On the other hand, PLC virtualization involves abstracting the physical PLC hardware and running multiple virtualized instances of controllers on a single physical device. SCADA applications can also be migrated from physical devices onto VMs.

Advantages for OT virtualization

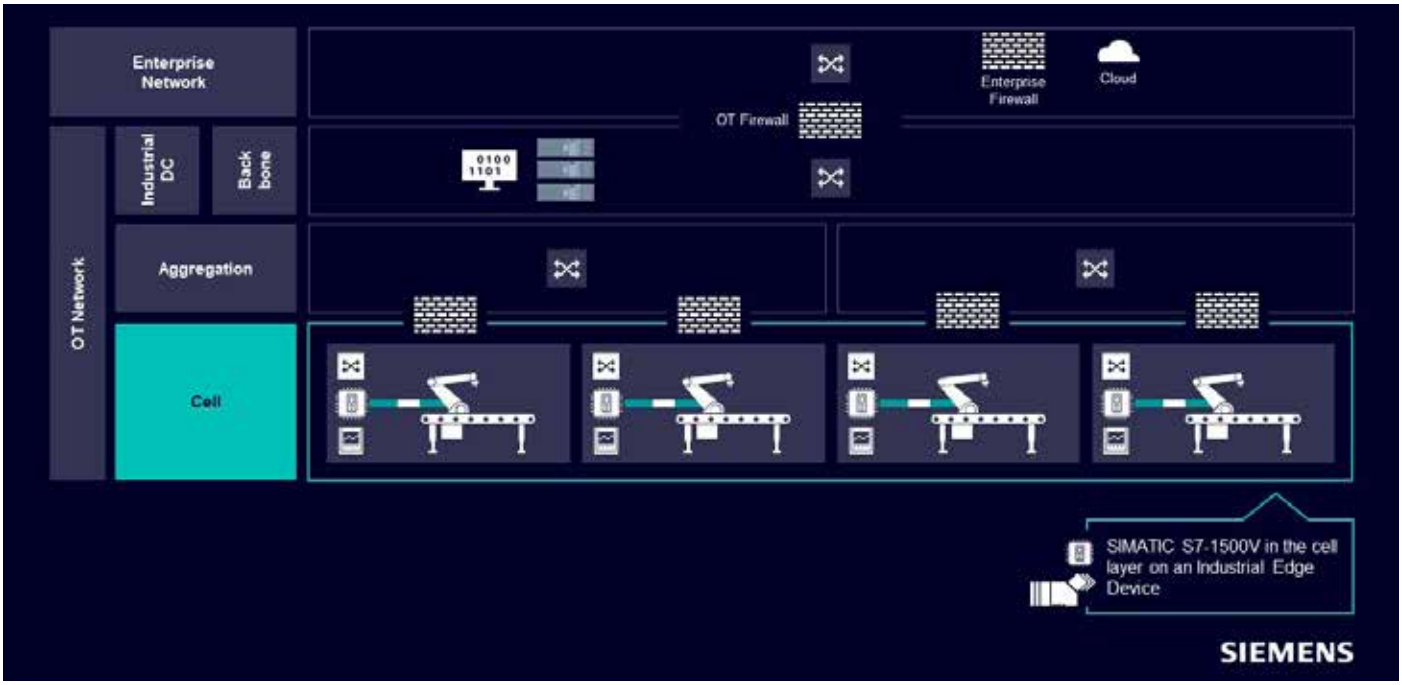
Virtualization offers several advantages in the OT context. One of them is cost savings. By virtualizing servers and PLCs, companies can consolidate their hardware infrastructure – thus reducing the number of physical devices needed. This consolidation results in cost savings in terms of hardware procurement, maintenance, power consumption, and space requirements. Ultimately, this also promotes the sustainability aspect of companies.

The efficient use of resources is a second advantage of virtualization in OT. By dynamically allocating computing resources such as processors (CPUs), memory, and storage based on demand, companies can optimize the resource utilization. This ensures that resources are used efficiently.

Flexibility and scalability are also improved through virtualization. VMs can be easily created, cloned, and migrated, allowing companies to quickly adapt their production to changing operational needs. In addition, this scalability improves the efficient resource allocation and the ability to scale the system up or down as needed.

Simplified management is a fourth advantage of the virtualization. Centralized management tools and platforms optimize the management, configuration, and monitoring of virtualized servers and PLCs. This centralized control improves the operational efficiency and reduces the complexity of managing a large number of physical devices.

The virtualization also provides a secure and isolated environment for testing and development purposes. Virtualized servers



SOURCE: SIEMENS

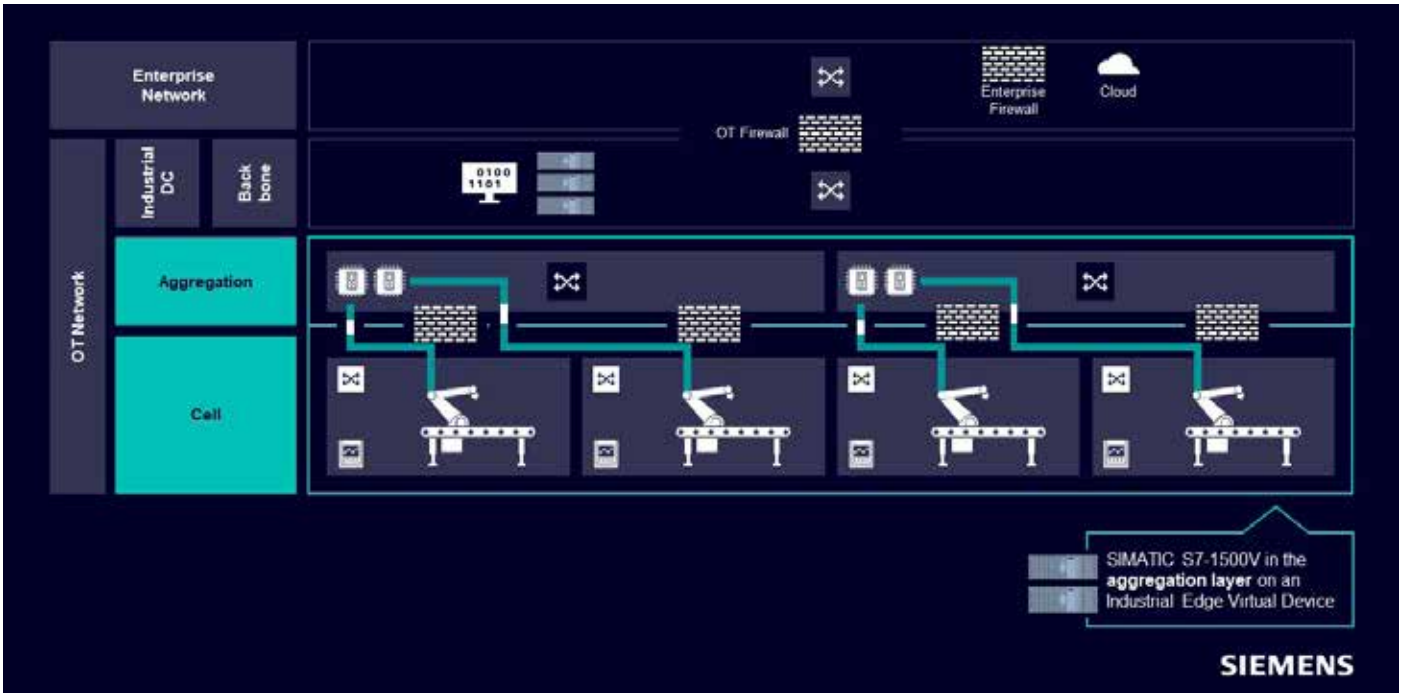
All applications and PLCs of a single machine or production cell are consolidated on an industrial PC within the existing environment. In this case, the requirements for the network change only at the cell level.

and PLCs can be replicated, allowing the creation of separate environments to test new applications, configurations, or updates without impacting the production environment. Production downtimes or even planned outages during maintenance windows can thus be reduced.

Although virtualization offers numerous benefits, it is important to carefully plan, configure, and consider specific OT requirements such as real-time capabilities, high availability, and functional safety. When implemented effectively, virtualization can therefore significantly improve the efficiency, flexibility, and reliability of OT systems.

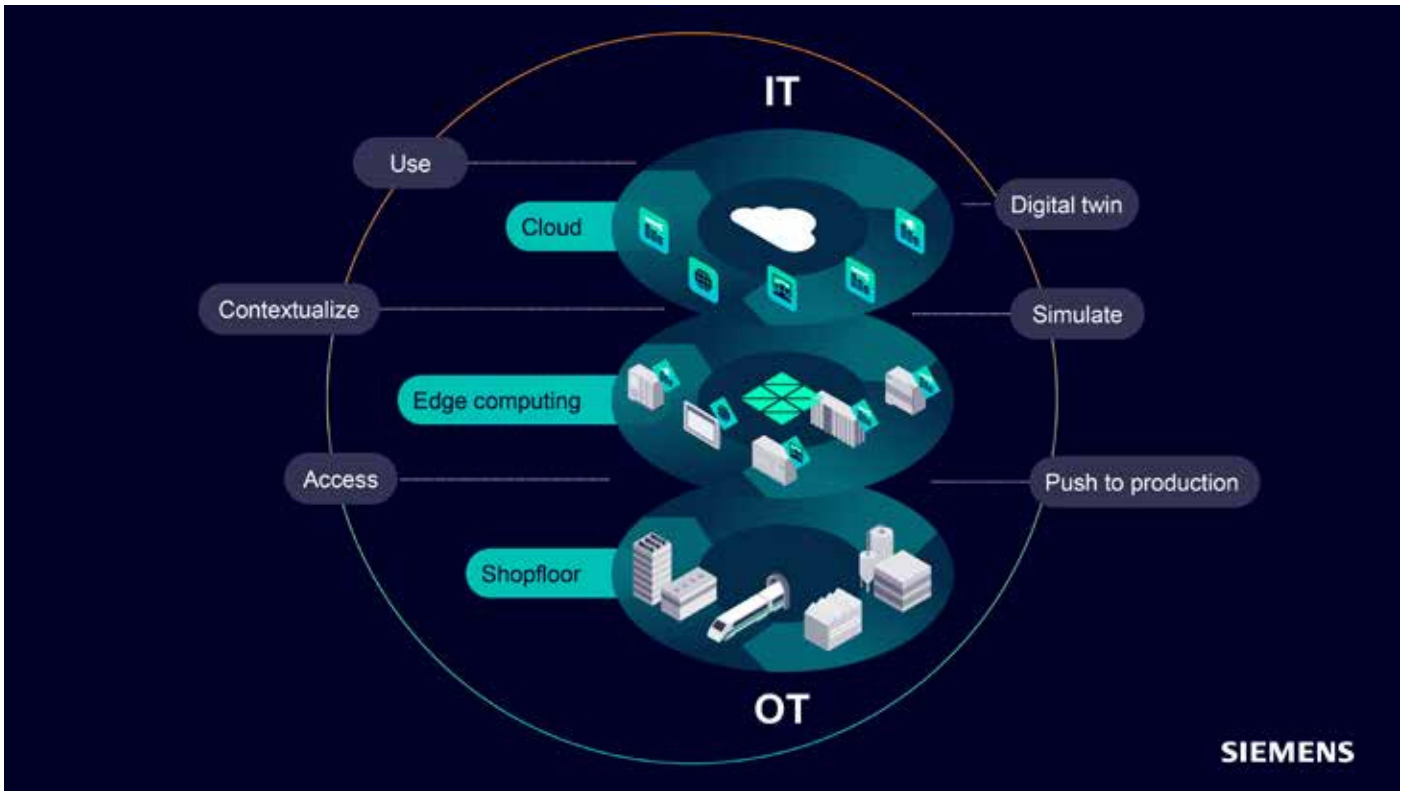
Virtualization as a Service and further solutions

As one of the leading industrial software companies, Siemens has proven expertise in complex OT environments and, with SIMATIC Virtualization as a Service, offers a perfectly coordinated, hardened, system-tested, and preconfigured virtualization platform for industry. Ready-made virtual machines can run on it – including the new SIMATIC S7-1500V, a virtual PLC (vPLC). This vPLC is available in the Industrial Edge ecosystem as an Industrial Edge app and enables the virtualization of PLCs in OT environments. The configuration will continue to be supported in the TIA Portal. This allows companies to seamlessly integrate the vPLC into their automation solutions, and efficiently implement their projects with the support of the TIA Portal.



SOURCE: SIEMENS

For better use of virtualization, it is necessary to consolidate the applications and PLCs of a production area or a production line. Consolidation at the aggregation layer increases the demands on the availability, scalability, and real-time capability of this network layer.



SOURCE: SIEMENS

The underlying know-how differs between IT service providers and OT experts. To bring both worlds together, Siemens offers corresponding training, services, and solutions consisting of hardware and software.

For a successful introduction of virtualization in OT, it is important to consider a network concept that is aligned with the virtual automation and provides optimal performance and investment protection. The implementation of a network concept based on network components from the SCALANCE family and SINEC software tools for network management offers stable connectivity and seamless integration with Siemens' industrial automation systems. This helps to ensure reliable and efficient communication between the virtual and physical devices in the OT environment, promote smooth operations, and maximize the benefits of the virtualization.

Location of the virtualization environment

When planning a network for modern manufacturing, the location of the virtualization environment should be taken into account. In the simplest case, all applications and PLCs of a single machine or production cell are consolidated on an industrial PC (IPC) within the existing environment. The requirements for the network change only at the cell level. When selecting the virtualization environment, attention should be paid to real-time capability in terms of program processing, but also in terms of the network. In particular, the data exchange between SIMATIC S7-1500V and the actuators and sensors via PROFINET places high demands on this.

In order to make even better use of the advantages of virtualization, it is necessary to consolidate the applications and PLCs of a production area or a production line. In this case, there are other points to consider. Consolidation at the aggregation layer increases the demands on the availability, scalability, and real-time capability of this network layer enormously.

For instance, a failure of a network connection lasting less than 10 ms could lead to a failure of the PROFINET communication with all virtual controllers – thus causing a failure of the entire production plant. Furthermore, it should also be noted that due to the consolidation of the automation technology, a very large number of PROFINET devices communicate via the aggregation network, and therefore the scalability of this network layer plays a major role. But also cybersecurity aspects and those of the functional safety need to be examined more closely in this case.

The availability of the network is the basis for success

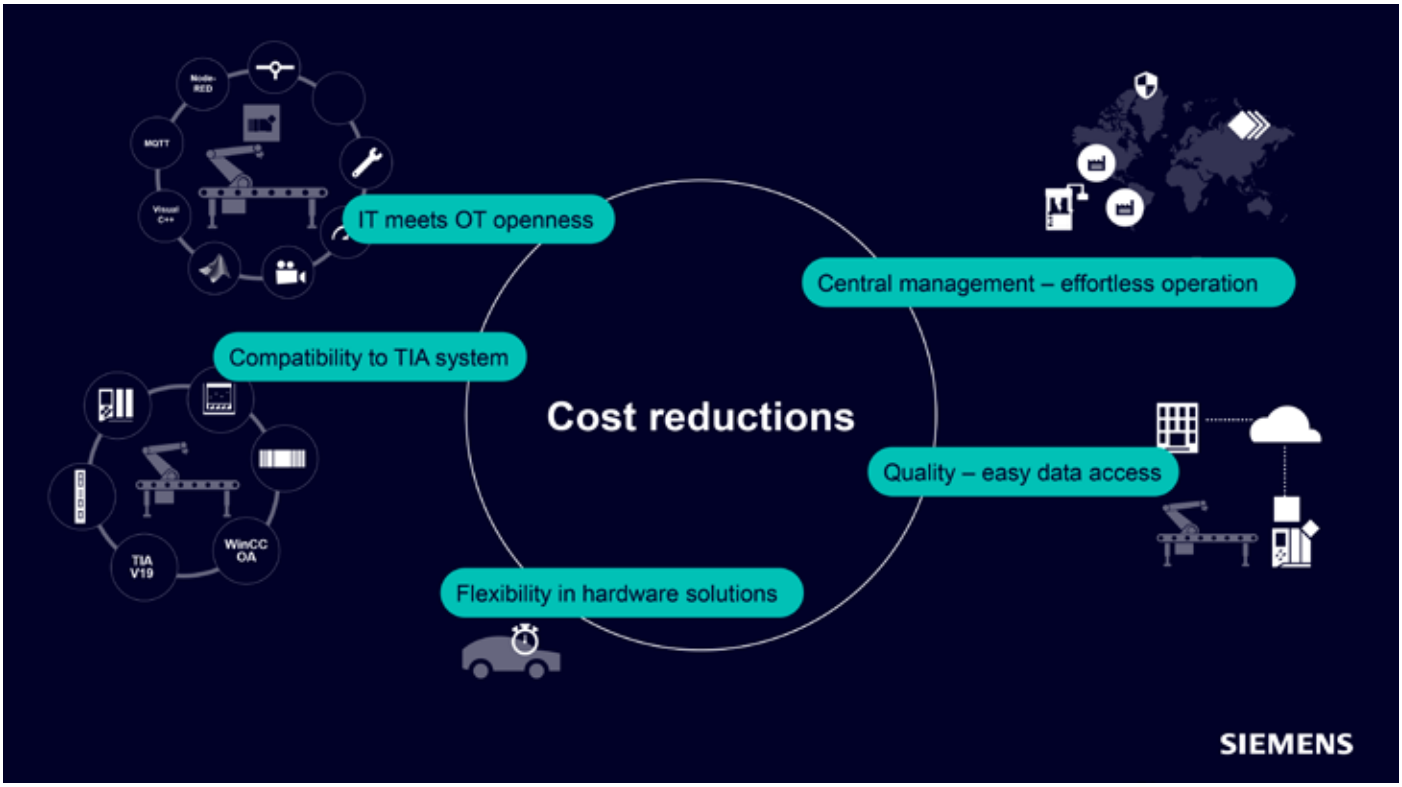
Within the cell or machine networks, the proven redundancy mechanisms based on the Media Redundancy Protocol (MRP) can continue to be used. This enables an efficient and reliable operation of the cell networks using the entire PROFINET ecosystem. Several cell networks are combined in an aggregation layer.

This consolidation simplifies the entire network structure and enables a seamless integration with other systems. To ensure seamless redundancy and minimize downtimes, the connection between the cells and the aggregation layer is established via the Parallel Redundancy Protocol (PRP). This standardized protocol (IEC62439-3) has already proven itself for many years in the field of energy supply and is now finding its way into the networks for automation technology.

Through targeted duplication of the data packets, transmission via redundant paths, and subsequent de-duplications, a seamless redundancy is achieved without any switching times. The server cluster, on which the vPLC is also hosted, is likewise connected via PRP, which increases availability accordingly and minimizes the impact of network interruptions.

Network scalability and QoS ensure flexibility

Several measures can be implemented to improve the network performance. On the one hand, the aggregation layer is equipped with bandwidths of up to 10 Gbit/s. This enables lower latency and increased network traffic – avoiding congestion and ensuring smooth communication across different segments of the network. In addition, a Quality of Service (QoS) system will be implemented that is specifically based on the Class of Service (COS) for PROFINET. This QoS framework prioritizes critical traffic, such as real-time control signals, by giving strict priority and



SOURCE: SIEMENS

allocating the necessary network resources. By minimizing latency and providing time-sensitive data in a timely manner, this approach guarantees an efficient and reliable communication.

Cooperation with leading manufacturers of virtualization environments ensures that these measures take effect not only in the physical but also in the virtual network – thus enabling a real-time capable, scalable, and highly available overall solution to be set up.

Cybersecurity needs to be considered

To implement cybersecurity in OT, Siemens recommends a multi-layered approach based on the proven "Defense in Depth" concept. This involves implementing multiple layers of security mechanisms to protect against different types of cyber threats. This approach ensures that even if one layer of defense is breached, additional layers are in place to mitigate the risk and prevent further unauthorized access.

In addition to cell protection firewalls, the implementation of SINEC software tools further increases the security of virtualized PLCs. SINEC Security Monitor tool continuously monitors the network for suspicious activity or anomalies, and provides real-time alerts and notifications to administrators. This enables a rapid detection and response to potential security incidents.

With the help of the SINEC Security Inspector tool, regular security assessments of the entire automation environment can be carried out. This helps identify vulnerabilities, misconfigurations, or compliance gaps that could potentially be exploited by cyber threats. By conducting security inspections on a regular basis, companies can proactively address security vulnerabilities and ensure the continued integrity and security of their virtualized network environment. Both tools SINEC Security Monitor and SINEC Security Inspector are operated on-premise.

SINEC Security Guard, on the other hand, is an intuitive cloud-based Software as a Service that automatically scans for vulnerabilities and enables security management. Thanks to being hosted in the Siemens cloud, the operator does not have to worry about anything else. The software can automatically assign known cybersecurity vulnerabilities to the production components of industrial plants.

In this way, operators and automation experts can identify existing security risks in their OT assets in the production without special cybersecurity know-how. They also receive a risk-based threat analysis. SINEC Security Guard then recommends risk mitigation measures and sets specific priorities. Finally, the defined remedial measures can be planned and tracked using the tool's integrated task management.

By combining the "Defense in Depth" approach, the implementation of cell protection firewalls, and the use of the SINEC software tools, companies can significantly improve the cybersecurity of their virtualized environments. This comprehensive approach helps mitigate the risk of cyber threats, protect sensitive data, and ensure uninterrupted and secure OT operations.

Conclusion

Even though companies are still in the early stages of virtualization in OT, the corresponding requirements should already be taken into account today when planning networks.

As a reliable partner, Siemens offers not only the automation systems, but also the necessary network infrastructure and matching consulting. Thanks to many years of expertise in industrial automation systems and advanced network functions, Siemens' SCALANCE products ensure stable connectivity and seamless integration with SIMATIC S7-1500V and other devices in the OT environment. This enables a reliable and efficient communication, promotes smooth operations, and maximizes the benefits of the virtualization.

By working with Siemens, companies can begin their journey towards virtualization with the confidence that they have a reliable and trusted partner to provide both the vPLC solution and the necessary network infrastructure. With the comprehensive support and solutions, companies can effectively plan and implement virtualization in their OT networks – thus paving the way for future industrial environments in a digital factory.

Wolfgang Schwering, Portfolio Owner Blueprints/Systems for Industrial Networks Digital Connectivity and Power, Siemens.

Visit Website

5G at the intelligent edge creates access to data

The merits of 5G wireless communications on the factory floor are obvious, but as with any networking technology that promises to disrupt the status quo, it will take time, resources, and a concerted effort to ensure all factories can benefit from the investment.

SOURCE: ANALOG DEVICES

5G base station.

TODAY, THE MOST PRECIOUS RESOURCE IN the manufacturing industry isn't steel, coal or electricity - it's data.

With more than half of the world's energy being consumed by the industrial sector, there is an urgent need to double the efficiency of factories around the globe. To do this, we need real-time access to data, so that we can communicate faster, more reliably, and more securely on the factory floor.

With reliable and real-time data and easily reconfigurable systems, manufacturers can make decisions quickly such as scheduling maintenance, adjust a machine setting, or pivot from making shirts to face masks, as an example.

5G, with its high capacity and low latency, is making this possible – whilst also enabling manufacturers to add cutting-edge technologies, such as automated robots and IoT devices, into their operations.

But for these machines to work safely and securely, they need to be able to securely sense, measure, and interpret the real world. This requires converting analog data, including pressure measurements or vibrations, to digital data, to allow for more signal processing.

Intelligent edge

The highest quality data can be found at what we call the Intelligent Edge. Take a gigafactory, for example. When it comes to battery manufacturing a robot must apply uniform coating requiring a high degree of precision. This precision can be ensured through data from the Intelligent Edge. 5G gives us the ability to harness these insights at the Edge and make better decisions, thereby enhancing efficiencies overall.

5G is also accelerating efficiencies simply

SOURCE: ANALOG DEVICES

Eliminating wired connectivity by using 5G provides the manufacturing environment with more flexibility.

by making it safer for humans and machines to work together. Manufacturing processes are faster, more efficient, and more cost-effective when humans and robots operate in tandem.

With increased automation and robots taking on repetitive, dangerous work, manufacturers can augment human labor and ensure continuity of production. 5G's reliability and speed mean machine-to-machine communication and, increasingly, human-to-machine interaction is vastly improved, reducing the risk of accidents.

Eliminating the need for wired connectivity through 5G also provides the manufacturing environment with a lot more flexibility, in turn, augmenting process automation, remote monitoring, and maintenance and device life cycle management.

Consider a factory, for example, where the physical connectors have disappeared and command instructions are sent wirelessly between robot subsystems, increasing production speed while reducing costs. All of this is possible through a 5G wireless network because it maximizes communication, reduces the margin for error (or accidents), and importantly, keeps the technology secure from hackers or malicious entities.

SOURCE: ANALOG DEVICES

5G harnesses insights at the Edge to make better decisions, enhancing efficiencies overall.

Benefits of 5G on factory floor

The merits of 5G on the factory floor are obvious, but as with any technology that promises to disrupt the status quo, it will take time, resources, and a concerted effort to ensure all factories can benefit.

The transition from wired to wireless networking is a complex upgrade. Each industrial customer has a unique set of circumstances, from cultural dynamics to financial position to appetite for innovation that sways the organization's ability to make the significant upgrade to wireless.

That said, the number of digital factories will increase rapidly over the next few years as traditional manufacturing facilities come to the end of their life cycles. The COVID-19 pandemic taught many difficult lessons to firms about the risks of too much offshoring. As a result, many are now looking to bring their facilities closer to the customer.

This is opening the door to newer, more powerful facilities, underpinned by 5G technology. Once 5G is fully realized, we will be living in a world that holds the potential to dramatically improve life for all.

Fiona Treacy, Managing Director, Industrial Automation, ***Analog Devices.***

Learn More

Remote connectivity focus on performance and cybersecurity

A series of technology trends are driving the latest solutions for industrial remote connectivity by leveraging innovations such as OpenVPN to simplify management of multiple remote connections. More companies are looking for solutions to connect to their machines/devices remotely and security remains a highest priority.

SOURCE: ISTOCKPHOTO

"More companies are looking for solutions to connect to their machines/devices remotely. Remote connectivity has been used for several years, many times using a cellular modem/router on site, with the cellular modem/router in front of the devices and doing a port forward of incoming traffic to those devices. In recent years, security has become a higher priority," Jeff Marcum, Sales Engineer, Red Lion Controls.

INDUSTRIAL REMOTE CONNECTIVITY SOLUTIONS enable the ability for engineering and service personnel to connect securely to automation machines from anywhere in the world. Secure connections provide a vital link to implement data collection, programming and troubleshooting tasks, creating an effective method to collect and visualize machine data on user-friendly dashboards, with KPIs and alarms to prevent downtime.

For this Remote Connectivity update, the Industrial Ethernet Book reached out to industry experts to gain their perspectives on how remote connectivity technology is continuing to move ahead with a focus on improvements with connectivity software and an ongoing focus on cybersecurity.

Secure remote connectivity

Growing use of encrypted OpenVPN or IPSec tunnels for secure connections.

A series of technology trends and innovations are driving the latest solutions for industrial remote connectivity leveraging innovations such as OpenVPN to simplify management of multiple remote connections, Jeff Marcum, Sales Engineer for Red Lion Controls, told the Industrial Ethernet Book recently.

"More companies are looking for solutions to connect to their machines/devices remotely. Remote connectivity has been used for several years, many times using a cellular modem/router on site, with the cellular modem/router in front of the devices and doing a port forward of incoming traffic to those devices. In recent years, security has become a higher priority, and companies are adopting encrypted tunnels for connection – normally OpenVPN or IPSec tunnels," Marcum said.

"Remote connections are commonly used by engineers, technicians and OEMs for regular maintenance of devices, programming changes of a PLC or HMI (for example), troubleshooting and data collection or monitoring," Marcum added.

Although remote connectivity is often used for accessing equipment in remote locations (an oil field for example), that is not always the case, Marcum added. Remotely connecting to a machine on the factory floor

SOURCE: RED LION

Red Lion FlexEdge platform.

can be a big advantage for technicians and engineers as well, allowing them to make configuration changes, troubleshoot and maintain equipment without having to travel to multiple sites.

Leveraging technology

Red Lion's FlexEdge platform provides the ability to easily access company assets remotely by offering an optional cellular interface that can be used for direct connection to the unit or port forwarding through the unit to end devices. OpenVPN tunnels are easily created on the FlexEdge as well (on any active interface) allowing secure / encrypted connectivity to not only the FlexEdge itself but equipment behind the unit.

Users can create Point to Point tunnels, Many to One tunnels (where one FlexEdge acts as a server to multiple clients), or tunnels to a company owned OpenVPN Access Server.

Marcum said that what makes this technology unique is the ability for Red Lion's FlexEdge to operate as an all-in-one protocol converter, router, cellular gateway, VPN tunnel endpoint, and more, that will displace multiple pieces of hardware in an application.

"Being a Layer 3 device, the FlexEdge is a router and firewall that can sit between different networks providing routing capabilities and security," Marcum said. "With its modular design the user can select the type(s) of network interface is needed for each application, including cellular, Wi-Fi and additional Ethernet interfaces."

FlexEdge can serve as an OpenVPN client, server or both simultaneously, providing secure connectivity wherever it's located. If VPN tunnels aren't necessary, the cellular interface on the FlexEdge can allow users to remotely access the FlexEdge itself as well as equipment behind it.

"The FlexEdge is more than a network device however. With Red Lion's Crimson® software, not only can it provide connectivity to equipment in remote environments, it also provides a suite of automation capabilities including protocol conversion, system control, virtual HMI, data logging, MQTT communication and more," Marcum said.

Applications and industries

Almost any type of application or industry can benefit from remote connectivity solutions. Examples include Oil and Gas, Water/Wastewater, Utilities and even the factory floor. Many companies or machine builders have equipment at truly remote locations or multiple remote locations (e.g. Oil and Gas).

Having the ability to connect to the devices on site without the need to travel to those locations can offer huge savings in time and expenses. Mobile equipment, such as Frac Trucks, are another example use case for remote connectivity. If needed, engineers or technicians can connect to the devices on the truck for maintenance or necessary configuration changes no matter where the trucks are located.

Engineering challenges

Most companies have equipment in multiple locations. Those locations can be spread out over a region, country or even around the world. Engineers and technicians need the ability to access on site equipment (PLCs, HMIs, etc) for regular maintenance, configuration or to quickly resolve an issue. Being able to remotely connect to assets can greatly save on the time and cost of someone having to drive (or even fly) to the site.

"Challenges that arise when considering remote connectivity include deciding what type of network connection is available or needed (cellular, local Ethernet connection, etc), are tunnels needed, what type of tunnel and how many? The type of hardware needed to facilitate that connection has to be decided on as well. Lastly, once those decisions are made, someone has to understand how to provision that remote access device and methodology being used," Marcum stated.

Red Lion's FlexEdge is designed to make setting up communication easy. FlexEdge offers a cellular interface that can be used for direct connection to the unit or port forwarding through the unit to end devices.

"OpenVPN tunnels are easily created on the FlexEdge as well (on any active interface) allowing secure / encrypted connectivity to not only the FlexEdge® itself but equipment behind the unit," Marcum said. "Users can create Point to Point tunnels, Many to One tunnels (where one FlexEdge® acts as a server to multiple clients), tunnels to a company owned OpenVPN Access Server."

Increased complexity to support IoT and IIoT devices

Robust connectivity and seamless integration a priority to address AI, machine learning, encryption and firewall requirements.

According to Lars Walpurgis, Product Owner Sinema Remote Connect at Siemens, remote connectivity solutions are moving forward to leverage 5G communications and accommodate new IIoT requirements while also addressing heightened security concerns.

"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. Furthermore, edge computing brings processing power closer to data sources, reducing latency and improving efficiency," Walpurgis told IEB recently. "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."

"The increasing demand of 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," Walpurgis said.

He added that 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. Its high reliability and seamless integration with various existing systems and network protocols make it adaptable and versatile for different industrial needs.

SOURCE: ISTOCKPHOTO

"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. Furthermore, edge computing brings processing power closer to data sources, reducing latency and improving efficiency," Lars Walpurgis, Product Owner Sinema Remote Connect, Siemens.

Remote connectivity focus

Walpurgis 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.

Siemens offers the SCALANCE M series of industrial routers, which provide secure remote access to machines and plants. This solution supports VPNs, 5G communications, firewall functionalities, and various mobile and broadband connections, ensuring reliable and secure communication.

Key benefits include reduced downtime, efficient maintenance, and enhanced data security.

Moreover, SINEMA Remote Connect, Siemens' management platform for remote networks, is a server application which facilitates simple, secure remote access to widely distributed machinery and plants, such as for 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. 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.

Addressing customer pain points

"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. "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."

The vital importance of cybersecurity solutions

Remote solution leverages IEC 62443 security standards.

Sébastien Thinnes, Product & Marketing Director at Ewon, underscores the significance of cybersecurity and IEC 62443 for customers.

SOURCE: EWON

"The security of our IIoT solutions is paramount, By implementing IEC 62443 standards, we ensure that our products provide robust protection against emerging threats, safeguarding our customers' industrial operations," Sébastien Thinnes, Product & Marketing Director, Ewon. Recently, the Ewon Cosy+, a solution for remote access, was assessed against IEC 62443-4-2 criteria by NVISO, a globally recognized cybersecurity expert.

"The security of our IIoT solutions is paramount," Thinnes said. "By implementing IEC 62443 standards, we ensure that our products provide robust protection against emerging threats, safeguarding our customers' industrial operations."

Ewon remote solutions from HMS Networks have always prioritized security. Recently, the Ewon Cosy+, a solution for remote access, was assessed against IEC 62443-4-2 criteria by NVISO, a globally recognized cybersecurity expert, for cybersecurity. As the industry evolves, so do the standards of excellence, with IEC 62443 emerging as the benchmark for cybersecurity in industrial automation technology.

Understanding IEC 62443 standards

The IEC 62443 standards provide a comprehensive framework for safeguarding industrial equipment against cyber threats, complementing the already established ISO 27001 framework, which focuses primarily on IT security. The IEC 62443 standards outline the essential requirements for protecting industrial systems from security breaches. For machine builders, systems integrators, and plant operators, compliance with IEC 62443 is crucial for IIoT security.

According to Cédric Bassem, Senior Manager Application and Product Security at NVISO, "One of the strengths of IEC 62443 is that it provides a framework that IIoT manufacturers can use to align their device's security requirements with the cybersecurity ambitions of the factory owners."

How to implement IEC 62443 standards

According to eWon, developing a secure automation solution begins with identifying risks through a detailed threat analysis for the involved systems and components. This leads to the creation of a robust security plan. The next step involves establishing appropriate processes and ensuring staff are trained in security protocols. Security extends beyond technology to encompass well-defined processes and qualified personnel.

Given the evolving nature of cyber threats, it is vital that protection systems adapt over time. Continuous monitoring, maintenance, and updates are essential to maintaining security.

IEC 62443-4-2 criteria

With Ewon remote connectivity solutions from HMS Networks, security has become the cornerstone priority for product developers. And this commitment to cybersecurity is demonstrated through compliance with certification standards such as ISO 27001.

To maintain the highest cybersecurity standards, HMS Networks has partnered with NVISO, a leading independent organization specializing in industrial cybersecurity. Nviso strengthens the Ewon security measures by conducting regular testing, providing trainings and other recurrent security verifications.

Recently, with the support of NVISO, the Ewon Cosy+ was evaluated against IEC 62443-4-2 standards. Based on the assessment results provided by Nviso, Ewon reports that its product will seamlessly integrate into customer environments and support their IEC 62443 implementation and roadmap.

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

Operational solutions for industrial network resiliency

Industrial networks are characterized by their need for timely data transmission and high reliability. The occurrence of a single point of failure within the network can disrupt communication between machines, imposing operational challenges to industrial automation systems.

IN THE INDUSTRIAL WORLD, FAST RECOVERY and fault-tolerant networks are critical for ensuring process operations and reliability. In this article, we will explore the significance of network resiliency protocols in mitigating downtime and safeguarding critical processes, which are vital in environments where system failures equate to substantial risks and costs.

In industrial environments, such as energy production, railway systems, maritime operations, and manufacturing, ring topologies are commonly deployed to interconnect machinery, sensors, meters, and control systems across extensive geographical areas, plant-wide manufacturing cells, where network connectivity may be constrained.

These industrial networks are characterized by their need for timely data transmission and high reliability. The occurrence of a single point of failure within the network can disrupt communication between machines, imposing operational challenges to industrial automation systems. Consequently, conventional spanning tree protocol is inadequate, as it does not offer sufficiently rapid convergence in the event of network disruptions within these specific settings.

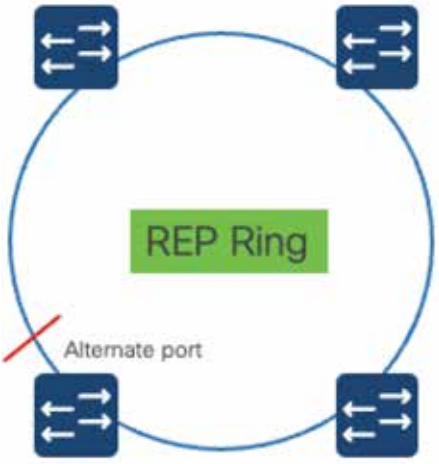
Ring topologies and redundancy protocols

To address these challenges, advanced layer 2 protocols have been developed to effectively manage network rings. These protocols ensure fast convergence times on the order of sub seconds, manage redundant network paths, and prevent loops. Protocols such as the Cisco Resilient Ethernet Protocol (REP), Device Level Ring (DLR), Media Redundancy Protocol (MRP), High-availability Seamless Redundancy (HSR), and Parallel Redundancy Protocol (PRP) are widely implemented in such scenarios.

Resilient Ethernet Protocol (REP)

The Resilient Ethernet Protocol (REP), a proprietary protocol developed by Cisco for use in ring topology, can recover from link or node failure in 50ms. It operates by chaining ports within a logical grouping known as a segment. When all ports are operational, the protocol designates one port to be blocked. This port is called an alternate port. Data is not forwarded through a blocked port, but the local link status between adjacent neighbors continues to be monitored for topology changes.

In the event of network failure, the protocol unblocks the blocked port, which then transitions to forwarding state, thereby resuming traffic flow.



SOURCE: CISCO

REP ring topology.

Resilient Ethernet Protocol is feature rich. It also facilitates VLAN load balancing which optimizes the distribution of network traffic. It supports complex ring topologies such as multiple rings and subrings and is interoperable with spanning tree protocol.

While REP ports do not run simultaneously with the Spanning Tree Protocol, it is possible for a switch to support both a REP ring and STP concurrently. In such configurations, if the REP segment detects a failure, it sends out an STP Topology Change Notification from the REP ring to accelerate the STP's convergence process.

Device Level Ring (DLR)

Device Level Ring (DLR) is an EtherNet/IP™ protocol defined by the Open DeviceNet® Vendors' Association (ODVA), generally found in manufacturing. DLR is designed primarily for a simple, single-ring topology that requires fast convergence. It does not support overlapping rings.

In DLR network, at least one device is configured as the ring supervisor. Ring supervisor monitors the health of the ring by sending beacon frames to detect network integrity. Each device along the ring relays the beacon frames to the next hop.

If beacon frames fail to reach the secondary port of the supervisor, or a links status message is received from ring nodes, the supervisor unblocks the blocked port to resume traffic flow.

DLR does not interoperate with other redundancy protocols such as spanning tree protocol. A gateway node in the ring serves as a bridge between DLR ring and external networks, transmits frames to ports that are not part of the DLR network.

The default beacon interval is 400 microseconds, which enables ring recovery times of approximately 3 milliseconds for a ring consisting of 50 nodes.

Media Redundancy Protocol (MRP)

Media Redundancy Protocol (MRP) is defined in the International Electrotechnical Commission (IEC) standard 62439-2, commonly deployed in conjunction with PROFINET in manufacturing.

In an MRP ring topology, there are typically two roles of devices - Media Redundancy Manager (MRM) and Media Redundancy Clients (MRCs). Media Redundancy Manager manages and monitors the health of the ring, while the Media Redundancy Clients are the member nodes of the ring.

Media Redundancy Manager regularly initiates and circulates control frames from one of its ring ports and receives them back from the ring over its other ring port, maintaining bidirectional checks to monitor the health of the ring. To avoid network loop, Media Redundancy Manager keeps one of its ports in blocked state during normal operations.

When detected failure or recovery, Media Redundancy Manager sends out TopoChange frames via both of its ring ports to Media Redundancy Clients to quickly react to the network change.

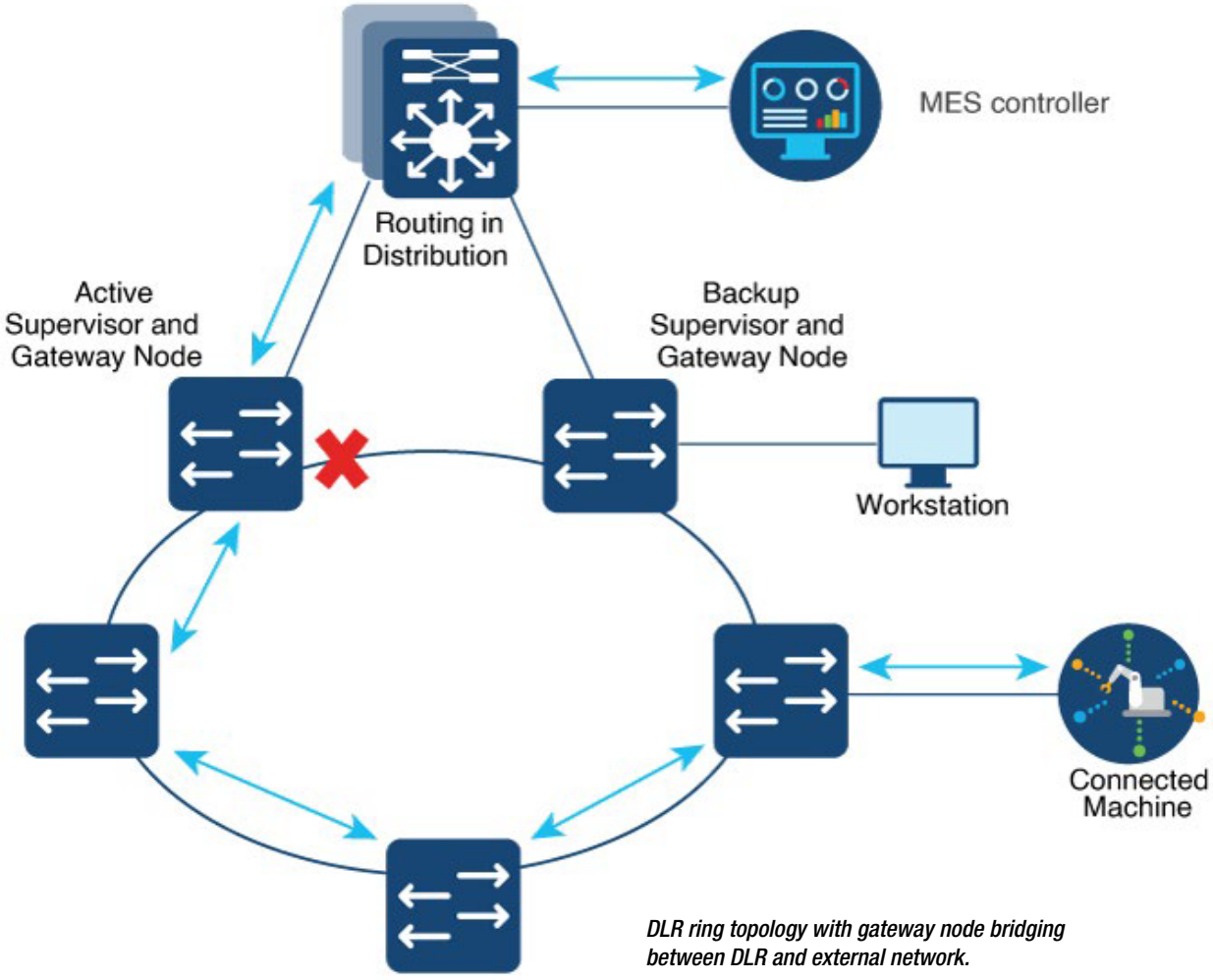
If Media Redundancy Clients detects a port going offline or coming back online, it relays this information to Media Redundancy Manager by sending LinkChange subtype frames.

Media Redundancy Protocol supports multiple MRP rings and is interoperable with spanning tree protocol at uplinks.

Lossless resiliency protocols

While network protocols like Spanning Tree Protocol, Resilient Ethernet Protocol (REP), Media Redundancy Protocol (MRP) and Device Level Ring (DLR) detect network faults and reconfigure network path in the event of network failures, network recovery times can vary from seconds to milliseconds.

SOURCE: CISCO



DLR ring topology with gateway node bridging between DLR and external network.

Lossless resiliency protocols such as High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP), on the other hand, are designed to deliver uninterrupted redundancy, well suited for critical Industrial Automation and Control Systems (IACS) infrastructure that requires zero recovery time to maintain continuous operation and maximum up-time in the event of network disruptions.

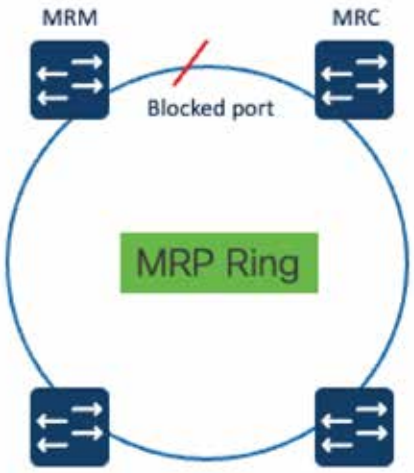
High-availability Seamless Redundancy (HSR)

High-availability Seamless Redundancy (HSR) protocol, as defined in International Standard IEC 62439-3, is designed for ring topologies to attain zero recovery time, ensures no frame is lost in the event of a network failure. HSR operates by sending duplicate packets over a ring topology.

In HSR network, HSR end nodes participate in implementing redundancy. They are implemented in a ring with two interfaces per end node, and relaying frames between these two interfaces called port A and port B.

Nodes with dual interfaces connected to the HSR ring are known as Doubly Attached Nodes implementing HSR(DANH). Singly Attached Nodes (SAN) are connected to the HSR ring through a RedBox (Redundancy Box), which serves the role as DANHs to provide connectivity and redundancy on behalf of the SAN. Devices that do not support HSR are connected to a Redbox, from which the Redbox generates the HSR headers on behalf of these devices.

HSR end nodes send a duplicated copy of packets to destination to both the clockwise and counterclockwise directions in the ring, with the addition of HSR header which contain a sequence number for the end node to decide which frames to be used or discarded. When the designated node receives the first frame, it removes the header and processes the frame. When the duplicated packet arrives, the node discards the frame with the same source address and sequence number.



SOURCE: CISCO

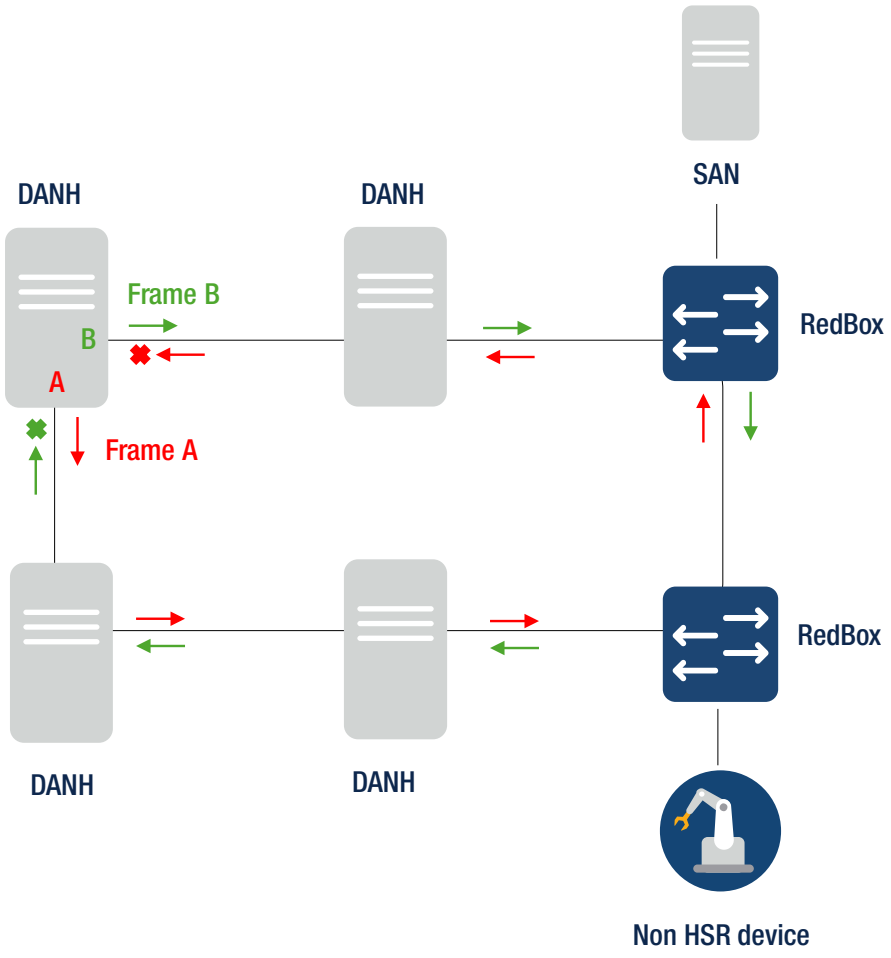
MRP ring topology

If failure occurs in the ring, there is always another copy flowing through the network. Therefore, the HSR system can provide zero switchover time, lossless redundancy during failure and recovery.

In contrast to common ring redundancy protocols that only one primary path is active at a time which result in frames drop during convergence, HSR maintains continuous traffic flow over the other ring direction uninterrupted, and hence zero recovery time could be achieved.

Parallel Redundancy Protocol (PRP)

Parallel Redundancy Protocol (PRP) is another hitless redundancy protocol, designed to interwork with arbitrary network topologies



HSR topology with duplicated packets sent to clockwise and counterclockwise directions.

SOURCE: CISCO

and is not limited to ring implementations. It operates by sending duplicate packets over two independent, disjointed, layer 2 parallel networks referred to as LAN-A and LAN-B, thereby offering a flexible option that can be seamlessly integrated into existing network topologies, and there is no requirement for LAN-A & LAN B switches to be PRP aware.

In PRP network, PRP end nodes also participate in implementing redundancy. When a Dually Attached Nodes (DANs) transmits data, it sends two identical packets simultaneously across LAN-A and LAN-B to the destination. To differentiate between these duplicates, a redundancy control trailer (RCT) containing a sequence number is appended to each frame. When the designated node receives the first frame, it processes the frame and discards subsequent duplicate frame. In the event of a path failure, the unaffected path ensures continuous data flow, negating the need for recovery period.

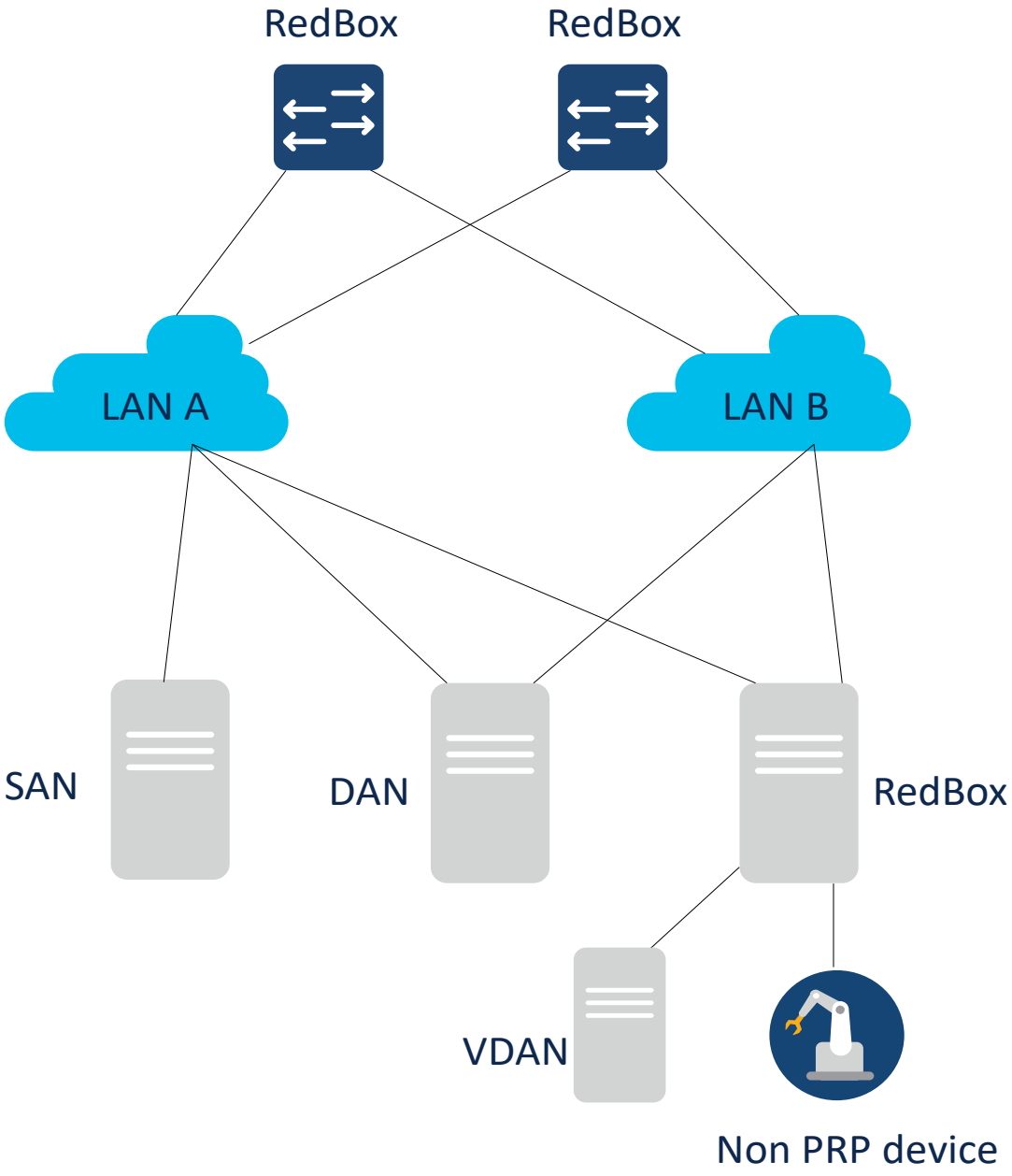
Endpoints that connect solely to one of the networks, LAN-A or LAN-B, are known as Singly Attached Nodes (SANs).

In scenarios where an end node is not equipped with dual network connections, or does not implement PRP, it is typically connected to a RedBox which facilitates both connectivity and redundancy. A node connected behind a RedBox appears to other nodes as if it were a DAN and is therefore called a Virtual DAN (VDAN). The RedBox

	Topology	Packet Duplication	Recovery Time
PRP	Any (two parallel networks)	Yes	0 ms
HSR	Ring	Yes	0 ms
DLR	Ring	No	3 ms
MRP	Ring	No	30 ms
REP REP Fast	Ring	No	50 ms 25 ms
RSTP	Any	No	1000 ms

SOURCE: CISCO

Redundancy protocol comparison.



SOURCE: CISCO

PRP topology with two parallels and disjoint LAN-A and LAN-B network.

itself functions as a DAN and acts as a proxy for its VDANs.

Redundancy protocol considerations

The choice of redundancy protocols depends on the specific requirements of the network, the criticality of avoiding frame loss, and other key factors.

1. *Application requirement of convergence time:* The specific requirements of industrial systems or applications influence the choice of protocol. HSR and PRP support zero convergence time, REP and MRP offer convergence times at around 50 ms for fiber connection and 3 ms respectively, and DLR typically offers fast recovery times suitable for EtherNet/IP networks.

2. *Network topology:* Network topology plays a role in protocol selection. HSR is designed for ring topologies; PRP can be deployed in any topology if LAN-A and LAN-B are two disjoint networks; DLR is specific to EtherNet/IP rings, REP is used for general ring topologies with benefits such as VLAN load balancing, and MRP is typically found in PROFINET networks.

3. *Industry standard:* It is crucial to ensure the choice of protocols adhere to industry standards and certifications if it is a mandatory requirement. HSR and PRP are based on the IEC 62439-3 standard, while MRP is based on the IEC 62439-2.

4. *Ease of configuration and troubleshooting:* Ring protocols are generally easy to set up and troubleshoot. While HSR and PRP offer highest availability, they also come with increased complexity and specific requirements. For instance, end hosts must support HSR or PRP. Additional network bandwidth is required for duplicated packets, and PRP requires two separate and parallel networks for LAN-A and LAN-B.

Minimize downtime, maximize efficiency

Cisco industrial networking solutions are designed to be robust and resilient. Cisco Industrial Ethernet switches enable users to build highly resilient deterministic networks that help you minimize downtime, enhance reliability, increase process efficiency, and reduce operating costs. With support for several different redundancy options, Cisco switches also provide the flexibility to choose the redundancy mechanism that works best for individual use cases. Please visit cisco.com/go/ie, or setup a free, no obligation, call with one of our industrial networking experts.

Casca WM Kwok, Technical Marketing Engineer - Industrial IoT, ***Cisco.***

Visit Website

Angle-of-arrival solution for indoor asset tracking

Wireless connectivity and positioning technologies address the growing need for high-performance positioning systems which reduce operational costs and maximize sustainability by optimizing inventory management along with material and people flows.

SOURCE: U-BLOX

Based on Bluetooth LE AoA (Angle-of-Arrival), u-locate delivers positioning accuracy levels down to 10 centimeters while ensuring extended tag battery lifetimes at an affordable price point.

U-BLOX HAS LAUNCHED A COMPREHENSIVE Bluetooth Angle-of-Arrival solution to enable reliable indoor asset tracking. Including support for interoperability using the omlox™ standard, u-locate offers every necessary hardware, software and middleware component for indoor positioning.

Indoor positioning solution

The u-locate technology is a complete indoor positioning solution, offering the optimal combination of accuracy, cost and power consumption. Based on Bluetooth LE AoA (Angle-of-Arrival), u-locate delivers positioning accuracy levels down to 10 centimeters while ensuring extended tag battery lifetimes at an affordable price point.

The flexible and modular u-locate solution targets RTLS (real-time location system) solution providers and systems integrators, with end-user indoor tracking applications in warehousing, manufacturing, healthcare and many more. The easy-to-configure mobile application includes an extensive management support tool and anchors with self-aware orientation, removing the pain of complex solution installations and ensuring reduced times to market.

u-locate's advanced AoA positioning algorithms deliver market-leading accuracy while reducing the cost of tracking assets, enabling a wider range of use cases. The combination of Bluetooth 5.1 technology with the optimized antenna configuration of u-locate delivers exceptional levels of positioning accuracy, without compromising power consumption. The u-locate solution scales easily as the end-user installation grows, and futureproofing is underpinned with OTA (over-the-air) software updates ensuring continuous access to new features and updates.

The flexible solution can be tailored according to the needs of the application, and consists of a positioning middleware (u-locateHub), a positioning engine (u-locateEngine), anchor points (u-locateAnchor) and tags (u-locateTag). It can be complemented with GNSS (Global Navigation Satellite System) products from u-blox, to guarantee seamless indoor and outdoor localization.

u-locateHub complies with the omlox global interoperability standard and its well-documented API platform contains various APIs, supporting integration with multiple vendor solutions. By joining omlox, u-blox recognizes the importance of contributing to a growing ecosystem, and promoting global interoperability of positioning solutions.

"We are delighted that u-blox is entering the omlox ecosystem, by adopting the standard into u-locate, its new RTLS solution for indoor positioning systems," says Dr. Matthias Joest, Committee leader for omlox. "omlox is the world's first locating standard. It specifies flexible locating solutions that allow customers to benefit from lower integration costs, while ensuring future-proof setups. Having u-blox – recognized leader in locating technologies – as member and supporter of omlox, is a huge benefit for our fast-growing ecosystem."

With u-locate, u-blox is leveraging its deep expertise in wireless connectivity and positioning technologies to address the growing need for high-performance positioning systems which reduce operational costs and maximize sustainability by optimizing inventory management along with material and people flows.

Application report by ***u-blox.***

Visit Website

Motion control and measurement data acquisition in perfect sync

PC-based control and EtherCAT have combined to automate a compact sporting goods test machine. The system delivers precise measurement results using standard components from the automation specialist, and hardware costs were cut by around 4,000 U.S. dollars per machine.

SOURCE: BECKHOFF AUTOMATION

The CX5130 Embedded PC (left) and ELM3502 measurement terminal (metal module on right) save space in the control cabinet of the compact test machine for lab environments.

THE MODERNIZED IMPACT TESTER FROM Automated Design Corporation (ADC) demonstrates the benefits of seamlessly integrated control and measurement technology from Beckhoff. In the dynamic testing of cushioning elements for sports shoes, the system delivers precise measurement results using standard components from the automation specialist. The hardware costs were cut by around 4,000 U.S. dollars per machine.

ADC's redesigned Impact Tester shows how well the traditionally disparate disciplines of measurement technology and industrial automation can work together. "The impact testing system, like most others, is more industrial than typical desktop lab-type boxes, but it now offers extended data acquisition (DAQ)," says Thomas Bitsky, Jr., Vice President and Lead Developer at ADC. Founded in 1986 by Thomas Bitsky's parents, the company based in Romeoville, Illinois, today supplies R&D systems to numerous renowned sporting goods manufacturers.

ADC needed to meet several requirements when upgrading the Impact Tester. Precision motion control, real-time fieldbus communication and fast cycle times were necessary, and a more intuitive HMI was mandatory. Beyond that, ADC wanted the solution to overcome the boundaries between traditional measurement and control technology.

The DAQ industry has remained siloed for far too long, according to Thomas Bitsky. In the past, however, the high sample rates needed to ensure the required measurement quality could only be found in the components from select vendors. But when using a legacy DAQ controller running LabVIEW™ software, automated test handling requires a separate PLC, Thomas Bitsky explains: "These scenarios add cost, communication delays and cabling nightmares." Also, the motion control and DAQ technologies must synchronize perfectly for accurate, reproducible test results, which creates challenges when using separate solutions. In order to minimize losses at the interfaces, ADC decided to use system-integrated measurement technology in a flexible control platform from Beckhoff.

High-end measurement technology in a standard I/O system

EtherCAT offers many benefits, but the main advantages for ADC are speed and bandwidth. For analog data acquisition during impact testing, EtherCAT measurement terminals from the ELM series with oversampling capabilities are used. Oversampling means reading data multiple times per control cycle for enhanced time resolution of a signal and increased accuracy.

ADC's redesigned ASTM-compliant Impact Tester combines high-end measurement with intuitive operation.

SOURCE: BECKHOFF AUTOMATION

Thomas Bitsky, Jr. (left), Vice President and Lead Developer at ADC, works closely with Dave Zimbrich, Applications Engineering, and Mike Rauch, Regional Sales Engineer, both from the Beckhoff team in the Chicago area.

With this high level of performance, ADC was able to use commercial off the shelf (COTS) measurement terminals from Beckhoff to eliminate expensive, specialized hardware. The high-end ELM3502 measurement terminals are fully integrated into the standard Beckhoff I/O system and offer dual-channel measurement in a ruggedized metal housing. With sampling rates up to 20 ksps, the terminal covers most advanced measurement requirements for ADC. However, the scalable ELM series also offers terminals that support sampling rates up to 50 ksps.

"We had been using other Beckhoff measurement terminals – particularly the EL3356 analog input terminal, which works well for industrial applications. But our test and measurement customers needed sampling in the kilohertz range that only legacy DAQ vendors offered previously," says Thomas Bitsky and adds: "The ELM terminals delivered the sampling rates we needed, along with perfect synchronization to the controller via EtherCAT. Now, the machines can execute a test very quickly. In one scan, I get all motion and load data, and our measurement accuracy and repeatability look as good if not better than what we got with the traditional chassis-style controller."

Scalable, standard components

TwinCAT 3 delivered a universal engineering environment, which facilitated the implementation, according to Thomas Bitsky, and also easily integrates LabVIEW™ and other third-party software. With TwinCAT, engineers can program in the languages that they are most familiar with or that best fit the project, including the available IEC 61131-3 languages and their object-oriented extensions, function blocks and computer science standards found in Microsoft Visual Studio®. "We lean on TwinCAT to save programming time," Bitsky explains.

On the controls side, ADC relies on a Beckhoff CX5130 Embedded PC. The DIN-rail-mounted, fanless machine controller saves machine space and delivers ample computing power for data acquisition and motion control in the test systems. The scalability of the Embedded PCs from Beckhoff also allows ADC to increase performance levels when needed, they say.

Compact drive technology from Beckhoff ideally complements the needs of the test systems that usually have to fit in limited lab environments at sporting goods manufacturers. The EL7211 servo terminals (driving the AM8100 servomotors) and EL7041 stepper motor terminals deliver high-performance drive technology in an I/O slice form factor, and are installed in the control cabinet along with the EL5101 encoder interface.

"We can also use third-party motors and drives, and if they're EtherCAT-based, the integration is incredibly simple. We use the motion control libraries in TwinCAT for all of these devices," Thomas Bitsky says. "Most of our applications require simple point-to-point motion. We apply a specified load to the material, which requires synchronization between the load cell input and motion controller, and then read the position. If you go past that load, the test will fail to execute.

"The legacy, chassis-style controllers just don't have the power to support this functionality," he adds. "But the distributed clocks in EtherCAT ensure synchronization of load versus position. So with the integrated Beckhoff technologies, we're able to do things that would be impossible otherwise."

Reduced time and costs

The modernized impact tester machine adheres to the ASTM F1976 and F1614 standards for testing the impact attenuation of cushioning in athletic shoes. The use of standard automation components, including the high-end measurement technology in an I/O module format, led to cost savings of about 4,000 U.S. dollars per machine. The Beckhoff solution also reduced wiring, assembly and programming time. The 24/7 support from Beckhoff proved reliable and efficient when ADC needed assistance.

Since ADC fills a unique gap in testing and automation, it's important for the company to safeguard its intellectual property. Here, TwinCAT serves up additional value-add, according to Applications Engineer Dave Zimbrich from Beckhoff: "The OEM Certificate feature that we offer allows ADC to encrypt and password-protect its code. This means no matter where their test machine ends up, their code is safe."

*Application story by **Beckhoff Automation.***

Learn More

groov devices offer flexibility, scalability for SCADA expansion

Paloma Irrigation and Drainage District reduces downtime and pump repair costs. Automation in particular and especially pump lubrication, minimized component wear and tear, leading to significantly fewer breakdowns and an estimated $300,000 annual cost reduction.

THE PALOMA IRRIGATION AND DRAINAGE District (PIDD), spanning 30,000 acres in Gila Bend, Arizona, underpins the region's agricultural production. It supplies water to diverse crops, including alfalfa and cotton, and supports dairy operations, contributing to the area's varied agricultural output. Additionally, the district provides domestic water services to nearly 100 homes.

District Manager Robert VanHofwegen heads the water management network, ensuring effective delivery through a combined system utilizing Gila Bend Canal and groundwater sources. This approach fuels both agricultural growth and the prosperity of the local community.

More than just irrigation, the PIDD safeguards the environment and upholds the community's water rights. Their commitment to sustainable water practices aligns with Gila Bend's agricultural vision, ensuring long-term prosperity for both flourishing fields and surrounding homes. In this resource-scarce landscape, the district plays a crucial role in sustaining the thriving agricultural hub.

SOURCE: OPTO 22

Gila Bend main canal at Gillespie Dam.

Paloma Irrigation lift station.

Challenges

But in 2019, the PIDD faced several pressing challenges, culminating in the need for a strategic shift towards an Industrial Internet of Things (IIoT) approach. Here's a closer look at the key issues:

Inefficient Manual Operations

Time-consuming & laborious: Technicians relied on manual controls and frequent site visits for monitoring and adjustments, reducing efficiency and introducing delays.

High maintenance costs: Frequent pump failures due to lack of continuous monitoring resulted in annual maintenance expenses of $300,000–$400,000, creating a financial burden for the district.

Reactive management: The district's inability to proactively respond to changes in water demand or system failures hindered optimization and problem prevention.

Limited Visibility and Control

No real-time monitoring: Absence of real-time data left the district unaware of issues that were impacting water delivery.

No remote control: Inability to remotely control systems limited flexibility and timely responses to issues, potentially leading to supply interruptions.

These challenges highlighted the critical need for a more modern, cost-effective, and data-driven approach to water management, paving the way for the district's exploration of IIoT solutions.

First try: Raspberry PI

In a bid to address the challenges of outdated systems and modernize operations,

SOURCE: OPTO 22

Gillespie Dam lift pumps.

PIDD District Manager VanHofwegen explored an unconventional solution: Raspberry Pi®. These low-cost, versatile devices offered a potential entry point into leveraging IIoT technology for improved water management.

Their affordability allowed VanHofwegen to experiment with IIoT applications without significant upfront investment.

Raspberry Why?

Leveraging Raspberry Pi proved successful, laying the groundwork for the district's IIoT strategy. PIDD also adopted Node-RED®, a user-friendly flow-based programming tool, and FlowFuse™, a platform for remote device management, to more easily integrate hardware with online services.

Node-Red's visual programming eliminated the need for extensive coding, enabling the development of sophisticated irrigation management solutions at a low price. Remote management capabilities improved, significantly reducing reliance on manual checks.

Raspberry Bye!

Despite initial success, Raspberry Pi solutions presented new challenges. While cost-effective and adaptable, they displayed limitations in reliability and durability. Sensitive to environmental fluctuations common in industrial settings, they also required substantial customization, delaying the expansion of digital transformation projects.

These vulnerabilities highlighted the inefficiencies in deploying consumer-grade technology in a demanding industrial context. PIDD needed a solution that was not only robust and reliable but also streamlined for quick deployment. Their experience led the district to seek an industrial-grade alternative better suited to their needs.

SOURCE: OPTO 22

PIDD groov EPIC enclosure.

The move to *groov*

Faced with limitations of Raspberry Pi, Paloma Irrigation and Drainage District sought a robust, industrial-grade IIoT platform. This search led VanHofwegen to a solution that transformed their operations: groov devices from industrial automation manufacturer Opto 22.

"I don't remember exactly how I found it, but what turned me on was that it was ready out of the box to be integrated with our existing Node-RED-based strategy. Beyond that, groov devices fit well into our future plans to migrate to Ignition® SCADA. Everything about it seemed designed around ease of use and reliability, which was exactly what we needed," VanHofwegen recalls.

Reasons for selecting *groov*

Industrial durability & reliability: With a proven track record in harsh environments—unlike the more sensitive Raspberry Pi—groov products reduce maintenance and ensure operational stability.

Affordability: groov RIO units at roughly $1,000 each are significantly cheaper than existing industrial-grade pump monitoring/control solutions, making them a more cost-effective option.

Modular design: groov EPIC's modular design allows for customization of I/O per pumping station, with the flexibility to

SOURCE: OPTO 22

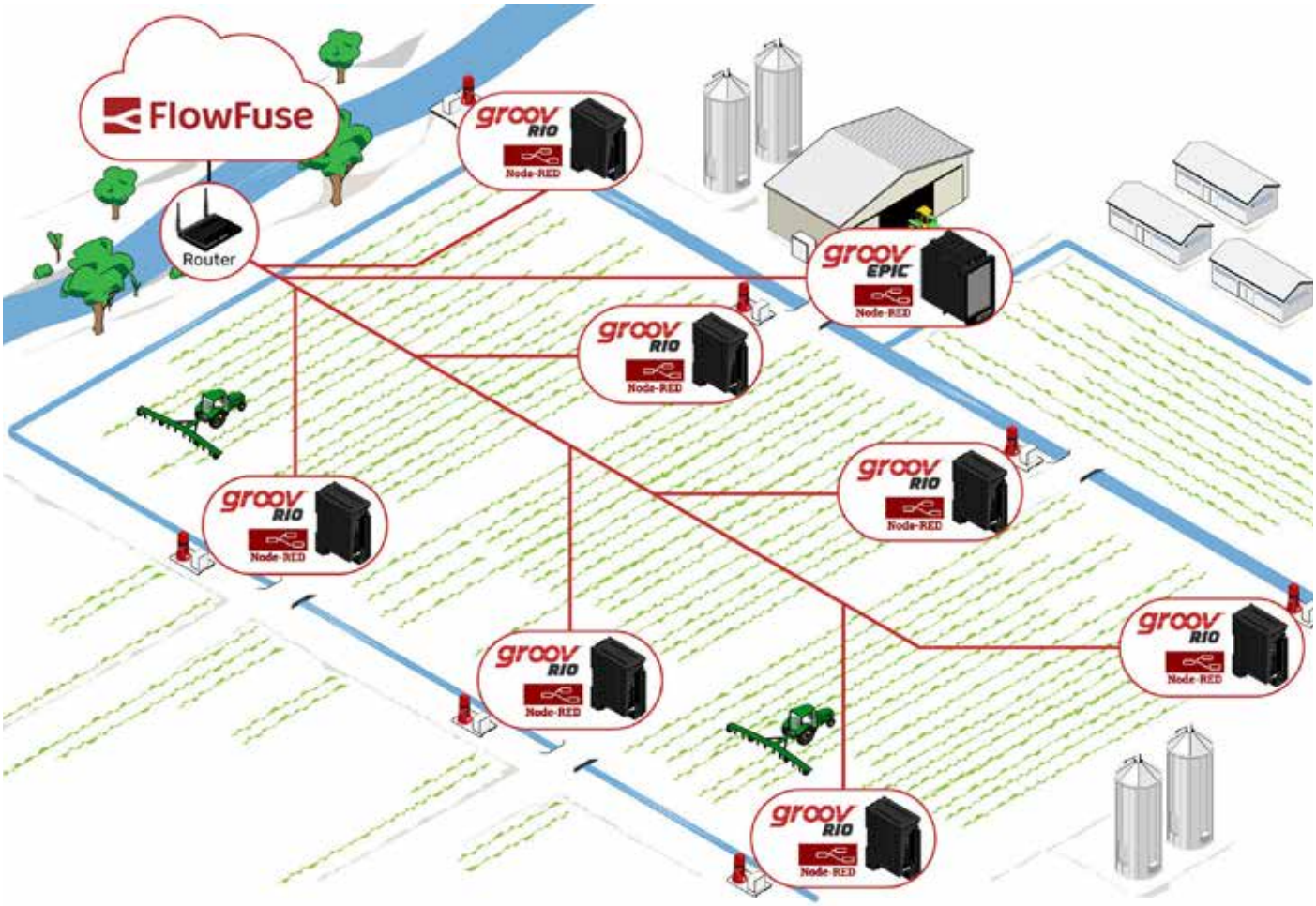


Illustration of PIDD site technology.

expand as needed.

In selecting groov products, PIDD embarked on a new phase of its modernization journey, now armed with technology that aligned with their goals for efficiency, reliability, and future scalability. They were poised to transform their water management practices and set a potential new standard for precision and control.

The *groov* learning journey

In the initial exploratory phase, VanHofwegen actively engaged with Opto 22's online training resources, YouTube® tutorials and demonstrations. These materials comprehensively cover groov product functionalities and proved crucial for understanding MQTT integration, which was vital for the district's IIoT roadmap.

The detailed walk-throughs and use-case scenarios in Opto 22's videos offered practical insights into the real-world capabilities of groov products, confirming their alignment with the district's needs.

This, combined with the district's existing MQTT expertise and HiveMQ® broker usage, underscored the potential for seamless integration and robust data communication, ultimately solidifying their decision.

Technical deep dive: OT and IT come together

Paloma Irrigation and Drainage District worked to bridge the gap between operational technology (OT) and information technology (IT) for seamless data flow and efficient management.

Automating Key Functions

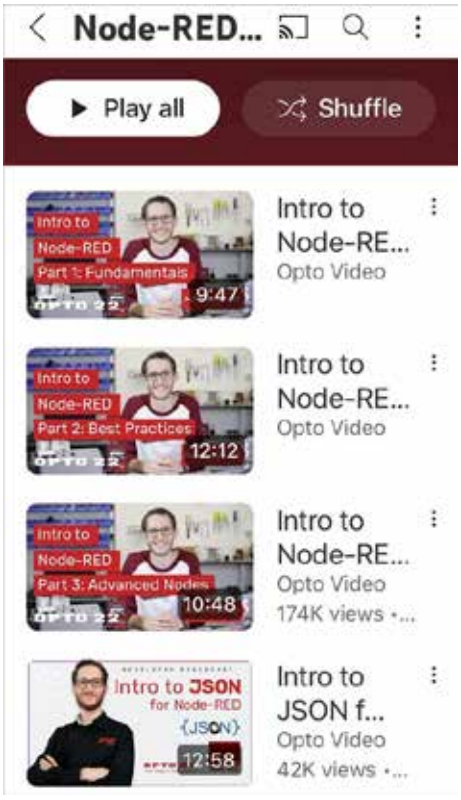
Leveraging his existing Node-Red expertise, VanHofwegen automated key functions like pump and oiler control, tank level control, environmental monitoring, and data transfers at pump stations. Automation reduced the need for frequent onsite visits and manual checks.

Innovation with AI

PIDD used ChatGPT® to simplify Node-RED flow development with JSON code Automating code creation empowered team members with varied skill sets and also boosted system flexibility.

Secure, Real-Time Data Communications

The team adopted MQTT communications for efficient and secure transmission of operational technology (OT) data across the network. This publish/subscribe



communication methodology enabled remote monitoring of water levels, pump statuses,

SOURCE: OPTO 22

PIDD solar-powered, automated control gates.

and informed decision-making. Security was prioritized through a centralized internet connection, minimizing cyber threats.

Actionable Insights from Raw Data

FlowFuse, already integrated within their IIoT strategy, offered a robust platform for transforming raw data into user-friendly dashboards, providing actionable insights accessible to all technicians. Additionally, FlowFuse complemented Node-Red's data flow capabilities by offering a secure environment for application deployment and monitoring.

Results and impact

While the PIDD's digital transformation is still in its infancy, VanHofwegen and his team have already ushered in a new era with the following clear benefits:

Reduced downtime & maintenance costs: Automation, especially pump lubrication, minimized component wear and tear, leading to significantly fewer breakdowns and an estimated $300,000 annual cost reduction. "This is easily going to pay for itself!" exclaimed VanHofwegen.

Enhanced remote monitoring & control: MQTT and FlowFuse enable real-time oversight of water levels, pump statuses, and other critical parameters, which resulted in fewer water shortages (reduced from monthly to yearly occurrences) and improved service reliability. As VanHofwegen notes, "Most times we are able to address and resolve issues before customers find out we are nearly out of water."

Positive impact on personnel: Operators appreciate the user-friendly technology and reduced need for manual checks, allowing for more efficient deployment and productivity. PIDD was able to maintain its existing staff but deploy them more effectively—a win-win.

Future prospects and final thoughts

Paloma Irrigation and Drainage District's initial IIoT journey offers valuable insights for organizations considering similar endeavors. Here are some key takeaways:

Demonstrating value and building upon success: Early ROI validation through small-scale IIoT projects using consumer-grade solutions can pave the way for more robust industrial deployments. Additionally, leveraging open-source tools and standard protocols makes it easier to transfer knowledge and scale up your system, supporting future expansion and efficiency improvements.

Positioned for further growth: PIDD has now established an IIoT foundation that positions them well for future enhancements. The scalable *groov* products and exploration of advanced solutions like Ignition SCADA integration hold promise for further water management efficiency and sustainability gains.

Application case history article by ***Opto 22.***

Learn More

Revolutionizing precision: the role of IoT in modern CNC technology

IoT's integration into CNC machines promises unprecedented levels of efficiency and precision, reshaping traditional manufacturing processes. This article delves into how IoT elevates CNC technology, detailing its benefits, applications, and the challenges it brings.

SOURCE: ISTOCKPHOTO

Critical criteria for selecting the right unmanaged switches include reliability, durability and conformity along with data transmission and installation.

THE FUSION OF THE INTERNET OF THINGS (IoT) and Computer Numerical Control (CNC) technology represents a transformative evolution in manufacturing, enhancing not only machine operations but also the entire production landscape.

What is IoT?

IoT refers to a network of interconnected devices that communicate and exchange data without human intervention. By embedding sensors and software in physical objects, IoT breathes intelligence into them, enabling automated and more efficient processes.

This technology is not limited to smart homes and consumer devices; it's making significant inroads across various sectors, including manufacturing, healthcare, and transportation, by offering smarter, data-driven insights.

What is CNC technology?

Computer Numerical Control (CNC) technology brings automation to machining processes such as drilling, milling, and turning through precise computer directives. CNC machines are prized for their accuracy, reliability, and ability to produce complex geometries with minimal human oversight. As a staple in modern manufacturing, CNC technology's adaptation to IoT is not just innovative but necessary for a competitive edge.

How does IoT enhance CNC technology?

IoT's role in CNC operations unlocks several transformative features:

- *Real-time data monitoring:* Continuous feedback from CNC machines allows for immediate adjustments and enhanced monitoring of production activities.
- *Predictive maintenance:* IoT enables predictive analytics to forecast machine failures before they occur, reducing downtime and maintenance costs.
- *Remote operation capabilities:* Operators can manage and troubleshoot machines from remote locations, enhancing operational flexibility.
- *Enhanced precision and automation:* IoT integration facilitates finer control over CNC machines, increasing the precision of operations without additional human intervention.

SOURCE: ISTOCKPHOTO

With its ability to bring real-time data, predictive analytics, and enhanced operational control, IoT is set to redefine the landscape of modern manufacturing.

Benefits of integrating IoT with CNC Machines?

Integrating IoT with CNC machines brings numerous advantages:

- *Increased efficiency:* Automated processes and optimized machine use reduce idle times and enhance throughput.
- *Reduced operational costs:* Efficient resource use and preventive maintenance cut down costs significantly.
- *Improved safety:* Enhanced monitoring helps in identifying and rectifying potential safety hazards, ensuring safer workplace environments.
- *Enhanced data collection and analysis:* IoT provides a wealth of data that can be used to refine processes and improve product quality.

Challenges integrating IoT with CNC?

While the integration of IoT with CNC technology offers extensive benefits, it also presents several challenges:

- *Security risks:* Increased connectivity exposes CNC machines to potential cybersecurity threats, necessitating robust security measures.
- *Integration complexities:* Merging IoT with existing CNC systems can be complex and costly, requiring significant technological adjustments.

IoT-enabled CNC applications in various industries

The application of IoT-enhanced CNC technology spans several industries, significantly impacting:

- *Automotive:* Streamlining production lines and improving component precision.
- *Aerospace:* Enabling the manufacture of complex, lightweight components critical for aerospace applications.
- *Consumer Electronics:* Enhancing the efficiency and precision of electronic component production.
- *Healthcare:* Improving the fabrication of medical devices and equipment with higher precision and control.

Case Studies: Success Stories of IoT in CNC

Several industries have seen remarkable success with IoT in CNC, including:

- *Automotive:* Major car manufacturers have integrated IoT to optimize their machining processes, resulting in reduced production times and improved quality.
- *Aerospace:* Aerospace giants use IoT for CNC machining in the aerospace industry to produce more reliable and precise components, pushing the boundaries of aviation technology.

Core components of IoT in CNC machines?

Key components of IoT in CNC include:

- *Sensors and actuators:* Collect data and act upon it to adjust operations in real-time.
- *Data analytics platforms:* Analyze the vast amounts of data generated to enhance decision-making.
- *Network connections and protocols:* Facilitate the seamless transfer and communication of data across devices.
- *User interfaces and control systems:* Allow operators to interact efficiently with IoT-enhanced CNC machines.

Future trends: where is IoT in CNC heading?

Emerging trends in the integration of IoT in CNC focus on:

- *Increased adoption of AI and machine learning:* These technologies are expected to further enhance automation, making CNC machines more intelligent and self-sufficient.
- *Market growth:* As industries continue to realize IoT's potential benefits, its adoption in CNC processes is set to increase, driving significant market growth.

Step-by-step to implementing IoT in CNC technology

Implementing IoT in CNC involves:

- *Assessment and planning:* Evaluate current CNC capabilities and define IoT objectives.
- *Choosing the right technology and partners:* Select appropriate IoT technologies and collaborate with experienced partners.
- *Implementation process:* Integrate IoT devices and software into existing CNC systems.
- *Monitoring and maintenance:* Continuously monitor the system and perform regular maintenance to ensure optimal operation.

Best practices for IoT security in CNC?

To ensure safe IoT operations in CNC, consider:

- *Robust authentication and encryption protocols:* Secure all data exchanges to prevent unauthorized access.
- *Regular security audits:* Conduct frequent security checks to identify and mitigate potential vulnerabilities.

Conclusion

The integration of IoT into CNC technology is not just an enhancement—it's a revolution. With its ability to bring real-time data, predictive analytics, and enhanced operational control, IoT is set to redefine the landscape of modern manufacturing. As this technology continues to evolve, its impact on CNC technology promises even greater efficiencies, pushing the boundaries of what's possible in manufacturing.

*Technology article by **Techni Waterjet.***

Visit Website

High speed backbone for Ethernet and CAN bus-based field devices

AUTBUS broadband bus technology provides a solution for industrial networking that integrates Time-Sensitive Networking (TSN) and IPv6 technologies into a two-wire broadband bus system. Engineered to meet the demands of smart manufacturing, AUTBUS offers high bandwidth and real-time communication capabilities.

A MULTI-DROP DATA NETWORK OPERATING as a high speed backbone for Ethernet and CAN bus-based field devices offers cost and space savings thanks to just one data cable, multi-protocol transmission and a multi-drop connection. With the ABN300 series, KLG Smartec presents an Ethernet AUTBUS signal converter based on the AUTBUS industrial data bus standardised by the IEC.

AUTBUS data connection

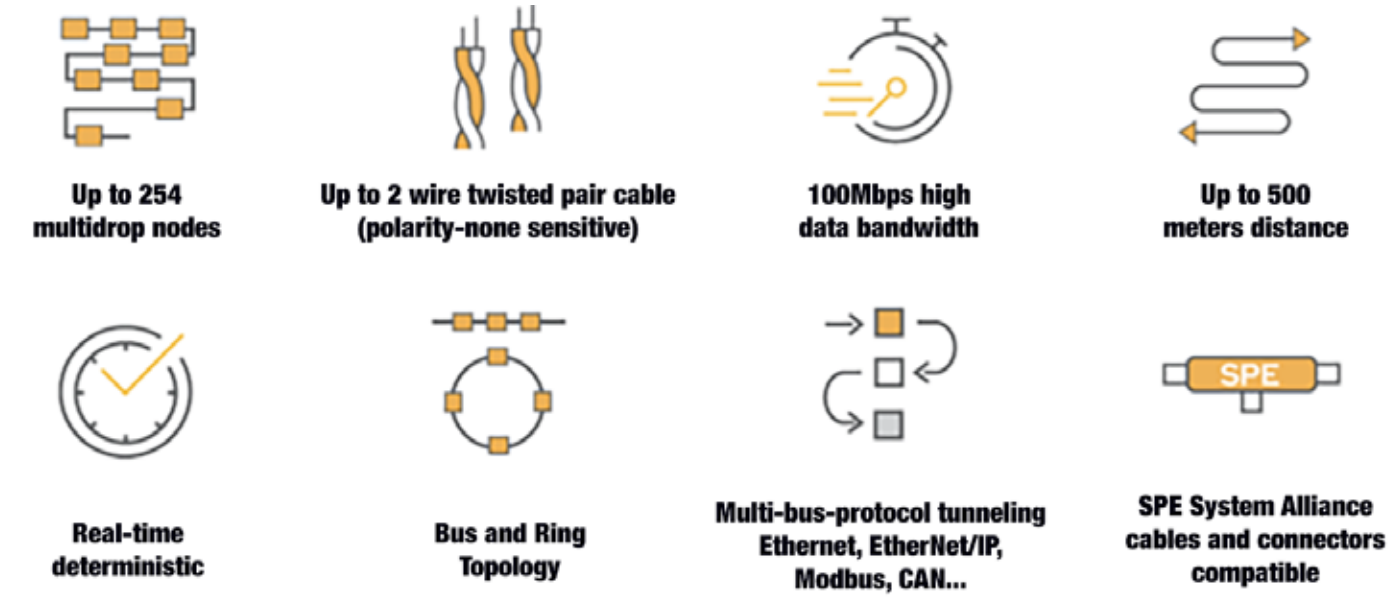
The ABN300 series supports an AUTBUS data connection and, depending on the model variant, an additional interface for data transmission from devices with Ethernet, CAN or RS485 data connections. The ABN300 series enables the effective transmission of data protocols based on these interfaces via the AUTBUS data backbone network.

With a size of only 30x115x68mm and a weight of 200gr., the ABN300 signal converter series is suitable for integration into a wide variety of housing types and control cabinets thanks to its slim housing and integrated top-hat rail mounting clamp or with the optional screw fastening. The ABN300 series requires a supply voltage of 24-48 VDC, has a power consumption of only up to 3 watts and is designed for ambient temperatures of -40 to +70°C.

SOURCE: KLG SMARTEC

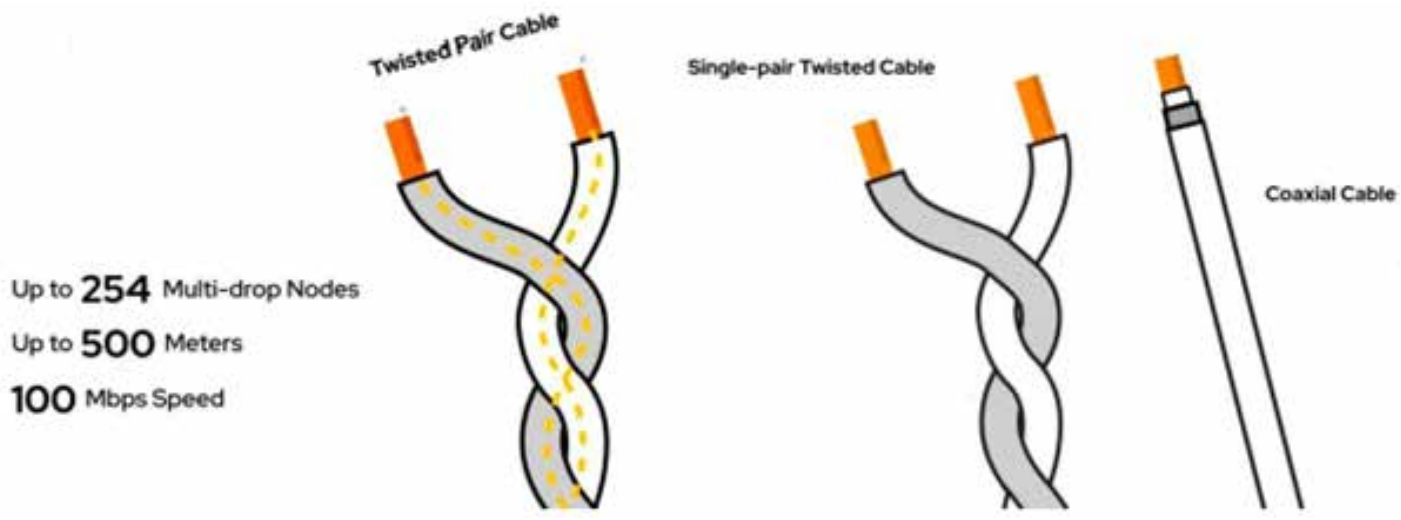
With the ABN300 series, KLG Smartec presents an Ethernet AUTBUS signal converter based on the AUTBUS industrial data bus standardised by the IEC.

AUTBUS is an industrial broadband fieldbus that was standardised by the IEC in 2023. AUTBUS supports data transmission via a balanced cable, e.g. a simple twisted pair cable, or via an unbalanced cable, e.g. a coaxial cable. With a qualified twisted and shielded two-wire cable of type AWG-16 to AWG-26, up to 254 multidrop data network nodes can be reached over a distance of up to 500 metres at a data transmission speed of



SOURCE: KLG SMARTEC

AUTBUS offers a series of technology advantages compared to alternative solutions.



SOURCE: KLG SMARTEC

Key technology benefits of AUTBUS.

100 Mbps. Compatibility with the data cables and connectors originally specified for Single Pair Ethernet (SPE) means that a stable data network can be installed, but it is also possible to use simple PCB connectors.

On a physical level, AUTBUS utilises OFDM (Orthogonal Frequency Division Multiplexing) technology to adapt to channel conditions and protect against narrowband interference, making AUTBUS a perfect solution for industrial communication technology in harsh environments. OFDM technology is used in wired and wireless communication. With its characteristics such as broadband, low latency and determinism, AUTBUS is predestined for the field of industrial wired data communication. The critical deterministic challenges exist in a variety of industrial applications for which AUTBUS can be of great benefit.

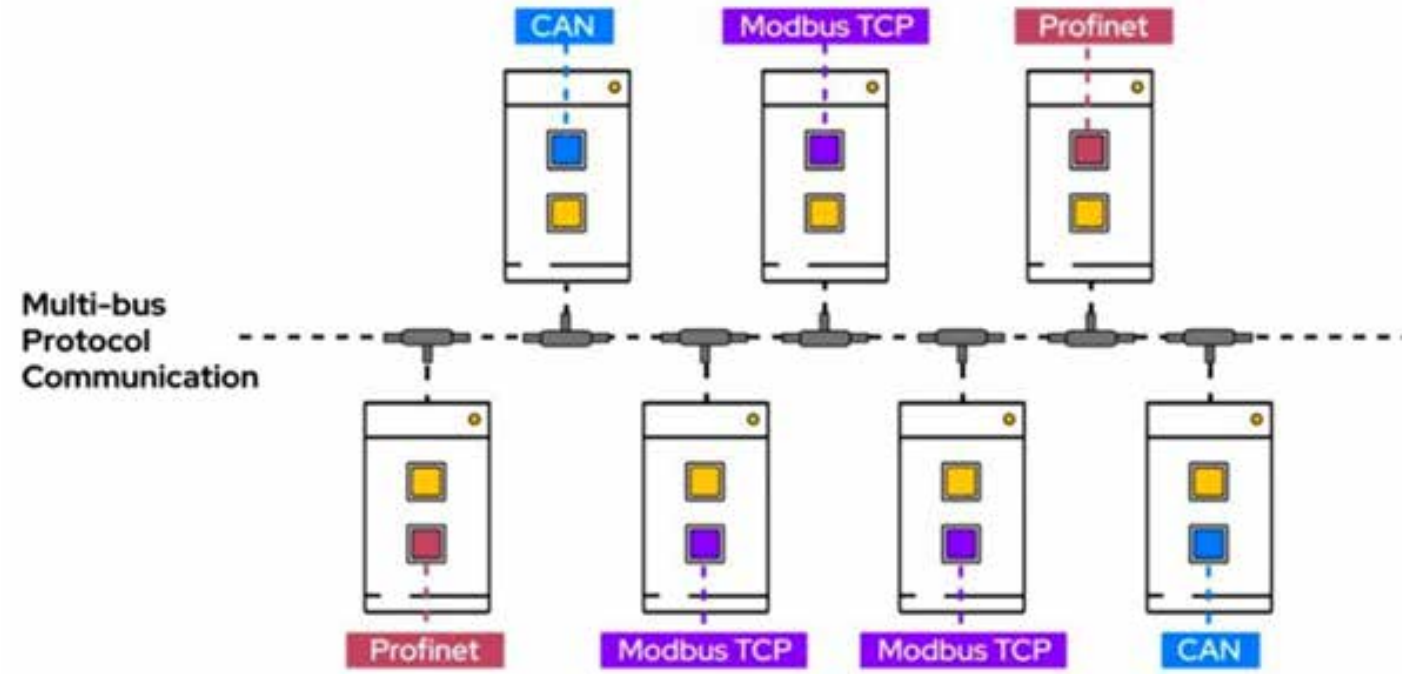
Technology advantages

A major advantage of AUTBUS is data transmission via a virtually uninterrupted data backbone network using a daisy-chain device connection. The twisted two-wire cable can, for example, be tapped directly and without cable interruption via a special SPE-T connector with a maximum stub length of upto 50 cm or the data cable can be disconnected and connected to a PCB connector with four 2-way bridged connections supplied directly with the ABN300. If the SPE connector or the PCB connector is disconnected from the ABN300, the AUTBUS backbone network is not interrupted as the cable is still bridged.

Increased reliability is achieved by connecting the two ends of the data cable together, taking into account the maximum cable length of up to 500 metres. This creates a data network ring without the need for an active ring redundancy manager. This makes it possible to connect end devices with an Ethernet connection or several such end devices to the AUTBUS backbone network via an unmanaged Ethernet switch.

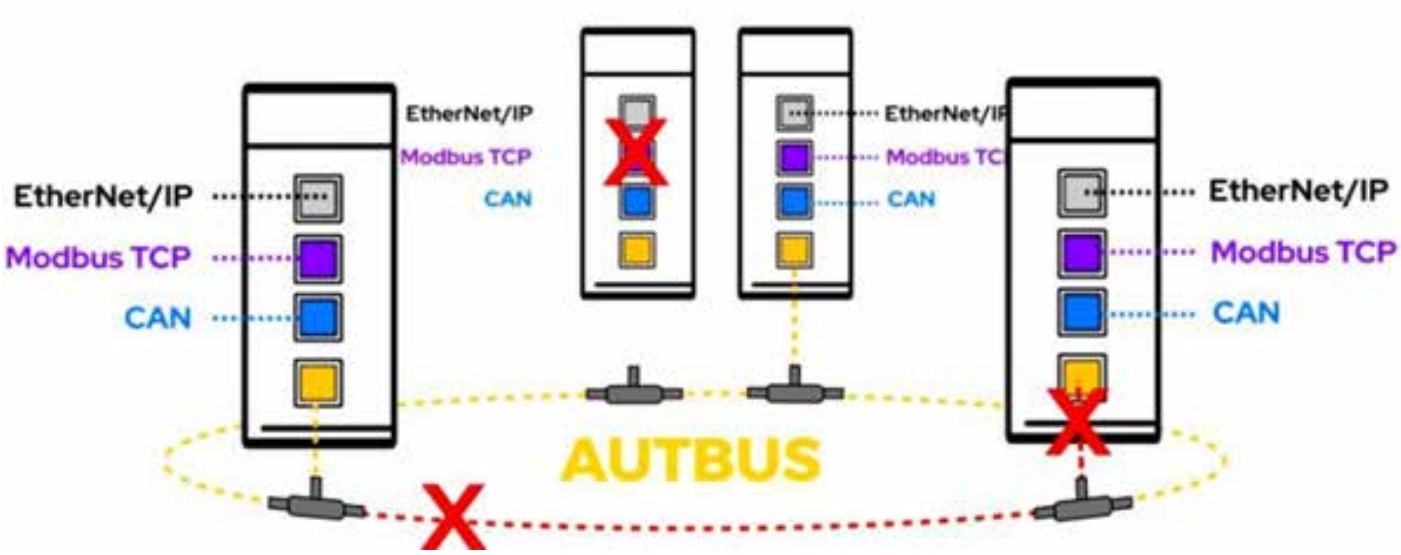
AUTBUS also supports multi-protocol transmission through data tunnelling, i.e. Ethernet-based transmission protocols, for example, but also CAN bus or RS485 can be transmitted transparently from one data connection point to another simultaneously via the passive AUTBUS Multidrop Backbone without these protocols having to be translated or additionally configured.

Thanks to the standard AUTBUS Plug & Play (AP&P), the devices are very easy to install



SOURCE: KLG SMARTEC

Multi-bus protocol communications provides support for PROFINET, Modbus TCP and CAN communications.



SOURCE: KLG SMARTEC

Key technology benefits of AUTBUS.

and configure. Depending on the end device, the operating mode is selected via a rotary switch integrated on the front and a DIP switch. A software configuration tool is also available for special applications.

Any ABN300 converter can be defined as the master for the entire AUTBUS communication; all other ABN300 converters are configured as clients. It is also possible, for example, to define the assignment of the data bandwidth if necessary, e.g. if devices with different transmission rates are to be integrated, such as the networking of e-charging stations and additional surveillance cameras or a WiFi router in an e-charging park

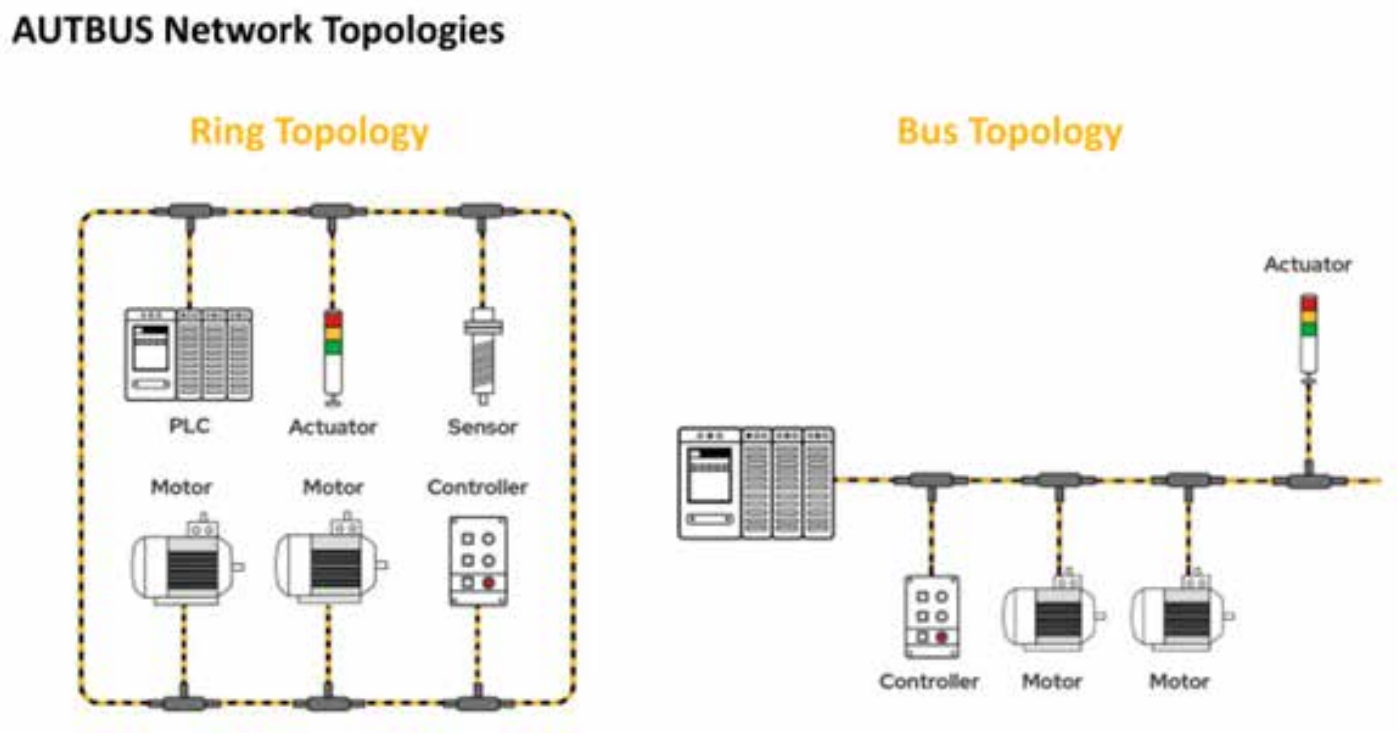
The main features of AUTBUS and the ABN 300 are:

- Up to 254 multidrop nodes
- 2-wire twisted pair cable (polarity insensitive)
- 100Mbps high data bandwidth
- Up to 500 metres distance
- Deterministic in real time
- Bus and ring topology
- Multi-bus protocol tunnelling: Ethernet based protocols, CAN, RS485
- Compatible with the Single Pair Ethernet connectors and cables

AUTBUS data networking and economic efficiency using the example of an e-charging station park.

In many e-charging station parks, the charging stations are networked with star-shaped Ethernet data cabling. A 16-port Ethernet switch, for example, is used as the central data switch. The energy manager, all e-charging stations and other IP-capable devices are each connected to the Ethernet switch with a data cable. If, for example, 10 charging stations, an energy manager, 2 surveillance cameras and possibly a router are to be connected, at least 14 data cables of different lengths are required.

If the charging station park is to be expanded, a new data cable must be laid for

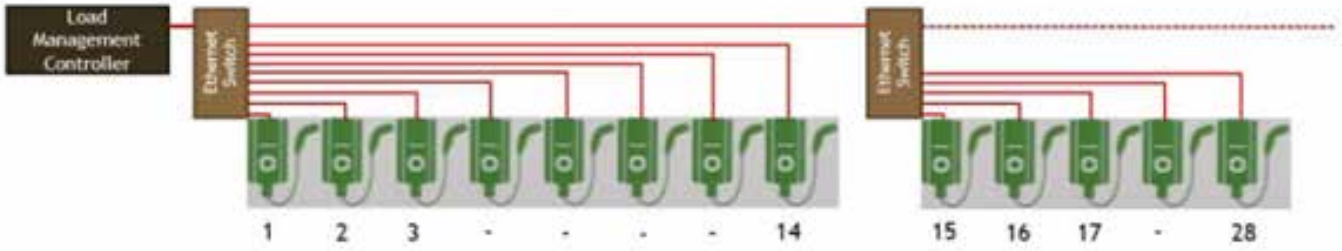


SOURCE: KLG SMARTEC

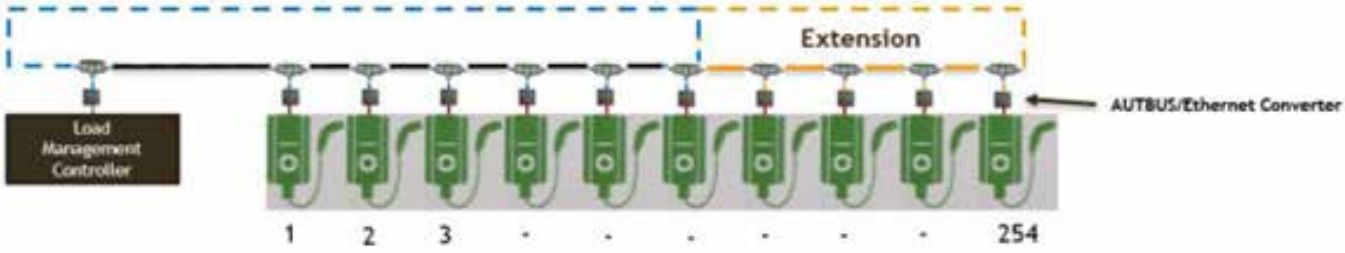
AUTBUS network topologies.

SOURCE: KLG SMARTEC

Typical Ethernet start network topology



AUTBUS-Ethernet Multidrop Converter with bus or ring topology to connect EV Charging stations.



AUTBUS EV chargng solution.

each additional charging station. Based on a simplified calculation with total cabling costs of 5 euros per metre of data cable laid, a distance of 5 m between the Ethernet switch and the first charging station, a distance of 2.5 m between the 30 charging stations in total, the installation costs for the 1238 m of data cable will amount to approx. 7000 euros. This also includes a second Ethernet switch, which has to be integrated after 15 charging stations, and 30 data cables, which are laid as a large bundle via a cable route.

Alternatively, users can install an AUTBUS data network and only need a high-quality, shielded and twisted 2-core data cable and connect the e-charging stations to an AUTBUS Ethernet converter ABN300 each. 78 metres of data cable and 30 AUTBUS Ethernet converters ABN300 are required for this. This results in total costs for laying the data cable and the AUTBUS ABN300 converters of approx. 3500 euros, which corresponds to a saving of 50% compared to Ethernet star cabling. If you want to retrofit more charging stations, you only need one approx. 2.5 metre long data cable and one ADM300 converter per charging station for up to 254 connected charging stations. If the two ends of the data cable are then connected with another data cable over the entire length, a data ring with increased reliability is created.

Summary

The AUTBUS ABN300 converter series is an optimised data communication solution, e.g. as a backbone data network for EV charging stations, PV systems and building automation.

Cost savings result from the use of only one data cable and the resulting reduced installation effort, but also from faster commissioning due to reduced connection errors, which in turn reduces the need for specialised IT specialists.

Longer system life is provided thanks to ring redundancy of the data network.

Easy system expansion is achieved through cable extension and multidrop connections.

For more information on the ABN300 converters, visit www.klgsmartec.com and for more information on AUTBUS technology, visit www.AUTBUS.org.

*Technology report by **KLG Smartec.***

Visit Website

Power Over Ethernet for industrial network applications

PoE has evolved to support high-density, widely distributed industrial networks that increasingly rely on edge computing. PoE++ systems can now deliver up to 90W per port, enough to operate the newest and most power-hungry network IoT sensors, devices and controllers, reducing the dependence on traditional power outlets.

SOURCE: ANTAIRA

IEEE PoE Specifications								
Standard	**802.3af**			**802.3at**	**802.3bt**		**802.3bt**	
Type	**Type 1**			**Type 2**	**Type 3**		**Type 4**	
Name / Year	PoE / 2003			PoE+ / 2009	Hi PoE / 2018		Hi PoE / 2018	
Voltage	44V/50V				50V		52V	
Supported PD Class	1	2	3	4	5	6	7	8
PSE Output Power to Single PD	4W	6.7W	14W	30W	45W	60W	75W	90W-100W
PD Input Power	3.84W	6.49W	13W	25.5W	40W	51W	62W	71.3W
Ethernet Pairs	2-Pair			2-Pair or 4-Pair	4-Pair			

IEEE PoE Standards.

POWER OVER ETHERNET, OR POE, IS A WIDELY used term to refers to any technology that enables an Ethernet device to receive and send power over the same cable as data. With this article, we'll provide an overview of PoE technology to help you determine which PoE solutions are compatible with your network application.

Power over Ethernet: A brief history

In the 1990s, prior to the IEEE stepping in, "power injection" was the label used to describe the concept of supplying electricity over an Ethernet cable. So-called "power injectors" had no intelligent protocol or safety considerations. They only worked by supplying the power over Ethernet, either AC or DC current, utilizing the spare pairs that 100Base-TX Ethernet did not use. In doing so, power injectors basically emulated how traditional PSTN (public switched telephone network) landline phones operate.

Standardizing Power over Ethernet was first proposed by the IEEE 802.3 Working Group in 1999. The group's original standard, IEEE 802.3af, was ratified in 2003 thus ensuring interoperability across a broader range of connected devices.

IEEE 802.3af established a uniform, safer way to deploy PoE. It defined Powered Devices (PDs) as equipment that received power and Power Sourcing Equipment (PSE) as those that supplied power. PDs and PSEs would operate within a voltage range of 44-57V with a maximum power output of 15.4W per port. Power could be sent to a PD using two of the four twisted pairs that are available in typical Category 5 (Cat 5) cable by pins 4 and 5 or pins 7 and 8, or by data using four twisted pairs by pins 1 and 2 or pins 3 and 6.

Notably, the IEEE 802.3af standard included a mechanism to protect connected devices that do not support PoE. Specifically, a 25-kW resistor is placed in between the power pairs of the powered device, so that transmit power is only supplied by the power source if something close to that resistive value is detected.

Increased PoE power demands

As mentioned earlier, IEEE 802.3af specifies a maximum output of 15.4W per port. Yet due to cable power loss, the minimum guaranteed power available at the PD is only 12.95W per port. While that is plenty of power for simple devices, it falls short of the power and consumption needs of new higher wattage devices being deployed in Smart City and Industrial Internet of Things (IIoT) applications.

To remedy this situation, the IEEE 802.3 Working Group approved IEEE 802.3at, its second PoE standard, in 2009 that featured a new power class that could deliver up to 30W on the port and maximum guaranteed power of 25.5W to a PD. Although this altered the existing standard, IEEE 802.3at still supplied power over two pairs and it topped out at a safe 57V port voltage. IEEE 802.3at allowed for high power on-hungry devices, such as PTZ cameras, alarm systems and wireless access points, to be powered by a nearby PoE-enabled industrial Ethernet switch or other PSE. IEEE 802.3at is also backward compatible with the original standard.

The newest PoE standard, IEEE 802.3bt: Type 3- 45W or 60W (PSE) / 51W (PD); Type 4- 90W (PSE) and 71.3W (PD), was ratified in 2018. IEEE 802.3bt was designed to stay ahead of power demands since there simply aren't many devices on a network that need more power than 90W in PoE delivery today.

Unlike previous standards, IEEE 802.3bt focuses on using all four twisted-pair cables within a single cable or standard Ethernet cable rather than two. The standard includes support for 2.5GBASE-T, 5GBASE-T, and 10GBASE-T, while previous PoE standards have a maximum speed of 1-Gbps.

Because of IEEE 802.3bt, the ongoing

SOURCE: ANTAIRA

IEEE 802.3af established a uniform, safer way to deploy PoE.

shift to Ethernet-based industrial control systems and the merging of IT and data lines in OT networks is certain to be accelerated. Having data and 90W PoE supplied by a single Ethernet connection is ushering in a new era for industrial networks.

Active PoE vs Passive PoE

Now that we have a better handle on PoE standards, let's look at two other terms that are often misunderstood: active PoE and passive PoE.

Active PoE, also referred to as standard PoE, is any form of PoE in which Powered Devices (PD) and Power Sourcing Equipment (PSE) negotiate the proper voltage via a handshake procedure to ensure a valid PD is connected. During the handshake, the active PoE switch (PSE) applies voltage to verify the presence and value of a resistor within the PD. It then delivers the amount of power based on the response of the PD. Should the handshake not be completed successfully for any reason, the PD won't receive the maximum power delivered from the PSE, protecting the PD from harm.

Passive PoE is the non-standard form. Passive PoE switches, adapters, injectors or other PSE have no negotiation or communication procedure and therefore do not conform to any of the IEEE standards we discussed. In general, a passive PoE PSE will supply electricity on the spare wire pairs of the twisted pair cable it is connected to at a specific fixed voltage, whether the connected end-devices supports PoE or not. However, since there is no standard, it is possible for passive PoE to be implemented with gigabit Ethernet despite all four pairs of wires being used for data transmission.

Passive PoE PSEs are mainly divided into 12V, 24V, and 48V fixed output voltages. If you are planning on using Passive PoE as a power source, you must match the exact voltage of the passive PoE PSE to the exact voltage of the data terminal equipment or powered device. If not, it may sustain electrical damage once connected. If you know the voltage and have no plans on expanding the network, Passive PoE can serve as a simple, cost-effective way of powering cameras, Wi-Fi access points, VoIP phones, and other IoT devices.

Adding PoE to industrial networks

The simplest method of adding these PoE powered devices to a network is via a PoE enabled industrial switch. In that case, all that is required is to run an Ethernet cable from the industrial switch port that delivers power to the PD. But what if there is no PoE enabled Ethernet switch on the network to supply power? Here are a few PSE options:

SOURCE: ANTAIRA

The Antaira LMP-1204G-SFP-bt-24-T-BOS 12-port industrial Gigabit PoE++ managed Ethernet switch is embedded with four 10/100/1000TxEthernet ports that support IEEE 802.3bt for a maximum of 95W/port.

PoE injectors are deployed with a PD and the non PoE enabled networking switches. It typically features an RJ45 Ethernet in, an RJ45 Ethernet out and a Power in that goes to a wall outlet or power source.

PoE midspans are a type of injector but are used to power devices at distances within the traditional 100-meter limit of Ethernet cables.

PoE media converters transparently link two different media, such as fiber to copper, supplying both power and distance extension when the PD is far away from the nearest available network cable or industrial switch.

PoE splitters are commonly used for deploying remote non-PoE devices with no power loss and no nearby AC outlets. PoE splitters are used together with industrial PoE switches and PoE injectors. They supply power by separating the power from the data and feeding it to a different input that a non-PoE compliant device can utilize, as opposed to accepting both data input and power input and combining them into a single output.

Since its introduction, power over Ethernet has been a game-changer in the world of connectivity and has greatly simplified the installation and operation of a variety of devices, from surveillance cameras and sensors to access points and HVAC. PoE has evolved to support today's high-density, widely distributed industrial networks that increasingly rely on edge computing. PoE++ systems can now deliver up to 90W per port, enough to operate the newest and most power- hungry network IoT sensors, devices and controllers, reducing the dependence on traditional power outlets.

Henry Martel, Field Application Engineer, ***Antaira Technologies.***

Visit Website

IO-Link master blocks

Added features, coupled with on-machine capability, provide a boost in functionality and performance.

Rockwell Automation advances automation efficiency with enhanced ArmorBlock 5000 IO-Link master blocks.

Manufacturers can further streamline operation processes and reduce deployment time with the release of an enhanced firmware and Add-on Profile (AOP) update in the Allen-Bradley® ArmorBlock 5000® IO-Link master blocks. The newly added features, coupled with the On-Machine™ capability, provide a significant boost in functionality and performance for applications within demanding industrial environments.

Highlights of the new capabilities in ArmorBlock 5000 IO-Link master blocks include:

Generic IO-Link profile allows compatibility with a wider range of IO-Link devices, enabling expanded machine capabilities for existing automation systems.

Process Data only mode further simplifies the IO-Link integration experience by transmitting data specified by the IO-Link master block device.

Automatic download of IODD files via the IO-Link device registration tool helps to simplify the workflow, speeding up configuration and optimizing overall efficiency.

SOURCE: ROCKWELL AUTOMATION

EDS file import/export functionality enables more efficient project deployment where users can leverage the same EDS file across different machines.

Change type functionality allows the replacement of an IO-Link master block with a different power variant without device and software reconfiguration.

Rockwell Automation

Visit Website

Functional safety technology

The SCP 211 safety CPU from SIGMATEK offers fast processing speeds and extensive memory.

A programmable safety system is a must-have to develop machines and systems modularly, economically and in a short time. With the SCP 211, SIGMATEK offers a very powerful safety CPU that supports new functions on the software side that simplify the creation and handling of safety applications. Safety development is carried out in the LASAL SAFETYDesigner on certified function blocks based on PLCopen.

Following the example of object-oriented programming, which has characterized SIGMATEK controllers on the application side for 25 years, it is now possible to create customer-specific macro libraries for safety applications. The special feature of the LASAL safety macros is that they can be structured in a multi-level hierarchy. Each macro is encapsulated in itself and can be tested independently as it has its own CRC test value. This significantly reduces the effort required for overall tests to obtain certifications.

The LASAL SafetyDesigner offers developers of safety-related applications the option to design them completely parameterizable and therefore very flexible. It is only necessary to create one safety application for a machine or system with numerous options, which applies to all equipment variants.

SOURCE: SIGMATEK

Parameter lists as engineering turbo

The parameterization, i.e. the adaptation to the often customer-specific concrete machine, takes place via a parameter list. Like the application itself, the parameter list is also protected. To ensure security, password-protected mechanisms are used when transferring the lists for setting different equipment variants.

SIGMATEK

Learn More

Layer 3 rackmount Ethernet switches

High-bandwidth Ethernet switch portfolio speeds up data-driven transformation of industrial applications.

SOURCE: MOXA

Industry-leading Layer 3 rackmount Ethernet switches for high-bandwidth industrial networks.

INDUSTRIAL DIGITAL TRANSFORMATION drives extensive deployment of IoT and AI-enabled technologies, requiring high-bandwidth networks offering low latency and higher data transfer speeds.

Moxa has announced new MRX Series Layer 3 rackmount Ethernet switches that support 64 ports with up to 16 ports of 10GbE speed to accelerate data aggregation for industrial applications and help users build high-bandwidth network infrastructure to realize IT/OT convergence with the EDS-4000/G4000 Series Layer 2 DIN-rail Ethernet switches supporting 2.5GbE uplink options.

The rising number of connected devices and increasing adoption of data-intensive applications like video data transmission are boosting the requirement for high-bandwidth networks. Video surveillance and AI-oriented applications with ultra-high definition (UHD) videos are examples of these demands. Furthermore, the analytic needs for more intelligent applications for business innovation also make the MRX-Q4064/G4064 Series ideal Ethernet switches for handling high-bandwidth transmission requirements.

"Although there are many high port density, high-bandwidth commercial Ethernet switches on the market, they seldom are tailored for industrial applications," said Paul Hsu, product manager of Industrial Ethernet Infrastructure Business at Moxa. "To fulfill demands of aggregating data transmissions in large-scale industrial applications, the MRX-Q4064/G4064 Series is designed with multiple 10GbE ports and industrial-grade reliability to maximize high-bandwidth network uptime for continuous industrial operations."

The MRX-Q4064/G4064 Series combines impressive switching performance with a sophisticated exterior and is the winner of the Red Dot Product Design 2024 award. The rackmount Ethernet switches offer industry-leading 16 and 8 10GbE ports, respectively, aggregating large-scale data transmissions. In addition, our port trunking features allow grouping up to eight 10GbE ports into a single 80 Gbps link to maximize transmission bandwidth. The MRX-Q4064/G4064 Series delivers both system and network reliability. Continuous system operation relies on stable operating temperatures and power supplies. Intelligent temperature control functions, 8 fan modules, and dual power supply modules ensure MRX-Q4064/G4064 Series uptime and stability. Moxa's Turbo Ring and High-availability Static Trunk (HAST) technologies provide redundant network paths and connectivity to achieve high availability for large-scale network infrastructure.

The MRX-Q4064/G4064 Series was developed to simplify deployment and maintenance for engineers. The modular design of its Ethernet interfaces, power supplies, and fans tremendously increases deployment flexibility. Our rackmount Ethernet switches have built-in LCD Modules (LCMs), allowing engineers to check device status and quickly troubleshoot. Hot-swappable modularity empowers module swaps without affecting operations.

Game-changing Layer 2 DIN-rail Ethernet Switches Strengthen Network Resilience

While the new MRX-Q4064/G4064 Series Layer 3 switches bridge IT and OT networks, an interoperable, secure, and reliable Layer 2 switch is equally essential as a building block for converged industrial networks. Our EDS-4000/G4000 Series Layer 2 switches not only feature 2.5GbE uplink options that work perfectly to build high-bandwidth networks with the MRX-Q4064/G4064 Series Layer 3 switches, but also support the multitude of industrial protocols, network security features, and network redundancy technologies required to streamline multi-system integrations with secure and reliable connectivity.

Moxa

Visit Website

Industrial networking solutions

Ethernet-APL field switch and plantPerfect Monitor for industrial network condition monitoring.

Ethernet-APL field switch

Softing Industrial presented its new "aplSwitch Field" at ACHEMA 2024. This state-of- the-art 16-Port Ethernet-Advanced Physical Layer (Ethernet-APL) Field Switch with optional PROFIBUS Process Automation (PA) proxy is designed for use in Zone 2 and establishes seamless connectivity down to the field level.

The "aplSwitch Field" enables the transparent connection of "Two-Wire Intrinsically Safe Ethernet" (2-WISE) Ethernet-APL field devices to higher-level Industrial Ethernet networks, providing these devices with intrinsically safe power. Additionally, the "aplSwitch Field PA" variant supports the connection of both Ethernet-APL field devices and PROFIBUS PA devices, ensuring smooth integration into existing industrial systems.

Advanced Features and Compatibility of "aplSwitch Field" The "aplSwitch Field" offers easy integration into leading Distributed Control Systems (DCS) and Asset Management Systems (AMS) with 16 Ethernet-APL spur "2-WISE" ports, supporting PROFINET with Media Redundancy Protocol (MRP) ring topology.

It is compatible with major systems like Emerson, Siemens, and ABB, ensuring stable networks through ingress/egress support. Extensive diagnostics are facilitated by integrated PROFINET functions and a local display, enhancing commissioning and maintenance processes. The "aplSwitch Field" is designed for installation in Ex Zone 2, with connectivity for field devices in Ex Zone 0 and 1. It has a robust housing with protection class IP30.

Flexible power classes and migration options: "aplSwitch Field" and "aplSwitch Field PA" variants The "aplSwitch Field" variant supports both Power Class A and Power Class B. This ensures that field devices with higher power requirements can also be operated without any problems. The PA variant – "aplSwitch Field PA" – enables the migration of existing PA infrastructure to Ethernet-APL topology.

SOURCE: SOFTING INDUSTRIAL

The aplSwitch Field establishes seamless connectivity down to the field level.

"plantPerfect Monitor" provides a comprehensive condition monitoring solution.

plantPerfect Monitor for condition monitoring of industrial communication networks

Softing Industrial also presented "plantPerfect Monitor", an innovative solution for comprehensive condition monitoring of industrial communication networks and installed systems.

"plantPerfect Monitor" provides detailed insights into the status of industrial networks. Version 1.00 is designed for use with Softing's hardware gateway "smartLink HW-DP", which enables controller-independent access to PROFIBUS DP networks.

Softing Industrial will launch an extended version of the "plantPerfect Monitor" for status monitoring of PROFINET devices in the fourth quarter of 2024. That version will be compatible with Softing's "smartLink HW-PN" hardware gateway.

Central access and comprehensive monitoring for PROFIBUS devices

"plantPerfect Monitor" provides centralized access to real-time and historical data. Through live inventory, it provides an overview of all installed PROFIBUS devices and monitors the status of all connected PROFIBUS devices, including PROFIBUS diagnostic messages. Convenient access is provided via a web browser and can be shared by multiple organizations and users. The solution is deployed using a container architecture on a Windows workstation.

Modern technology for plant operators and maintenance personnel

"plantPerfect Monitor" is a specifically designed for plant operators and maintenance personnel. It enables efficient monitoring of industrial networks and facilities. With state-of-the- art technology, "plantPerfect Monitor" meets the requirements of a modern and safe Operational Technology (OT) application, setting new standards in condition monitoring.

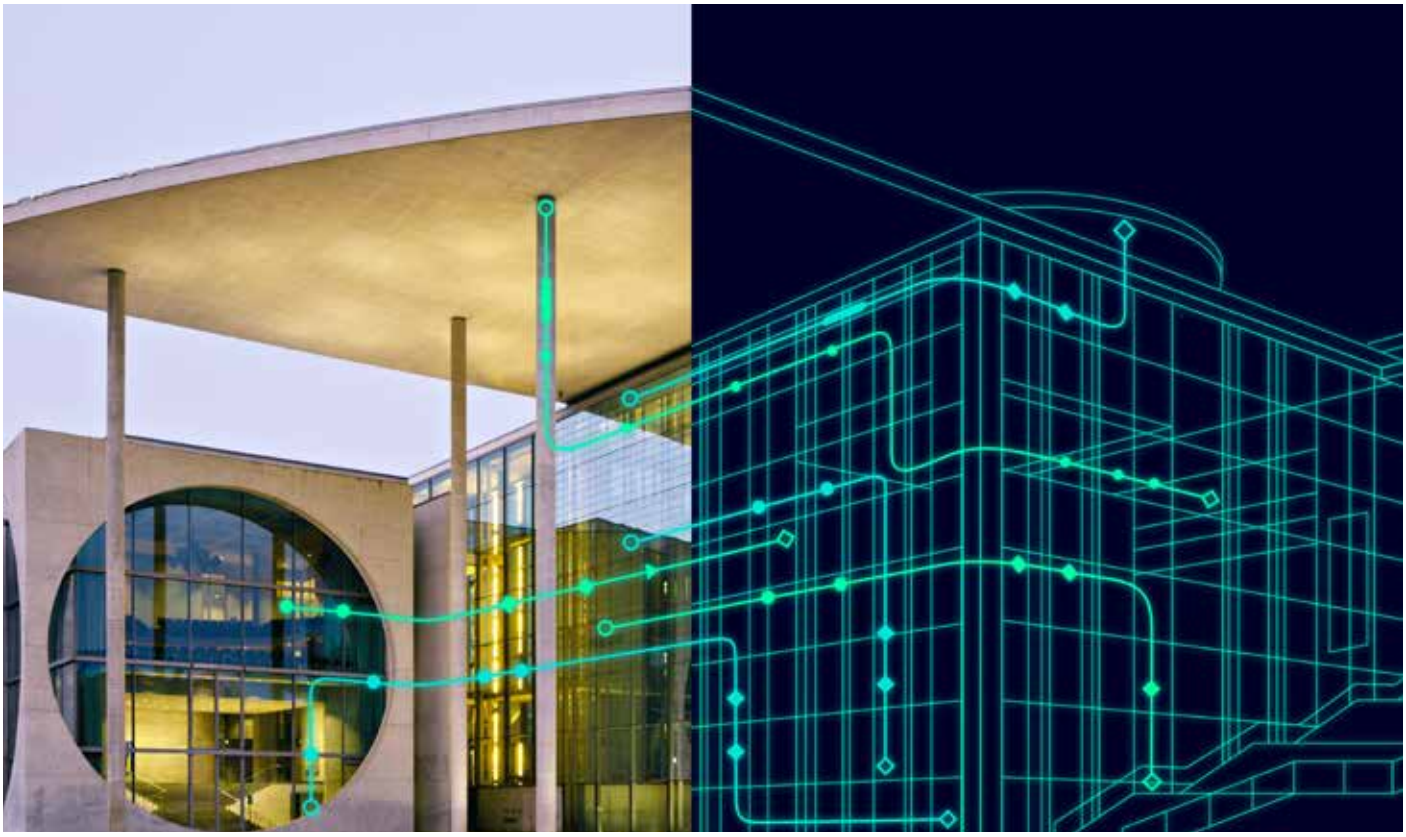
https://industrial.softing.com/products/network-management-tools/plantperfect-monitor.html

Softing Industrial

Visit Website

Standardization of digital twin languages

Solution converges Digital Twin Definition Language with W3C Thing Description Standard.



SOURCE: SIEMENS

Standardizing Digital Twin languages is crucial for interoperability.

Siemens and Microsoft have announced a collaboration to converge the Digital Twin Definition Language with W3C Thing Description Standard.

Collaboration highlights

- Standardization will foster collaboration, accelerate innovation, and facilitate the exchange of digital twin models and data
- Collaboration with the W3C working group set to propel the convergence effort, bringing about a unified standard to unlock commercial potential being held back by IoT fragmentation

In a collaborative move with the W3C Consortium, Siemens and Microsoft have announced their commitment to converge the Digital Twin Definition Language (DTDL) with the Thing Description standard from international standards organization, W3C.

By unifying both languages, customers are offered consistent modeling experiences, mitigating fragmentation in an evolving IoT landscape. With customers typically deploying a mix of vendors in their infrastructure leading to lock-in and high integration efforts, this convergence will allow for simpler system integration and interoperability.

As virtual replicas of physical objects, processes, or systems that mirror their real-world counterparts in a digital environment, digital twins enable organizations to monitor, predict, and improve the performance of their assets, enhancing efficiency and reducing costs.

Standardizing Digital Twin languages is therefore crucial for interoperability, ensuring seamless communication and integration between different digital twin systems and platforms.

With Siemens already facilitating the emerging W3C Thing Description standard for future products in building management, power distribution and smart grids, extending this interoperability strategy to Microsoft Azure will bring about substantial benefits to customers.

"We see the convergence of two very similar Digital Twin languages like the DTDL and the W3C Thing Description as an essential move that will enable customers to describe the physical world in a way that is agnostic to specific IoT platforms," said Thomas Kiessling, Chief Technology Officer at Siemens Smart Infrastructure. "This strategic alliance underscores our commitment to fostering collaboration and embracing openness."

Microsoft's Digital Twin Definition Language enables modeling of the physical world with Azure services, while the W3C Thing Description standard provides an interoperable representation of device interfaces and their incorporation of standard industry ontologies. Both languages have revealed many conceptual similarities during the initial stages of convergence.

"Ever since we invented the Digital Twin Definition Language and open-sourced its specification and reference implementations, we planned to standardize it through a consortium like the W3C. Therefore, merging DTDL with W3C Thing Description, in close partnership with Siemens, is the natural next step in our journey to democratize digital twins in the industry," said Erich Barnstedt, Chief Architect Standards, Consortia and Industrial IoT, Azure Edge and Platform team, Microsoft Corporation.

Siemens

Visit Website

USB-IF certified hubs

New second generation UPort USB 3.2 hubs are 10x faster than USB 2.0 hubs.

SOURCE: MOXA

In order to be certified by the USB Implementers Forum, Moxa UPort USB 3.2 hubs underwent extensive testing for connection, communication and power capabilities.

NEW MOXA USB-IF CERTIFIED HUBS OFFER seamless compatibility among a wider range of industrial devices.

Moxa is offering what the company says are the world's first industrial USB Hubs certified by the USB Implementers Forum (USB-IF). With USB 3.2 Gen 1 SuperSpeed 5 Gbps data transmission rates through every port, the new UPort USB 3.2 Series hubs deliver ten times the performance of USB 2.0, even in heavy-load applications.

Depending on the model, Moxa UPort USB 3.2 hubs can expand a single USB port on a host PC to either four or seven USB ports for seamless communication to a variety of USB upstream (type B) and downstream (type A) devices such as sensors, analyzers, cameras, and other peripherals.

USB-IF certification

In order to be certified by the USB Implementers Forum, Moxa UPort USB 3.2 hubs underwent extensive testing for connection, communication and power capabilities.

USB-IF certification verifies a number of strict electrical requirements for the SuperSpeed USB operation per the USB 3.2/2.0 specification. As a result, Moxa UPort USB 3.2 hubs:

- Support SuperSpeed USB 3.2 Gen 1 for up to 5 Gbps USB transmission.
- Are fully compliant with interoperability requirements.
- Have sufficient power for devices to function.
- Facilitate a smooth transition back to SuperSpeed operation from the suspended state.

Moxa UPort USB 3.2 hubs provide 900 mA power for all ports in compliance with the USB-IF Battery Charging Specification (BC 1.2), allowing for flexible USB expansions without the need for additional adapters. When BC 1.2 support is successfully detected and confirmed by the hub, Port 1 delivers a 1.5 A current to expedite the charging process. With a power range of 12 to 48 VDC, Moxa the hubs are perfect for mobile applications, as well.

Industrial strength

In addition to USB-IF certification, Moxa is the only USB-IF certified USB hub with FCC/UL certification to ensure the industrial safety and electromagnetic requirement. Moxa UPort USB hubs are ruggedly engineered for industrial environments, featuring a sturdy metal housing and an expanded operating temperature range of -40° to 85° C (0° to 60° C standard).

To avoid serious damage from Electrostatic discharge (ESD), the hubs incorporate ESD Level 4 (contact 8 kV, air 15 kV) protection, qualifying them for installation in sensitive medical, industrial and process control operations.

Using the extensive diagnostic LEDs and built-in LED indicators (UPort 400A models only), an administrator can quickly check the status of each port independently, saving time and money.

Six USB 3.2 hubs

The Moxa UPort USB 3.2 line consists of four 400A Series models and two 200A Series models. The UPort 200A Series is a general-purpose USB 3.2 hub, while the UPort 400A Series is a heavy-duty industrial design.

Included in the UPort 400A Series package is a high retention USB cable with a latch and screw lock to prevent accidental disconnection between the hub and the host computer. All hubs can be wall-mounted or installed onto a DIN-Rail for convenient access to the port connections.

Moxa

Visit Website

Distributed control system update

Enhanced control system software for seamless data integration and improved operational performance.

SOURCE: EMERSON

DeltaV distributed control system update features expanded connectivity via Ethernet-based protocols and streamlined state-based control execution

EMERSON IS FURTHER EXPANDING THE DeltaV™ Automation Platform with the DeltaV Version 15 Feature Pack 2 update for its distributed control system (DCS). This feature pack release empowers users to easily transition to a DeltaV DCS from more third-party control systems, expands support for data-rich Ethernet device networks and reduces the complexity of state-based control implementations.

As plants try to capture the most elusive performance gains to meet today's ever-increasing efficiency and sustainability goals, they are looking for technologies that modernize control without excessive engineering risk, overhead and downtime. The latest release of the DeltaV control system continues the regular cadence between major DeltaV releases to help users more quickly realize the project savings and operational efficiencies that come with new features for their control system software.

"DeltaV Version 15 Feature Pack 2 provides users new functionality, capabilities and enhancements to further expand seamless data and I/O integration as well as applications to more easily modernize their operations, improve connectivity and collaboration, and lock in operational excellence," said Claudio Fayad, vice president of technology for Emerson's process systems and solutions business.

Today's plants need to reap the benefits of modern, digital technologies that optimize operations and improve sustainability. However, one of the most common barriers to control system modernization is the high cost and labor requirements of transitioning I/O. DeltaV IO.Connect, which lets users replace legacy control systems with modern DeltaV software and controllers while leaving legacy I/O infrastructure in place, now supports multiple third-party control systems.

Plants can now transition to a modern DeltaV control system from the most common third-party systems right away—immediately reaping the benefits of modern control—and transition their I/O infrastructure gradually, on their own schedule, to minimize downtime and risks.

Ethernet-based, high speed, data rich device networks continue to gain popularity across the automation landscape and will only accelerate as Advanced Physical Layer extends the application range in process and hybrid industries. With this latest release, the DeltaV control system has increased the types of data as well as the diagnostic capabilities of the wide range of supported Ethernet-based communication protocols including PROFINET, EtherNet/IP, OPC UA, and Modbus TCP. These enhancements advance the solid foundation of DeltaV automation to exchange increasing volume and variety of data from the next generation of field device networks.

State-based control is a key enabler as many plants drive toward autonomous and semi-autonomous operations to reduce downtime and minimize safety risk. With DeltaV Version 15 Feature Pack 2, engineering and operations teams now have more options for how state-based control sequences execute when operations dictate a change in logic. This optional behavior enables safe and reliable operations while improving the flexibility and maintainability of state-based logic. To improve operator situational awareness the watch area capability of DeltaV Live has also been enhanced to persist as operators navigate between displays.

Emerson

Visit Website

16-port Industrial Ethernet switches

New 16-port Industrial Ethernet switch supports mission-critical operations in rugged environments.

Red Lion has launched new N-Tron® NT116 unmanaged switches to provide performance and reliability in harsh industrial environments.

The NT116 unmanaged switch offers exceptional reliability and performance for data acquisition, Ethernet I/O and process control. Compact in size and including 16 high performance copper ports (10/100BaseTX RJ45), the unit is housed in a rugged industrial metal enclosure. The NT116 offers high shock and vibration tolerance, and all ports have built in ESD and surge protection. Users benefit from an exceptional 1.2M hour MTBF rating, in a slim, space-saving design that operates in temperatures from -40°C to 85°C.

For robust network support, the NT116 supports full wire speed communications of up to 3.2 Gb/s throughput. The unit uses store-and-forward technology and supports full and half duplex operation. Two 10-49 VDC power inputs are provided for redundancy.

The N-Tron® NT116 is the next evolution of Red Lion's 116TX unmanaged industrial ethernet switch. In addition to IEEE 802.3 compliance and marine, railway and rolling stock certifications, the new switch carries UL Ordinary and Hazardous locations as well as ATEX and IECEx certification.

SOURCE: RED LION

Red Lion's new N-Tron® NT116 makes critical performance data easier to gather. Its rugged and hardened design provides the durability and reliability needed to withstand the extreme conditions found on factory floor control networks and in oil and gas, utilities, wastewater treatment, alternative energy, rail, intelligent traffic control and transportation applications.

Red Lion

Visit Website

Building automation controllers

Automated Logic adds two new controllers to its OptiFlex family.

Automated Logic has announced the expansion of its OptiFlex controller line for the WebCTRL building automation system. Two new controllers join the OptiFlex family, including the OptiFlex 022 (OF022- E2) zone controller and the OptiFlex compact segment router (OFCSR-E2). These controllers feature dual IP ports for convenient daisy-chain deployment and a compact footprint for more flexible system design.

The OptiFlex 022 (OF022-E2) zone controller is engineered to deliver unparalleled efficiency and reliability for modern building environments. Featuring dual IP ports for convenient daisy-chain deployment, the OF022-E2 supports two universal inputs and two analog outputs, ensuring versatile control options for a variety of applications. Its smaller form factor not only simplifies installation but also optimizes space, making it an ideal solution for areas requiring dependable and precise environmental control.

Complementing the OptiFlex 022, the OptiFlex compact segment router (OFCSR-E2) is designed to facilitate seamless migration from traditional serial network segments to fast and performant IP backbones. The OFCSR-E2 offers robust routing capabilities between BACnet®/IP, BACnet Ethernet, BACnet/ARCnet, and BACnet MS/TP networks, with native support for IPv4. It is equipped with three physical communication ports: two 10/100 Mbps BACnet IP/Ethernet ports and a high-speed EIA-485 port that can be configured for BACnet/ARCnet or BACnet MS/TP. Additionally, the device features a USB port for local access.

SOURCE: AUTOMATED LOGIC

Automated Logic

Visit Website

Rockwell and Microsoft alliance

Alliance to enable intelligent factories by helping achieve sustainability goals and operational excellence.

SOURCE: ISTOCKPHOTO

Partnership leverages a shared vision of creating and delivering the best solutions to empower the future of industrial operations.

ROCKWELL AUTOMATION AND MICROSOFT HAVE announced significant technology integrations connecting the physical and digital industrial worlds.

"Rockwell's partnership with Microsoft is a shared vision of creating and delivering the best solutions to empower the future of industrial operations," said Nicole Denil, global vice president, market access, Rockwell Automation.

"We simplify complexity in how manufacturers design, operate, and maintain their enterprises and empower their people. Visitors to the Rockwell stand in the Microsoft booth at Hannover Messe will see how Rockwell Automation helps empower leading manufacturers globally to reduce waste in their operations and achieve sustainability goals through streamlined industry solutions."

With Rockwell's FactoryTalk edge and cloud solutions, manufacturers bring together artificial intelligence, IoT, and automation solutions to allow people, processes, and technology to operate seamlessly between physical and digital environments. With Microsoft Azure's adaptive cloud approach, manufacturers can unify and streamline siloed teams, sites and systems while scaling applications and insights. Together, Rockwell and Microsoft will provide cutting-edge industrial transformation solutions across the value chain, rapidly and at scale, with AI-assisted design, connected data, and agile production optimization.

Additionally, the recently announced partnership between NVIDIA, Rockwell and Microsoft allows the creation, real-time management, and simulation of digital twins that will be accelerated with the use of Microsoft's AI assisted tools and cloud technology.

Finally, with the integration of Rockwell Automation's Plex manufacturing execution system (MES) with FactoryTalk® DataMosaix™ and Microsoft's Cloud for Manufacturing, manufacturers benefit from transformative artificial intelligence (AI) tools that help drive productivity, safety, and quality. These tools focus on resolving quality issues with corrective actions and root cause analysis.

Bringing intelligent factory to life

Innovative offerings demonstrate how integrated digital twins and generative AI expedite time-to-market as organizations and systems scale. One illustrates how to connect digital and physical assets for autonomous intelligent factories. It utilizes digital design with differentiated digital twin simulation and artificial intelligence through FactoryTalk Design Studio Copilot for a simplified customer experience of industrial operations.

Also on display at the recent Hannover Show was a digital twin simulation of a quality inspection process, inspired by Rockwell's customer Nestlé. The digital simulation is augmented by a physical installation of product sorting and autonomous material handling for packaging. Production line sorting is represented through a factory digital twin, imitating the manufacturing of one of Nestlé's products.

"Manufacturers are always looking for ways to drive modernization, optimize efficiency, and reduce costs," said Dominik Wee, corporate vice president, manufacturing and mobility, Microsoft. "By combining Microsoft's AI capabilities and trusted cloud platform with Rockwell's industrial automation solutions, manufacturers will have the tools they need to speed up these objectives and create smart factories of the future.

Rockwell Automation

Visit Website

Bus coupler module

IDEC Bus Coupler Module facilitates flexible control signal connectivity.

The compact SX8R Bus Coupler from IDEC Corporation bridges a wide range of proven I/O modules with major industrial networks—such as EtherNet/IP, Modbus TCP, and CC-Link—supporting adaptable automation designs.

The new module,empowers users to easily deploy I/O modules throughout equipment and systems. This supports the industry design trend of using smaller, decentralized control panels to simplify installations and reduce wiring complexity, resulting in overall cost efficiency.

The SX8R Bus Coupler is a way to design distributed remote I/O systems, or to expand the I/O count for controllers with limited base unit I/O points. For example, the SX8R works natively with IDEC PLC FC6A I/O modules, which are available in over 40 models encompassing a variety of discrete and analog signal types and counts. Each SX8R supports up to 7 I/O modules on the base unit, and up to 8 additional modules with the use of an expansion power supply, for a total of up to 15 I/O modules. A single SX8R can therefore support up to 480 discrete points (input and/or output), 120 analog inputs, and/or 60 analog outputs, depending on the configuration. The maximum number of SX8R nodes possible on a network is dependent on the host unit and the protocol—for instance, this means 255 nodes for Modbus TCP, 32 nodes for EtherNet/IP when using an IDEC FC6A Plus PLC, and 16 or 8 nodes for CC-Link when using specific Mitsubishi PLC models.

SOURCE: IDEC

IDEC

Visit Website

Ethernet integration increases efficiency

Enhanced Temperature Concentrator System with Ethernet integration increases measurement efficiency.

Moore Industries has released a significant product update to the TCS Temperature Concentrator System. The TCS originally consisted of the TCM Temperature Concentrator Module and the HMC HART® -to-MODBUS RTU Converter, which work together to reduce the cost of transmitting multiple temperature sensor measurements in both general-purpose and hazardous area applications by concentrating and transmitting up to 32 signals over one MODBUS RTU based network.

The latest update enables a HES HART-to-Ethernet Gateway System to be used with the 16-channel TCM Temperature Concentrator Modules, allowing for Ethernet-based communication. The HES is available in a single-channel or 4-channel model and can connect with up to two TCMs per channel, allowing up to eight TCMs to communicate with one HES. This allows 128 different temperature signals to flow over an Ethernet link from the field to a MODBUS/TCP-based host. Additionally, these temperature readings can be read by a HART-IP-based host or viewed with any off-the-shelf web browser since the HES includes an embedded web server. Unlike the HMC, the HES can communicate with up to sixteen HART devices per channel. Each 16-channel TCM is considered one HART device, so if two TCMs are connected on a particular HES channel, 14 additional HART devices can still be connected to the channel along with the TCMs.

The TCM Temperature Concentrator Module converts its signal inputs to standard HART protocol, which allows the HES to poll each TCM using a device-specific HART command. This device-specific command enables the TCM to send all 16 channel values in one HART message packet, thus increasing throughput and response time.

The TCS system significantly reduces the cost of transmitting multiple temperature sensor measurements in both general-purpose and hazardous areas.

SOURCE: MOORE INDUSTRIES

Moore Industries

Learn More

Integrated production control system

Yokogawa upgrades its CENTUM VP integrated production control system, strengthens networking support.

THE RELEASE OF CENTUM VP R6.11.10 provides an enhanced version of the CENTUM VP integrated production control system that is a core product in the OpreX™ Control and Safety System family of solutions from Yokogawa.

With this new version of CENTUM VP, plant uptime is improved through the addition of a redundancy function to a new IO card that supports communications via the PROFINET communications protocol for industrial networks. Furthermore, to reduce project costs and improve efficiency in plant operations, functional enhancements have been made to the Unified Alarms and Conditions Server (UACS) and the CCC Inside for the Yokogawa CENTUM VP compressor control solution.

Development background

PROFINET is one of the most widely used Ethernet-based industrial communications protocol worldwide, boasting superb real-time performance. In 2019, Yokogawa developed an IO card that supports PROFINET. While this enabled the monitoring of the operation of PROFINET-compatible devices from CENTUM VP, more needed to be done to improve reliability and uptime.

To meet this need, Yokogawa has developed a new PROFINET IO card that supports a redundancy function, and by doing so, has made high reliability and high uptime a reality.

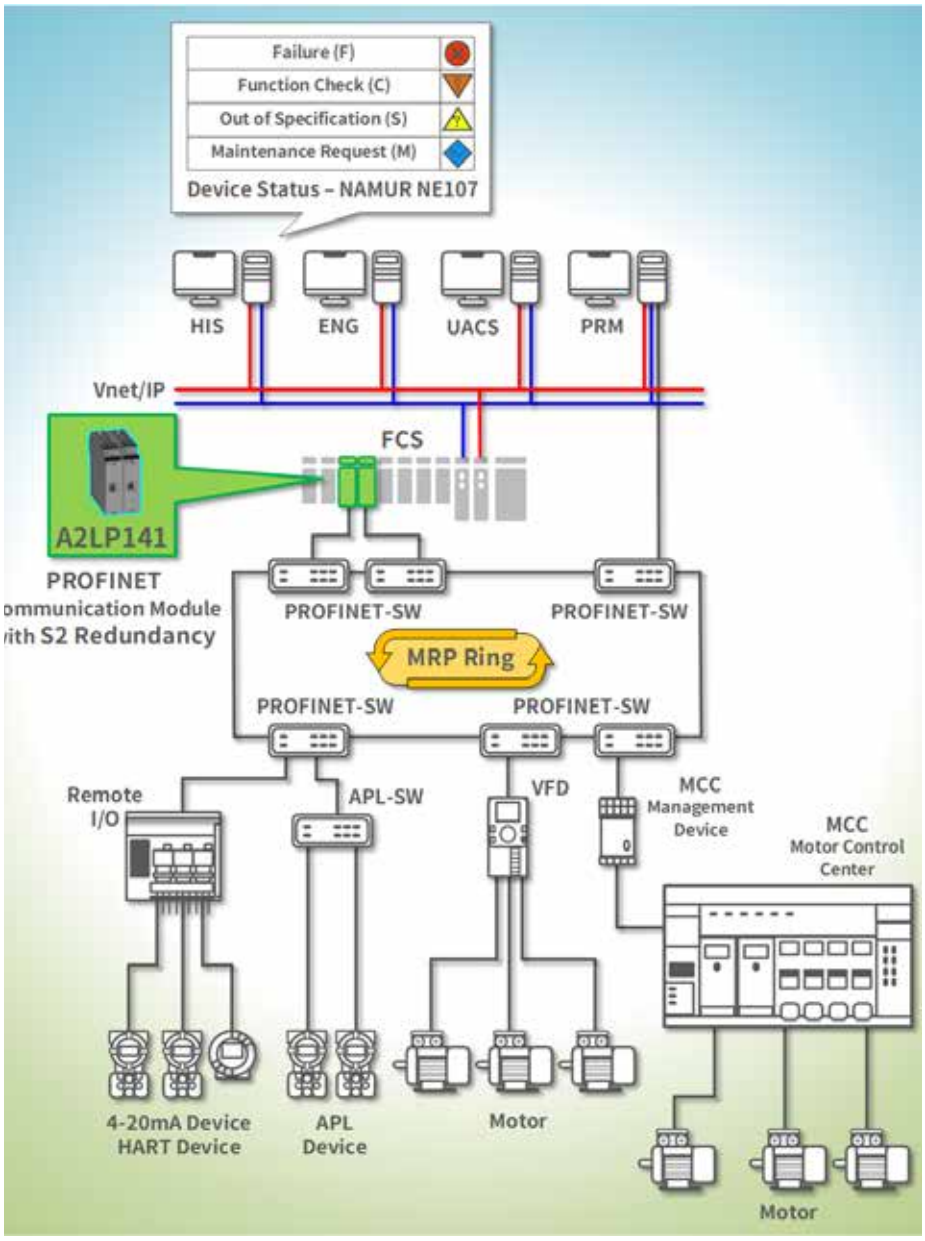
The new CENTUM VP release also features functional enhancements to the UACS and the CCC InsideTM for the Yokogawa CENTUM VP compressor control solution that will improve the efficiency of operations and engineering at plants.

Product features

PROFINET IO card redundancy support for greater reliability and increased uptime.

To improve plant uptime, an S2*1 redundancy function has been added to the new PROFINET IO card, enabling its use in a redundant configuration. Thanks to this and enhancements that have been made to the card's network diagnostics function, this device has been certified by a third-party agency as having all the PROFINET functions for Conformance Class*2 B (CC-B), including the system redundancy that is so important in process control.

By supporting the use of NAMUR NE107*3 compliant self-diagnostic information from devices that support PA Profile 4.0*4 and enabling the use of a motor control center that centrally controls motor power sources, remote I/O and Ethernet Advanced Physical Layer (Ethernet-APL) compatible device operation monitoring are also now possible, and this expands the scope of control that is possible with a single control system.



SOURCE: YOKOGAWA

System architecture of CENTUM VP PROFINET.

Improved plant operational efficiency with alarm management that supports NAMUR NA102.

When a specific alarm has been suppressed in the UACS, the suppression status can now be displayed in the Human Interface Station (HIS) graphics. By enabling the implementation of alarm management in compliance with NAMUR NA102*3, this can help to improve operational efficiency throughout a plant.

Seamless integration of process and compressor control systems.

It is now possible to undertake integration and engineering using a single CENTUM VP project database for the process and compressor control systems. This release of CENTUM VP also enables process and compressor control systems to be connected to a Vnet/IP*5 control network within the same domain. As such, this allows highly seamless system integration and helps to reduce project and maintenance costs.

Yokogawa

Visit Website

Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

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

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 ethernet book

Industrial Networking & IIoT