July/August 2021 125
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking & IIoT

Technology Showcase

Industrial Edge technology innovations

Page 25

How edge technology fuels digital transformation 6

No more kicking the can.

Here's the cybersecurity guide you've been looking for.

Get the ***groov* EPIC Cybersecurity Technical Guide** to learn more about:

- Creating secure zones and conduits between IT and OT networks (ISA/IEC 62443)
- Protecting legacy automation with device-level firewalls
- Restricting and centralizing user access
- Securing remote access with embedded VPN
- Encrypting communications with SSL/TLS certificates, HTTPS, and MQTT

groov EPIC™

Download your copy at: **op22.co/cybersecurity**

MADE IN THE USA

Made and supported in the U.S.A.
Call us toll-free at 800-321-6786 or visit www.opto22.com

OPTO 22
Your Edge in Automation.™

GET CONNECTED...

Visit our new website at: www.iebmedia.com

Industrial edge focus

Welcome to the July/August 2021 issue of the Industrial Ethernet Book. In this issue, we provide unprecedented coverage of Industrial Edge Computing with more than 40 pages of editorial devoted to this important topic.

In the 2021 special report in this issue, we offer comprehensive coverage by highlighting the perspective of technology leaders on how Industrial Edge solutions and products are shaping factory applications.

A total of ten companies added their insights to two major feature stories in this issue. One page 6, the article "How Industrial Edge technology fuels digital transformation" discusses how edge computing facilitates data processing at the edge of a network, close to the edge devices, and avoids the issues of sending all the data directly to the cloud.

Key topics include the use of CPU virtualization and open communication to create a virtualized software environment, and the benefit of being able to access data from machines and send it to the cloud without the need for gateways.

Another topic of interest is the use of microservice architectures which implements a solution where, instead of a monolithic software that handles all tasks, the automation application is split into multiple apps, with each app performing a specific task.

On page 27 of this issue, we also present our Industrial Edge Product showcase lead story " Industrial Edge impact on smart manufacturing". Industry experts comment on the current evolution of control technology, open source Linux applications, industrial PCs configured as both control computers and edge PCs, and the renaissance of Industrial Ethernet.

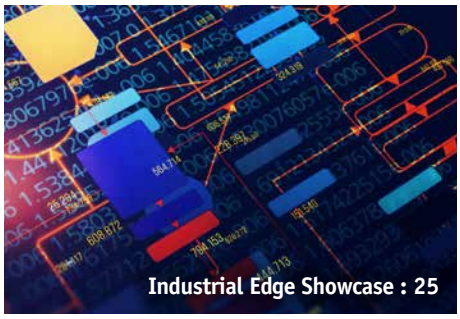
The bottom line is that industrial edge technology is enabling comprehensive IIoT solutions that extend from the edge to the cloud, and provide a powerful impetus in the convergence of IT and OT operations.

The range and types of solutions are remarkable, as a broad set of vendors provide ways to make edge computing solutions more effective for smart manufacturing.

According to Pierfrancesco Zuccato, senior product manager at Eurotech, “Ethernet is the new renaissance for connectivity in industrial applications. Up to now, we’ve had a multitude of different types of specialised and even proprietary interfaces to work with and Ethernet is increasingly becoming a strong candidate to replace most, if not all, of those interfaces.

That comment alone underscores the primary role that Industrial Ethernet and the Industrial Edge will be playing in the future of automation and control networking.

Al Presher



Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2021.**
Deadline for editorial: September 10, 2021 **Advertising deadline:** September 16, 2021
View Industrial Ethernet Book website for latest news and products: www.iebmedia.com.

Editor: Al Presher, editor@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +1 585-598-4768
Free Subscription: iebmedia.com/subscribe

Published by IEB Media, Div. of Stratejus, Inc. Box 1221, Fairport, NY, 14450 USA ISSN 1470-5745

Technology brings two-wire Ethernet to process automation

Industry leaders announced at the ACHEMA conference a major milestone in the launch of Ethernet-APL technology, and the availability of products for automation in the process control industry.

ETHERNET-APL TECHNOLOGY IS AVAILABLE, the standards are complete, and products are entering the industrial market. Collaboration with key standards organizations and industry partners has resulted in technology availability for the new two-wire, intrinsically safe physical layer known as Ethernet-APL.

The numerous barriers to deploying high-speed Ethernet enabled instrumentation in hazardous process automation facilities are now resolved with the introduction of Ethernet-APL technology. Ethernet-APL is the new two-wire, intrinsically-safe physical layer suitable for use in demanding process automation applications.

Ethernet-APL's benefits

Ethernet-APL's benefits include dramatically improved communication speed, hazardous area reach, power to field instrumentation, and long cable runs. Leading standards development organizations FieldComm Group, ODVA, OPC Foundation, and PROFIBUS & PROFINET International (PI), as well as 12 major industrial project partners, have worked together successfully over the past three years under "The APL Project" to create this new physical layer solution for field instrumentation. With the release of the specifications, engineering guidelines, and conformance test plans by The APL Project, end users can now expect components from leading suppliers, with first products now available from select vendors.

Ethernet-APL is an extension of the specification for Single-Pair Ethernet (SPE) based on 10BASET-1L, which can support every higher-order Ethernet communication protocol. By making adjustments to the physical layer, the requirements necessary for reliable operation in process-related plants are satisfied. The principal requirements are high-speed Ethernet based communications, operation in potentially explosive areas, and an ability to install long cable lengths of up to 1,000 meters. The electrical parameters that an Ethernet-APL device must meet to ensure "intrinsically safe" ignition protection are defined in the technical specification of the IEC TS 60079-47 (2-WISE or 2-Wire Intrinsically Safe Ethernet).

The APL Project to bring Ethernet to the field has been underway for several years, and it is with much excitement and anticipation that this initial technology launch is announced. The APL Project has defined port profiles to create the Ethernet-APL concept for multiple power levels with and without explosion hazardous area protection. Ethernet-APL port profiles, including electrical power classes, shield connection options, and segment lengths, have been finalized. Markings on devices and instrumentation will indicate power level and function as sourcing or sinking. This will provide a simple framework for interoperability from engineering to operation and maintenance. Engineering guidelines and best practices for planning and installation are also now complete and available in an engineering directive document that will support users when designing and commissioning networks utilizing Ethernet-APL. This facilitates an easy transfer of knowledge for a smooth adoption of Ethernet-APL. Standard Ethernet diagnostic tools will assist new or seasoned instrument techs and engineers in their daily work, providing for a shallow learning curve.

As a single physical layer, Ethernet-APL will be able to support EtherNet/IP, HART-IP, OPC UA, PROFINET, or any other higher-level network protocol. Activities are underway to finalize conformance testing at the leading standards development organizations that are a part of the APL Project. The test specifications now published will assure the quality of products and verify that a product complies with the parameters defined in the APL port profiles specification. The APL Project team has also cooperated with semiconductor manufacturers who will offer 10BASE-T1L Phys for Ethernet-APL on the market. Additionally, the 12 APL Project industry partners are finalizing development of products that will be available in the marketplace soon. The multivendor demonstration in Karlsruhe, Germany, displayed digitally during ACHEMA Pulse showing participation across different product vendors and networks, highlights the multiple options and interoperability that Ethernet-APL will offer end users.

*News report from **Ethernet-APL.***

View article on IEB website

TTTech Industrial acquires Nebbiolo Technologies

TTTECH INDUSTRIAL AUTOMATION AG HAS acquired core technology and strategic customers from pioneering fog/edge computing start-up Nebbiolo Technologies in a deal closed in May. Integrating features and know-how from Nebbiolo Technologies will support TTTech Industrial's commitment to delivering the world's most advanced industrial edge computing platform to its customers.

TTTech Industrial has also founded a US subsidiary in Silicon Valley to expand its activities in the North American market. Kannan Devarajan, one of the co-founders of Nebbiolo Technologies has joined TTTech Industrial North America Inc. as Managing Director.

TTTech Industrial is a leading provider of industrial IoT solutions, and partners with key players in IoT such as Intel and Microsoft. The company's Nerve software platform has been at the forefront of industrial edge computing since its launch in 2016. The foundation of TTTech Industrial North America supports the expansion of commercial operations in the US and Canada, with the technology and customer assets acquired from Nebbiolo Technologies forming the nucleus of these activities.

Nebbiolo Technologies is renowned as the pioneer of fog computing, with patented technology that is foundational to industrial edge computing concepts. The company was named a Gartner Cool Vendor in 2017 and was recognized as the Customer Value Leader in the IIoT edge computing market by Frost & Sullivan in 2019. The combination of existing Nerve product features with Nebbiolo Technologies' expertise will provide customers with an unparalleled solution for software management at the edge, remote connectivity, edge analytics, high-availability, and security.

*News report from **TTTech Industrial.***

View article on IEB website

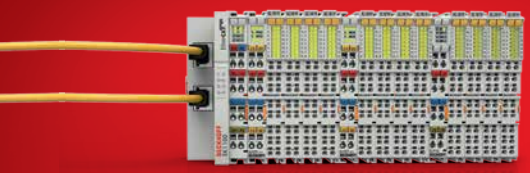
System-integrated overcurrent protection with EtherCAT interface

Extremely space-saving and flexibly usable

www.beckhoff.com/overcurrent-protection

In the EtherCAT Terminals from the EL922x series Beckhoff integrates the overcurrent protection for the fusing of 24 V DC systems – including EtherCAT interface – in a compact 12 mm. Transparent plant monitoring via EtherCAT is thus also directly integrated. The EL922x can supply both consumers outside the terminal network and further terminals inside it with a fused voltage – simply and conveniently. Virtually all typical requirements can be met through the individual settings. The range consists of a total of 19 different standard and high-line terminals with a particularly high number of analysis options.

EtherCAT



Direct overcurrent protection integration in the I/O system

New Automation Technology **BECKHOFF**

How Industrial Edge technology fuels digital transformation

Edge computing facilitates data processing at the edge of a network, close to the edge devices, and avoids the issues of sending all the data directly to the cloud. Automation and control networking vendors weigh in on the latest technologies for the Industrial Edge, and how it is contributing to digital transformation.

INDUSTRIAL EDGE TECHNOLOGY IS PLAYING an increasingly significant role in the digital transformation of industrial companies and smart manufacturing, in particular. The growing number of sensors and smart devices generating terabytes of data, along with the need for quick and reliable processing of this data, has motivated development of a common IoT architecture for edge devices communicating with IoT cloud platforms.

In this special report, the Industrial Ethernet Book offers comprehensive coverage and offers the perspective of industry leaders on how Industrial Edge technology and products are shaping factory applications.

Impact on the shop floor

CPU Virtualization and open communication

According to Thomas Berndorfer, a member of the Executive Board at TTTech Industrial, one of the key technologies for the introduction of Industrial Edge applications is CPU virtualization.

"Virtualization allows applications to run side-by-side on the same standard IPC hardware. Running applications as Docker containers or in Virtual Machines at the edge reduces hardware costs, improves resource efficiency, and gives easy access to data straight from the machine," Berndorfer said.

"Open source hypervisors such as ACRN from the Linux Foundation also provide virtualization for real-time applications. This even enables the integration of soft PLC functionality on an edge computing platform, further improving efficiency and data access."

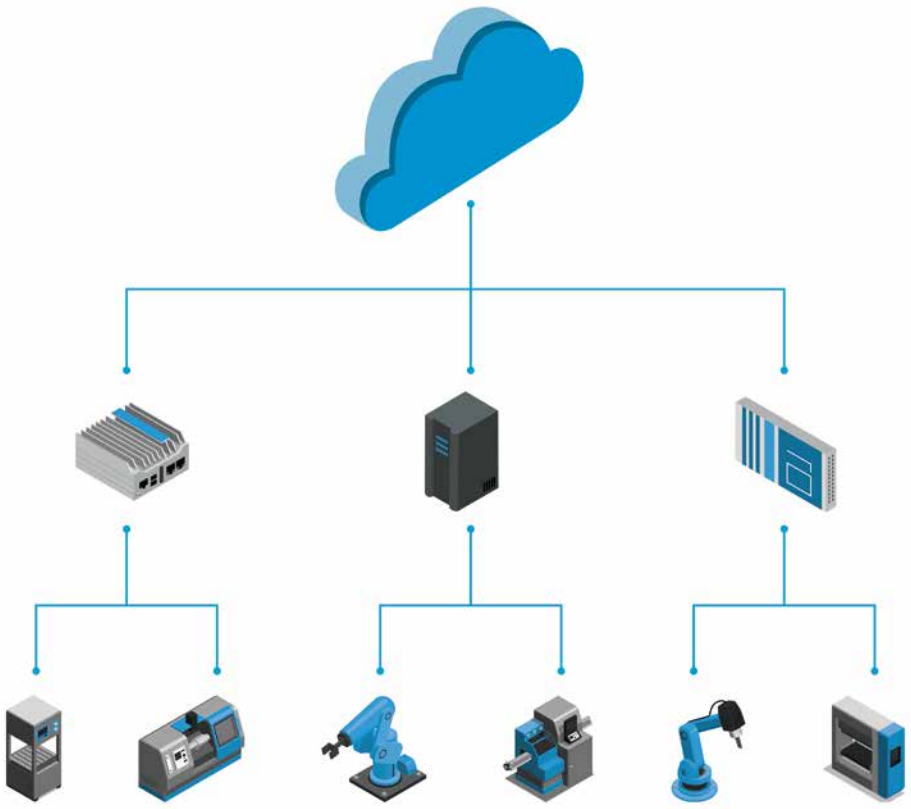
He added that open communication is another key element of industrial edge computing. Standards such as OPC UA ensure that information can be shared from sensor to cloud in a uniform way. Industrial applications running at the edge, especially within a virtualized software environment, benefit from being able to access data from machines and send it to the cloud without the need for gateways.

Focus on industrial applications

Berndorfer said that edge computing is unique in the way that it enables powerful applications to run on the shop floor, i.e. close to the machines that are generating data. In this way it is an extension of cloud computing, which also consolidates various software and large amounts of data in one place.

Unlike with cloud computing, running industrial applications at the edge allows data to be processed with lower latencies and with fewer security issues.

This gives users the opportunity to analyze and use data in real-time to achieve even greater levels of production efficiency and higher system uptime. By running analytics and complex applications at the source (the network edge) and only sending selected data to the cloud, edge computing also helps to reduce the need for expensive server hardware and bandwidth.



SOURCE: TTTECH INDUSTRIAL

Edge computing allows machine data to be collected on the shop floor and processed close to the machine for real-time operation, before selected data is transferred to the cloud for storage and/or further analysis.

Technology benefits

"Real-time collection, processing, and storage of data enables faster decision making and better process planning, especially for the complex environment of a "smart factory" that needs to work autonomously and with maximum efficiency," Berndorfer said. "Edge computing allows manufacturers to gain in-depth insights into how machines are running and performing. It increases response time in case of technical problems and ensures that downtimes are limited thanks to accurate planning and scheduling of predictive maintenance."

Customers and engineers also have access to real-time data e.g. when servicing a machine. With edge computing, manufacturers can also

set up digitalization initiatives in brownfield sites where no or unreliable Internet connectivity is available.

An edge platform allows for multiple functions to be converged on one device, thus decreasing the cost of hardware. It also offers options for the inclusion of legacy applications and devices, e.g. via a web-based management system. With an edge computing platform, software and devices can be updated and new application deployed remotely, saving travel cost and minimizing the potential of mistakes.

Challenges engineers face

"Automation engineers face a myriad of challenges that edge computing helps to address. A big challenge is how to retrofit existing systems for industrial IoT applications," he added. "This requires gaining access to machine data and running advanced new software solutions without disrupting the existing infrastructure. Edge computing provides a platform to enable retrofitting whilst reducing costs."

Other challenges are service and maintenance. Especially in a post-COVID world we see the difficulties of relying on on-site maintenance. In coming years, this is likely to become even more inefficient and expensive. By enabling remote service and maintenance, edge computing can reduce travel and engineering costs, as well as enabling new 'as-a-service' offerings that replace traditional service level agreements.

SOURCE: TTTECH INDUSTRIAL

An edge computing platform with a central management system enables remote software updates and deployment of applications to machines worldwide.

Edge computing devices

Security and flexibility fuel possibilities

Kris Dornan, large controllers marketing manager at Rockwell Automation, said that industrial edge computing devices create the foundation that make edge applications possible. These devices replace "white box" PCs on the plant floor by moving your plant-floor compute hardware into your controller cabinet, controller chassis or even the controller itself.

On this foundation, engineers can then deploy an operating system and software applications that use capabilities like digital twins, analytics and machine learning that create new possibilities in your operations.

"An industrial edge computing device can be an industrial computer that sits in the same chassis as your controller, a compute module that sits on the same rack as the controller or an industrial controller with a built-in computer," Dornan said.

"No matter which option you choose, you get similar outcomes. You get a computing solution that can be housed and secured in the same location as your controller. And by putting your control and compute components in closer proximity to each other, or by combining them into one platform, you can speed up the information flow in your operations," he added.

Unlimited possibilities

Dornan said that the end result is that the possibilities for what you can do with edge computing devices are nearly unlimited. For example, you can combine them with vision systems to detect anomalies on high-speed conveyance lines, providing a fidelity of timestamp that may not otherwise be possible. You can improve process visibility by creating an application that calculates a process value that otherwise is difficult to measure or where a sensor is susceptible to environmental factors. And you can use "trial and error" simulations to test production changes in a safe, virtual environment before implementing them in your physical operations.

According to Matt Masarik, design software marketing manager at Rockwell Automation, PCs are increasingly being removed and prohibited from the plant floor for security reasons.

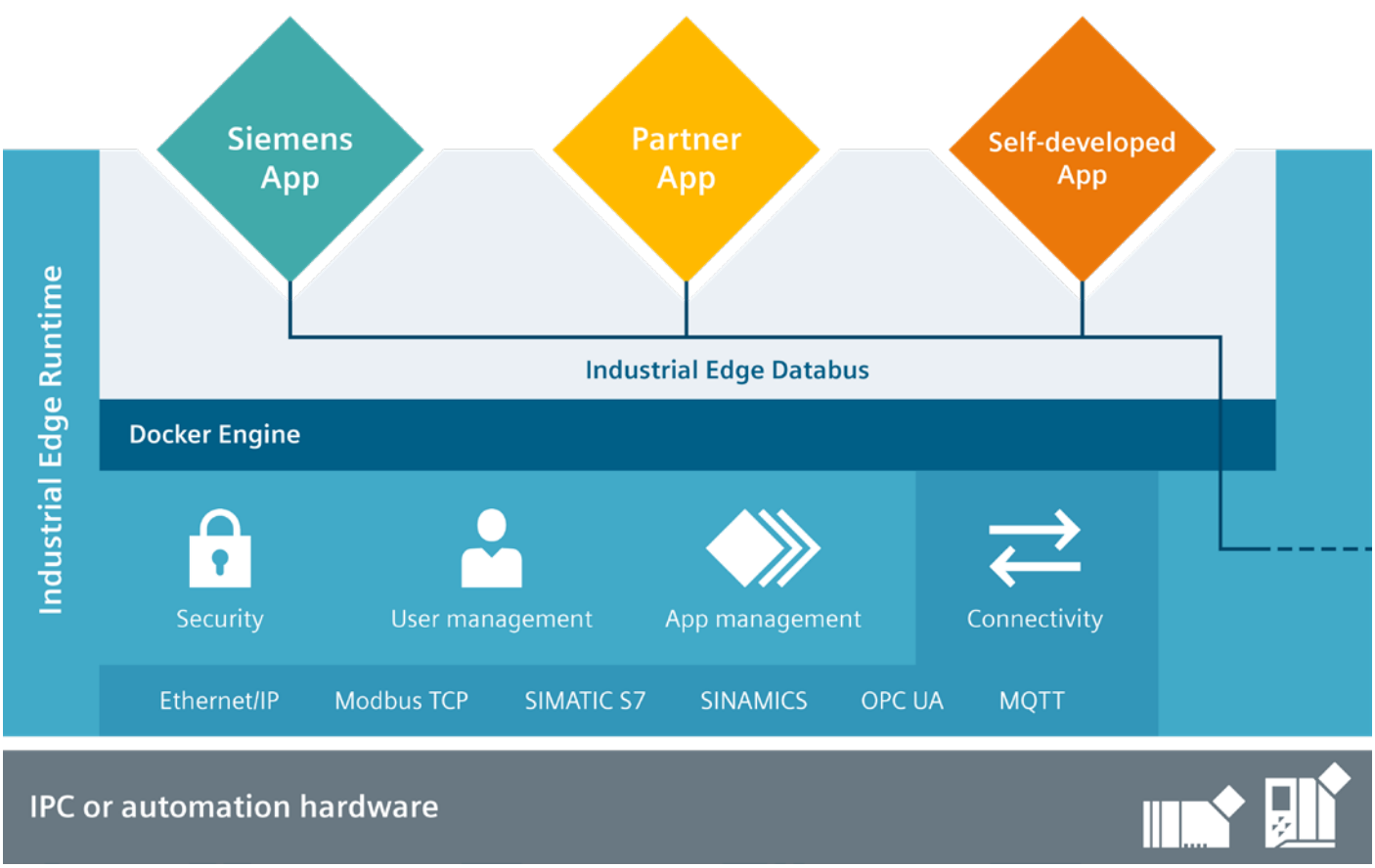
"Industrial edge computing devices provide a means of retaining this crucial computing capability, while at the same time strengthening cybersecurity and improving responsiveness and decision making," he said.

For starters, edge computing devices offer inherent cybersecurity benefits. They can reduce your attack footprint by allowing you to remove not only PCs from the plant floor but also components like cabling and switches that are required to tether the PCs to your systems. Edge computing devices also allow you to use advanced capabilities like voice- or face-recognition software to create more secure access to your assets.

Additionally, the ability to create software applications for an edge device can help you monitor, manage and optimize your operations in new ways. For example, instead of staff sifting through historical performance data and manually making changes to improve your process, your edge application can continually learn your process and optimize it in real time. Or your edge application can compare how your actual performance compares against the ideal state and identify where you're falling short.

"In addition to addressing cybersecurity challenges, industrial edge computing devices can help address another concern: the changing workforce," Masarik said.

Many operators and engineers who are accustomed to tethered control rooms and who use ladder logic and function block programming are retiring. And as they retire, they're being replaced by a new generation of workers who have different talents and



SOURCE: SIEMENS

With Siemens Industrial Edge, all apps are based on the Docker technology and communicate via a central data bus.

skillsets. These workers have different expectations for technology – specifically that it be "smart" and connected to a mobile device. They're also more familiar with other programming languages, like Python and Java.

"Edge computing devices align with the expectations and skillsets of these workers," he added. "For example, some edge computing devices include a library of application programming interfaces (APIs) that allow different programming languages to communicate with the control processor. This can allow engineers to use their preferred programming language to code some or maybe even all of a controller's logic."

Microservice architectures

Multiple automation apps each performing a specific task.

Thomas Haneder, Marketing Manager, Industrial Edge Ecosystem at Siemens said that in industrial edge applications, they see a clear trend towards the use of apps in discrete and process manufacturing.

"Instead of a monolithic software that handles all tasks, the automation application is split into multiple apps, with each app performing a specific task," Haneder stated. "For example, connectivity apps connect the edge system to existing shop-floor devices such as PLCs or provide northbound connectivity to different cloud environments. Other apps cover data storage or visualize data for the operations engineer."

According to Haneder, the underlying technology used by these apps is a microservice architecture, e.g. based on the Docker standard. This technology enables solutions where apps are loosely coupled and thus extremely modular. With this trend there will be more and more applications and services that complement each other.

An open ecosystem will emerge where independent app developers can contribute their domain expertise. Edge app users will benefit from this trend as they will be able to choose the best apps for their solution from a variety of offerings.

Unique microservice architecture

Haneder said that, because of the microservice architecture, an overall solution can thus be realized from various individual apps that communicate with each other via a defined interface. The interface can be realized by an API or by messages encoded with a predefined data format, exchanged via an MQTT-based data bus.

"Other apps can use this open interface and extend the functionality of the underlying base app. Therefore, it is possible to realize a modular and manufacturer-independent automation solution. For example, a connectivity app from vendor A can be used to collect data from a specific plant, machine or device, this data can be stored in data storage app from vendor B, and then displayed by a homegrown app based on an open source library. The individual apps are encapsulated in themselves and are subject to their own lifecycle management, which allows individual services to be updated independently of the overall system," he said.

With this microservice architectural style, apps can be developed by utilizing DevOps practices such as continuous integration and continuous delivery (CI/CD) which results a faster time to market. This is especially relevant if apps are developed in-house.

Potential impact on manufacturing

One major impact he sees will be that the number of available apps and therefore the possible solutions for a specific use cases will increase tremendously. The customer can thus put together a customized solution consisting of apps from different vendors or extend existing applications through in-house development and due to the modularity without affecting the behavior of the overall system.

Apps will be distributed via digital marketplaces and subscription-based business models will emerge more and more. Thus, customers can quickly access ready-made

solutions and expand their system as needed.

Applications are completely independent of the hardware used and can therefore be ported to more powerful edge hardware depending on the computing power requirements. Automation solutions can thus be scaled better. Docker technology allows access to a variety of available images that can be modified and used to create homebrew apps, enabling rapid prototyping of automation solutions.

Challenges for engineers

"In the automation environment assets as well the relationship between them must be managed efficiently to meet OEE targets. This task becomes exponentially complex at scale. The reason for that are different software or software versions per facility, legacy automation systems and therefore many different protocols but also the management of user access rights," Haneder said.

With the usage of apps and the concept of centralized management of applications and devices, introduced in Siemens' Industrial Edge system, he added that it much easier to implement a SW and HW lifecycle management.

"Security patches and software updates can now be managed and distributed centrally with one click, no more manual installation. This allows an efficient execution of maintenance activities," he added. "Furthermore, with the centralized and remote management a machine or plant builder can extend the functionality of its plant, machine event on-the-fly and is able to introduce new digital business models to his customers. System integrated connectivity apps gives the automation engineers the possibility to connect automation systems and devices from different vendors."

IT technology in factory

Software platforms with portals, use of containers, Node Red and more.

Hilscher's IIoT Business Development Manager, Craig Lentzkow, sees several specific technologies enabling Industrial Edge applications. These include: use of software platforms with portals; use of containers to run applications; Node-RED running in a container; and connectivity of sensors directly to the cloud (bypassing PLCs, IO-Link Masters, etc.).

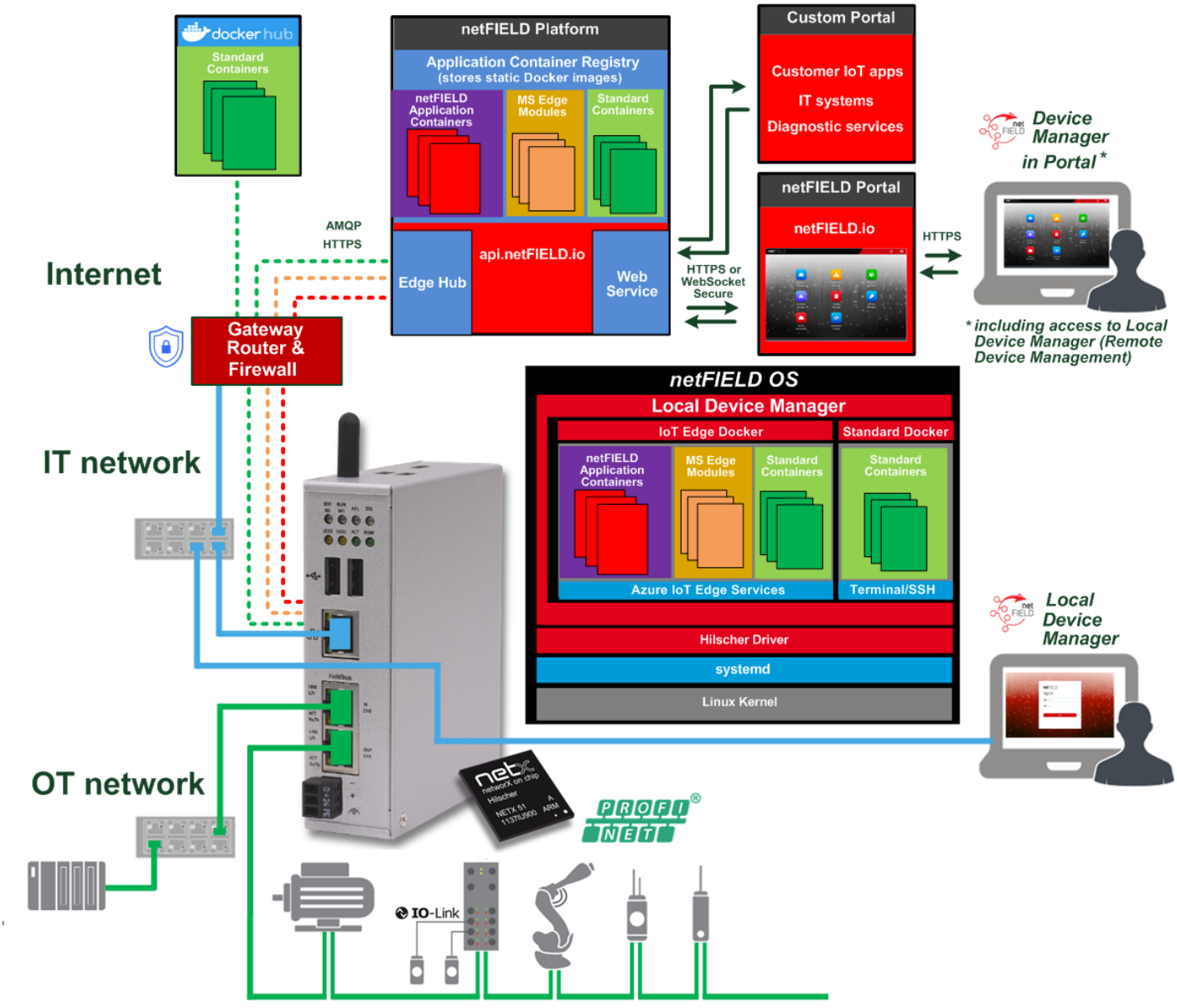
Hilscher recently introduced the netFIELD portfolio of IoT solutions, which enables centrally deployed workloads to be processed at the edge at scale. Based on end-to-end managed services, netFIELD encompasses four edge-enabling technologies.

1) Use of Software Platforms with Portals to manage Edge Devices and Application Containers from remote locations. Scalability to manage millions of devices. Platforms connect the Edge Gateway O.S. to the Portal. The Portal provides an open environment for the configuration of the system with minimal or no programming required.

2) Use of Containers to run applications provides application portability and adds a layer of security by preventing third-party applications that may contain malware from contaminating the system. Containers can be removed and added via the netFIELD platform. This allows customers to easily implement Edge Computing in the Edge Gateway. Customers can include AI applications for data analysis and SCADA applications for tracking, alarming, and trending of data.

3) Node Red, running in a container, provides for a graphical way of extracting data via the Edge Gateway from controllers and I/O devices on machinery. The data can be real-time information and can be routed, customized and protocol converted without additional programming. Converted data is typically routed to Cloud servers or Edge Gateway Computing services for further analysis by AI software.

4) Connectivity of sensors directly to the cloud is possible with sensorEdge Gateways, which are part of the netFIELD portfolio. The sensorEDGE Gateway offers a simple and secure



SOURCE: HILSCHER

Software portals, containerized applications, and direct Sensor-to-Cloud connections are some of the technologies enabling Industrial Edge applications. Illustrating this is the netFIELD solution portfolio from Hilscher.

way to use sensors to monitor critical machine operations. Select sensors can be connected, via IO-Link technology, directly to the cloud by using an "Edge Gateway on a chip" that is embedded in the IO-Link module. No controller, PLC, or IO-Link Master is required.

Industrial application solutions

Lentzkow stated that what is unique in Industrial Edge Computing Solutions is not the technologies themselves, but the application of these known IT technologies to the factory floor. Using these open, standards-based technologies provides customers with greater flexibility and lower costs. The results are solutions with advantages such as:

- Remote management of edge devices
- Graphical tools to process real-time manufacturing data
- Container management technology to improve app portability and security.
- Scalability to manage millions of devices
- Cloud or on-premise-based data storage
- Zero touch on-boarding of edge gateways

The demo box for the sensorEDGE gateways illustrates there is no need for a PLC or IO-Link Master to connect sensor data to the internet..

Specific benefits that can be realized are:

- Detection of potential failure of machine components often referred to as "Predictive Maintenance". This allows users to schedule repairs "just-in-time" instead of incurring unplanned downtime that can costs hundreds of thousands of dollars.
- Production process improvement using analytics against real-time process data.
- Use of digital twin technology to compare real process events with virtual optimized processes, which creates the ability to see where improvement in the real-time production process can be implemented.

continued on pg. 12

Edge gateway solves challenges for food processing OEM

An edge gateway allowed a food processing equipment OEM to offer an effective solution for managing and accessing real-time data. Users can access operational data locally without providing access to their private machine data that is routed to the cloud for preventive maintenance monitoring.

A FOOD PACKAGING EQUIPMENT OEM NEEDED help designing a system architecture that would allow an end user with a global footprint to access their data in real-time while significantly reducing the OEM's maintenance costs.

They also needed to enable their user to access operational data locally without providing access to their private machine data, which was routed to the cloud for preventive maintenance monitoring.

System challenges

Here is a summary of the challenges that the OEM faced in creating and managing an effective system solution:

- Needed access to real-time data globally
- Local access to operational data without access to private machine data
- Needed to avoid higher OEM maintenance costs
- Needed to reduce server management and licensing costs

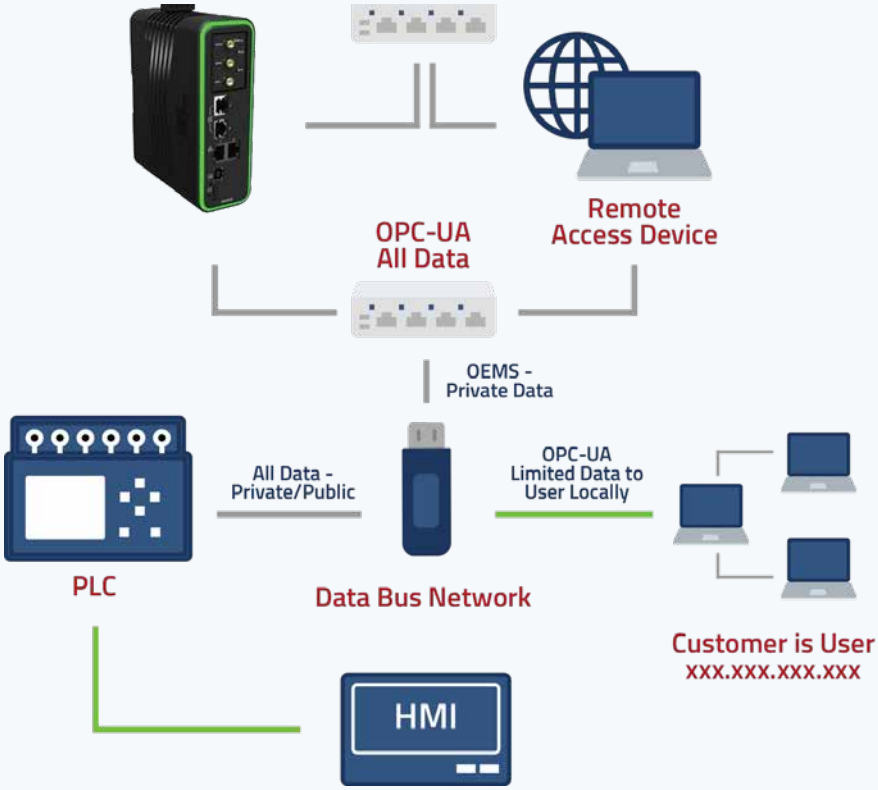
The original architecture included industrial PCs and a centralized protocol server, which captured and transmitted all available data to the cloud. The operational dataset that the user required was sent back to them.

This architecture resulted in exorbitant server management and licensing costs, totaling almost $1 million annually. In addition to the on-going costs, there was also no way to share real-time data with the user, which inhibited their ability to drive efficiency

The Solution

Red Lion provided an elegant solution through the use of a FlexEdge™ DA50A device powered by Crimson®. The advanced automation FlexEdge gateway was installed at the machine layer, connecting and communicating with multiple different PLCs through Crimson's robust protocol conversion functionality.

With Crimson, simple applications can be set up quickly using a step-by-step process to configure communications protocols and define data tags for access.



SOURCE: RD LION

The modular design of the FlexEdge DA50A makes designing for compatibility with rapidly evolving communications standards as easy as replacing a field-installable sled. Regardless of the brand of PLC or other equipment specified, the FlexEdge platform powered by Crimson, enables connectivity to virtually any device in a system.

An extensive menu of built-in, point-and-click serial and Ethernet drivers map controller data to PLC registers in seconds. Built-in communications drivers inherently know how to talk to PLCs, PCs or SCADA systems—so no code is required to establish communication.

Leveraging FlexEdge's OPC-UA Server enabled different datasets to be distributed based on the credentials used. Crimson configured the credential-based datasets and routed the local data to the user and the larger, private, OEM dataset to the OEM's Gateway Panel layer, which was another FlexEdge gateway with a built-in OPC-UA Client.

The OPC-UA Client device captured the OEM's private machine data and sent it to the cloud via MQTT.

Results

- Gateway installed at machine layer
- Different datasets can be distributed based on credentials used. Easily configurable credential-based datasets
- Elimination of $1 million in annual licensing fees
- Increased efficiency and access to real-time data

Ultimately, the OEM eliminated their $1 million in annual licensing fees and provided their user the real-time data they needed to monitor their operational output and increase their efficiency.

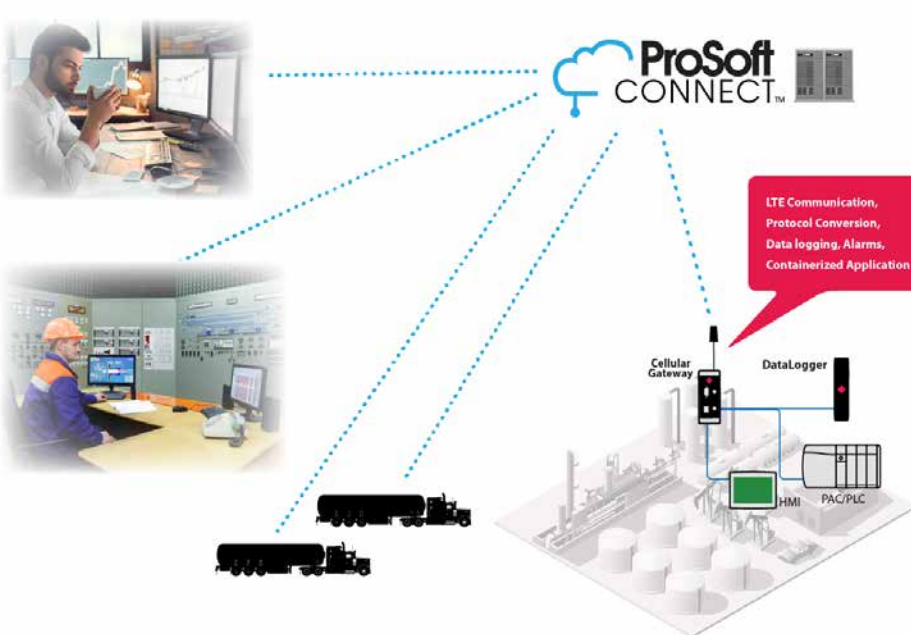
Colin Geis, Director of Product Management - IIoT, ***Red Lion Controls.***

Visit Website

He added that overall manufacturing benefits included reduced machine downtime, streamlined supply chain, improved product quality, reduced cost of manufacturing, happier customers.

"My observation is that the automation engineers are having to learn what these IT technologies can bring to the manufacturing process and how to implement and use these IT technologies," Lentzkow said.

"Training is a 'must have' for these automation engineers. IIoT systems are primarily information gathering systems and they run parallel to the process control systems. They require different tool sets than those used in the OT environment. Knowing how to program using higher-level code such as Node js, C++ and Python are beneficial in creating customer specific solutions, but not necessarily required."



SOURCE: PROSOFT

Industrial edge application leverages OT and IT infrastructure data for continuous optimization to achieve increased efficiency and productivity.

Leveraging IT & OT data

Continuous optimization, efficiency and productivity

According to Vishal Prakash, Strategic Product Manager at ProSoft Technology, to explore the Industrial Edge more effectively, it is useful to define Industrial Edge Computing, Applications, and Gateway.

Industrial Edge Computing: an ability to process time-sensitive data in real time, closer to the source of the information to enable better information flow and real-time decision making, which will improve productivity and response times, and provide better insights into the process.

Industrial Edge Applications: a fully formed end user application that leverages IT+ OT infrastructure and data with business analytics for continuous optimization.

Industrial Edge Gateway: a single device with upstream and downstream connectivity and edge computing capabilities. Upstream connectivity can be to cloud or other business enterprise systems. Downstream connectivity is to field devices like PLCs, RTUs, sensors, and other smart instruments using industrial protocols like Modbus, EtherNet/IP, DNP3, IEC61850, OPC UA, and MQTT.

Enabling Industrial Edge apps

Prakash told IEB that the main technologies enabling industrial edge applications are:

- Ubiquitous & reliable connectivity technologies such as LTE, 5G, and Wi-Fi
- Decentralized computing infrastructure and cloud computing
- Containerized applications
- Increased intelligence and processing power with small form factor for field sensors and automation controllers

"Reliable and high-speed connectivity with reduced latency is a key enabler for industrial edge applications as it allows real-time information exchange between devices and processes. This enables continuous optimization and more current information for better decision-making, leading to increased efficiency and productivity," Prakash stated.

"Decentralized computing infrastructure and cloud computing is another enabler for industrial edge applications as users can off-load data that is not real-time or not as critical to be processed and analyzed in the cloud. This frees up local computing resources for real-time data processing and other actions that can increase productivity and efficiency."

Containerized applications

Prakash said that containerized applications is a relatively new concept in the OT world, but is quickly becoming a key enabler for industrial edge applications as it allows the user to deploy applications consistently and quickly, ensuring consistent results for the same machine and process in any location.

And if the results are made available in the cloud for further analysis, then it will be easy to analyze the impact of the containerized application.

And finally, significant progress in the field of microprocessors has enabled field instruments like sensors and meters to operate faster and more reliably while continually reducing their form factor.

Automation controllers have become smarter and more powerful. These developments enable industrial edge computing because the user has access to more accurate, full data as quickly as possible.

"Industrial edge applications are not new to the industrial world. A PLC or RTU running a remote pump station that has the ability to turn the pump ON and OFF is a very simple industrial edge application," he added. "The same can be said for a controller that is running a remote well pad. But, these are simple and linear examples of edge applications."

Today, an industrial edge application leverages OT and IT infrastructure data for continuous optimization to achieve increased efficiency and productivity. A digital or smart well pad uses edge computing capabilities not just to turn the well pad on and off but to operate the system securely, safely, and proficiently.

A smart well pad likely includes a dedicated PAC (Programmable Automation Controller) that is deterministic to control the process of oil production and a gateway to handle communications to an enterprise SCADA (Supervisory Control and Data Acquisition) and/or to a cloud-based information system.

The communications gateway with edge computing capabilities allows the well pad to optimize productivity by using commercial data points like current market demand, pricing, and the product delivery schedule for optimal production. The deterministic PLC will communicate with smart field instruments like temperature sensors, pressure transmitters, valves, and flow meters to ensure the oil is produced safely.

"So, what is unique with this technology is the asynchronous operation of the industrial edge computing gateway and traditional controller that can share data for optimal efficiency," he said.

Impact on manufacturing

Prakash concluded that there are several technology benefits of industrial edge computing. One significant benefit is better security. Threats are persistent, and as such,

security has to be continuous. With the power of cloud computing and edge computing, processes and devices can be continuously monitored and any threats can be quickly identified, isolated, and notified for action.

Another benefit is latency. Manufacturing processes are looking for continuous optimization. But to achieve this, the processes need to be able to analyze data from multiple sources, manipulate the data, and use the result to increase efficiency. With edge computing capabilities, this can be done locally. Traditionally, all of this data would need to have been sent to a central host to analyze and forward the results – this requires more bandwidth and creates a potential single point of failure and delays. These factors affect the process' productivity and efficiency.

"Main challenges faced by automation engineers today are increased IT (Information Technology) / OT (Operational Technology) convergence, increased security requirements, the need for continuous optimization, and data collection from smart field devices. Industrial edge computing can help solve these challenges. Let's look at each of the challenges in more detail," Prakash said.

"IT/OT convergence is the integration of OT and IT networks to facilitate sharing of data that can be used to increase productivity. Edge computing horsepower can help manufacturing processes and systems understand and use IT and enterprise data successfully."

Focus on security

Since threats are persistent, security has to be continuous. While IT/OT convergence has many benefits, the increased connectivity between OT and IT networks does increase the risk of nefarious attacks on OT systems. Given that OT's top KPI (Key Performance Indicator) is to keep the machine running, edge computing plays a critical role in boosting OT's defense. The capabilities of an edge compute device means that it can be easily integrated with IT security, increasing overall reliability and efficiency.

"Continuous optimization is every manufacturer's dream. Optimization requires reliable data from all sources and the ability to analyze the data quickly with results being acted upon," Prakash added. "This requires processing power. Edge compute devices provide a decentralized compute infrastructure that can reduce bandwidth and latency, positively impacting productivity."

"Smart field devices provide a copious amount of diagnostic data and other information that is very useful for predictive maintenance, enhancing the life of assets, reducing mean time to repair, and other objectives. To capture and store this information, then analyze and act, processing power and space is required. Edge compute devices are built for this."

SOURCE: TTTECH INDUSTRIAL

Industrial edge applications leverage effective software tools to simplify system management.

Process, organize & analyze

Addressing storage, security and real-time performance

Specific technologies enabling Industrial Edge applications in 2021 and beyond focus on storage and processing power and complete platform solutions to handle large amounts of data, according to Dr. Al Beydoun, President and Executive Director at ODVA.

"Local gateways with enhanced storage and processing power are making industrial edge applications possible today. These gateways will likely evolve into more substantial server like appliances as the amount of data for analysis continues to increase. IT technology makes it possible to create containers to allow applications and data to be separated for various use cases and business function needs through software from Docker, Amazon, Microsoft, Google, and so forth," Beydoun said.

"Free applications, such as Node-Red, allow for custom flow-based programming to visualize and analyze device/machine performance and/or operations data. Complete platform solutions that can process, organize, and analyze large amounts of data are made available through traditional industrial automation vendors."

Beydoun added that EtherNet/IP contributes to the efficiency of edge computing by making key network health and device diagnostics easily available. EtherNet/IP offers a Standard Network Diagnostic Assembly that creates a known object address inside a device to make a consistent set of diagnostic information with context quickly accessible. Consistent content in a common location, without having to send numerous messages to different CIP paths within the device, is made available regardless of the device type or vendor.

Free edge applications

Free edge applications provide the ability to directly map to device I/O and diagnostics as well as to create custom algorithms making it possible for end users to solve tough operational challenges in an agile manner and to provide custom visualization to operators and management on the fly at a low cost.

"Platform edge solutions enable larger scale solutions such as data lakes that pool data from all around a plant for more detailed analysis via out of the box tools or data scientists," Beydoun added. "An example of a device that can generate a massive amount of data and can benefit from fast, local processing is an Automated Guided Vehicle (AGV) that needs to keep up to date with a constantly changing factory floor environment."

One of the potential impacts on manufacturing of low-cost edge computing that can be programmed simply and flexibly is the ability to avoid the temptation to go back to paper and pencil or Excel spreadsheets when a new operational problem arises. Additionally, more comprehensive edge platforms can provide for machine learning that can identify potential device failures, like a motor starting to break down, before it happens and alert management to costly operational trends such as a compressor running inefficiently, to save money.

Engineering challenges

According to Beydoun, automation engineers face significant challenges with the high cost of storing and analyzing data in the cloud, security concerns with sending confidential data outside of factory walls, and the need to have real time results from algorithms.

Edge computing can help shift a variable cost from the cloud to a fixed cost with an edge gateway or appliance. Security concerns are also minimized by keeping confidential data such as food recipes local. Finally, edge devices that keep the data onsite are less likely to suffer from connection outages or time delays.

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

PROFINET lays the foundation for modern edge concepts

Besides a traditional controller, there is an increasing need for additional devices or applications for making optimizations. But it's not always easy to connect quickly and also they can produce data that remains unused. Edge concepts present an interesting approach, and PROFINET technologies can support the process.

INDUSTRY 4.0 HAS INSPIRED MANY COMPANIES to develop their own programs, services, devices or other automation components in order to analyze and better understand their machines and systems. Today, 90 percent of the generated data remains unused because the analysis, integration or processing is too complex or impractical in conventional automation components.

And yet it's worth taking a closer look at this wealth of data. Besides the actual measured values, it's possible to identify trends here, such as energy consumption or other long-term diagnostic values that are not typically analyzed in a controller. Due to the data volumes and algorithms, it's also too complex to integrate diagnostic methods with the aid of artificial intelligence.

And manual work is still required for connecting company-specific software into the existing automation world. "Regular updates are indispensable when it comes to making sure that software, operating systems and security measures are up to date and stable. Many companies have a hard time with this, if they are honest with themselves," said Karsten Schneider, PI Chairman.

SOURCE: PI

Edge applications can use PROFINET to help better understand machine performance using the huge amount of unused data.

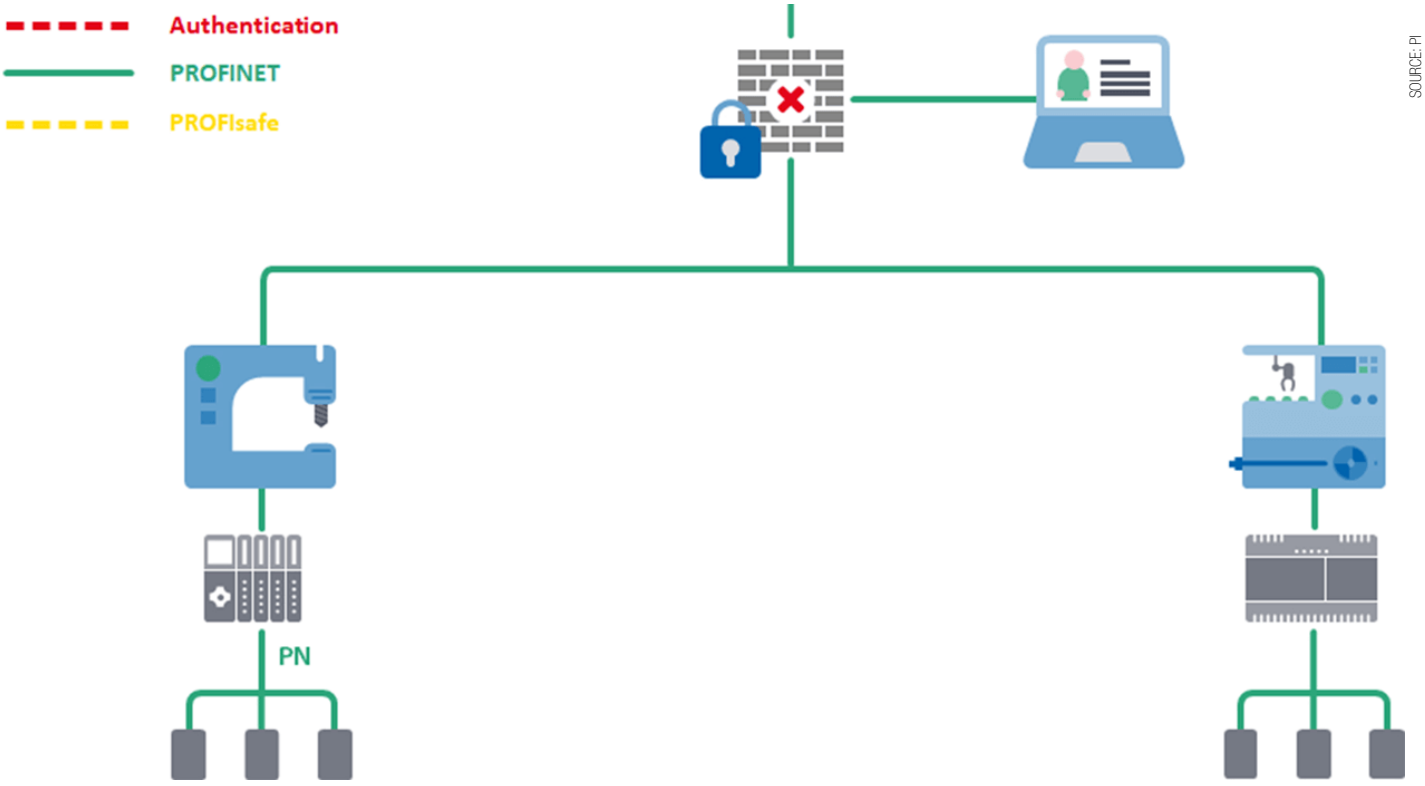
"At the same time, of course, companies want to offer their customers new, intelligent digital products and services. But the effort involved in processing data at the field level can be immense – not to mention issues such as scalability and security," he added.

Key factors in vertical integration

At the same time, the path to a new technology is always a dynamic process. To present just one example here, five years ago it was considered a good solution to direct as much data as possible to the cloud, where it would then be processed.

In the meantime, however, users have realized that it makes sense to process at least part of the data closer to the source – namely, on the edge of the network – due, for example, to latency or bandwidth considerations.

This is where edge components come into play, serving as key factors for vertical integration. They transform additional production data into usable information. It is less important whether this involves



SOURCE: PI

New machine concepts using edge computing and integrating PROFINET and PROFIsafe networking technology.

existing devices in the network that have edge functions, or devices that were added later.

The biggest advantage is that edge components make it possible for data to be processed almost in real time, directly at the source, with a minimum of network traffic. This is also appealing when it comes to data sovereignty. All data remains in the company, and the user decides whether the data should be passed along or not. In any event, it is intended to make life easier for the user or to organize production more efficiently.

New paths with less effort

The major advantage of edge solutions is that they don't require sophisticated reprogramming or updates to the actual automation solution. And they are generally less expensive than a PLC. "The integration of processing capacity on an edge functions much like the apps on our phones – but in secure mode, of course, and in a manner that is suitable for industrial use," explained Schneider.

But there are also other applications in which edge approaches demonstrate their advantages. For example, data is sometimes needed in another form and must be preprocessed in order to standardize raw values or calculate mean values. Or it can happen that, when starting operations, the PLC or other function is not yet available, and yet data is still needed from various devices. Edge concepts are able to work without an PLC, for the start.

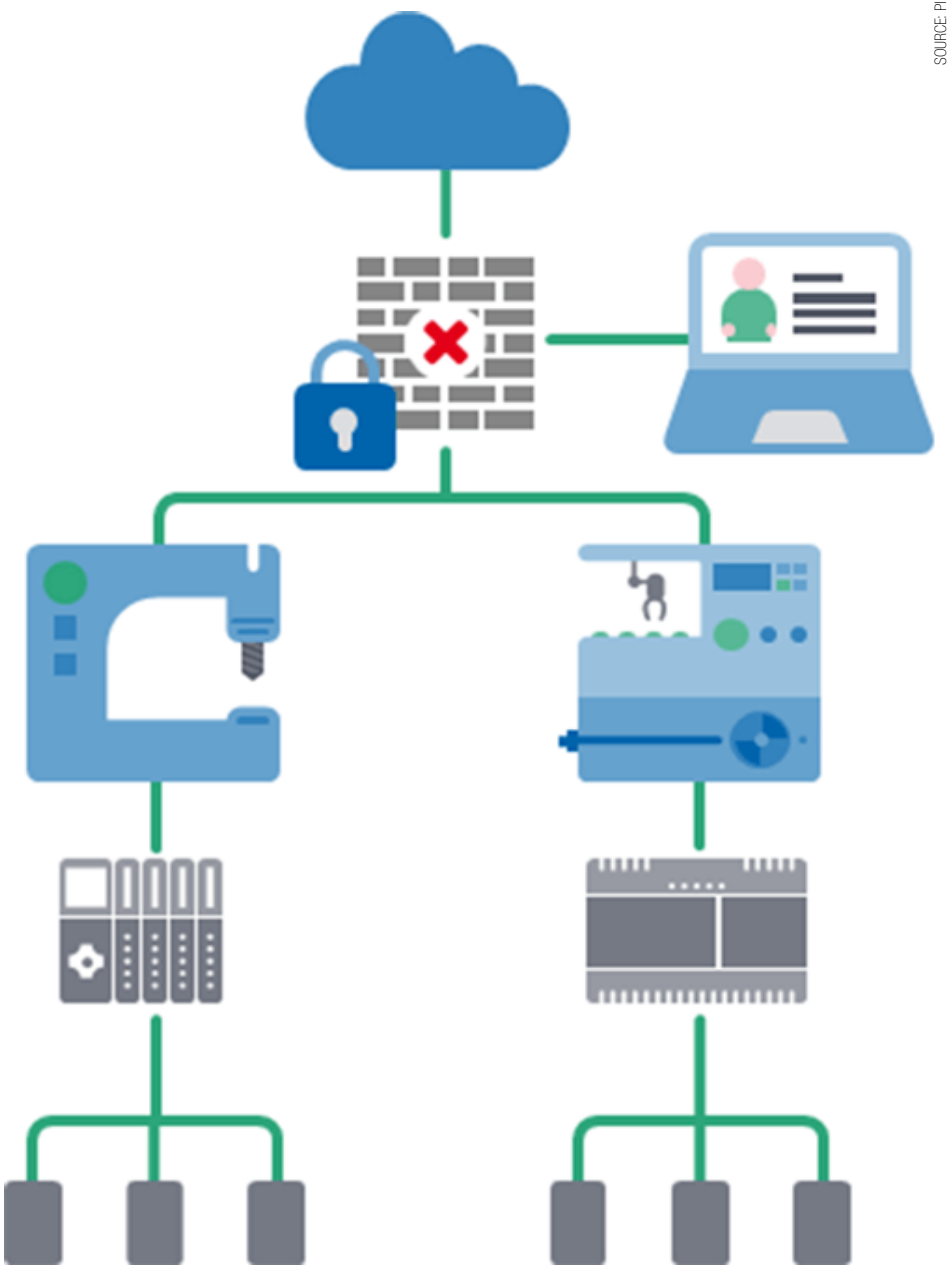
"Likewise, it can be necessary to virtually load additional functions during the course of operations, similarly to how we do it with apps," added Schneider.

In some cases, it may also be necessary for the data collection not to strain the resources of a PLC. "Many controllers often just need a yes/no decision. But usually there is additional useful data available, which is easy to analyze separately by means of an edge application. This could include long-term diagnostic or maintenance data, for example," said Schneider.

"Even if different proprietary communication protocols are used or you need a central location for data, network devices and security configuration, it makes sense to use an edge approach as a data hub," he added.

It's also possible to preprocess data in the edge and then transfer the data to a cloud. This can be done to have access to larger computer capacities or to avoid a continuous strain on the cloud connection. Sometimes a lot of data is collected over an extended period of time in order to facilitate a more detailed analysis.

Edge components don't always have to be viewed separately. They can also be integrated directly next to the controller. Close cooperation between the systems can even be advantageous if an analysis of the data requires close congruence to the condition of the control program or the machine.



SOURCE: PI

New machine concepts integrating edge computing.

Structure to the flood of data

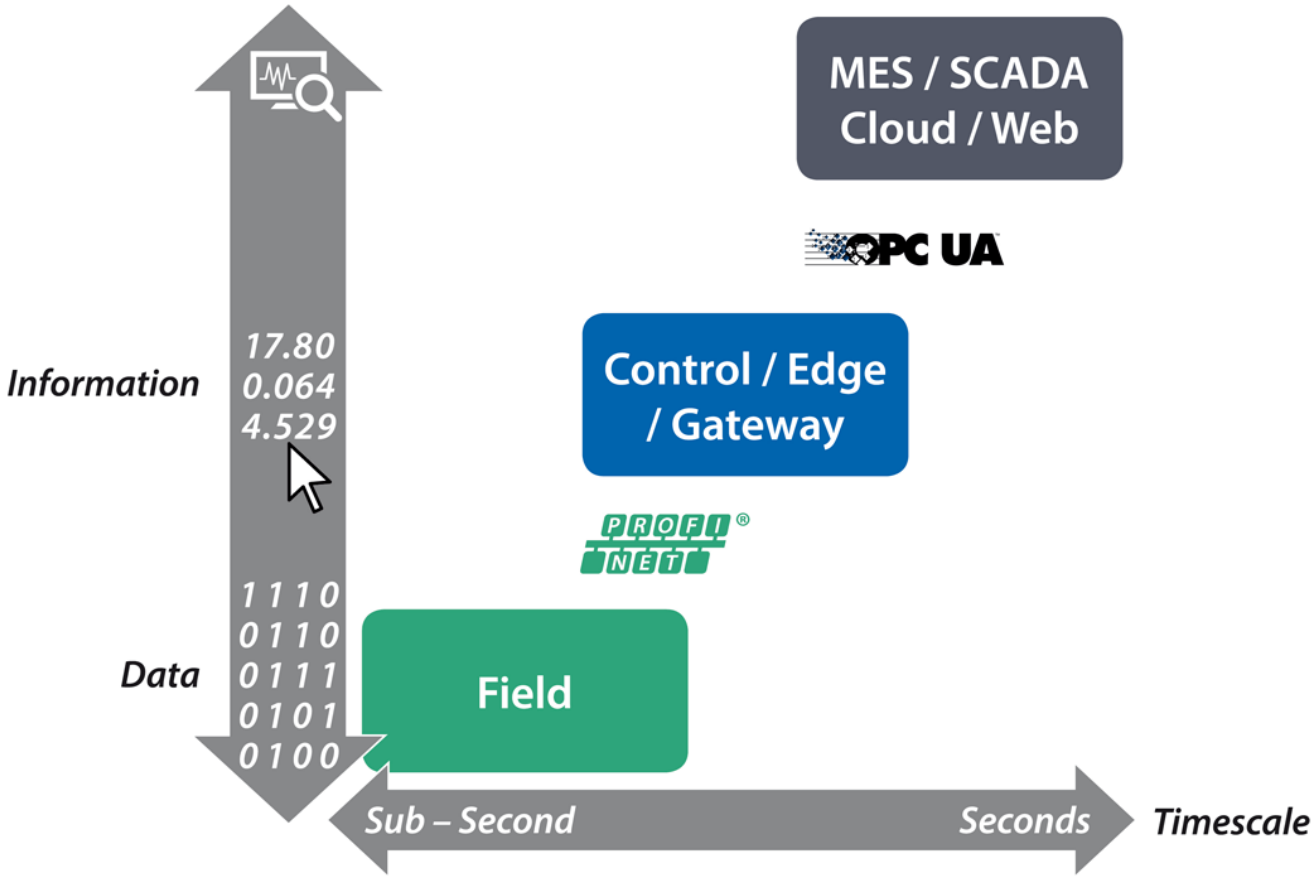
And yet we shouldn't underestimate the need for functioning, secure and fast communication. Each of these edge applications requires data, and not just any data.

The data must be usable and applicable. The data is typically already stored, either as data records that have already been standardized by PROFINET, or as optional additional manufacturer- or device-specific data records. "If I don't know the context, the data is of no use to me," said Schneider.

The increasing number of data sources makes it necessary to have standardized information models. And this is where the PROFINET technologies come into play. They are easy to integrate into existing higher-level enterprise systems, including MES and ERP systems (manufacturing execution systems and enterprise resource planning systems).

Data from the automation network can be made available in real time from almost anywhere in the company.

"At PROFINET, we started focusing on modularity and continuity 20 years ago. And the issue of semantics has always been high on our agenda. This is especially beneficial to us now, because we know how to standardize data," Schneider explained. He cited identification and maintenance data as typical examples here, along with various



SOURCE: PI

OPC UA in PROFINET Controller or Edge-Gateway.

profiles such as PROFIdrive or the PA profile, which are already processed in PROFINET in a way that allows them to be used by other devices. "These properties will be even more important in the future," Schneider said.

The big advantage for device manufacturers is that they don't really need to do anything if their customers use edge concepts, since PROFINET is already standardized. The implementation is also quite simple; after all, the culling of the data has been defined through the PROFINET services since the very beginning, meaning it's included in the corresponding technology packages.

And how does it work in practice? Thanks to PROFINET and OPC UA, every edge component can be integrated. The data mapping typically takes place with the help of OPC UA's object modeling capabilities, either with one's own specifications or combined in accordance with relevant standardized OPC UA companion specifications, such as the OPC UA for PROFINET. Here, data that is collected from PROFINET devices in real time is aggregated and analyzed. The data is preprocessed on the spot, without interrupting the actual processing. If the available PLC doesn't support OPC UA, external edge gateways can be used instead. This is implemented, for example, in process automation when using the NAMUR open architecture (NOA) concept.

Meanwhile, there are edge applications with PROFINET, and the infrastructure is continuing to be built up. "PROFINET already possesses a high degree of standardization – for instance, relating to I&M data or diagnostic formats. The application profiles are also helpful. We have a lot of experience in this area," says Schneider, citing just one of many examples. Additionally, PROFINET ensures parallelism which means multiple devices can be accessed simultaneously, besides the controller.

A final advantage is that PROFINET networks enable edge devices to directly access OPC or TCP/IP devices. Since OPC UA has established itself as the de facto standard for the interoperable exchange of information from the workshop to the highest level (vertical communication), this is the most efficient way to move semantic information within a system. This is a perfect fit for PROFINET, given its ability to operate various protocols independently of one another in the same Ethernet network.

The journey from here

Edge computing not only allows for the easier diagnosis of errors; it also facilitates new business models. One possibility here is payment systems between machines, for example. Up to now, the focus has been only on the data that a device provides. But what about the additional information that could also be of value? Would it not be possible to develop a business model for using this additional data – essentially a microeconomy at shop-floor level? Even for such scenarios, a good system of data collection and analysis is the crucial foundation.

Edge computing serves as a bridge between automation and cloud computing. Since the industry is constantly changing, technologies must remain flexible. That's why there will not be just one technology in the future; rather, users will select the one that is most viable for their purposes – be it edge, controller and/or cloud technology. The most important aspect will surely continue to be that of security, which will be implemented either in the edge itself or on the next-higher level.

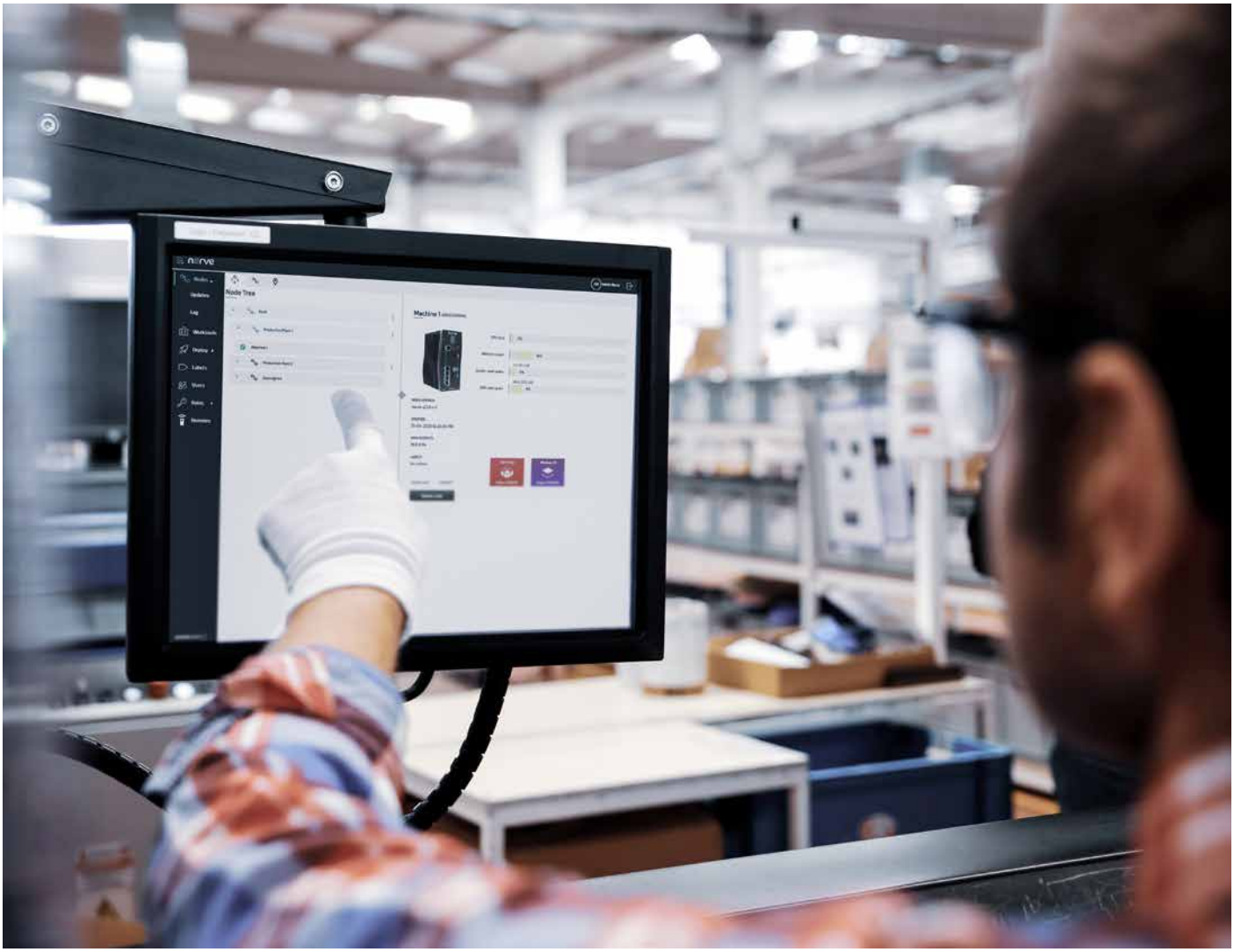
A greater focus will be placed on the principle of "security by design" in order to cover all security aspects from the very start. PI will support its users along the way, regardless of which solution they choose. Independently of how the issue continues to develop, PROFINET's basic architecture (with parallel data traffic) and the high standardization of data is a necessary and solid foundation, thus ensuring the sustainability of systems and production processes.

Xaver Schmidt, Head of the Working Group I4.0, ***PI (PROFIBUS & PROFINET International.***

Visit Website

Industrial Edge: remote access methods and security

Remote access to assets at the industrial edge iimproves flexibility for many workflows in diagnostics and maintenance. This was true before the pandemic, but it has become even more relevant now. And just like remote working in general, we expect the trend towards more flexible remote access to continue.



SOURCE: TTTECH INDUSTRIAL

As digitalization and connectivity in manufacturing increases, secure remote access to industrial assets is becoming more important.

REMOTE ACCESS TO RESOURCES OVER THE internet is an everyday experience for all of us. We use a web browser or similar technology to search for information or buy goods online many times every day, often without thinking about the amazing technologies and distances that are involved.

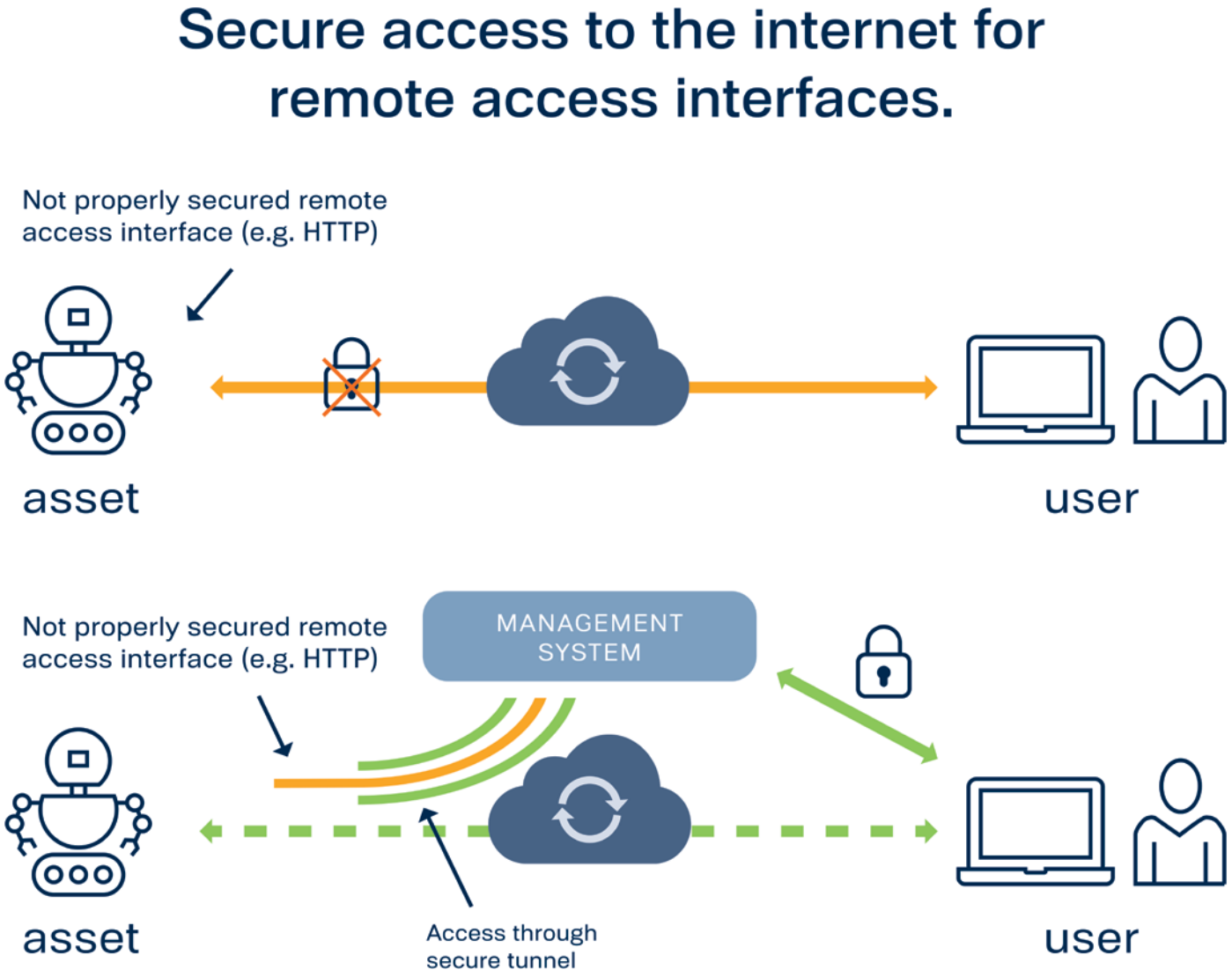
This is especially true in the times of COVID-19 and the sudden increase in working from home, where the need for remote access to company resources from outside the company network through a VPN, via RDP or some other interface has become ubiquitous.

That is not yet true to the same degree for remote access to industrial automation equipment and assets on the shop floor. The operator will usually be close to the machinery to access HMIs and panels, even if the interaction itself would not require this physical proximity. In this article, we are considering various use cases and methods for remote access to the industrial edge and OT equipment.

As this article happens to coincide with the largest and most severe wave of cyber-criminality against industrial systems and critical infrastructure so far, security considerations which need to have high priority for industrial automation related technologies and solutions anyway now become a truly predominant issue. We will therefore discuss various methods for remote access, their benefits and restrictions, and also highlight security-related aspects.

Abundant remote access targets

Assets at the industrial edge can come in many sizes and performance ranges, and this is reflected in the various methods for



SOURCE: TTTECH INDUSTRIAL

Remote access to assets for unsecure interfaces (e.g. HTTP). Secure access can be established via a trusted central management system .

remotely accessing these assets.

A PLC might have an SSH daemon for remote access, while a multi-core edge server might host several Virtual Machines (VMs) along with some Software-Defined Networking (SDN) management entity and a Baseboard Management Controller (BMC), each of which may have one or more management or data interfaces to be considered for remote access.

Some targets for remote access offer old-style command-line shell interfaces, others present a webservices-based REST API. OPC UA servers are becoming more prominent, as are GUIs via HTML5. The favorite for human remote users is remote desktop access with high-definition graphics provided via Xserver, VNC, TeamViewer, RDP; the options are endless.

Some of these interfaces offer no or insufficient authentication and protection methods and are intended for remote access from within a trusted network only. However, which network can be trusted and is guaranteed to be free of security risks? Taking a defensive view on security, we should require proper security – at least SL 2, speaking in terms of IEC 62443 security levels – for any access to any component in the network. That is not the case today.

For example, some assets contain a simple webserver which presents access to some of the asset's data or management via unencrypted HTTP protocol only. Such an interface could technically be made available for remote access by port forwarding or port triggering mechanisms, but it might not be a good idea to do so without restricting the remote access to the unsecured interface to trusted counterpoints (e.g. address whitelisting on the firewall) and tunneling over a secure transport protocol. But is it even feasible to define trusted counterpoints if we want to be flexible?

Centralized access vs. point-to-point

When we want to get remote access to an asset, the most obvious strategy is to use a direct network connection from the user's equipment to the entry point of the asset's local network, such as a router/firewall, which forwards the connection to the asset's local management interface.

This strategy is frequently found when the asset natively provides some remote access capability, such as a console or a webserver. The security of the user authentication depends on the capabilities of that specific interface – for example username/password/two-factor authentication or X.509 certificates, and possibly on the compliance of users with the guidelines . Assets which provide access interfaces with approved security mechanisms can be directly accessed point-to-point by any authenticated user from any location on the internet.

Unfortunately some of the most widely used methods for remote access to assets that support a GUI, such as TeamViewer, VNC, or local webservers, allow the configuration of less secure (but presumably more convenient)

authentication methods, for example a password.

Such possible security pitfalls can be addressed either by stringent enforcement of a sufficiently secure configuration of the authentication mechanism, or by "encapsulating" these remote access methods in a secure central management system environment. Users who want to gain remote access to an asset first need to log into the central management system and can connect to the less secure entry point for remote access at the asset from there.

An industrial edge management solution such as TTTech Industrial's Nerve should support secure remote access to intrinsically unsecure asset interfaces by tunneled port forwarding between the asset and the secure central management system. The management system can then be used from anywhere in the world as the trusted counterpoint for remote access to assets which do not support secure remote access by themselves.

Role-based access control

Remember the recent case where a "hacker" infiltrated a water treatment plant's network infrastructure in Florida thanks to a shared password for TeamViewer applications that granted full access at the plant? If we do not want to get caught up in a similar incident, then it would be a wise choice to follow the state-of-the-art in industrial security practices: The IEC 62443's Authorization Enforcement requirements mandate that access privileges to assets must be managed by a sufficiently fine-grained Role-Based Access Control (RBAC) system. Such an RBAC typically is based on a directory service, e.g. Microsoft Active Directory.

In such a directory service, individual user accounts are maintained along with state-of-the-art authentication, ideally two-factor but at least a "strong password" policy. Access rights and other privileges are granted to an authenticated user based on the roles of that user account or the groups that this user account belongs to. No singular "admin" or "operator" password or token exists, only user accounts that have the privileges to perform administrative tasks. This must also be the case for remote access.

The RBAC strategy has been in place for IT assets for what feels like a century (fun fact: Microsoft Active Directory was first released in 1999) and should equally be used for OT assets. Any method provided for remote access must first authenticate the user and then check the user's specific privileges for remote access – which can be fine-grained, e.g. "can modify resource X via remote access" or "can access resource Y read-only via remote access".

RBAC is just one important aspect to secure remote access. To meet the requirements for industrial security standards, logs of accesses and failed attempts need to be available, repeated failed attempts to gain access must result in temporary or permanent lock-outs, and changes to the privileges defined in the directory must be tracked. In this way, malicious attempts to gain access either by brute-forcing or by adding a back-door account (insiders are responsible for more than a quarter of cybercrimes) can be detected and mitigated.

The scope of required or recommended practices to achieve state-of-the-art security for industrial automation systems cannot be exhaustively listed here, but obviously must be addressed by anyone building and operating remote access capabilities for industrial edge and automation systems. Thankfully, solutions to support this are available – such as TTTech Industrial's edge management platform Nerve.

Customer experience

Remote access to assets by users is a very important part of Industrial IoT use cases. The use cases range from read-only access to data dashboards and monitoring of machine performance to software updates and patch management of production-critical applications.

More and more maintenance activities on OT assets are expected to be performed remotely, or at least with the option to perform them remotely. Even if the maintenance is regularly performed in the physical vicinity and only rarely over a remote access channel, it should look and feel the same for comfort and to minimize errors, and therefore should be based on a method that supports secure remote access by default.

A key feature of an industrial edge management system is the ability to enable secure remote access for many users to all kinds of status and control interfaces - from command-line shells, OPC UA servers, REST APIs, webservers etc. to the entire GUI of a VM. This is especially true for older, legacy interfaces which do not support state-of-the-art security mechanisms.

When setting up remote access to such a wide variety of assets, it is simply not feasible to constrain the management system to a single connection method – rather a mixture of SSH, VPN, RDP, HTTPS etc. is needed. Security considerations are critical and keep growing in importance, but many customers understand that they cannot expect all security guidelines to be heeded by human caution alone and prefer a solution that can securely encapsulate unsecure interfaces.

While the wide range of remote access methods is a fact of life, the requirements for systematic security – typically according to the IEC 62443 (or at least its main principles) – are also among the top priorities. Authentication for any kind of access, and obviously also for remote access, is already predominantly linked to a directory system via LDAP, so the basis for secure RBAC operation is also laid in many cases. There must be no more incidents where critical infrastructure is accessed by a "hacker" discovering a local account with a weak or default password.

There can also be valid exceptions to the RBAC strategy: Sometimes a third party that does not have any regular access to or relationship with the asset owner's infrastructure might need access to a very specific asset and only to that specific asset. For example, the asset vendor's maintenance team may need to perform an upgrade to the asset's firmware. This is clearly a security-related process and it must be ensured that only authorized third parties can gain remote access to perform the maintenance task. However, adding a dedicated user account for each of the vendor's maintenance team members to the asset owner's directory services seems excessively burdensome.

For such cases, it may be desirable to have a well-documented process to temporarily give the minimum necessary remote access privileges to a "local user" account on that specific asset and let the maintenance crew use that account. Obviously, the user account which can enable and manage this "local user" account must be a properly secured and authorized regular account in the RBAC, and all logging and auditing requirements must be met. We are currently investigating how this functionality can securely be implemented in TTTech Industrial's own edge computing platform Nerve.

Conclusions

Remote access to assets at the industrial edge is considered a very important capability by users because it greatly improves flexibility for many workflows in diagnostics and maintenance. This was true before the pandemic, but it has become even more relevant now. And just like remote working in general, we expect the trend towards more flexible remote access to continue.

However, security concerns must be on top of the priority list and cannot be subjected purely to ease of use considerations. Since many assets do not (yet) offer suitably secure methods for authentication and privilege management for their management and status interfaces, it is up to the edge management system – such as TTTech Industrial's Nerve – to provide a set of mechanisms to "encapsulate" these interfaces in a secure way and provide access only to properly authenticated users with appropriate privileges.

Georg Stöger, Director Training and Consulting, ***TTTech Industrial.***

Visit Website

Data optimization at the edge with local data processing

The industrial world is being driven to more and more "close integration" from sensors to the cloud. Industries need to start connecting their machineries and production to collective networks so that they can achieve e.g., Industrie 4.0 compliant, data driven production.

SOURCE: SIEMENS

Processing data close to production, using a fast and reliable connection, requires a plan for how and where the data can be processed efficiently.

THE FIRST STEP WITH CENTRALIZED DATA collection was to get data into the central database where it could be processed and analyzed. In most of the cases, this was done by streaming all possible data to databases. This meant that gigabytes to terabytes of data were pushed over the networks into data centers or clouds.

Processing data locally

Companies are now starting to realize that simply streaming all data out and then back in isn't necessarily the most functional way to do it. Data needs to be first processed close to the machines so that short-term, production relevant data can be quickly looped back to the machine's PLC and long-term data can be preprocessed and sent to central databases to be analyzed and archived.

Processing data close to the production, while having a fast and reliable connection to the machine's brains, requires a platform and a concept of how and where the data could be processed efficiently.

Body and soul for production

Hardware-wise this platform should have the same "body" and characteristics as the production machine itself - meaning temperature endurance, maintenance free, industrial grade components that have the same life cycle as the machine.

ARM processor architecture with long life memory chip is a good solution for this task, due to its fast and reliable operation and low power usage. This architecture is being used in industrial network components and PLCs.

In addition to reliable hardware, the local processing engine needs to have "a soul", an operating system that can grow and evolve according to needs. This is most obviously a place for a Linux environment. By selecting the "mother" of all Linux distributions, "Debian" fills this place.

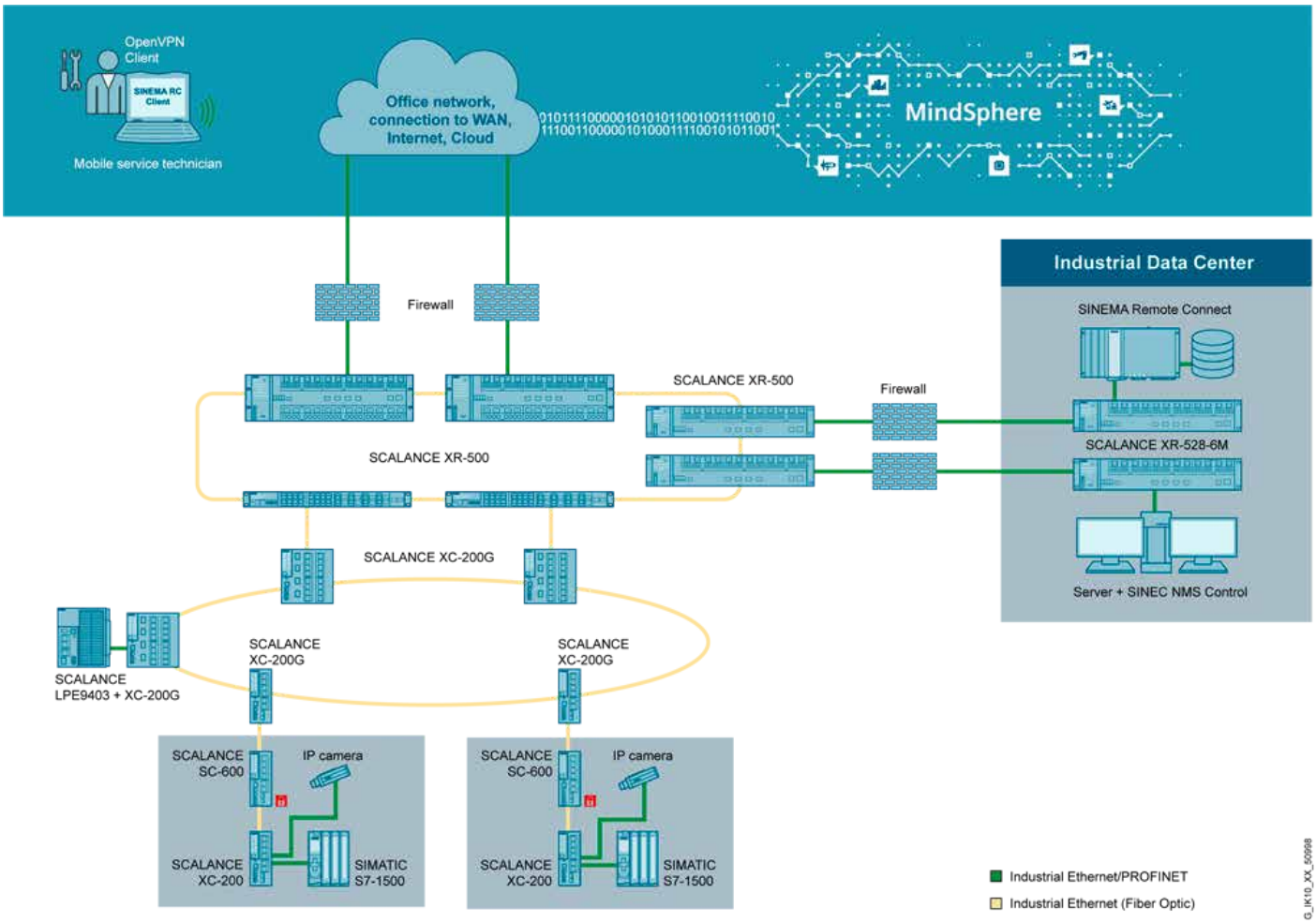
This platform needs to be able to analyze and process data, run security applications (IAD, IDS, firewalls), be open for a customized solution, utilize containerized applications and establish a secure connection to different platforms and ecosystems.

Faster and flexible commissioning

Spicing up the operating system with a fast and simple distribution of Edge application, Docker© platform offers a good and widely used solution.

Now, just by writing "apt-get" <application name>, "pull" <container name> in the command line or a couple of mouse clicks in containers or in the Industrial Edge central management platform, applications can now be quickly and easily commissioned in all local processing platforms.

SOURCE: SIEMENS



Local Processing Engine in the shopfloor.

This allows for a faster and more flexible way to do commissioning for various applications and gives customers a breeding ground for their data processing projects.

Multitasker for the shop floor

There are production plants and machines that are connected to factory networks as segmented network cells. Communication between the cell and the SCADA system has been already setup and it is currently working.

The user has to decide for his production plant in a data mining application which data must be collected and how often. The SCADA system already collects data from the machines and plants, but this is only for operation and monitoring restricted data. Adding new data points and forwarding them to upper-level systems takes a lot of effort and may lead to an upgrade of the SCADA system. This is typically not wanted.

Placing a processing engine that can gather and process all kind of data, flexibly inside or close to the cells sounds like a good option. Creating a cell dedicated small application that talks with the machine transparently without any effect on existing communications would be the solution.

The next step is to establish who will create this application and where it will be hosted. The decision has been made that IT takes responsibility of developing the software, while automation takes responsibility of maintaining the hardware on the shop floor. An ideal hardware solution is a processing engine that allows open-source applications and container-based architecture.

While the data mining project is running, it is clear that an additional application could be integrated to improve maintenance of the production machines in the factory. These enhancements would change production from reactive troubleshooting to proactive and preventative maintenance. The company decides to pursue these changes in order to reap these benefits.

Automation wants to have applications that are simple to use and capable of providing them with relevant information. Searching for applications from different sources reveals that there are several possibilities to implement existing applications from open sources. A deep dive into the analysis identified that both the data mining and troubleshooting applications should be hosted on the same hardware due to the same requirement for data source connectivity and maintenance. As a solution, they will need a multitasker platform for the shopfloor.

The perfect match for the application is found from Siemens generated, industrial use application specially for process network analyzing. This application is also developed to run as container on an ARM based device called Scalance LPE9403, which is a local processing engine that has the power to run multiple applications simultaneously as containers.

By locating this device at the cell or aggregation level in the automation network, they can concentrate on data gathering and analyzers in one hardware platform without compromising applications availability.

Integrating Edge computing into the shop floor with a robust and flexible platform can optimize machine and plant availability and performance, improve data-driven decision making and enable machine builders to develop new business models.

Milouni Sheth, Marketing Operations, ***Siemens DI PA.***

Visit Website

Integrated data & control for process automation OEM

An Oil & Gas OEM uses integrated data and control to deliver reliable automated pressure testing. Integration on a single backplane has been the key to dramatically lowering cost, improving uptime, accessing data and expanding utilization.

ENGENUITY PROVIDES CONTROL AUTOMATION and data integration solutions across several industries, with a primary focus on advanced technologies for oil & gas customers. Through their work in this industry, they identified specific deficiencies in validation pressure testing of blowout preventers (BOPs) and well control equipment.

Pressure tests must be completed every few weeks in order to maintain the safety and integrity of drilling facilities. They are typically executed and recorded manually, taking hours to complete. Since it can cost as much as $6.00 per second to operate the associated valve arrays in an offshore drilling application, testing can cost millions of dollars annually.

In collaboration with customers like Shell International Exploration and Production Company, Engenuity developed a set of fully automated hydrostatic test execution and reporting products. Their reliability solution uses the *groov* EPIC edge programmable industrial controller for precise process control, automatic text and email notification, and process history storage and replication.

Grace under pressure

Using Engenuity's BOPX testing software, users can map out valve arrays and identify validation pressure limits for each component in the system. Using a patented constant-pressure/variable-volume pumping method, BOPX brings the system to pressure while precisely measuring the injected fluid and objectively comparing measurements against validation criteria.

SOURCE: OPTO 22

EZ Vision readout and leak detection system.

Engenuity's EZ Valve retrofittable actuator works with the BOPX test manager to add automated monitoring and control to manual valve arrays. The system can actuate up to 70 valves through as many as 30 test sequences.

Finally, Engenuity's EZ Vision readout uses an innovative acoustical leak detection system to pinpoint the location of leaks in large-manifold systems.Collected data can be mapped between tests for comparison and reliability purposes and used to generate PDF reports. Depending on an installation's size and operations, Engenuity's BOPX pressure testing system can save 10-20 hours for each full test with a fully integrated system.

SOURCE: OPTO 22

EZ Valve retrofittable actuator.

How it works

BOPX offers sophisticated modeling, analytics, and presentation functions. But while Engenuity has added many features over the years, Ted Royer, a controls engineer with Engenuity, stresses that "all the test software is on EPIC. [BOPX] is just an interface now." Let's see how Engenuity uses groov EPIC to bring this awesome system together.

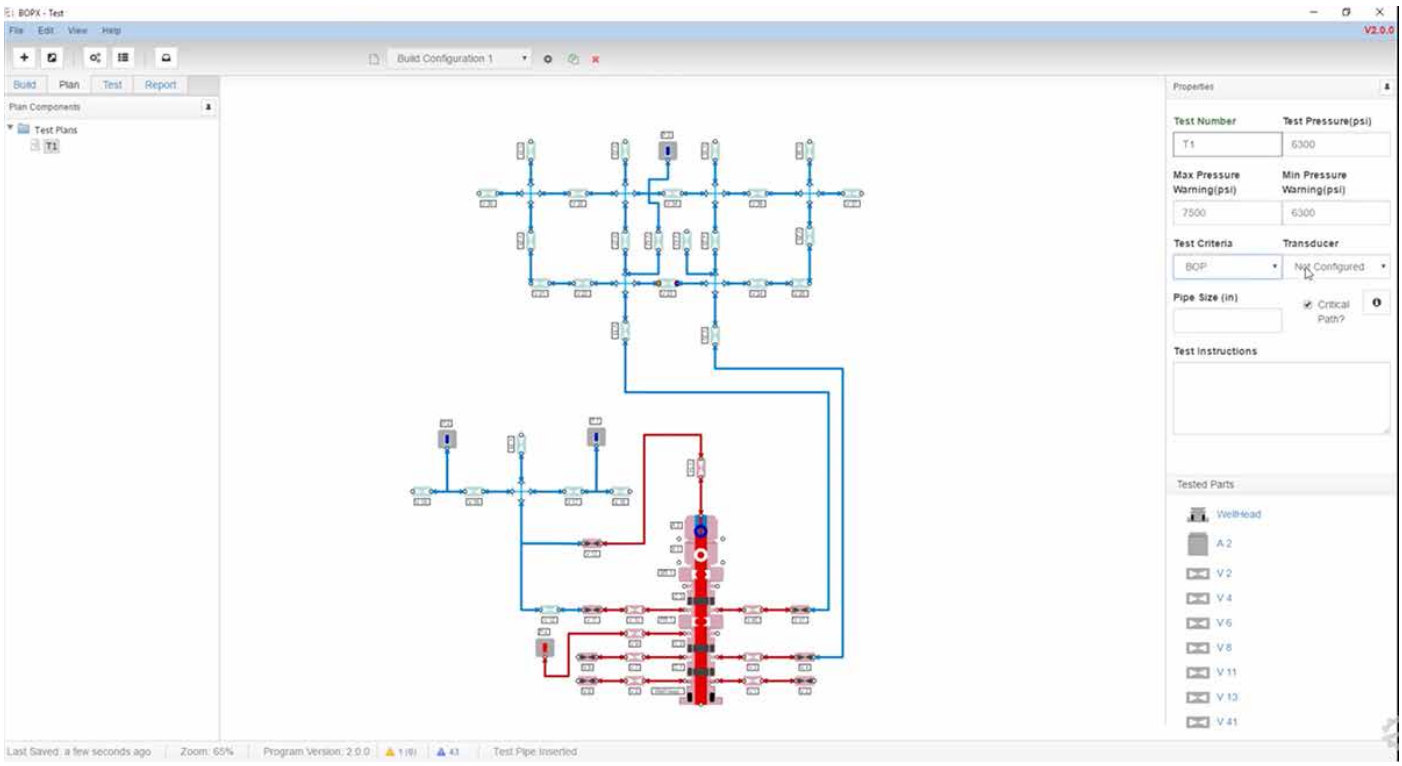
Secure configuration

BOPX's primary role in test execution is to send configuration data to the groov EPIC edge controller over a Modbus/TCP connection.

"We could do other things, but we needed a way to show where the data was," explained Royer. "Customers want it their way, so you need to be able to say, OK, we can do that."

And typically, Engenuity's customers want to work with traditional protocols like Modbus so they can easily verify that configuration parameters are transmitted correctly.

However, an unsecured Modbus connection could pose a risk to operations, so Engenuity uses groov EPIC's configurable firewall to protect critical control data. One of the edge controller's two network ports is configured as a read-only customer interface joined to an untrusted network called the Manufacturing Demilitarized Zone (DMZ). The other network port is joined to a separate trusted network,



Engenuity's BOPX testing software lets users map valve arrays and set limits.

named the Manufacturing Zone, where all I/O and control communication takes place.

The EPIC's design prevents routing traffic between its two ports, so there is no risk of untrusted connections tampering with configuration, execution, or process history data on the trusted network.

Process control & alarm notification

With configuration data securely transmitted, the edge controller begins executing test scenarios. Generally, automated valve manifolds and EZ Valve and EZ Vision connections are integrated directly into the EPIC's local I/O modules, but if a large amount of high-speed processing is required (typically in the 3-4 ms range) Engenuity sometimes uses a separate groov EPIC as remote I/O. In that case, the remote EPIC handles all of the control independently and simply reports back to the primary edge controller. As test execution proceeds, the primary controller monitors the process.

"We have a really well-developed alarm system we've developed over decades," Royer added. "It runs in the controller, not the HMI, so it's available to other systems," including external mail and messaging services, which the control program (written in PAC Control) contacts to generate email and text notifications for a range of conditions.

Process history storage

The primary controller also stores any process data generated during testing to an internal MariaDB server. A popular and proven open-source database management system, MariaDB is available in a cryptographically signed package from Opto 22's Linux repository. Using the free secure shell (SSH) license for groov EPIC, Engenuity can download and install this and many other applications for execution directly on their edge controller.

To transfer data from the control engine to the database, Engenuity uses Node-RED, an open-source IoT platform originally designed by IBM, which is pre-installed and integrated into groov EPIC's management layer. Node-RED provides thousands of functions for connecting and processing data from different sources, including devices, databases, and web services.

Engenuity configures Node-RED to monitor I/O, process variables, and events, then transmit these data points to the internal MariaDB server.

Data integrity and availability

Because testing data is used to validate the safety and efficacy of the system, customers need frequent access to process history and often require additional protections to ensure data integrity. Engenuity accomplishes this using MariaDB's built-in replication function.

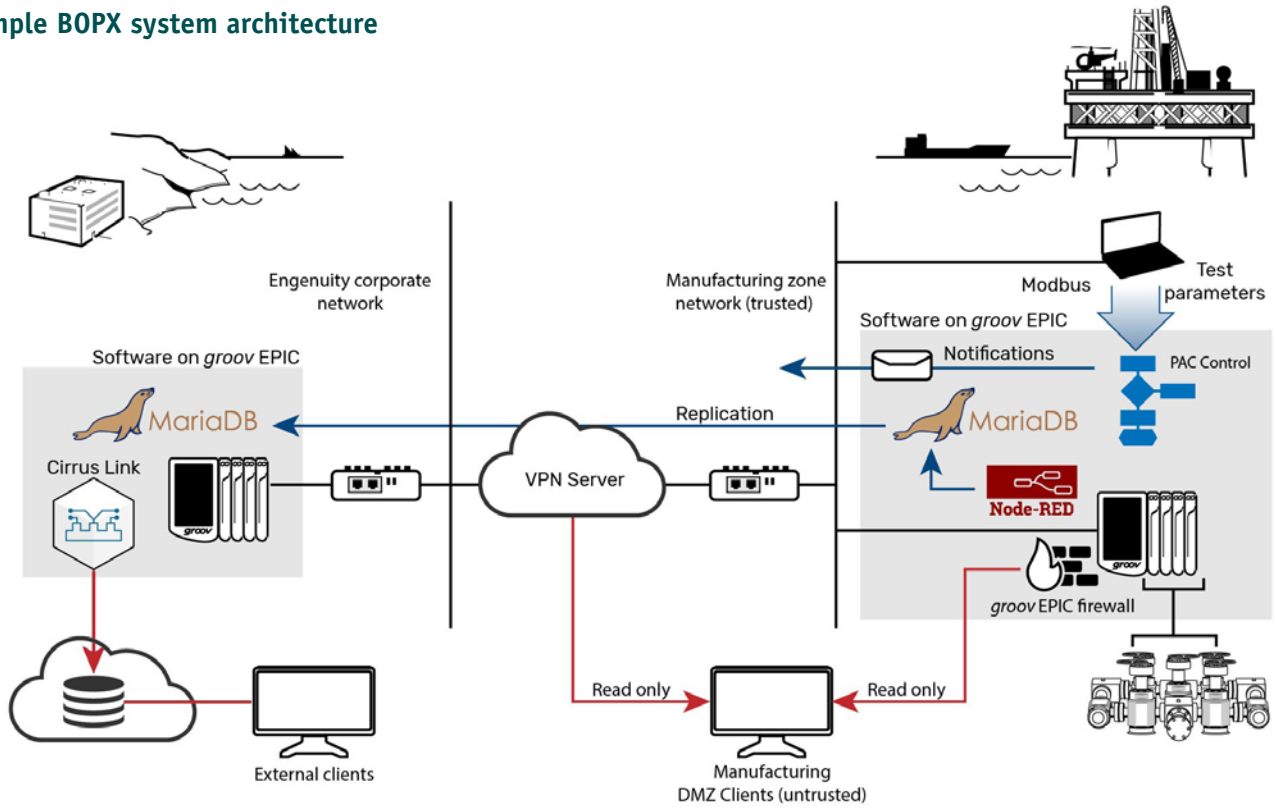
"Typically, on an oil rig, customers just have a WiFi connection to the equipment, which isn't super reliable," Royer explained, "and they want to be able to log in and see data from previous runs. Sometimes they want to pull massive amounts of records, even entire jobs, into an Excel spreadsheet. It doesn't have to be real-time, though, so we will set up another controller here in the office that serves as a replica for the one that's in the field."

Periodically, the MariaDB server housed

SOURCE: OPTO 22

Pressure tests performed every few weeks maintain the safety and integrity of drilling facilities.

Example BOPX system architecture



SOURCE: OPTO 22

in the on-shore replica requests database replication from the off-shore primary controller. In response, the primary MariaDB server sends a transaction log to the replica, which it uses to update itself.

Instead of burdening the primary EPIC with large data requests, customers can connect to the replica, providing them with data redundancy and high availability. "We have plenty of bandwidth here [in the office]," added Royer, "so it gives them the best of both worlds."

Of course, transmitting sensitive data between networks over long distances creates security concerns, and Engenuity's network architecture again plays an important role.

To facilitate secure data exchange with the primary edge controller, Engenuity joins the replica controller to the off-shore Manufacturing Zone network using a point-to-point VPN connection.

Engenuity then grants customers read-only credentials to this private network. In fact, every replica controller in Engenuity's offices connects to the outside through a separate, dedicated VPN appliance. "It's simple and as bulletproof as we could make it," said Royer.

Enterprise connectivity

In the case that a customer wants to distribute process data beyond a single site, Engenuity takes advantage of groov EPIC's integration with Ignition Edge® from Inductive Automation®. Like Node-RED, this application comes pre-installed on all EPICs. It is used most often to provide OPC UA integration of third-party devices and PLCs.

However, the Ignition platform has a modular architecture that allows users to install a range of additional components, including connectivity solutions from third-party provider Cirrus Link® Solutions. Engenuity uses Cirrus Link's cloud injector modules, which allow groov EPIC to send OPC tag data directly to cloud services like AWS, Azure, Google Cloud, or IBM Cloud. Once there, customers can access testing data around the world.

Why EPIC?

Engenuity's BOPX system uses intelligent, integrated automation to reduce the costs associated with validated pressure testing. Testing is required for regulatory compliance, and the cost of downtime may be $15-20k per hour, so BOPX must execute quickly and consistently in order to deliver value to the customer.

Engenuity has standardized on groov EPIC over traditional PLC control, ultimately, because it helps them provide more reliable operation and efficient support.

"EPIC I/O is high quality, and you need to have very stable I/O for these applications," noted Royer. "[But] there are so many advantages to having a full control system that can tell you what's wrong…. I'll get a text [from the control system] in the middle of the night, and I'm already logged in by the time they call me. I can tell them exactly where the problem is, and, usually, it's something simple."

Naturally, Engenuity's customers reap the benefits as well. With high uptime and automated testing, they are able to reduce on-site staff and have adapted more easily to remote operations.

However, Royer is also quick to point out the value that off-shore sites place on equipment that can be installed in the field.

"[Customers] don't have space for racks of servers. These [IT rooms] are non-classified areas in the middle of hazardous areas. They need all this air conditioning and so on to keep this IT stuff going. They are designed to be half full and [typically] they are overfull. So now you are going to replace that with stuff that can go outside in a NEMA 4 box. [Our groov EPIC's] got nine servers on it and we haven't even taken up one foot of space! If you want another one, it's only another $1,500."

"You cannot do this with a traditional controller," Royer argued. "That's been the big leap with Opto 22: the hybrid controller allows you to do it all."

With groov EPIC, Engenuity eliminates complex multiproduct integration requirements and delivers seamless operation and instant data access either in SCADA, IoT, or hosted data applications.

Jeff Hilpert, president at Engenuity, added, "The integration of data and control on a single backplane has been key to dramatically lowering cost, improving uptime, accessing data, and expanding utilization."

Josh Eastburn, Director of Technical Marketing, ***Opto 22.***

Visit Website

industrial ethernet book

Industrial Networking & IIoT

Product Showcase

Industrial Edge: use cases & solutions

Learn about the technology megatrends shaping the newest generation of Industrial Edge application and product solutions.

Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

Offering the 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

Industrial Edge impact on smart manufacturing

Industrial Edge technologies are making an impact on smart manufacturing. In this special report, industry experts comment on the current evolution of control technology, open source Linux applications, industrial PCs configured as both control computers and edge PCs, and the renaissance of Industrial Ethernet.

Edge data processing is being used to filter, sanitize, and transform data into interoperable formats before transmission directly to databases or cloud services.

INDUSTRIAL EDGE TECHNOLOGY IS ENABLING comprehensive IIoT solutions that extend from the edge to the cloud, and provide a powerful impetus in the convergence of IT and OT operations.

In this special showcase, the Industrial Ethernet Book looks at how edge technology is making an impact on smart manufacturing. Industry experts weigh in on the leading trends in edge computing, and we present the latest new solutions for manufacturers.

Evolution of control technology

Edge solutions driven by application and networking security standards.

Industrial control technology is evolving from traditional formats like RTUs, PLCs, and PACs to edge-oriented options like edge programmable industrial controllers (edge controllers or EPICs) and edge I/O, according to Josh Eastburn, Director of Technical Marketing at Opto 22. These formats provide general-purpose processing, networking, and storage in the field, which create a foundation for embedding other critical technologies.

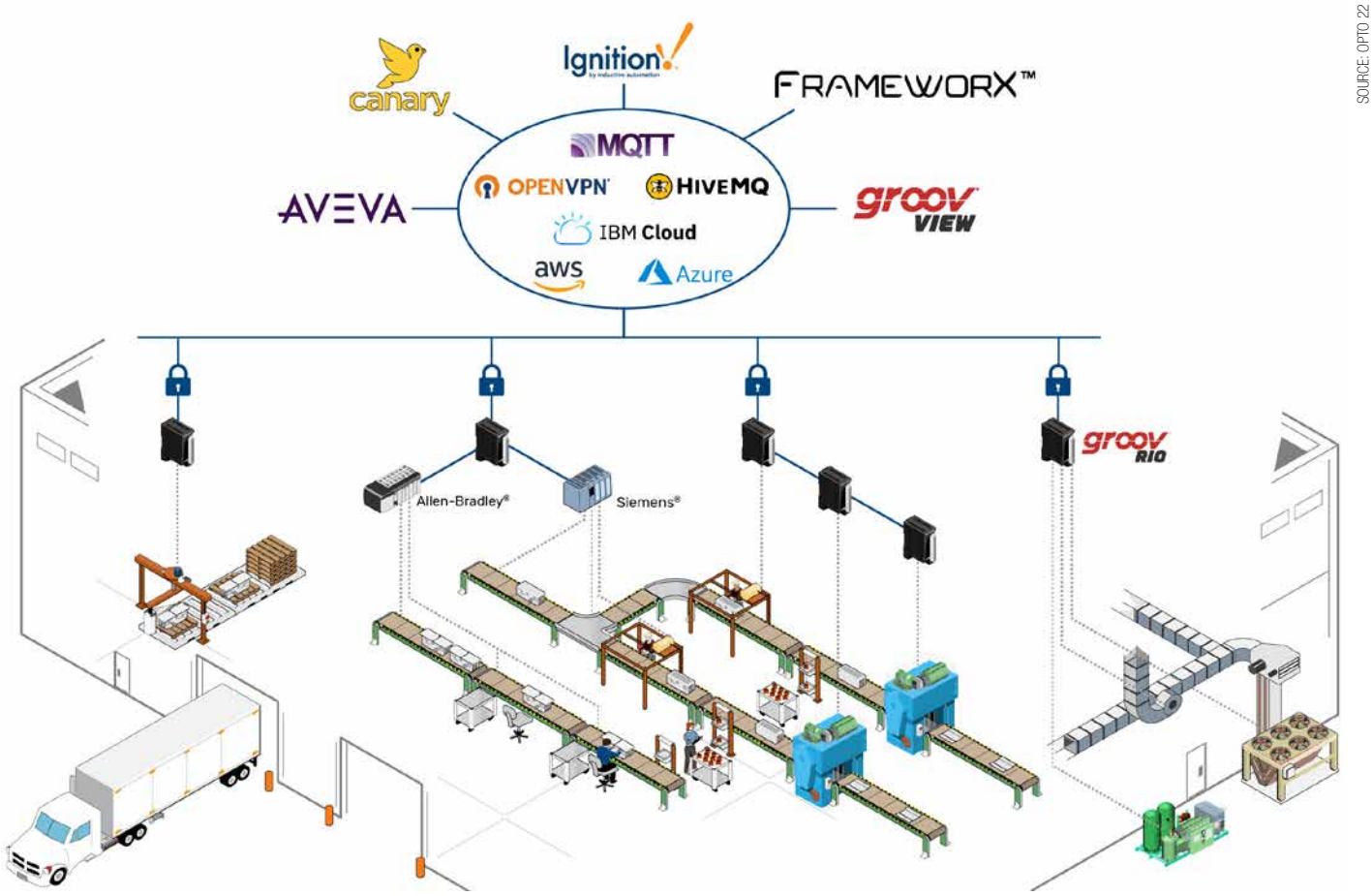
"At the top of that list, are application and networking security standards like user authentication, firewalls, and SSL/TLS encryption," Eastburn told IEB recently. "The lack of these features in industrial devices has been a showstopper for years in terms of bridging IT and OT systems, but with them in place, edge-to-cloud communication is entirely feasible."

"And if edge-to-cloud or IIoT is the goal, MQTT is another critical enabling technology," Eastburn added. "Designed for the internet of things (IoT), this protocol supports lightweight, secure communication for distributed edge devices. When paired with Sparkplug B payloads, interoperability, state management, and fault tolerance are also boosted."

Technology stack at field level

According to Eastburn, edge controllers and I/O combine traditional automation functions with embedded tools for security, communication, and data processing that previously required many layers of hardware and software.

For example, moving data from a single field device into business applications might require transferring data through PLC, SCADA, MES, and ERP systems. Low-level systems have lacked the protocols to establish secure



SOURCE: OPTO 22

An example of a simple yet highly scalable and comprehensive IIoT network using Opto 22 groov RIO edge I/O modules.

connections to high-level systems directly or to provide data that was usable by those systems.

"Edge-oriented automation embeds the necessary technology stack at the field device level, allowing for flatter, more scalable architectures. Embedded communication and security tools enable edge devices to secure brownfield devices and bridge disparate automation networks. Edge data processing can be used to filter, sanitize, and transform data into interoperable formats before transmission directly to databases or cloud services," he said.

Embedded MQTT clients in the field can publish data to a shared MQTT server or redundant server group located anywhere the network reaches: on premises, in the cloud, or as part of regional fog computing resources.

Clients publish data only on change rather than cyclically, dramatically reducing bandwidth consumption.

And rather than requiring connections to field assets from every interested application, the MQTT server itself distributes these updates to any subscribers of that data. The burden on the network and device increases at a much slower rate than with traditional poll-response protocols found in many of today's automation systems.

Large scale integrated systems

Eastburn said that edge control provides a foundation for large-scale integrated industrial systems that scales more securely, reliably, and affordably than previous technologies. Digital transformation projects have so far been limited to large, well-funded enterprises, but with this foundation, it has become possible for even small organizations to achieve. By processing data at the edge and reducing the complexity of the architecture, engineers save in data transmission and middleware licensing costs, as well as in the labor required to design, install, configure, and maintain data systems.

"Many companies are getting trapped in pilot purgatory with early IIoT designs that are based on the traditional hierarchical architectures. Edge control lets designers break out of that trap and scale smoothly from proof-of-concept to production system," he added.

The challenges that automation engineers face with these advances in edge computing is that each layer of hardware and software adds cost and complexity to large-scale integration projects, both of which inhibit system growth, stability, and security.

"The majority of valuable industrial data is found in brownfield systems, but integrating this data is challenging because of the lack of security or IT-friendly communication protocols and data formats," Eastburn said.

"A common objective for early IIoT projects is to focus the system on transporting data to cloud services for processing and analysis. However, raw data streams are costly to transport, store, and process," he added.

Open source Linux apps

Combined with traditional determinist industrial controls

According to Charles Norz, Automation Product Manager WAGO Corporation, industrial control has been around for decades and has proven itself as technology to increase yields and quality. Linux based systems have also been around for a long time and been used and embraced in IT applications, however they have not been that predominate on the plant floor.

"Edge devices are changing the way systems are architected by combining the proven technologies of industrial control with open source Linux based applications to further increase plant floor performance," Norz told IEB recently.

Norz added that, as the competitive landscape is now on a global scale,

manufacturing is taking advantage of IIoT systems that integrate plant floor equipment with cloud based services. Centralized data enables engineers, maintenance, order services, and product line managers to have an enterprise view of manufacturing, equipment health and production. Plant floor operators are now connected workers. They have a clear view of the current operating state of their equipment plus data on upstream and downstream processes enabling them to make informed decisions.

"This is all made possible with edge devices, that is equipment that combines determinism that is needed for real time control on the plant floor with IT based applications that provide valuable analytics to the connected worker as well as aggregated and contextualized information for the enterprise," Norz said.

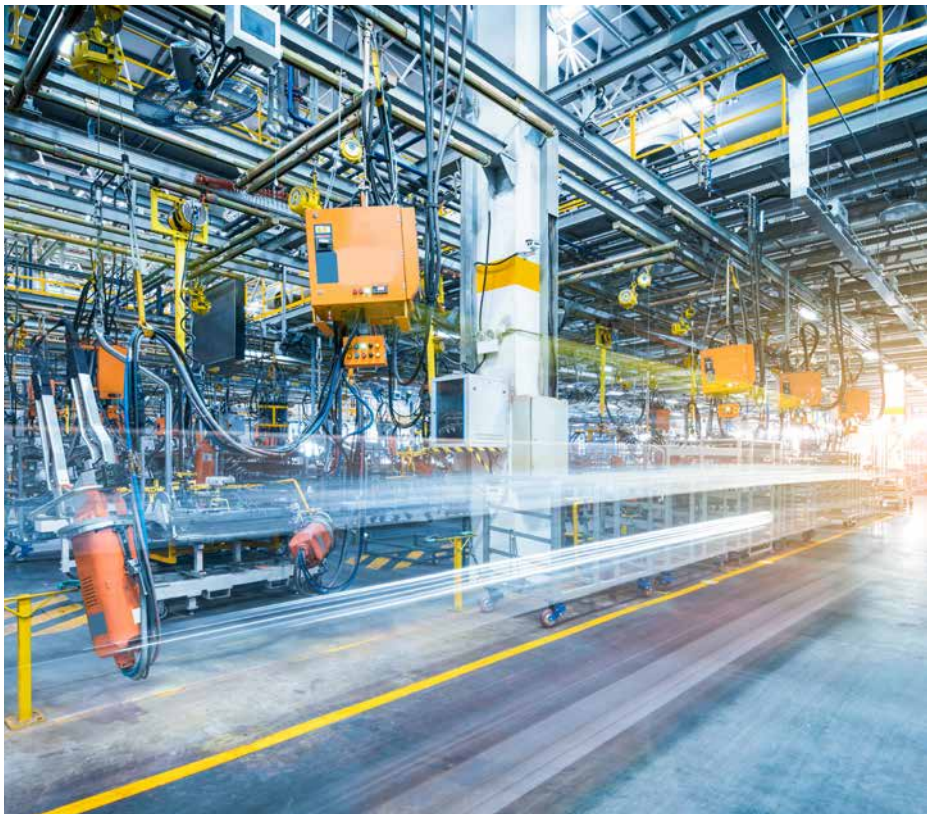
IT and OT combined

Automation engineers are faced with the need to live in both the OT and IT world. They require tools that can on one hand interface with real time I/O on plant floor equipment, and on the other hand be able to run algorithms for machine learning applications or collect data for historians all while exchanging data with Cloud based applications.

Norz said that edge devices have become this tool, and automation engineers can utilize traditional IEC 61131 based control languages such as Ladder, Structured Text, or Function charts with a real time operating system.

"Within the same device, they are able to use Linux based applications running in Docker Containers for heavy data computation that output analytics for the connected worker and enterprise staff. Edge Devices need to support industrial network protocols such as MODBUS, EtherNet/IP, EtherCAT for interfacing with machinery that operates in real time. They also need to support IIoT Protocols such as MQTT and OPCUA to interface with Cloud Services applications," he said.

"Edge devices are the duality of today's smart connected world. They monitor and control in real time, and they offer systematic computational analysis of data for the plant floor as well as the enterprise."



Industrial edge applications create customized solutions for smart manufacturing. The integration of an industrial bus system into the edge device makes it possible to merge existing control data with additional information directly in the edge device, allowing Industrial PCs to be configured as both control computers and edge PCs.

Customized edge solutions

Leveraging industrial PCs as edge devices

Felix Wildemann, Product Management - Industrial PC at Beckhoff Automation, told IEB that industrial edge applications always prove successful when a customized solution is used for the specific application. This not only requires software and hardware to work in perfect harmony, but also requires the edge device to be seamlessly embedded into the application concept. Beckhoff achieves this harmony not by using dedicated edge devices, but by allowing Industrial PCs to be configured as both control computers and edge PCs.

"The integration of an industrial bus system into the edge device makes it possible to merge the existing control data with additional information directly in the edge device," Wildemann stated.

"An edge solution has to be designed as a retrofit package in a brownfield scenario, or as an IoT solution in brand new plants, to ensure that it does not impair the availability and real-time capability of the controller. That said, it must be possible to collect, process, prepare, and restore relevant process data to facilitate tasks such as making process data reliably available and optimizing the plant on a retroactive basis," he said.

Industrial PCs on the edge

Following this approach, Beckhoff offers a scalable portfolio of extremely compact, modular, and versatile Industrial PCs that can be perfectly adapted to the respective edge scenario.

These ultra-compact Industrial PCs in the C60xx series fit into almost any machine concept and can easily be installed as additional edge components.

Two alternative operating systems that support Beckhoff's own TwinCAT control software are available in the form of Microsoft Windows and TwinCAT/BSD. This allows the edge device to effectively speak the same language as the machine. In this way, data can be acquired on the machine side via the TwinCAT ADS protocol or via OPC UA without the need for a change in the program code for the control computer in TwinCAT.

The same applies to the Beckhoff C7015 IPC with IP 65/67 protection, which is equipped ex factory with an EtherCAT P port. EtherCAT P can be used to query a range of sensor data directly using the edge device in the field.

In addition, an IoT solution from Beckhoff always offers the option of communicating directly from the controller to the cloud, as a complete concept from a single source for control, data acquisition, and secure communication.

Depending on the effort required for pre-processing and preparation of the process and plant data collected in the edge device, the appropriate CPU can be selected from the Beckhoff portfolio. The spectrum ranges from the 1-core processor to the 8-core Intel Core i7.

The C7015 IPC with Intel Atom processor (up to four CPU cores) can be integrated directly into the machine with corresponding I/O box modules and via EtherCAT P. This allows edge computing with additional sensor data to be incorporated into the machine without requiring additional control cabinet space.

Opening up to the outside world

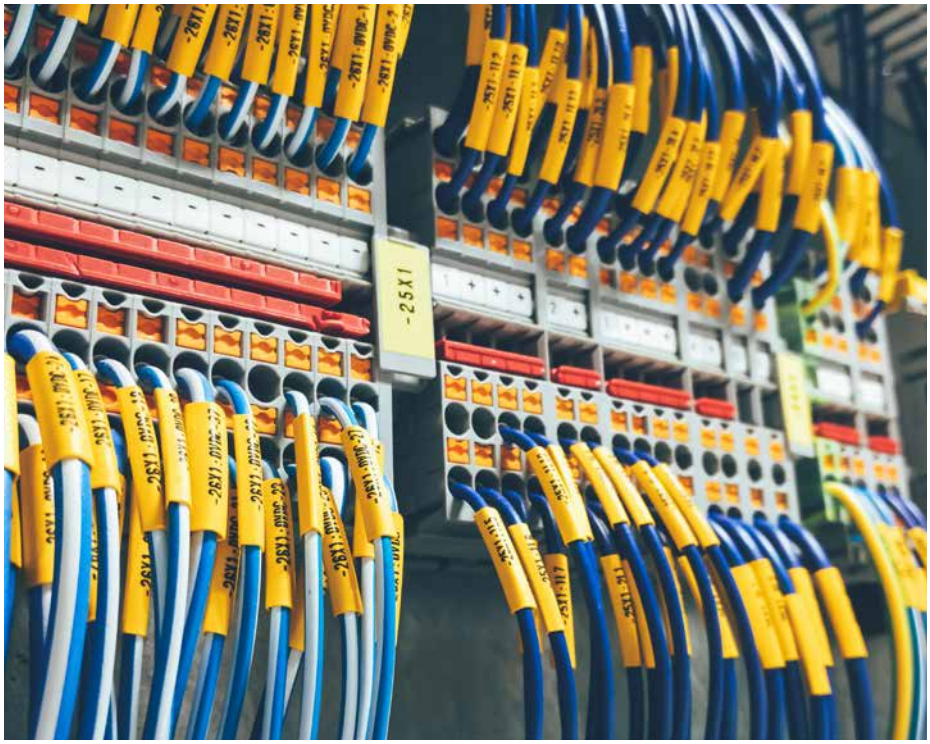
"Classic automation takes a very cautious approach to opening up and networking with the outside world, because the safety and stability of the production plant could be called into question when it is networked with IT," Wildemann added.

"The ability to directly network both worlds is not without its compromises, but edge computing can circumvent many of these compromises by offloading IoT functions from the controlling IPC. This allows IoT functions to be integrated into a production plant without directly impacting the control software while still reaping the benefits."

He added that, nevertheless, an edge solution only works if both hardware and software are optimally scalable to the approaches of IoT and the controller. "Fortunately enough, Beckhoff offers this functionality in abundance, since our Industrial PCs with TwinCAT software can be used as both control computers and edge devices."

Industrial Ethernet renaissance

Rise of Ethernet as the universal fabric for industrial applications



"The rise of Ethernet as the universal fabric for industrial applications blurs the line between the domains of IT and OT, which traditionally have employed very different technologies, and even when the technology was the same, it used to be very rigidly partitioned. Ethernet brings much more than a uniform physical layer." -- Pierfrancesco Zuccato, senior product manager at Eurotech

According to Pierfrancesco Zuccato, senior product manager at Eurotech, "Ethernet is the new renaissance for connectivity in industrial applications. Up to now, we've had a multitude of different types of specialised and even proprietary interfaces to work with and Ethernet is increasingly becoming a strong candidate to replace most, if not all, of those interfaces. The introduction of standardised methods to improve the deterministic behavior of Ethernet, such as Time Sensitive Networking (TSN), are great enablers for most industrial applications, even for those that require near-real time control."

"As we move away from a fragmented landscape towards a smaller number of cases, new opportunities open up: for instance, Ethernet makes the bridging of OT and IT way simpler. This can dramatically help the implementation of more open and abstract representation of the physical world, with important benefits for maintenance, vendor independence, and ease of integration," he added.

Ethernet as universal language

Zuccato said that Ethernet is becoming a universal language. There are initiatives, like ITXPT in the transportation market, for example, where Ethernet is the main interface.

Workload consolidation is another example, while it is possible to implement relatively simple examples of workload consolidation that would not require Ethernet, the most important use cases would have Ethernet as one of the key ingredients.

"The rise of Ethernet as the universal fabric for industrial applications blurs the line between the domains of IT and OT, which traditionally have employed very different technologies, and even when the technology was the same, it used to be very rigidly partitioned. Ethernet brings much more than a uniform physical layer," Zuccato added. "It allows the creation of a single software context, eliminating the need for intermediate steps to bridge conversions between devices that belong to different contexts, even within the same factory floor."

He added that workload consolidation is one important trend that has now become affordable thanks to the hardware we have today; it delivers enough computational capability, performance, and capacity to enable virtualisation.

Not only is it now possible to manage embedded workloads using proven methodologies already widely adopted in the data centers, it is also a very convenient way to implement sophisticated schemes, like high availability, workload migration and so on. This brings real benefits in terms of downtime elimination.

With a single machine capable of running different tasks, less hardware is required, which means less running costs and less chances of failure. It's much easier to implement redundancy schemes, because virtual machines allow you to migrate tasks from one physical server to another seamlessly, therefore incrementing the reliability of the overall architecture. This is made possible by a number of technologies and Ethernet has a prominent role.

The pace of change

"One challenge facing automation engineers is the pace of change – it can be hard to keep up with all these new developments and technologies while understanding where and how they can make a difference," Zuccato added.

"It pays to find a partner that understands your unique operations and challenges, and how these technologies can be deployed and adapted to meet your needs. Automation engineers need to manage complex architectures that often contain a mix of legacy and cutting-edge technologies that need to be integrated in a reliable way."

This means that they may have to periodically make a number of complex changes across the various different areas, including software, functional safety, real-time, and hardware. It can be a very complex process, so it can be useful to have a partner with all the required technical expertise on board to support with these challenges.

These advances in edge computing, however, mean that we're moving towards more simplified and efficient ways of managing different parts of software applications and physical interfaces.

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

Edge computing APE module

Bringing Edge computing into industrial networks and harsh environments.

The RUGGEDCOM APE1808 is a utility-grade application processing engine (APE) module which plugs into most members of the feature-rich and cost efficient RUGGEDCOM RX1500 Multi-Service Platform family. Modular and field replaceable, the RUGGEDCOM RX1500 devices offer WAN, serial or Ethernet connectivity options.

The APE1808 with the RX1500 provides a secure and future-proof way to deploy Edge computing directly into industrial networks in harsh environments, bringing intelligence and data processing on a decentralized level in real-time – a key requirement for digitalization and the Industrial Internet of Things (IIoT).

With support for Linux and Windows 10, the RUGGEDCOM APE1808 provides a standards-based platform to host commercially available software and allows you to also implement your self-developed apps, eliminating the need for an external industrial PC. The RUGGEDCOM APE1808 can seamlessly integrate Siemens or third-party Edge computing applications to address today's growing challenges. Computation at the edge increases flexibility, helps operators gain valuable insights as it allows for quick response times for faster decision making, maximizes operational efficiency, and reduces risks/costs in industrial IoT applications. Processing data locally ensures that only relevant data is sent to IT/cloud systems and increases network performance by reducing latency. The APE1808 is also an excellent platform to deploy partner solutions for anomaly-based intrusion detection system and deep packet inspection to further increase network security.

SOURCE: SIEMENS

With an operating temperature range from –40° C to +75° C, the RUGGEDCOM APE1808 provides a reliable platform for networks in electric power, transportation, oil & gas, and other industries that experience harsh environments.

Siemens

Visit Website

IIoT gateway adds PROFIBUS DP

Softing expands IIoT gateway products for Industry 4.0 integration in process plants.

The new smartLink HW-DP from Softing Industrial Automation provides controller-independent access to PROFIBUS DP networks. In addition to HART IP and FDT, data for optimizing processes can now also be made available via an OPC UA interface. In addition, the new smartLink DTM enables FDT/DTM parameter setting for HART devices.

The smartLink HW-DP allows access to process data from PROFIBUS devices and HART devices connected to PROFIBUS remote I/Os, as well as secure export to any system inside or outside its own network. Users in the process industry who want to adapt their communication architecture to modern IIoT use cases can integrate smartLink into existing plants in a simple and cost-effective manner.

Until now, access to data relevant for optimization processes was possible via HART IP for HART devices and FDT for PROFIBUS DP. The new version V 1.10 additionally provides an OPC UA interface.

This means that any HART IP and OPC UA clients, such as Emerson's AMS Device Manager or the Android app DevComDroid, can now be used to configure, monitor, and evaluate field devices via these open communication standards. With the new smartLink DTM, FDT/DTM parameters can now also be set for HART devices.

SmartLink is straightforward to implement and independent of the automation components in place. All the data are provided using open, standardized interfaces including HART IP, OPC UA and FDT to simplify system integration and management.

SOURCE: SOFTING

smartLink enables easy integration of Industry 4.0 applications into PROFIBUS & HART systems.

Softing

Visit Website

Local processing engine for edge apps

Flexible local processing engine provides reliable data processing and analysis in the field.

SCALANCE LPE is a small, robust local processing engine with a powerful CPU. It is flexibly usable for cloud and edge applications that allow you to significantly boost the efficiency of your plants. With SCALANCE LPE, data can be collected, analyzed, and forwarded to higher-level systems such as cloud platforms.

Acquiring manufacturing data, such as temperature, maintenance information, and utilization rates, along with pre-processing on the SCALANCE LPE opens up numerous possibilities in terms of predictive maintenance or anomaly detection. Applications running directly on the device can take over important services in the plant like network services or simple visualization tasks.

Thanks to its powerful CPU, the processing engine can handle several applications simultaneously. Its Linux-based operating system allows you to implement your own self-developed apps as well as applications available on the market (such as Docker©) with one device.

SCALANCE LPE is designed for use in temperatures ranging from –40°C to +60°C. The processing engine is fanless, provides a redundant power supply, operates without batteries (less maintenance effort) and fits in any control cabinet thanks to its compact design. Several mounting options are possible, e.g., SIMATIC S7-1500 and S7-300 DIN rail mounting and direct wall mounting. Due to the SIMATIC S7-1500 design, the processing engine is optimally suited for integration into an automation solution with SIMATIC S7-1500 components. Seamless integration into the SCALANCE network components as well as the SINEC network management portfolio.

SOURCE: SIEMENS

Local processing engine enables future-ready machine and plant concepts as well as edge applications.

Siemens

Visit Website

Ultra-compact Industrial Edge PCs

Space-saving IP 65/67 Industrial PC hardware with flexible mounting for advanced Industrie 4.0 solutions.

Following current trends, this space-saving IP 65/67 Industrial PC hardware with flexible mounting options is suited for implementing advanced Industrie 4.0 solutions. A wide variety of onboard interfaces enables the networking of machine or plant sections in the cloud or other networks. Moreover, an integrated EtherCAT P connection offers possibilities for the direct connection of actuators and sensors via EtherCAT P Box modules with IP 67 protection. Decentralized of complex diagnostic or condition monitoring tasks is possible.

The compact Beckhoff module motherboard and the housing combination of die-cast zinc and aluminum have been developed in typical Beckhoff style for industrial suitability, long-term availability and reliability. Despite passive cooling, the C7015 is suitable for a temperature range up to +50 °C. A wide range of interfaces (3 x LAN, 2 x USB, mini DisplayPort, EtherCAT P), a minimum of 40 GB M.2 SSD with 3D Flash and integrated Intel Atom CPU (up to 4 cores) with continuous multi-core support for TwinCAT 3 make the C7015 a platform for different tasks: simultaneous, high-performance automation under harsh real-time conditions, visualization and communication. This makes the ultra-compact Industrial PC suitable for use in conventional machine control, or as an edge device for implementing advanced Industrie 4.0 solutions.

The C7015 Industrial PC is one of the most compact devices in its performance class in the Beckhoff portfolio.

SOURCE: BECKHOFF

In addition to its compactness, the C70xx series offers versatile mounting options for machine or system integration.

Beckhoff

Visit Website

Seamless handoff to mobile devices

Improve the performance of edge systems with more powerful HMI software solutions.

Machine operators can now pass control of their machine seamlessly between the main HMI and their mobile devices to improve the performance of edge systems. A new feature of B&R's mapp View HMI solution ensures that the controls and information they need are always at their fingertips, so they can move freely around the plant floor as they continue working.

"Until now, HMI terminals have restricted machine operators to working within a certain radius," said B&R software expert Manuel Sánchez. "If they can't reach the screen, they can't control the machine."

B&R's web-based HMI solution now enables them to take control of the machine with them on their mobile device wherever they need to go. Once the task is complete, they simply pass control back to the main HMI.

The new QRViewer widget available in B&R's mapp View HMI solution generates dynamic QR codes in the machine's user interface. In addition to handing off HMI operation to a smartphone, these codes enable a variety of other convenient new features to optimize machine performance and availability.

In the event of an error in the system, operators can quickly access help documentation, instructional videos, part numbers and more – right on their smartphone. When viewing historical performance data, they can access higher-level ERP systems and track batches throughout the entire supply chain.

SOURCE: B&R

Machine operators can now hand off control of the machine from the main HMI to their mobile device and move freely around the plant floor as they continue working.

The right information, in the right place, at the right time helps keep the machine producing safely with minimal downtime.

B&R Automation

Visit Website

Shock and vibration resistant

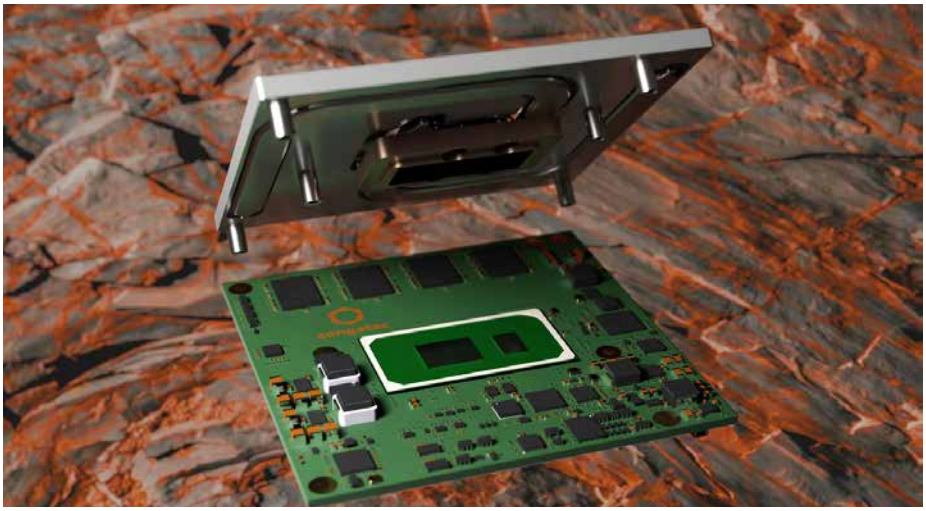
Computer-on-Modules provide shock and vibration resistance in transportation and mobility applications.

Congatec, a vendor of embedded and edge computing technology, has introduced a new 11th Gen Intel Core processor based Computer-on-Modules with soldered RAM for high levels of shock and vibration resistance.

Designed to withstand even extreme temperature ranges of -40°C to +85°C, the new COM Express Type 6 Computer-on-Modules provide full compliance for shock and vibration resistant operation in challenging transportation and mobility applications. For price sensitive applications, congatec also offers a cost optimized Intel Celeron based shock and vibration resistant variant for the extended temperature range from 0°C to 60°C.

Typical customers for the new range of Computer-on-Modules based on the Tiger Lake microarchitecture are OEMs of trains, commercial vehicles, construction machines, agricultural vehicles, self-driving robots and many other mobile applications in the most challenging outdoor and off-road environments. All these applications can now benefit from super-fast LPDDR4X RAM with up to 4266 MT/s and in-band error-correcting code for single failure tolerance and high data transmission quality in EMI critical environments.

The value package includes rugged mounting options for the COM and carrier bundle, active and passive cooling options, optional conformal coating for protection against corrosion due to moisture or condensation, a list of recommended carrier board schematics, and for highest reliability, shock and vibration resistant components.



SOURCE: CONGATEC

Shock and vibration resistant devices are an important application area as digitization requires more protection.

Congatec

Visit Website

Bringing edge computing to production

Open, flexible edge computing platform provides a software infrastructure for shop floor and the cloud.

Machine builders and plant operators are facing a rapidly changing industrial environment. By running analytics and other complex applications at the edge of the network, manufacturers can make process improvements in real-time and increase production flexibility and responsiveness while also reducing the volume of data being sent to the cloud.

Nerve enables users to:

- Collect machine data in real-time, store and analyze it
- Consolidate multiple functions on one device
- Manage and deploy software remotely
- Display connected devices and software

Nerve provides a secure, virtualized software environment that enables customers to run multiple industrial applications side-by-side on a standard industrial PC. Users can choose to either run software in lightweight Docker containers or entirely within a Virtual Machine.

Nerve is also optimized to run real-time Virtual Machines where critical tasks can be executed at high-speed, allowing industrial PLC applications to be moved into the virtualized environment without losing any performance guarantees.

SOURCE: TTTECH INDUSTRIAL

Secure, virtualized environment lets users run multiple industrial applications side-by-side on a standard industrial PC.

All applications hosted in the Nerve software environment can be managed remotely from the web-based Nerve Management System. Once a Docker container or Virtual Machine is uploaded to the Management System's repository, it can be deployed to machines and factories around the world even by non-IT staff with the click of a button.

If you are interested in trying Nerve, sign up for a free trial at the link below.

TTTech Industrial

Sign Up for Free Trial

Industrial-grade routers

Gateway and router bringing added power to the Digi XBee ecosystem.

Digi International has introduced the newest addition to its line of industrial-grade routers with the introduction of Digi IX15, the only fully functional industrial cellular gateway with Zigbee support.

Serving as both a gateway and router, Digi IX15 delivers greater value by giving companies a complete, cost-effective IoT solution.

Digi IX15 works seamlessly with Digi Remote Manager® for efficient configuration, deployment, monitoring, and management of thousands of mission critical devices and assets from a single desktop, tablet or smartphone.

Digi IX15 brings greater power to the company's acclaimed Digi XBee® ecosystem, including modules, code libraries, and the award-winning Digi XBee Tools suite. Digi IX15 is equipped with the latest Python programming implementation to bring greater reliability, simplicity, and security to edge computing and simplify all phases of the product development lifecycle.

In today's fast-paced market, competitive advantage relies on rapid development and deployment. Digi IX15 accelerates time-to-market for industrial customers seeking lower-cost alternatives to DIY gateway designs for networking operations.

SOURCE: DIGI INTERNATIONAL

The Digi IX15 is claimed to be the only fully functional industrial cellular gateway with Zigbee support.

One of the few IoT gateways on the market certified for C1D2 deployments, the rugged Digi IX15 is designed for the harsh conditions commonly found in industries such as oil and gas, water/wastewater, energy, and agriculture.

Digi International

Visit Website

Connectivity for remote operations

Fusion Bridge dual-radio gateway delivers seamless Wi-Fi connectivity to remote 900 MHz networks.

Data is everywhere, but Wi-Fi is not. If remote operations lack on-site connectivity to gather and share real-time, business critical data, efficiency suffers. Today, Boulder-based FreeWave Technologies introduced a reliable way to connect remote assets and unlock siloed operational data: Fusion Bridge.

The dual-radio bridge adds WiFi access point connectivity to remote 900 MHz networks. A plug and play option for existing ZumLink Networks, it makes it easy for enterprises to connect multiple devices and sensors in the field, access real-time data, drive new operational efficiencies and improve asset management.

"Fusion Bridge solves a real problem for enterprises that have remote assets generating critical data in the field and requires staff to physically monitor or collect it directly," said FreeWave CEO Kirk Byles. "Manual data collection is time-consuming, can introduce human error and is highly inefficient. But it also delays decision making, which not only adds costs, but also minimizes the ability for companies to proactively mitigate business risk. Fusion Bridge is another example of how we are working to help customers address real problems and add capability to existing network communications without substantial investments."

SOURCE: FREEWAVE

New solution is for those looking for a platform to deliver remote security intelligence applications including human or vehicle presence alerting, activity monitoring and remote access protection outside of network range.

Fusion Bridge is over-the-air compatible with ZumLink networks and accommodates any WiFi device, including tablets, sensors, smartphones and security cameras. It offers an easy, browser-based configuration that is OEM-ready and features a fully customizable interface.

Freewave

Visit Website

Edge management solution

Edge Builder addresses the edge management challenge within Industrial IoT systems.

IOTech has announced the launch and availability of Edge Builder, its end-to-end management solution for edge systems. Edge Builder provides a comprehensive, flexible and open solution that simplifies and automates the management of edge systems at scale.

To ensure that Edge Builder addresses the market opportunity, IOTech has been working with partners and potential customers during the development phase of the product.

As the number of industrial IoT devices and the data that comes from them grows at a rapid rate, the problem of managing these edge infrastructures becomes critical. Traditional Cloud or IT-based management solutions can struggle with factors such as edge scale, intermittent connectivity, device/sensor connectivity, legacy platforms and resource constraints at the edge.

The problem is multi-dimensional in scope and includes both the provisioning and management of the edge nodes and also the application workloads deployed on the nodes. Other key issues include dealing with aged and heterogeneous infrastructure (legacy equipment, brownfield nodes and devices) and that the OT lifecycle is often measured in decades, not years. Designed to meet the specific needs of edge systems, Edge Builder provides light touch provisioning and complete lifecycle management for both edge nodes and their applications. Currently it supports the deployment and management of containerized applications at the edge and in the future will also support the deployment of native binary applications.

SOURCE: IOTECH

Open and flexible end-to-end solution simplifies and automates the management of edge systems at scale.

IOTech

Visit Website

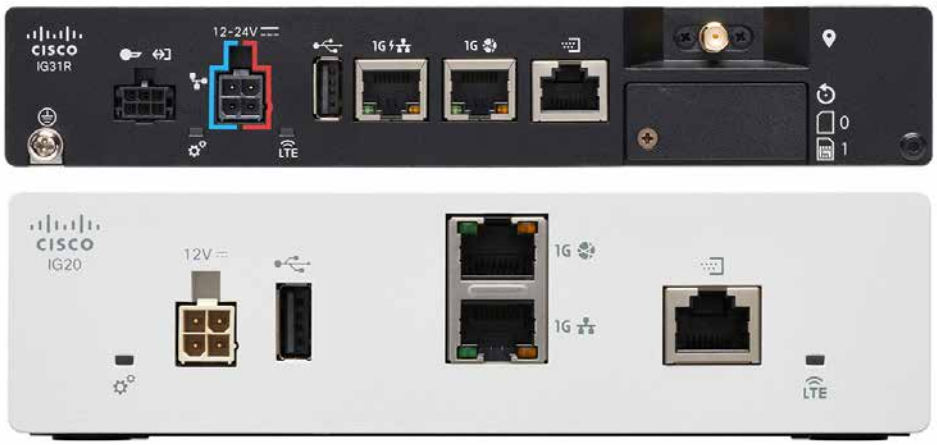
New 5G industrial router portfolio

Cisco unveils new 5G industrial router portfolio to unite IoT deployments and innovate at the Edge.

Cisco's new IoT router portfolio is what the company claims is now the broadest on the market, bringing reliable connectivity to any IoT edge use case to run connected operations securely and at scale.

The portfolio provides unprecedented modularity to future-proof the network with a broad variety of access technologies including Wi-Fi 6, 5G, 4G, Private LTE, FirstNet and Wi-SUN.

Leading brands around the world including Landis+Gyr are working with Cisco to unite edge networks and scale IoT deployments.



SOURCE: CISCO

Featuring 5G capabilities today, this new portfolio of 5G industrial routers will enable organizations to run connected operations at scale with choice of management tools suited for both IT and operations. The unified architecture simplifies collaboration between IT and operations and streamlines their deployments from the enterprise to the edge.

Catalyst industrial routers

The new portfolio of Catalyst industrial routers extends the power of enterprise networks to the edge with the flexibility, security and scalability needed for IoT success.

Featuring 5G capabilities today, the portfolio enables organizations to run connected operations at scale with choice of management tools suited for both IT and operations. The unified architecture simplifies collaboration between IT and operations and streamlines their deployments from the enterprise to the edge.

For most Cisco customers, the opportunity to improve efficiencies, the customer experience, and business results is achieved with data generated at the edge. Because the edge is all the places where organizations serve their customers and create revenue. The edge is diverse and is located anywhere and everywhere from utility substations and pipelines to roadways and the police cars and buses that run on them.

According to Gartner, 75% of data will be generated outside of the data center in these edge environments. This type of growth brings challenging new requirements.

Unite edge with routers

Whether it's connecting point-of-sale kiosks or a remote piece of equipment, edge use cases have different technology needs. Typically, organizations connect these environments in isolation, resulting in a fragmented network architecture, increased security vulnerabilities, and isolated data. As organizations accelerate digitization, they need a way to simplify management and security across the network and edge devices.

"Cisco offers a network from the enterprise to the industrial edge, with an architecture that provides visibility, automation, and security from campuses and branch offices to substations, remote operating locations, fleets, on-the-go connected assets, and beyond," said Vikas Butaney, VP/GM of Cisco IoT.

The new portfolio includes the following lineup of new products:

Three new Catalyst 5G Industrial Routers to securely connect mobile and fixed assets
These new routers are based on Cisco IOS XE to extend the enterprise network and SD-WAN to the edge.

This unified architecture provides IT and operational teams with consistent tools, eliminates training on new devices and technologies, and improves security. The new Catalyst routers are modular and also offer built-in edge compute to develop business apps and drive decisions at the edge.

New Cisco IoT Gateway Series for essential indoor or outdoor connectivity at mass scale

Packaged with Cisco's cloud-based IoT Operations Dashboard, these cloud-simple gateways are cost-effective and offer fast and simple set up; simply plug it in and power it on to connect previously unconnected assets.

5G modularity and scalability

The need for data means organizations will increase the number of devices connected and the applications supported. As 5G, Wi-Fi 6, and new technologies proliferate, the edge must be able to quickly adapt. The time is now to prepare the edge to handle the future.

The new Catalyst routing portfolio delivers the scale, flexibility and security to adapt as use cases evolve and new applications are needed.

It offers a broad choice of modules including 5G and LTE for public or private cellular networks, public safety applications like FirstNet, DSL, Wi-SUN, and upgradeable storage. Plus, the portfolio enables updating the CPU and battery in the field.

"Our customers need our hardware to be in play for 7-10 years in their operational environments. This modularity eliminates a rip and replace cycle to take advantage of 5G and whatever comes next," added Vikas. "Now they can easily take advantage of new technologies and future-proof their networking investments."

Built-in, end-to-end security

As industrial and enterprise networks converge with more assets connected, the threat of exposure at the edge increases. This ever-expanding attack surface presents complex cyber security challenges.

The Catalyst industrial router portfolio, based on Cisco's industry-leading cybersecurity architecture, delivers a holistic strategy to manage security across siloed IT and OT environments. The portfolio integrates Cisco Cyber Vision to provide full visibility from enterprise to the edge.

Cyber Vision embeds a sensor within the industrial network so security teams can detect threats to their industrial environments with operational context, enabling organizations to build a truly converged IT/operations threat management strategy – without the need for extra boxes and vendors. Plus, the portfolio supports secure remote access for operations and equipment monitoring/servicing.

The new Cisco Catalyst Industrial Routers were available starting in June 2021.

Cisco

Visit Website

PACEdge: industrial edge software

New edge software enables manufacturers to quickly develop and scale advanced machine analytics

The PACEdge industrial edge platform delivers scalability and open connectivity, making data and analytics accessible from the machine level to enterprise.

SOURCE: EMERSON

Emerson's Fluid and Measurement Motion Control business uses PACEdge dashboards software to monitor energy consumption, including gas and electricity, of its production lines to help drive its sustainability efforts.

Industrial edge platform

This new platform is designed to help manufacturers accelerate digital transformation projects by enabling users to quickly create and scale up performance-improving applications. The PACEdge platform simplifies application development by bringing together today's leading, open-source tools into a flexible, integrated and secure platform for utilizing machine data and analytics. The PACEdge release coincides with the launch of Emerson's new PACSystems RXi2-BP edge computer, a small form-factor industrial PC that enables high-performance analytics to be run close to the machine.

The PACEdge platform helps users securely collect, analyze, store and serve up machine data near the source or across enterprise systems. End users can easily build and deploy applications for a wide range of uses including monitoring energy, machinery health and productivity.

Emerson's modular, pre-configured development packages containerize applications to allow developers to start in a pilot environment with a few units, and then quickly scale to hundreds or thousands of units—without expensive network and server infrastructures or worrying about inconsistencies among operating environments.

"Many of today's edge solutions offer limited connectivity and toolsets, making it difficult to extend across assets, machines or plants," said Derek Thomas, vice president of marketing and strategy for Emerson's machine automation solutions business. "The PACEdge platform provides a complete solution that enables manufacturers to start right at the machine with the connectivity and flexibility needed to scale up as they progress on their digital transformation journeys."

Using modern IIoT protocols such as OPC UA, MQTT and REST, the PACEdge platform provides access to data from industrial control systems and field devices, as well as IT systems and cloud services for plant or enterprise data aggregation.

With drag-and-drop programming and embedded web interfaces and visualization, users can use this information to quickly create applications and dashboards to analyze and view operational data, such as overall equipment effectiveness, compressed air usage, energy consumption, acceleration and vibration and other sensor data.

Advanced applications can combine these outputs with external data sources (i.e., weather, public utility rates) and machine learning algorithms to drive better asset health and performance by detecting potential failures sooner. Operators in the field have immediate access to diagnostic and production information, allowing them to make better decision faster.

The RXi2-BP edge computer uses patented temperature management technologies to enable the small form-factor industrial PC to achieve optimum performance in difficult-to-access industrial locations without being limited by internal temperatures.

Emerson's enhanced industrial edge portfolio, which now includes PACEdge, PACSystems RX3i Edge Controllers, RXi2 Edge Computers and Movicon.NExT™ HMI and SCADA software, is helping customers digitally transform their industrial manufacturing operations from the machine-level to the plant.

Traditional big data analytics collects massive amounts of data for central analysis requiring costly infrastructure, expensive planning, and special skills, impossible for many industrial enterprises. Little data occurs when the data analyzed is at the machine level, where clearly identified challenges and goals can be quickly analyzed.

Emerson

Visit Website

AI processing capabilities at the edge

High performance computing and IoT capabilities to the Edge in the automotive and rolling stock sectors.

Leading-edge innovation sees Eurotech launch BoltGATE 10-12, BoltGPU 10-31 and BoltCOR 32-18 to bring AI power and processing capabilities at the Edge even in the harshest of environments Eurotech has launched three new products that can help deliver AI-powered applications and robust IoT projects in the automotive and rolling stock sectors.

BoltGATE 10-12

BoltGATE 10-12 is a rugged edge computer that simplifies connecting Edge devices with the cloud in both greenfield and brownfield applications. It is designed for transport companies that need to remotely manage Edge deployments and data and accelerate the development of IoT and Edge computing applications. A low power gateway, certified for use in rolling stock and automotive environments, and designed for heavy duty applications using a solid metal enclosure and rugged connectors. An internal battery protects the device from power interruptions, and allows for a safe shutdown with transient protection and vehicle ignition sense.

BoltGATE 10-31

BoltGPU 10-31 is a rugged subsystem for GPU-accelerated AI applications on board. Fanless and suitable for very rugged environments, it offers exceptional power efficiency and up to 21 trillion operations/second (TOPS) of accelerated computing. Powered by NVIDIA Jetson Xavier NX GPU, it allows AI processing to run on a device in the field, producing telemetry in the form of sensor readings or video capture, even in environments where network connectivity isn't reliable or even possible.

Commenting on these two new additions to Eurotech's product portfolio, Pierfrancesco Zuccato, senior product manager at Eurotech said: "The BoltGATE 10-12 dramatically simplifies bringing together applications in the field with the cloud. On the one hand, it's a rugged and connected device; while on the other, it provides a rich IoT framework that works seamlessly with most cloud platforms".

"The BoltGPU 10-31 is a workhorse for GPU-accelerated workloads both on-vehicle and in harsh environments. It's rugged, fanless and very compact but at the same time it provides cutting edge features and efficiency at the Edge, where ease of deployment and reliability are a must."

BoltGATE 32-18

Eurotech has also announced the BoltCOR 32-18, its newest GPU-accelerated server for AI applications at the Edge and on vehicles. This ultra-shallow server combines the extreme ruggedization of a fanless, ventless system with the computational power of a high-end CPU and universal deep learning accelerator.

Designed to operate even in the harshest of conditions, this highly reliable product features Eurotech's innovative cooling solutions enabling high performance and server-class computing in a compact and completely fanless and ventless unit.

Giuseppe Surace, Eurotech's CP & MO said: "The BoltCOR 32-18 is a game changer for Edge applications that require GPU acceleration and the highest level of reliability. Eurotech developed innovative cooling solutions to pack high level performance in this very compact and fanless unit."

Both the BoltGPU 10-31 and BoltGATE 10-12 are certified for use in both the rolling stock and automotive sectors, while the BoltCOR 32-12 is certified for rolling stock. Both the BoltGPU 10-31 and the BoltCOR 32-18 are available later this year and the BoltGATE 10-12 is available now.

SOURCE: EUROTECH

BoltGATE 10-12 is an edge computer for connecting Edge devices with the cloud for greenfield and brownfield apps.

BoltGPU 10-31 is a rugged subsystem for GPU-accelerated AI applications on board.

Eurotech

Visit Website

Three IIoT project risks and how to avoid them

Rather than fear the potential threat that come with IIoT projects, building security into the overall IoT architecture, and solving interoperability challenges will enable organisations to successful get their projects off the ground and take advantage of the innovative operational efficiencies they enable.

THE INTERNET OF THINGS IN AN INDUSTRIAL setting (IIoT) is widely becoming recognised as a game-changer for any organisation in the manufacturing or transportation of goods sectors. Juniper Research suggests that IIoT connections are likely to reach 37 billion by 2025 as businesses look to take advantage of its transformative impact on operations.

With the promise of efficiencies and resolving business challenges, IIoT is helping organisations boost their processes in a variety of different ways. The use cases for IIoT are endless and include predictive maintenance; the use of sensors to manage stock in warehouses and reduce waste; automated quality controls; and equipment monitoring in remote or difficult to reach locations.

However, although we're starting to see industry take advantage of smart warehouses, automation, and connected logistics, many businesses are reluctant to adopt IIoT as they are concerned over the security of these connected devices. And it's not just security that is hindering widespread IIoT adoption. Integration of legacy equipment with IoT and a lack of open standards are also causing industry-wide headaches. Here, we look at these three main barriers to IIoT adoption and consider how business can successfully navigate these complex hurdles:

IoT security

This is the number one concern for most businesses considering adopting IoT, as connected devices continue to be developed at a fast pace. In the race to get these devices to market, security standards or protocols can sometimes over-looked by manufacturers.

Firewall perimeters and VPNs often used to be enough to secure our networks from a data breach but not anymore thanks to the proliferation of mobile devices and connected applications, along with the increasingly sophisticated levels of attacks that businesses are being subjected too. IoT devices are connected and interconnected into a network and designed to collect and store growing volumes of data. From the edge to the cloud, security needs to be considered at each step as smart devices connect to each other, the Internet, and the cloud to exchange data.

Data breach fears continue to be the main reason that many businesses are slow to adopt IIoT technologies and for good reason, as an attack could cause the business to go offline for days or even longer. Creating a totally secure IIoT deployment is not a simple task, especially when it's a large, globally-distributed deployment. To prevent a cyberattack from happening in an IIoT environment, organisations must make careful buying decisions from the outset and prioritise products with in-built security above all else.

Lack of open standards

System integration is a big challenge for the IIoT ecosystem, where are all parts need to work together. However, with so many different devices, operating systems and programming languages deployed on edge infrastructures, integration is complex. Standardisation of IIoT protocols and technologies appears to be a long way from happening.

Most IoT edge solutions are based on integrated sensors, actuators, Programmable Logic Controllers (PLCs), field buses and protocols and it's often a combination of new and legacy operational technology that presents the first challenge. Some of these technologies and protocols are open standards-based, but many are not. Instead, they are proprietary and specific to certain vendors and vertical solutions.

This lack of open standards causes another issue for IoT security - creating a vulnerable IoT ecosystem with vendors forced to use a variety of hardware, software, third party services and APIs and patch methods. Just one unsecure device could cause network vulnerability and to avoid protocols being abused. Organisations need IoT solutions with secure identity, authentication, and encrypted communications. To encourage more wider adoption of IoT, device manufacturers and software developers must work towards providing a security model based on open and industry standards to ensure platform interoperability and best practice.

Legacy equipment and IoT

An organisation using IoT solutions to collect data in the field will need to connect legacy equipment such as industrial machinery, in-vehicle components, and power meters to the Internet. The most effective (but expensive) way to ensure seamless integration between field equipment and IoT applications would be to replace old kit with new IoT-ready versions. We see this practice frequently in the home where consumers replace old boilers with a smart heating solution enabling data collection and remote access and monitoring. Although we are starting to see equipment replaced with IoT-ready versions in industry, it's likely to be a slow and costly process.

For start-up businesses in the sector, choosing IoT-ready equipment is a no brainer, however for long-established businesses replacing kit that remains in good working condition may not be an option. Instead, organisations are retrofitting their assets with sensors, smart devices, and gateways to get IIoT projects underway. While this works in practice, the same issues around security and interoperability exist, and this complication is something we see hinder organisations from rolling out IIoT deployments.

Navigating these risks

Unfortunately, there is not a one size fits all solution that will work across every environment. And although industrial applications of IoT are an exciting proposition, navigating the associated risks can be a complex, expensive and time-consuming exercise. However, organisations don't need to put their IIoT project plans on hold or cancel them altogether, instead they should focus on these barriers to adoption and plan for creating a secure, and integrated end-to-end IIoT deployment from the outset.

Organisations firstly need to work out what they want to achieve and how IIoT will help them do it. The next step is to work with best-of-breed solution providers or partners who can help them identify the products that will enable secure, interoperable IoT in their specific environment, whether that's through retrofitting assets with IoT technologies or choosing smart solutions to replace end-of-life legacy equipment.

Those organisations that fail to successfully navigate these risks and delay IoT adoption risk being left behind by their competitors.

Giuseppe Surace, Chief product & marketing officer, ***Eurotech.***

Visit Website

Simplifying network performance at the edge

Economical plug-and-play unmanaged switches provide key performance features typically found only in costly and complex managed switches. Designers have options to obtain the best networking price/performance ratio by selecting unmanaged switches that incorporate key managed switch features.

CREATING HIGH PERFORMANCE AND SECURE Ethernet networks are top priorities for designers of any commercial or industrial systems using digital connectivity. Because Ethernet is so commonly deployed in many different settings, it can be tempting to select consumer-grade devices, even though far more capable hardware is available and warranted. Cost pressures often increase because professional-grade solutions like managed switches are relatively expensive, with much time required for complex configuration.

But another option is available in the form of industrialized unmanaged Ethernet switches, which incorporate the key performance features of managed switches in an easy-to-deploy form factor. This article identifies top features designers should look for, and it shows how the right unmanaged switches are easily employed in any Ethernet applications to deliver robust connectivity.

Digital need for speed

Many digital system applications have largely been standardized on Ethernet communications, due to the speed and bandwidth capabilities, not to mention the economies of scale based on such a massively deployed technology.

Nearly all types of electronic devices are produced with a level of intelligence so they can be linked to each other and to supervisory control and monitoring systems. Industrial internet of things (IIoT) initiatives are underway with many end users in an effort to gather as much data as possible from all sources, in support of remote monitoring and control—further driving the need for high-speed Ethernet communications.

This is true for diverse industries and applications—such as building automation, municipal traffic control, power utilities, water/wastewater treatment, processing industries—along with just about any type of manufacturing machinery or equipment. Supervisory devices may be dedicated controllers, programmable logic controllers (PLCs), hardware human-machine interfaces (HMIs), or locally installed PCs. Field devices range from IIoT sensors to intelligent devices, like RFID readers or process analyzers.

Basically, anywhere multiple Ethernet devices are to be connected, a switch is needed. Typically, 4-port switches are the smallest available, but many users find that the increasing number of field devices and the need for a user connection port push them into higher port counts. Many of these users find an 8-port switch to be an excellent balance between size and capacity.

SOURCE: IDEC

As modern machines take advantage of increasing numbers of Ethernet-connected devices, it becomes important to use switching technologies optimized for best performance.

Because so many commercial and industrial applications are largely mission-critical, any downtime due to network problems is unacceptable. The next step is to pick a model able to deliver the required performance and reliability, even in challenging physical locations.

Unmanaged versus managed

A basic unmanaged Ethernet switch is basically plug-and-play and typically requires no user configuration. Each port will auto-configure to match the connected device, and the switch will build MAC address tables to forward traffic with some level of intelligence. There are almost no security provisions. Unmanaged switches are very economical, and often considered for small networks where changes will not be needed, and average performance is acceptable.

Managed Ethernet switches are usually required if users want to increase communication speeds, minimize traffic and network loading, and improve network security. Each of these characteristics is desirable for many types of commercial and industrial installations, where equipment, devices, and digital services must reliably operate around the clock.

Unfortunately, managed switches usually must be configured by personnel with significant IT training, and these configurations must be maintained among all the switches on the network. The task can be daunting for users who simply want high-quality connectivity. Therefore, managed switches originally carried larger port counts and were deployed mostly in data centers, but today there are options in many sizes.

Both unmanaged and managed Ethernet switches are reliable devices, but even so standard consumer- or commercial-grade switches are not ideal for harsh or industrial environments, and many not be convenient to install in enclosures. Industrial-grade devices are preferred because they offer more flexible mounting and connection options, along with extended operating temperature ranges and electrical noise resistance, making them suitable for typical installation locations.

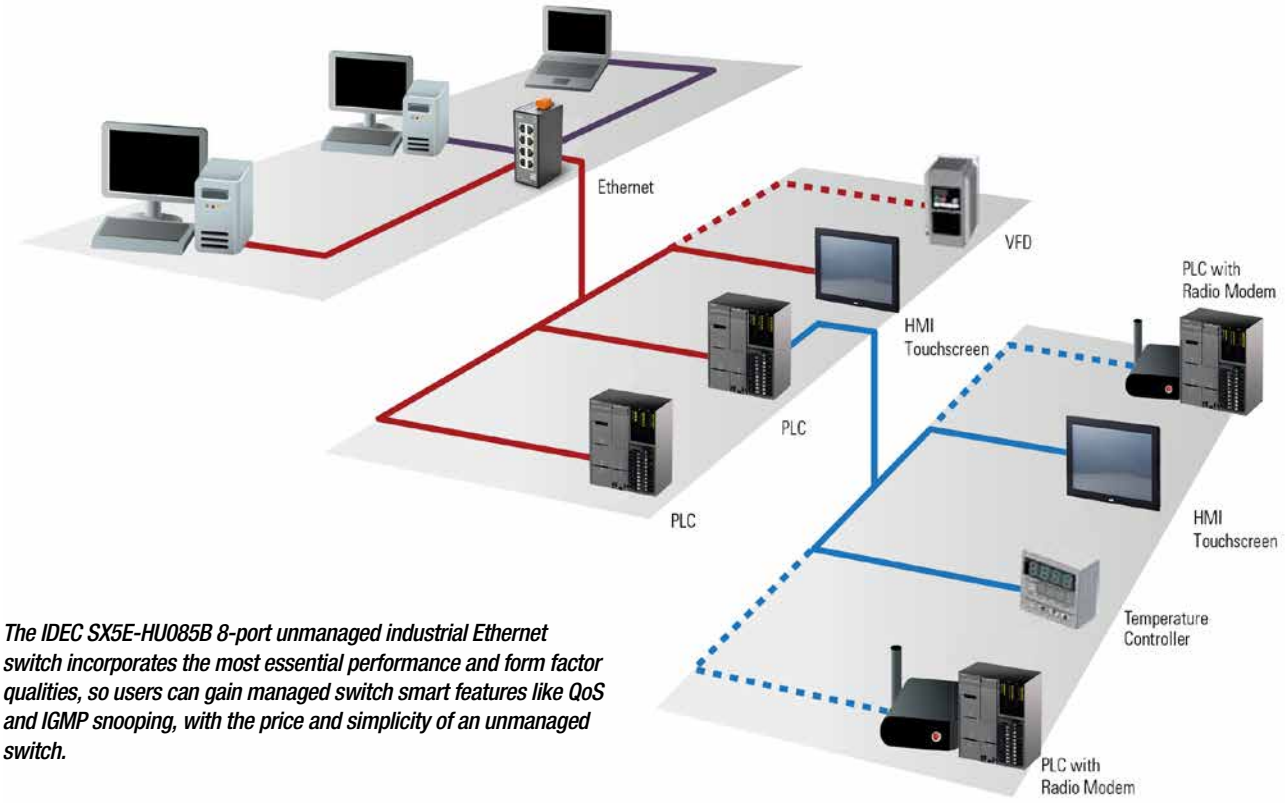
Essentials using unmanaged switch

As the need for high-performance and robust Ethernet connectivity is accelerating in many applications, users are taking another look at their options. A recent development is cost-effective unmanaged switches incorporating the following most essential managed features, with no configuration required.

Quality of Service (QoS)

QoS is a method used by switches to prioritize specified network traffic, so the most critical packets are handled first. For industrial applications, there are greatly increasing numbers of Ethernet devices congesting plant networks, creating concerns about communication latency and data loss.

SOURCE: IDEC



The IDEC SX5E-HU085B 8-port unmanaged industrial Ethernet switch incorporates the most essential performance and form factor qualities, so users can gain managed switch smart features like QoS and IGMP snooping, with the price and simplicity of an unmanaged switch.

EtherNet/IP is a common industrial automation protocol used for handling crucial communications between devices like PCs, PLCs, HMIs, input/output modules, variable speed drives, intelligent instruments, and much more. Therefore, an unmanaged switch which provides built-in QoS for EtherNet/IP traffic is a great advantage because it automatically guarantees priority for those critical data packets over other general traffic. Users need not configure QoS, but they should be able to easily turn it on/off with a single external DIP switch.

IGMP Snooping

Ethernet traffic may consist of some messages broadcast to all devices, others multicast to select devices, and still other unicast to one specific device. IGMP snooping is a method used by switches to monitor conversations between hosts and routers, and to create and maintain a map or filter of which links need which transmissions.

By delivering messages only where they are needed, IGMP snooping significantly reduces networking traffic and required resources. IGMP snooping is usually desirable, but user should be able to disable it by using the QoS DIP switch if necessary.

Broadcast storm protection

For Ethernet networks installed on-board equipment or within a larger facility, careful design and protocol choice can take advantage of network rings for redundancy. However, improper ring connections can result in duplicate messages that will cause the network to stall. For instance, with standard switches, if any user inadvertently connects two switch ports together, then messages will be repeatedly rebroadcast from the ports, increasing in number until they flood and overwhelm the network. Broadcast storm protection detects this issue and discards duplicate messages. As with QoS, no user configuration is required other than enabling this feature with a single external DIP switch.

Robust networking and form factor

There are a few other considerations designers should look for when selecting a switch for their commercial and industrial applications. For best flexibility, switches should always operate at speeds of at least 10 and 100Mb/s, with auto-negotiation of the speed, full or half duplex mode, and detection of straight-through or crossover cables.

Store-and-forward technology is the best chose for operation because it ensures each communication frame is fully received into memory and CRC-checked for integrity before forwarding it to the destination. This feature introduces a very short switching delay compared with some other strategies, but it secures the highest-quality communication.

Rugged metal housings are beneficial for industrial use to provide physical strength and superior performance with regards to electrical noise, electromagnetic interference (EMI), and electromagnetic compatibility (EMC), while an IP30 rating means the enclosure is designed such that solid objects larger than 2.5mm can't enter the housing. Furthermore, the RJ45 Ethernet ports should be supplied with IP30-rated covers to protect unused ports. Users need options to mount the switch to a 35mm DIN rail or a back panel within an enclosure.

It is important to look for an operating temperature range suitable for the environment, and only a few switches can work in the extended range of -40 to 75°C. Even if the full temperature range is not needed, devices with better ratings are built more robustly to provide greater reliability and a longer lifespan. Of course, designers also need to ensure that all approval ratings such as UL508, CE, FCC, and Class I Division 2 hazardous location approval are present as needed. A final note is that many critical applications have redundant power available, so the switch should be designed to accept two separate power supply connections for zero failover time if one power supply fails. Pluggable terminal blocks are a plus to make installation and servicing easier.

Improving network performance

Today's industrial and commercial applications commonly use large numbers of digital controllers, PLCs, and HMIs—along with increasing quantities of intelligent field devices—all of which rely on Ethernet.

Designers now have options to obtain the best networking price/performance ratio, with simple no-configuration installation, by selecting unmanaged switches which incorporate the most important managed switch features.

*Linda Htay, Automation Product Marketing Manager, **IDEC Corporation.***

Visit Website

Flexible SCADA offers savings for midstream water company

WaterBridge turned to modern technologies for a digital transformation that's saving a lot of money. The fast-growing company's new SCADA system uses edge computing and MQTT to collect data from 80 sites, with 200,000 tags.

WHAT COULD BE BETTER THAN HAVING A new, modern, flexible system for supervisory control and data acquisition (SCADA)? How about a system that also saves a lot of money, provides much greater access to data, and gives the freedom to do new projects without limitation? WaterBridge found all this and more.

WaterBridge is a midstream water-management company serving the exploration & production industry. Based in Houston, the company has pipeline networks for produced water transportation, disposal, recycling, and supply. It has 80 facilities connected by 980 miles of pipeline capable of handling 1.8 million barrels of water per day.

WaterBridge got the system it wanted from The Integration Group of Americas (TIGA). Based in Spring, Texas, TIGA is a systems integration and engineering services company focused on deploying technology for industrial markets. The company serves customers in a variety of industries.

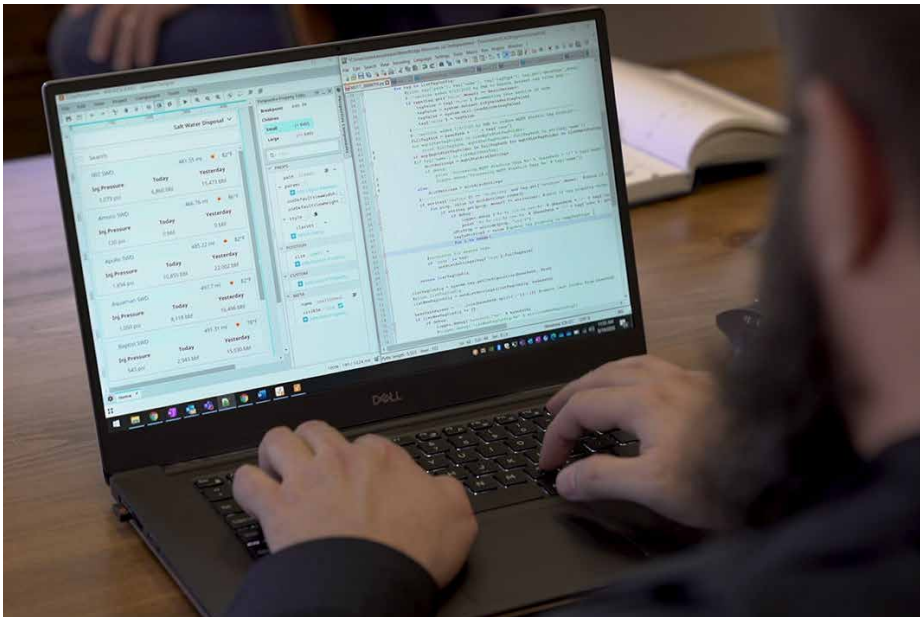
To meet WaterBridge's ambitious goals, TIGA implemented Ignition by Inductive Automation® — an industrial application platform with tools for building solutions in SCADA, human-machine interface (HMI), and the Industrial Internet of Things (IIoT).

SOURCE: INDUCTIVE AUTOMATION

Edge computing proved to be essential for WaterBridge including management of their truck-ticketing systems, collection of high-resolution data, and management of their camera systems.

TIGA and WaterBridge used the Ignition platform to create a new, open-standards system that would allow WaterBridge to better leverage emerging technologies, gain deeper insights into its operational data, connect to remote facilities with the efficiency and security of MQTT, and provide a better user experience.

And it's also saving a lot of money. "Waterbridge has seen a significant reduction in our operational costs using the Ignition platform," said Charles Lame, technical field services director for WaterBridge. "We believe we are saving about $500,000 a year. We do believe, however, that our improvements in reliability and runtime will net us even more savings."



SOURCE: INDUCTIVE AUTOMATION

WaterBridge's goals, included implementing Ignition with tools for building solutions in SCADA, human-machine interface (HMI), and the Industrial Internet of Things (IIoT).

Filling needs

TIGA's implementation of the SCADA system focused on application architecture, ancillary and data integration subsystems, UI/UX design/development, and external interfaces. TIGA also worked with WaterBridge to deploy Ignition Edge local HMIs at 80 saltwater disposal facilities, with industrial PCs and high-resolution monitors.

MQTT Transmission, which was created by Cirrus Link Solutions, was used for the transport of data to the centralized Chariot broker for high-resolution data collection and protection against data loss with store-and-forward capabilities. Ignition Perspective was used for a mobile-first, responsive design for the SCADA system, giving users a much better mobile experience.

WaterBridge had specific needs that TIGA responded to. "Before we entered into this project, we subscribed to a third-party SCADA system," said Lame. "It wasn't geared toward our operations, and getting enhancements and things changed was difficult at times."

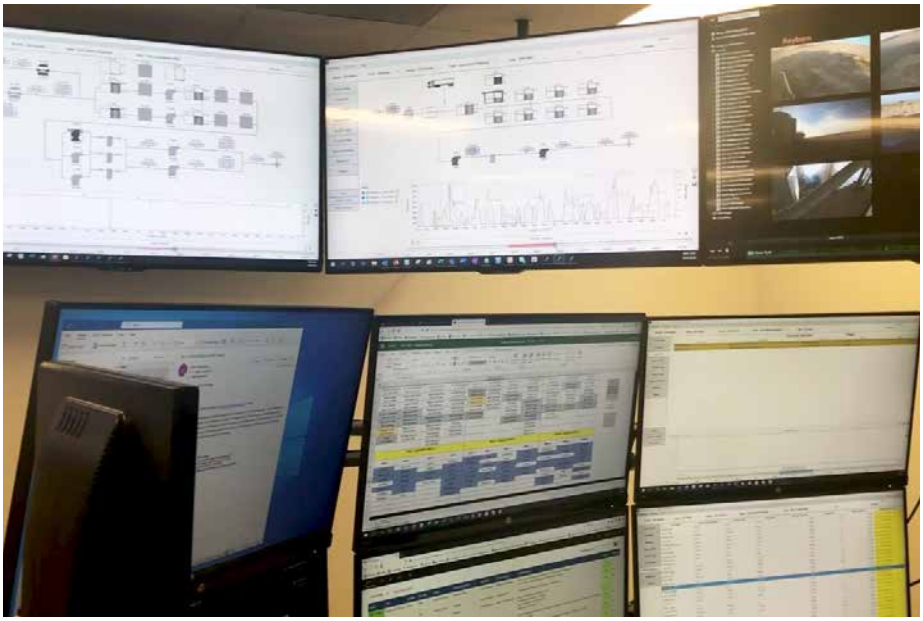
WaterBridge has experienced rapid growth in recent years, and the previous SCADA and control systems couldn't keep up.

They were unreliable and unstable. The system was unable to handle changes that WaterBridge wanted to make in order to improve operations. And the cost of the system was rising, since WaterBridge didn't own it.

"We're interested in deploying technology to serve the three engines that we think will fuel the modern economy, which are oil, water, and data," said John Miller, president of TIGA. The company's approach lent itself well to WaterBridge's desire to modernize and operate more efficiently. "Waterbridge needed this new system to operate and control their pipeline and saltwater disposal facilities to improve operations, mitigate risk, and reduce travel," said Trent Boudreaux, director of technical services for TIGA.

A hosted Microsoft Azure infrastructure was integrated with the SCADA system. Activities at the 80 remote facilities are centrally managed, while control and safety systems are also present at each location. The new enterprise SCADA system can be easily expanded when adding new locations.

With the software's unlimited licensing, there are no additional costs for new devices, connections, tags, or projects. The system currently has 200,000 tags and connects to 600 remote meters. At each of the 80 saltwater disposal facilities, the system collects data from more than 2,000 tags per second.



SOURCE: INDUCTIVE AUTOMATION

The system currently has 200,000 tags and connects to 600 remote meters. At each of the 80 saltwater disposal facilities, the system collects data from more than 2,000 tags per second.

A finer edge

"Edge computing is essential for WaterBridge," said Boudreaux. "It's perfect for management of their truck-ticketing systems, collection of high-resolution data, and management of their camera systems." The MQTT communications protocol is another big plus. "MQTT has been a big difference maker for us," said Lame. "We're able to get real-time data in our SCADA system. It helps us with leak detection and other operational data."

Collecting more data and storing it all in one location has improved operations and enabled a digital transformation. Key stakeholders can now make better, faster decisions based on real-time data. And more than 30 WaterBridge customers have the ability to monitor all aspects of the midstream allocation.

SOURCE: INDUCTIVE AUTOMATION

The new system allowed WaterBridge to gain deeper insights into its operational data.

WaterBridge has added new features recently, including a work request dashboard, virtual site visit, map overlays, Seeq API integration, and several other valuable tools. Additions are fast and easy now that WaterBridge has an open, flexible system. "The SCADA system is fully owned, operated, and maintained by WaterBridge," said Boudreaux. "They can deploy new features within a matter of a few days. And having centralized data from all facilities and assets, Waterbridge can operate their system as a whole, utilizing all of their facilities' assets across the board."

"The WaterBridge project was a great way for us to help our client transform themselves for the benefit of their operations," said TIGA's Miller. "That's with a phased approach, and with this SCADA platform, we're able to implement newer technology one phase at a time. It allows us to create smaller projects within a larger project so that our clients can see value very early on and continue the investment. We certainly plan to do more with it, because of its edge capability as well as the application development that we plan to do within the system that we'll deploy as modules. We see a lot of opportunity in the future. And we're planning to continue on with development with Waterbridge. They plan to leverage Ignition in every way possible as their enterprise SCADA system."

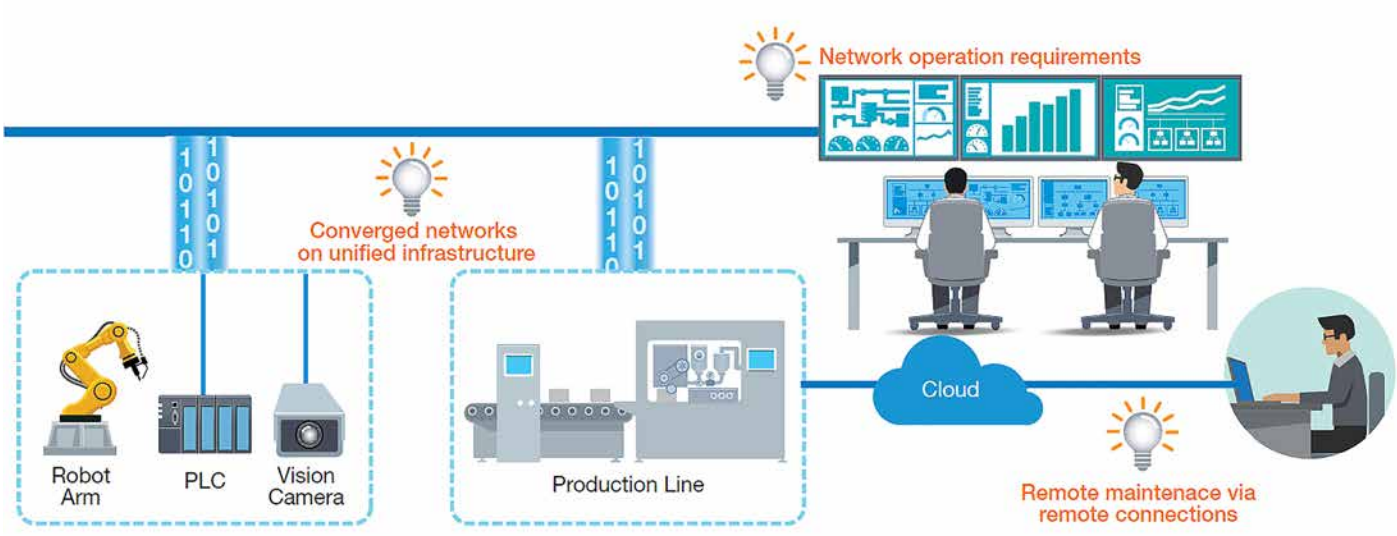
For his part, Lame looks forward to the continued collaboration. "TIGA's been a great partner to work with," he said. "They were a lifesaver. When I started at WaterBridge, we had no internal resources, and they were able to provide all the support that I needed."

Application article by ***Inductive Automation.***

Visit Website

Tips for getting Industrial IoT networks ready for the future

Managing industrial networks only in local control centers may not be feasible three or five years. It is therefore important to use network management software with integration interfaces such as OPC DA tags for SCADA system integration or RESTful APIs for external web services.

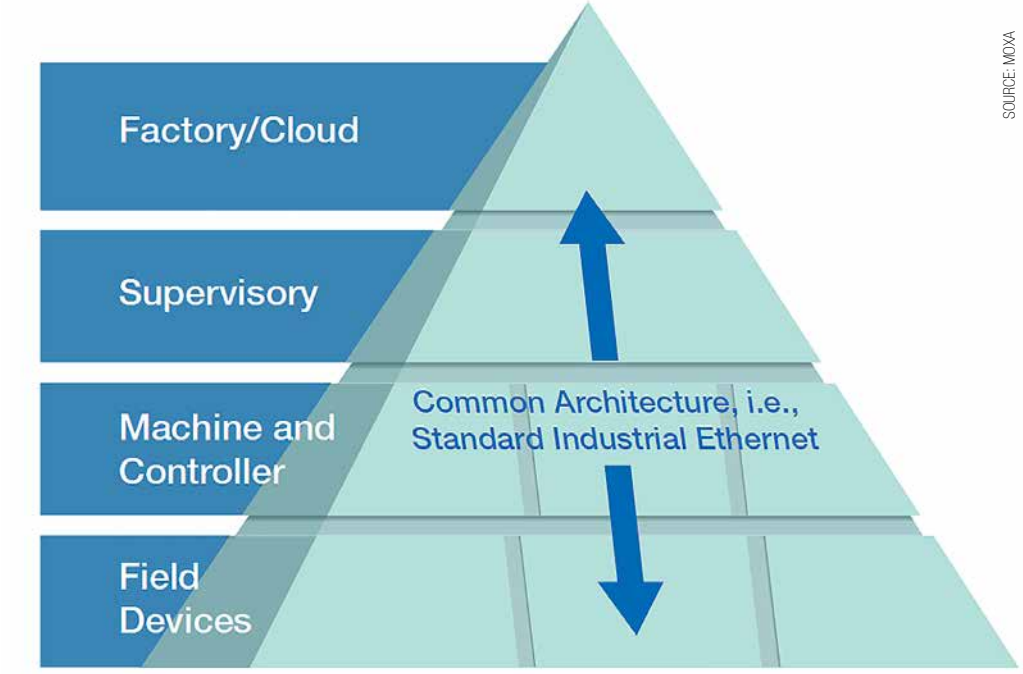


SOURCE: MOXA

Achieve Greater Integration With Unified Infrastructure.

IT MAY BE A TEMPTATION TO REST ON YOUR laurels when you finally have your IIoT networks up and running. Nonetheless, change remains the only real constant in life, and the world of industrial networking is no exception.

Your IIoT network may be sufficient for your current needs—it may even be ready for your foreseeable application requirements over the next several years. But what about the next decade or more? Change is always on the horizon, and we need to be prepared.



SOURCE: MOXA

Access Anywhere to Your Remote Machines With Hassle-free Cloud Services.

Since the early days of industrial automation, manufacturers have adopted a variety of purpose-built protocols and systems, instead of standard Ethernet technologies, for highly specialized industrial control applications.

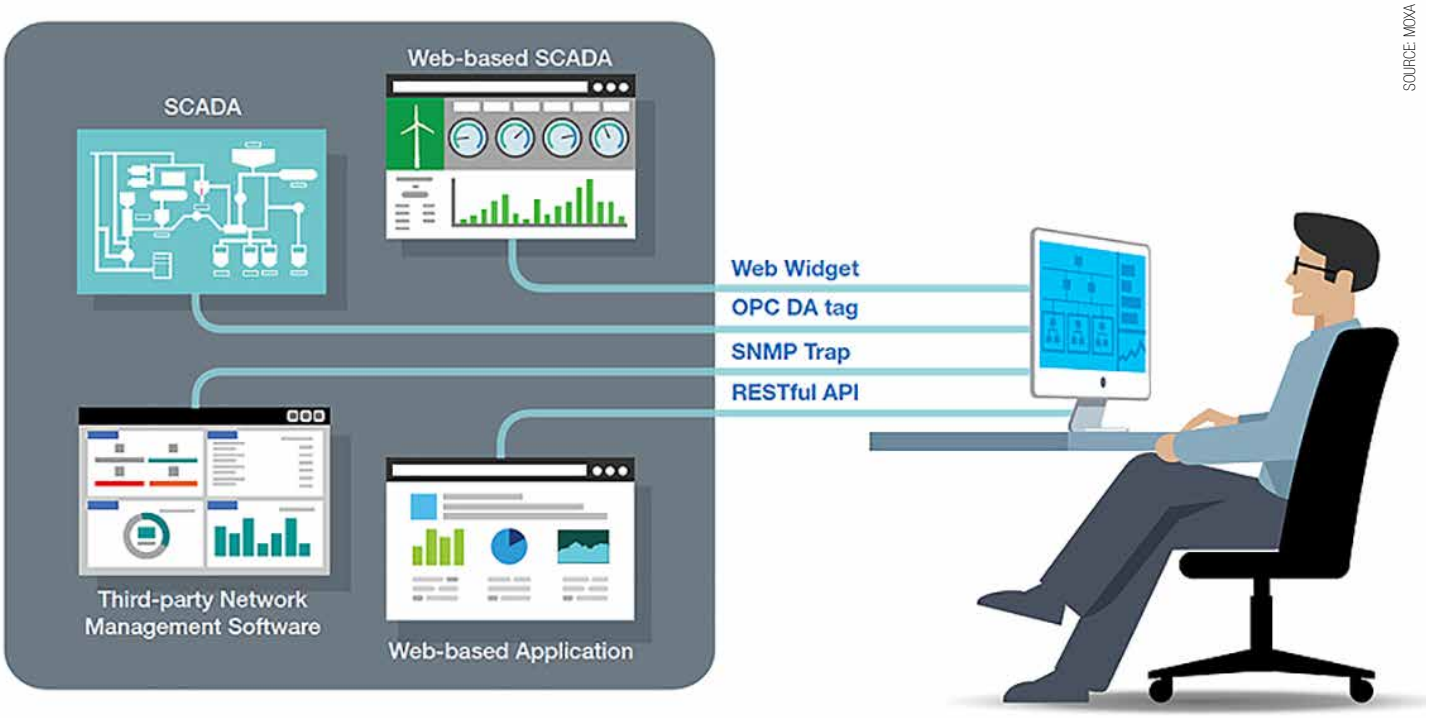
However, as the IIoT market is expected to grow at a CAGR of 24% by 2023, industrial networks of the future will in all likelihood be required to transmit large amounts of data between interconnected devices or collect data from remote devices.

With these growing demands on the immediate horizon, how well-prepared is your company for the future of industrial networking may determine your success in tackling new challenges. This section provides three considerations to help you prepare your IIoT-ready industrial networks for the future.

Integrated unified infrastructure

Over the years, various devices using different industrial protocols have been deployed on industrial networks to provide

SOURCE: MOXA



Visualize Your Network Status for Both OT and IT Professionals.

diverse services. Under these circumstances, network integration usually costs more than expected or becomes more difficult to achieve.

Manufacturers can either choose the status quo, that is, maintain their preexisting isolated automation networks with numerous purpose-built protocols of the past, or alternatively they can seek solutions to provide deterministic services and integrate these "islands of automation".

If our goal is to be ready for the growing demands on our IIoT network in the future, the choice is obviously the latter. The rule of thumb is to take potential industrial protocols into consideration and ensure you can redesign your networks in case any new demands arise in the market.

Time-sensitive networking (TSN) is a set of new standards introduced by the IEEE 802.1 TSN Task Group as an advanced tool box. With TSN, you can build open, unified networks with standard Ethernet technologies that reserve flexibility for the future.

Furthermore, you may consider selecting solutions offered by the key players who are advocating this new technology because they actively participate in TSN plugfests to complete the ecosystem and ensure compatibility among different vendors.

Hassle-free cloud services

Cloud-based remote access offers many benefits to IIoT customers, such as reducing the traveling time and expenses of sending maintenance engineers to multiple remote sites.

Furthermore, cloud-based secure remote access can provide flexible and scalable connections to meet the dynamic, changing requirements of the future.

However, operational technology (OT) engineers for water and wastewater treatment plants, machine builders, and other IIoT customers may find it cumbersome to set up and maintain their own cloud servers to provide new services and applications.

Indeed, considerable efforts are associated with setting up a new communication infrastructure, even if it is in the cloud. Fortunately, OEMs and machine builders can now deliver secure cloud-based services and remote access to their customers without having to maintain their own cloud servers.

One key issue to definitely scrutinize is the cloud server license scheme. Often, upfront costs may seem low for limited server hosts. However, these apparent cost savings on server hosts may actually make your project uneconomical due to a limited scale of connections.

Secondly, consider central management capabilities in order to flexibly expand remote connections in the future. With this said, carefully weigh the costs and benefits of incorporating secure remote access to your industrial networks. Always select solutions that can eliminate the hassles mentioned and help you focus on delivering more value and benefits to your customers.

Visualizing network status

You may have seen the following scene in a movie or photograph in the news. The control room of a metro system has a group of monitors showing the current status of each metro station in the system, the locations of all the moving trains, and so on. Managers or operators need to quickly judge the current situation and take action according to the information aggregated on the screens in front of them. This visibility helps them keep everything under control.

When complexity increases with greater connectivity on industrial networks, it can become very difficult to identify the root cause of problems and maintain sufficient network visibility. Control engineers often have to revert to trial and error to get the system back to normal, which is time-consuming and troublesome.

Therefore, in order to facilitate and manage growing industrial networks, network operators need an integrated network management software to make more informed decisions throughout network deployment, maintenance, and diagnostics. In addition, as your systems continue to grow, you will need to pay attention to a number of network integration concerns.

First, only managing industrial networks in local control centers may not be feasible three or five year later, especially when existing systems need to be integrated with new ones.

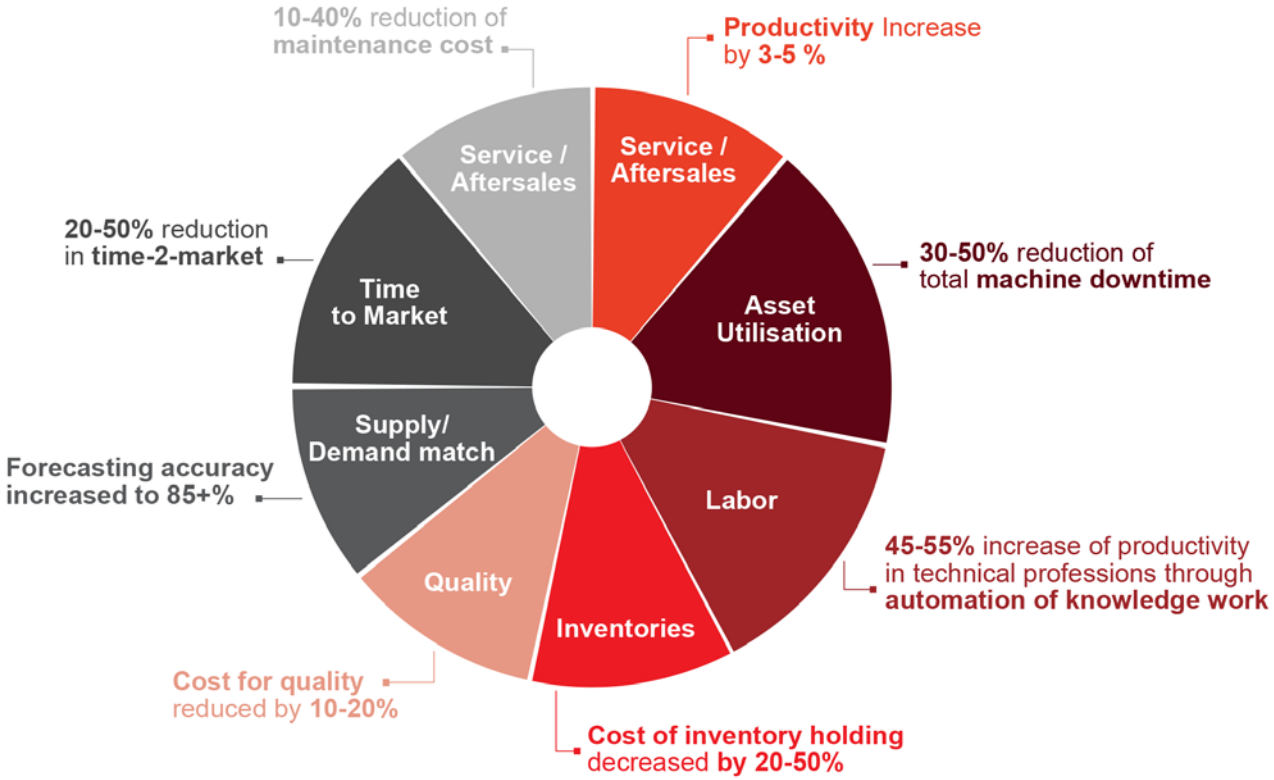
It is therefore important to use network management software with integration interfaces, such as OPC DA tags for SCADA system integration or RESTful APIs for external web services. Furthermore, an interface to facilitate third-party software integration is also a key criteria to ensuring future flexibility.

Application article by ***Moxa.***

Learn More

SPE: enhanced cloud access to sensors and peripherals

SPE, short for Single Pair Ethernet, is expected by many to revolutionize the way modern industrial communication networks operate. As technology advances and industrial applications are becoming increasingly digital, requirements for existing Ethernet wiring are shifting.



Value drivers and expected benefits of key categories in industrial production (source: McKinsey 2015).

IN THIS ARTICLE, INDUSTRIAL COMMUNICATION specialist Hilscher shines a light on the most recent developments and requirements for modern industrial communication and how two drilled cables are set to resolve them.

SPE and why it's necessary

SPE is expected to drastically change industrial communication due to significant cost and space savings, increased coverage in industrial plants as well as an overall improved performance. The main feature is that only two wires for communication and power over data line within the cables instead of up to eight.

Cable lengths of up to 1 km are possible as stipulated by the IEEE802.3cg, and the increasing number of sensors and actors as well as rising demand for more data has proven that conventional fieldbus systems are insufficient above certain cable lengths.

Industrial IoT requires standardized communication between applications and machines. From sensor up into the cloud, SPE enables data transmission along the entire industrial automation architecture based on an IP network.

Introduction

After several years of governmental activities to foster development of new industrial standards as well as rising demands from the market, digitization of modern production lines has picked up the pace recently. Over the course of the last decade, initiatives such as "Plattform Industrie 4.0", "Industrial Ethernet Consortium" or "Made in China 2025" foreshadowed the need for digital technologies and innovations in order to improve the performance of production facilities all around the world.

Numerous major industrial players as well as renowned consulting groups have since examined the potential that lies in new technologies to streamline industrial processes. A study published by the French consulting company Capgemini in 2015 saw a "new industrial paradigm" come to light with a "need for increased intelligence in embedded systems and value creation through smart services". Key success factors in this regard were advanced analytics for predictive production actions and process transparency, according to the Capgemini study.

A McKinsey analysis, also published in 2015, similarly concluded that "disruptive technologies will enable the digitization of the manufacturing sector".

The study, which was based on interviews with about 100 industrial companies, lists cloud technologies, advanced analytics, touch and next-level GUI, virtual and augmented reality, advanced robotics, and additive manufacturing as such groundbreaking innovations. The consulting company Accenture even titled such technologies as game-changing and stated that they could seize a "trillion dollar opportunity" the same year.

Based on the results of the studies conducted by a number of research institutions, they found several value drivers

for modern manufacturing as depicted in the following chart:

Interconnecting cloud and sensors

Following several years of research, many players have accumulated extensive knowledge about the needs and requirements of the manufacturing companies in terms of digitization and automation of machines and processes. One of the major problems when it comes to adopting cloud technologies in manufacturing is the vertical integration of sensors from the field level up to the cloud, where current Ethernet technologies are reaching their limits.

However, since the vertical integration from sensors to cloud is a very important pillar for modern digital business models, the benefits to extend IP networks down to the sensor level are becoming more and more evident:

- Enhanced visibility, diagnosis and control
- Access to all automation equipment through one semantic with OPC UA
- One common vendor-independent tooling
- Enhanced robustness and availability
- Enablement of predictive quality and maintenance

Single Pair Ethernet offers added value through thinner cabling, small footprint plugs and connectors and overall less required space for installation, overcoming the limits of current Ethernet technologies. For that reason, it is suitable to replace numerous existing fieldbuses in the sensor and peripheral area. However, a key question is how a deployment into the different areas in automation will happen.

First attempts on standardizing Ethernet based on two single wires were made by the automotive industry. The existing standards for in-car networks such as CAN, MOST or FlexRay were too costly in terms of cabling and software. Hence, a common standard to gradually replace these was found in the Ethernet technology.

However, the cabling effort for standard Ethernet was comparably high, which is why semiconductor company Broadcom made a first pitch with BroadR Reach in order to show that a simple twisted pair cable is sufficient enough to deliver high-speed data over shorter distances.

Following these first attempts, the Institute of Electrical and Electronics Engineers (IEEE) has picked up the standardization initiative under the well-known 802.3 Ethernet Standard and widened the scope to industrial and building area as well in order to address similar challenges there.

More than just two wires

One might ask, why nobody has come up with the idea of simplifying wiring in industrial manufacturing much earlier to utilize the advantages which SPE is now offering.

IEEE Standard	PHY standard	Transmission Speed	Cable Bandwidth	Cable length	Applications
IEEE802.3 cg	10Base-T1L	10Mbit	20MHz	1000m (STP)	Sensors, actuators and peripherals, machine controls train and bus networks, building automation
	10Base-T1S	10Mbit	20MHz	15m (UTP) 25m (STP)	Cabinet installations (no PoDL) half duplex
	APL	10Mbit		1000m (STP)	Intrinsically safe and Ex equipment
IEEE802.3 bw	(BroadR Reach)	100Mbit	166MHz	15m (UTP) 40m (STP)	Automotive
IEEE802.3 bp		1000Mbit	600MHz	15m (UTP) 40m (STP)	HMI, IPC, Camera, Motion & robotics
IEEE802.3 ch		2.5/5/10Gbit	4-5 GHz	15m (STP)	Vision sensing, IPC, HMI, Analytics, medical systems
IEEE802.3 bu					Power over Dataline (PoDL for SPE, max. 60W power transmission

SOURCE: HSSCHER

Overview of different SPE-related standards.

However, changing existing Ethernet networks to a whole new Standard such as SPE is not quite as simple as an unpretentious exchange of some cables implies. In addition, a number of specifications need to be considered to enable the expected benefits for different industries.

Different Physical Layer: Industrial Ethernet 10Base-T/100Base-TX, the most common standard currently used in industrial manufacturing, utilizes two twisted pairs of cables for a unidirectional transmission and reception data. In contrast, a single-pair Ethernet cable transmits and receives data via one twisted pair and therefore requires a different physical layer as well as different coupling and transducers.

Long distance transmission: Sensors, actuators and other peripheral field devices used in industrial automation often require very long cables in order to transmit and receive data. Hence, a strong demand for longer possible cable length came to light. Currently, SPE is able to cover distances for data transmission of up to 1000m instead of around 100m, which are possible with the current 100Base-TX standard.

Intrinsically safe: Safety is a critical issue for every industrial application, especially in the field of process automation. In addition to the demand for long distance data transmission, process automation companies have to pay particular attention to intrinsically safe transmission for hazardous and explosion-proof areas.

Power transmission: Many sensor communication fieldbuses currently in use also provide power transmission over communication cables. Hence, the single twisted-pair cable used for SPE must be able to supply the necessary power to operate remote sensors and actuators.

Application specific bandwidth demand: Applications in industrial manufacturing are very manifold and require different bandwidths. In addition to field level devices and sensors, which are well covered by a 10Mbit transmission speed, the idea was to also roll-out SPE for applications with a demand for higher bandwidths. Therefore, the IEEE also defined standards suitable for applications such as vision, motion and HMI including the respective physical layers.

IEEE Standardization & applications

All these requirements and demands from the industry towards SPE are being adopted by the IEEE and incorporated into global standards. In the table below you can see different SPE related standards defined by the IEEE and their specific transmission speed and application.

The table above shows that the 10Mbit Single Pair Ethernet Standard IEEE 802.3cg is split into three different iterations to reflect the different needs from various sensor, actuator and peripheral applications.

The 10Base-T1L is mostly applicable for sensors as it allows up to 1000m cable length in a point-to-point connection and fits very well into current installations.

	10Base-T1S	10Base-T1L
Transmission speed	12.5MBit	7.5MBit
	half-duplex multi-drop	full duplex
		echo-cancelled
Line-Coding	DME	PAM-3
Signal-Coding	4B5B	4B3T
Voltage	1Vpp	1Vpp (2.4Vpp)

Comparison between the two specified physical layer specifications of SPE.

In terms of defining the physical layers, which are addressed in the scope of the IEEE's SPE standards, the Advanced Physical Layer (APL) is exactly the same as T1L, but it is adding the necessary components for intrinsically safe data transmission for critical use cases such as hazardous and explosion proof areas.

In contrast, the 10Base-T1S allows for a multi-drop setup with much shorter cable lengths and a different PHY layer called PLCA (physical layer collision avoidance). Multi-drop is especially suitable for, among other things, cabinet installations or other short-range applications. Both systems require a different physical layer as shown in the table above.

Although the physical layer differs in some details between T1S and T1L, the connection to the upper layers remains the same. The IEEE has gone to great lengths in order to make sure that any system with a MAC and an MII connection can interface with the new PHY. That means that major changes only affect one OSI layer.

In addition, the IEEE 802.3bu standard is also defining a standardized power supply over the data line for applications up to 50W to a single endpoint. This feature allows backward compatibility to several existing sensor network standards that also power the connected sensor from a central power controller. Such a setup with contemporary power distribution is shown in the following figure.

The system requires a Power Sourcing Equipment (PSE) in order to deliver energy over the wires. Three different voltages are defined by the IEEE which are linked to specific power outputs. On the receiver side, the Powered Device (PD) in the above case requires a maximum of 50W at 48V, which can be delivered in a point-to-point T1L connection. At 24V the PD can still put out a max. of 10W with a regulated PSE. Such a system is largely compatible with the trunk and spur topology in process automation networks.

The standardization of Single Pair Ethernet, as stipulated by the IEEE to date, is well suited to support the demand of the industrial automation companies. Since the physical layer technology is already in use in some different variations in the automotive industry, industrial users can rely on an already field-proven technology when they start to implement it into their plants.

SOURCE: HILSCHER

The challenge is now to bring these advantages into existing IP-based networks that already enable many of the current data-driven business models. And challenges are plentiful.

For example, some of the industrial Ethernet standards do not have a 10Mbit transmission speed in their specs or have just started to include it. Therefore, a key question for existing fieldbus standards in factory automation, driven by groups like PI, ODVA and others, are the possible use cases in context of the current automation architecture. Currently several scenarios and potential integration scenarios into the field are in discussion.

For factory automation, there is already a standard that supports data access into each sensor in the system: IO-Link. Several sensor manufacturers are actively aligning their needs within the IO-Link standard. IO-Link already supports parameterization, diagnosis, and full integration into Industry 4.0 eco-systems. However, transporting IO-Link Frames up to 1000m based on SPE physical layer would transfer the former point-to-point sensor network into an alteration of a fieldbus system.

A discussion about the positioning of IO-Link in regard to SPE physical layer is on-going to resolve and avoid confusion. The current discussion reviews the potential use cases that could be enabled with an SPE physical layer, but by keeping the IO-Link ecosystem as is in order to maintain existing investments.

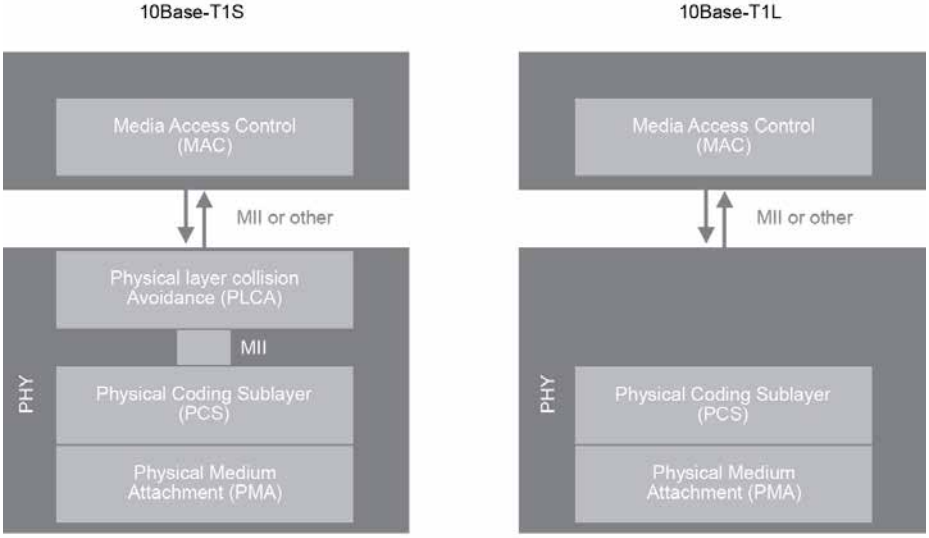
In order to show a possible deployment, the IO-Link Consortium has released a whitepaper containing several precedents of deployment scenarios (IO-Link Consortium, 2020) based on brownfield installations:

The example above allows for an integration of an IP67 SPE master into an existing installation of IO-Link as well as binary sensors and devices. The proposal in the whitepaper sets SPE mainly as a transport medium for IO-Link Frames to keep the IO-Link Eco-system largely as is.

A software-based Ethernet-to-IO-Link adapter makes it possible to maintain the data format and benefit from the extended range and other advantages of SPE, while simultaneously maintaining the existing infrastructure and installations.

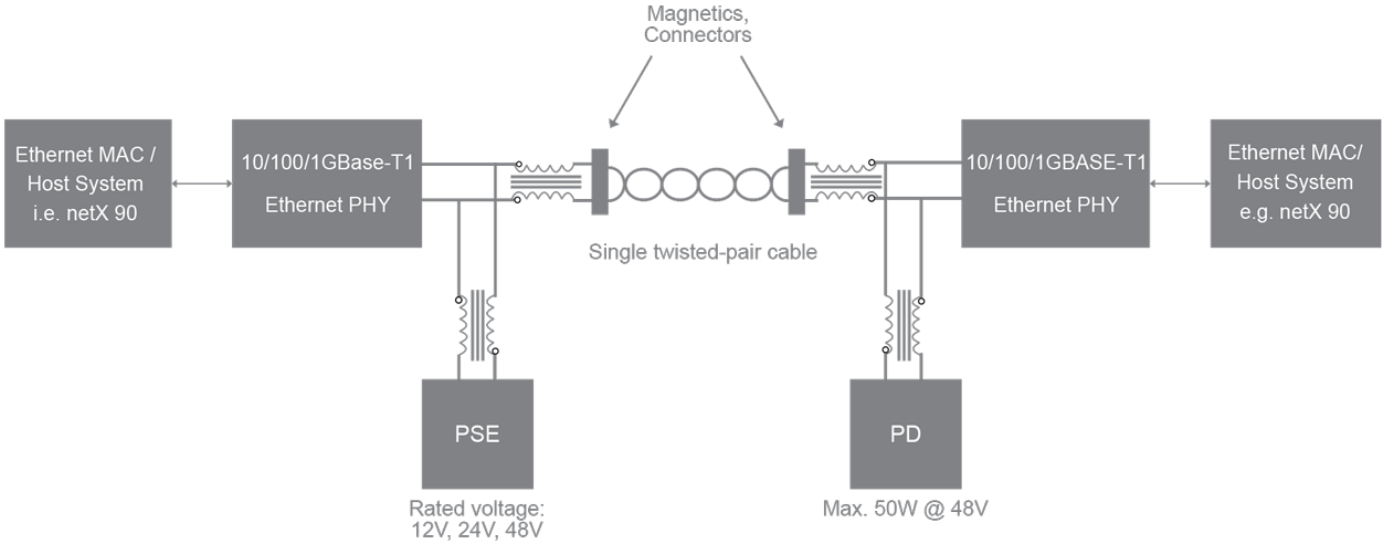
Hilscher participates in several projects of the PI group to contribute to the discussions on SPE for PROFINET. We also contribute to the IO-Link working group evaluating the benefits and challenges for a complementary integration of both standards into the field.

At the IEEE, we take part in the open topic discussions regarding the 802.3cg, in addition to the efforts by the ODVA on SPE



PHY connection to upper layer host system.

SOURCE: HSSCHER



System setup of a point-to-point connection with power distribution.

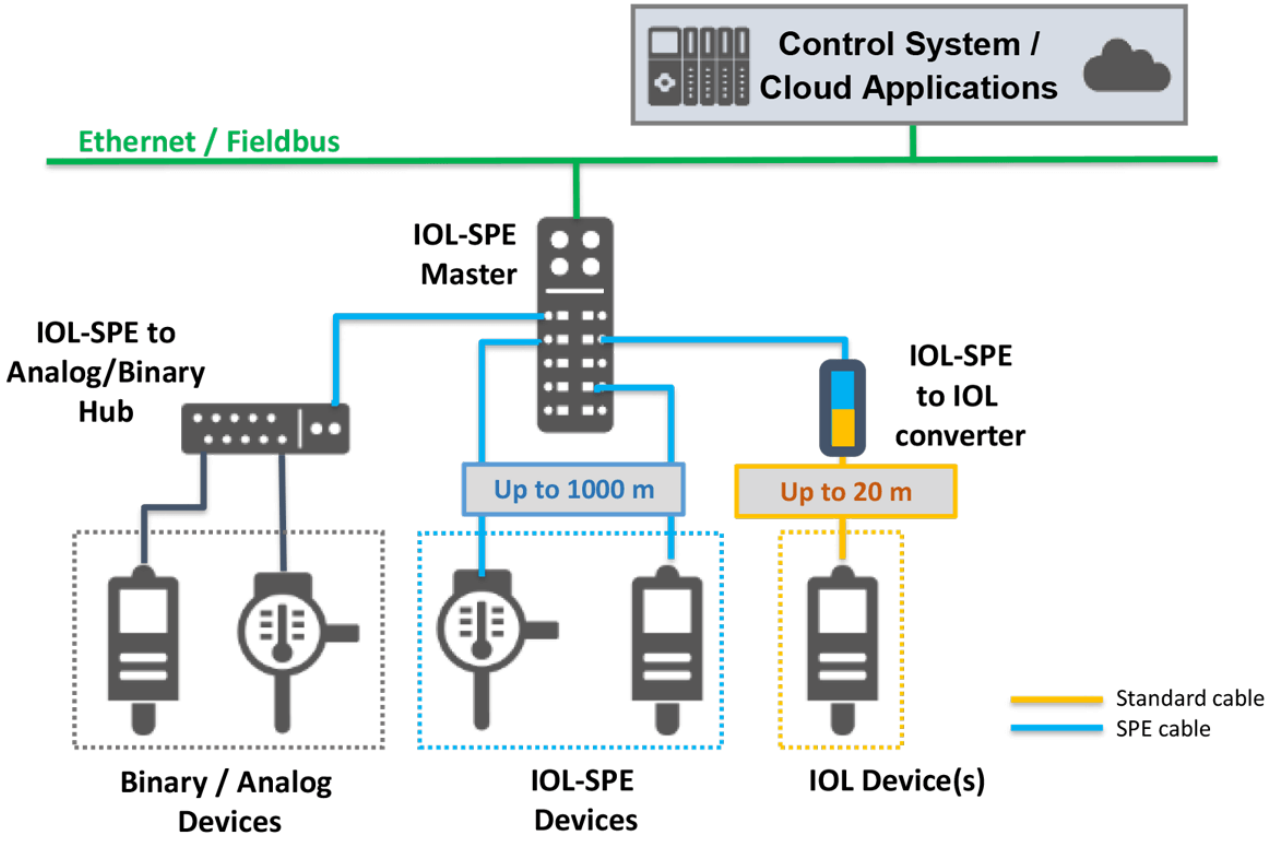
topics. Our goal is to help build a migration path for low-effort integration of SPE into existing systems and to support this with our communication competence and solutions.

netX: New Technology

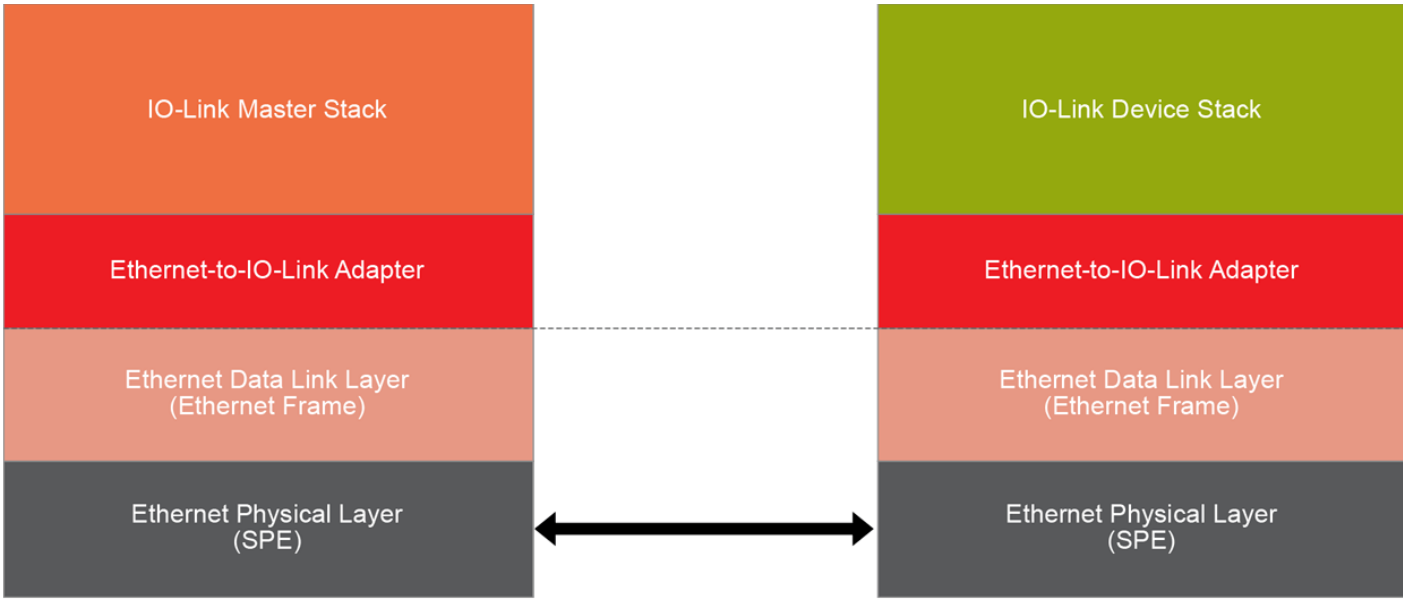
Hilscher's sophisticated multiprotocol chip solutions, the netX SoC product family, are at the forefront of SPE deployment worldwide. The netX 90 chip, as well as modules and PC Cards based on it, allows connection to external PHY products via MII interface. The internal xMAC processors enable the protocol specific switching between the two channels. On the left side of the following figure, the use-case shows two 10Mbit channels SPE port up to 1000m line length, connected to an IO-Link sensor network through our 4-channel netIOL Master chip for legacy implementations.

The middle use case shows an existing 100Mbit Real-Time Ethernet (RTE) system connected to a 10Mbit SPE network. In this case, one internal PHY and xMAC serves the 100Mbit side, the second xMAC with the external SPE PHY connects to the up to 1000m long two-wired cable of an SPE network. In the right side use case, the netX acts as a switched device between a 100Mbit based RTE and a 10Mbit SPE network.

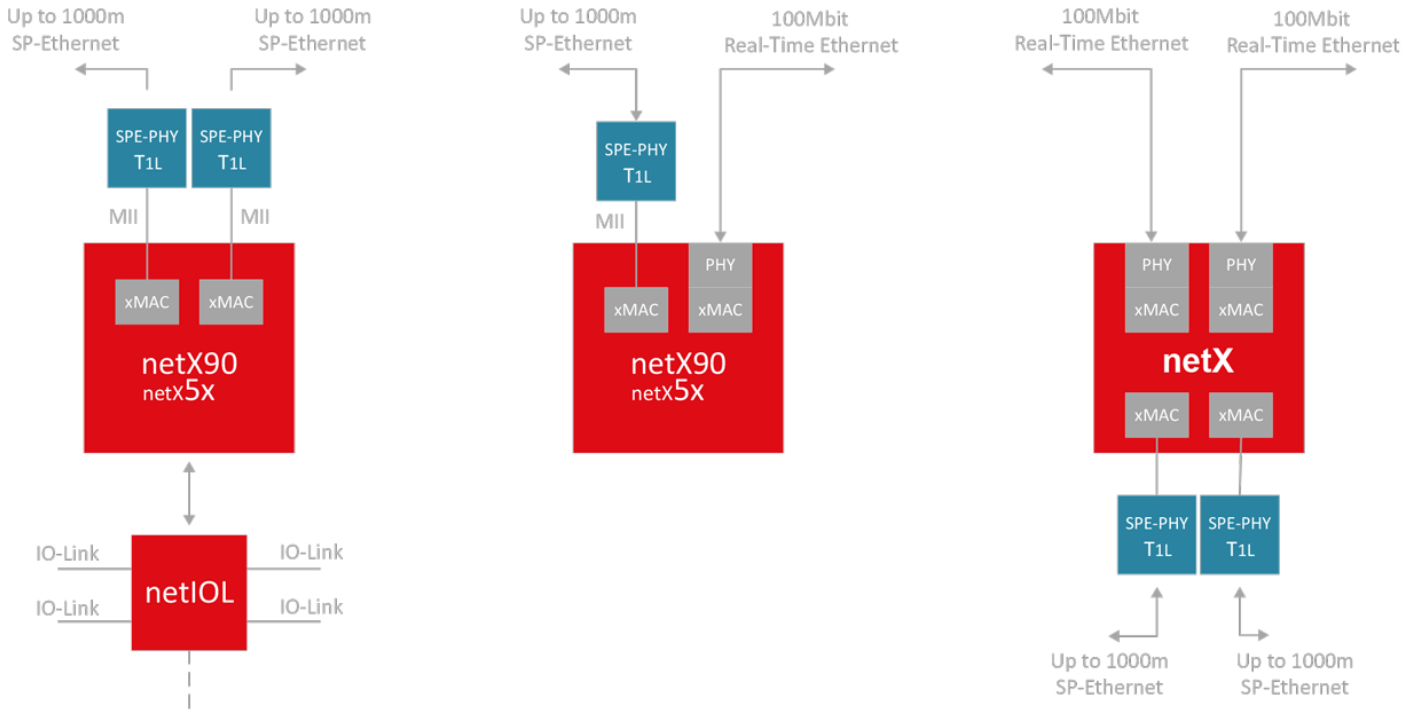
Hilscher has developed a first evaluation board with the netX 90 and SPE 10Mbit T1L PHYs for engineering and testing purposes. The board offers a simple extension of a 100Mbit network towards 2ch SPE to evaluate SPE in context of the different Industrial Ethernet Standards. Hilscher expects a starter



SPE installation in an IO-Link ecosystem (source: IO-Link Consortium, 2020).



IO-Link data integration into Ethernet hardware and datagrams (source: IO-Link Consortium, 2020).



netX-based configurations in SPE networks.

kit during the fourth quarter of 2021. As the standardization bodies are still in progress to finalize SPE in their respective releases, the diagrams above and the board are showing some of the possibilities and options to support brownfield installations based on netX.

With the progress in SPE definitions, we will release more options and solutions; stay tuned.

Conclusion

Single Pair Ethernet has reached a level of standardization that allows companies and whole industries to start adopting it into their systems, mainly focusing on a seamless connection from sensors up to the cloud based on Ethernet technology.

SPE benefits differ tremendously depending on the degree of digitization integration measures. The robust and smaller cables and connectors, the comparably high transmission speed, the distance of up to 1000m, a possible multi-drop set-up, and the opportunity for one vendor-independent tooling makes SPE an excellent solution for such a vertical integration of sensors and peripherals in various applications.

Subsequently, this leads to a different demand and pace when it comes to implementing SPE into advanced manufacturing systems.

Hilscher is expecting an early adoption and deployment of SPE in the process automation sector starting in late 2021 to enable digital business models. Hybrid and discrete Industries to follow with reference implementations based on the enhancement of relevant standards.

Niels Trapp, VP Business Development, ***Hilscher.***

Visit Website

Cost-effective upgrade of water pumping station control

Ethernet line extenders enable existing telecom cables to be used for new resilient data communications network supporting updated PLCs at a water pumping station. The ability to adjust data rates helped to create a very stable connection. Built-in tools assisted with troubleshooting and configuring the units properly.

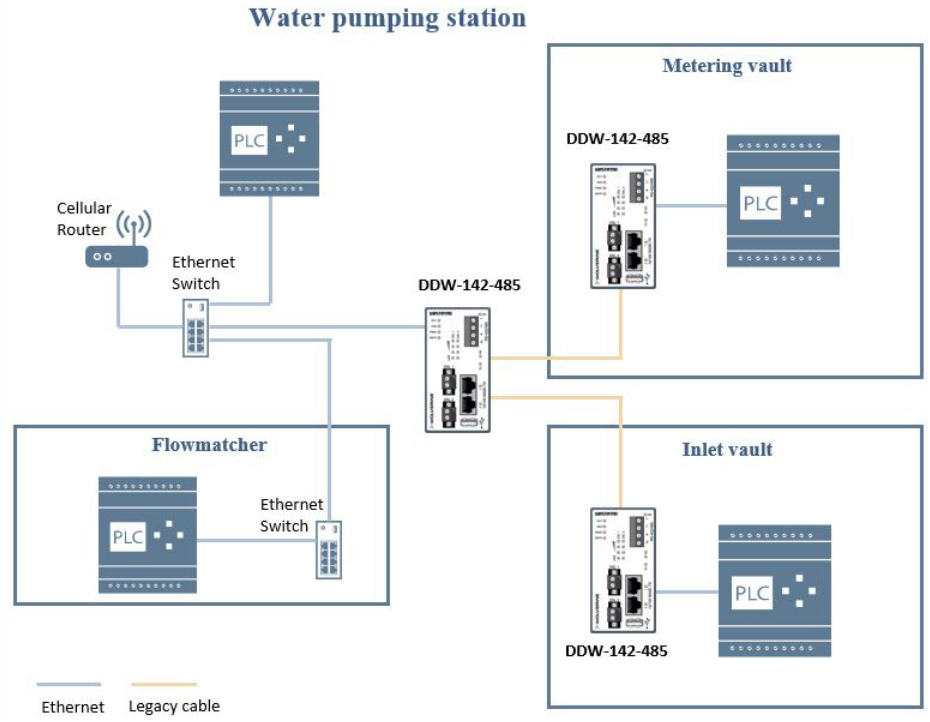
A COST-EFFECTIVE UPGRADE OF THE DATA communications network supports new PLCs at water pumping stations in Bedford Park, IL, USA. Westermo Wolverine Line Extenders enabled existing cabling to be reused for a new resilient Ethernet network, helping to reduce installation time and costs.

The aging PLCs that controlled equipment at three pumping stations were becoming obsolete, with maintenance requirements increasing and sourcing spare parts challenging. It was decided that the PLCs would be replaced, along with the supporting data network, which was based on a proprietary protocol and did not offer the necessary reliability or functionality.

Concentric Integration, specializing in utility technology, was tasked with upgrading the system to increase reliability and ensure support in the future. A new Ethernet network was required, but the cost of replacing existing cabling with fiber was not only very expensive, but also extremely time-consuming.

Concentric turned to Westermo for support and the company's Wolverine range of Ethernet line extenders provided the solution to this issue. The extenders utilise SHDSL technology on twisted pair cables to establish a high-speed remote connection between two Ethernet networks. Instead of installing fiber or radio links, the SHDSL technology provides a solution using the existing cables.

In total, nine Wolverine DDW-142-485 Line Extenders are being used to create networks supporting PLC to PLC communications for the three pumping stations. A single line extender is installed at the main pump stations and another at each underground metering and inlet vault. The Wolverine line extenders enabled data to be transmitted over a distance of about 0.3 miles from a remote site to each pumping station using an existing two-wire telecom cable. Critically, the Wolverine line extenders are designed to provide extremely reliable and resilient data transmission despite the noisy environment and several surge protectors at the pumping stations.



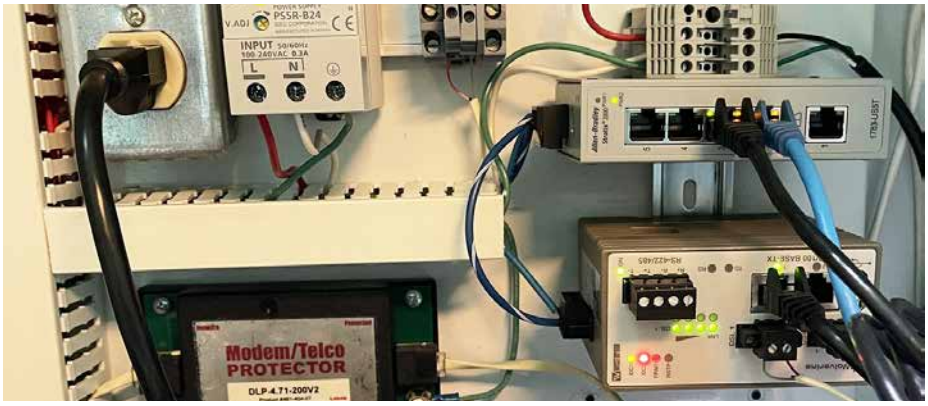
SOURCE: WESTERMO

Network architecture at the water pumping station.

The ability to adjust the data rates helped to create a very stable connection. The built-in tools within the Westermo WeOS operating system showing the signal-to-noise ratio and other statistics of the SHDSL line assisted with troubleshooting and configuring the units.

"The Wolverines can form a network over any type of copper cables, which made it possible to create a very cost-effective solution using the pre-existing telecom cable," explained Benjamin Campbell, technical engineer at Westermo. "The WeOS operating system, which has been developed to simplify configuration and management of the devices, made the upgrade easy and problem-free."

"Not only were we able to carry out the project efficiently and successfully, but the Wolverine Ethernet extenders enabled both significant project cost savings and time savings as we did not need to install new cabling," said Michael Klein, president of Concentric Integration.



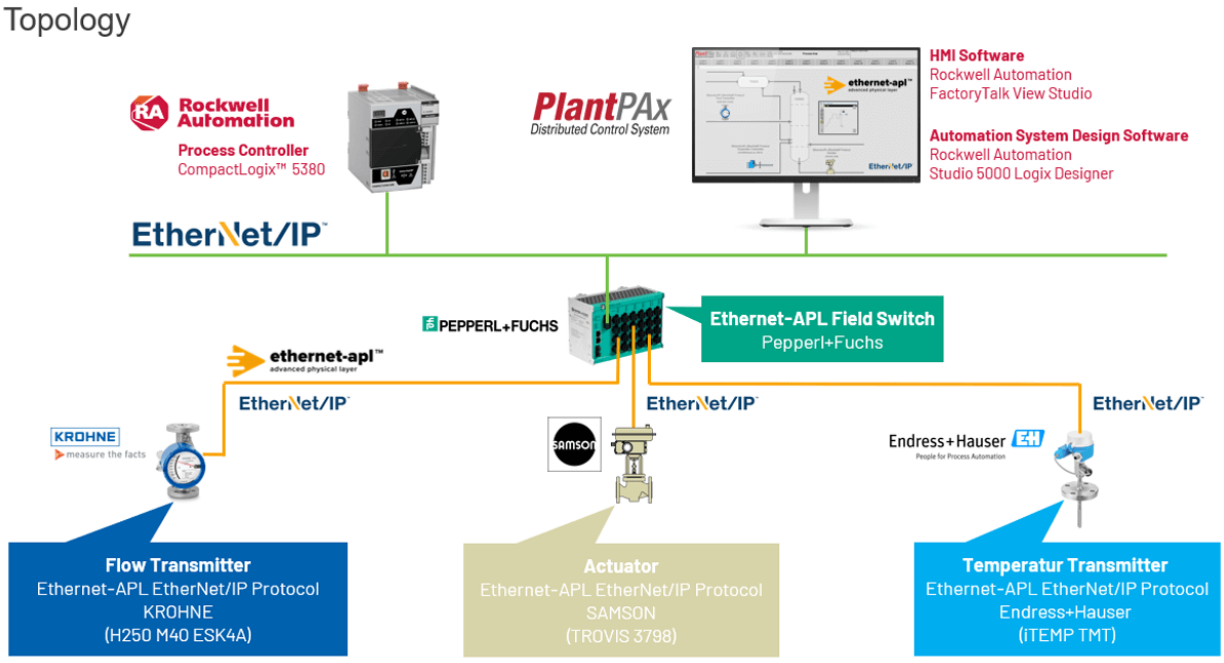
Wolverine line extenders (bottom right) remove the need to install new fiber optic cabling.

Application article by ***Westermo.***

Visit Website

Ethernet-APL: the future of process automation connectivity

Competition and cost pressures combined with Industry 4.0 have made device health status, operations analytics and predictive maintenance via the device, edge and cloud more important than ever. The process industries are poised for a major shift, with Ethernet connecting directly to field devices via Ethernet-APL.



SOURCE: ODVA

EtherNet/IP Network Portion of ACHEMA Pulse Ethernet-APL Multivendor Demonstration.

THE RELIABILITY, SECURITY, AND SAFETY requirements of process industries that are driven by their critical infrastructure role along with high fixed plant costs have led to usage of dependable and proven control technologies such as 4-20ma for far longer than most other industrial sectors.

Some of the downsides to this approach are that field device commissioning takes minutes instead of seconds and there is a limited amount of process and diagnostic information available beyond critical process variables.

Process fieldbus solutions offered potential device status and remote commissioning possibilities, but were not adopted on a mass scale due to concerns about training, maintenance, reliability, and interoperability resulting in a very limited overall industry change and benefit to end users.

Ever-mounting competitive and cost pressures combined with technology advances via Industry 4.0 have made device health status, operations analytics and predictive maintenance via the device, edge, and cloud more important than ever. Process industries are poised for a major shift, and the time has come for Ethernet to connect directly to field devices with the launch of Ethernet-APL.

Ethernet-APL Overview

Ethernet-APL is a combination of Single Pair Ethernet (IEEE 802.3cg-2019, 10BASE-T1L), engineered power, Intrinsic Safety (IEC 60079, 2-WISE), and Type A fieldbus cable (IEC 61158-2, for intrinsic safety). As a result, Ethernet-APL satisfies the process industry needs for long reach cabling of up to 1,000 meters per trunk length, powered infrastructure and intrinsic safety protection for all Class 1 hazardous Zones and Divisions.

The use of 2-WISE to define intrinsic safety protection enables simple steps for verification of intrinsic safety without calculations, and 10BASE-T1L allows for dramatically increased speed at 10 Mbit/s.

As it is just a physical layer, Ethernet-APL allows end users to access standard safety and security services built on IEC 61508 and ISA/IEC 62443 from the leading industrial automation standards bodies.

Additionally, Ethernet-APL will be able to support EtherNet/IP™, HART-IP, OPC UA, PROFINET, or any other higher-level network protocol. In summary, Ethernet-APL allows Ethernet to seamlessly extend from the field instrumentation to the plant process automation system to higher level enterprise resource planning systems and cloud environments, thereby reducing gateways.

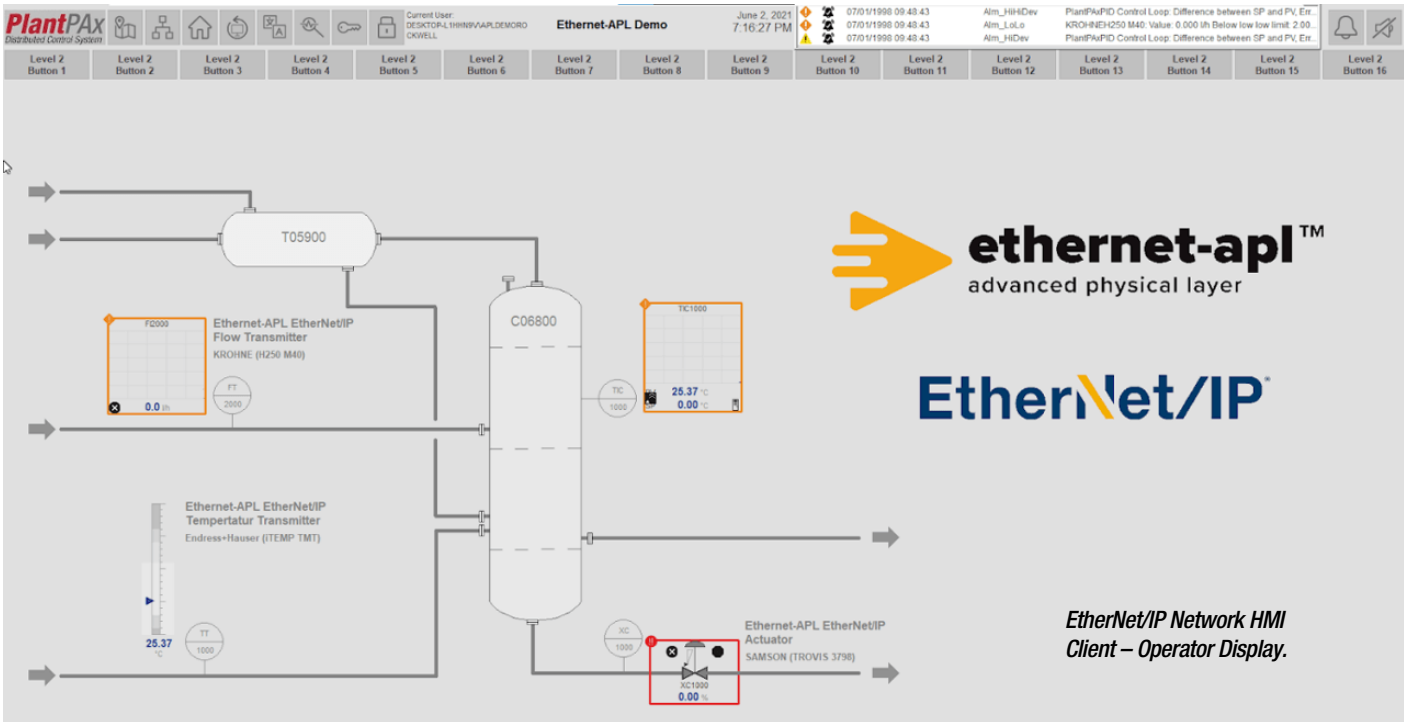
Ethernet-APL technology launch

"The APL Project" is made up of standards development organizations FieldComm Group, ODVA, OPC Foundation, and PROFIBUS & PROFINET International (PI), and 12 major industrial project members. After three years of successful cooperation, the APL Project launched the Ethernet-APL technology at the ACHEMA Pulse digital fair on June 15th, 2021.

The technology launch included the release of specifications, engineering guidelines and conformance test plans. The launch also includes defined port profiles that create the Ethernet-APL concept for multiple power levels with and without explosion hazardous area protection and standardized product marking.

Next steps include release of field devices from companies with initial products now available from select vendors. Ethernet-APL value was demonstrated during ACHEMA via a multivendor demonstration showing participation across different product vendors and industrial protocols, highlighting the options and interoperability Ethernet-APL offers end users.

SOURCE: ODVA



EtherNet/IP Network HMI Client – Operator Display.

Next steps for Ethernet-APL

It's likely that hybrid industries such as pharmaceutical or food and beverage will be early adopters of Ethernet-APL technology to take advantage of the significantly enhanced data visibility of field devices for use cases where field devices are significantly spread out requiring long cable lengths or are located in hazardous environments.

Traditional process industries will likely follow with adoption once the concept is proven via technology demonstrators, industry pilots, and internal testing. Process end users will gain the most value from adoption as the increased speed will enable advanced analytics, predictive maintenance, and enhanced operational management. The long cable length and intrinsic safety capability will make it possible for Ethernet to become the standard field device solution.

Additionally, process companies can potentially re-use existing installed Type A fieldbus cable that meets the resistance standards of 100 ohms with +/- 20 ohms tolerance for Ethernet-APL. The ability to potentially re-use Type A fieldbus cable and to have both power and communication on the same cable can allow for significant cost savings due to not having to run new cable.

EtherNet/IP and Ethernet-APL

EtherNet/IP communication networks will be able to utilize the Ethernet-APL physical layer in process plants, which will unlock the advantages of commercially based industrial control hardware, an object-oriented foundation, and standard internet protocol compatibility including TCP/IP, HTTP, FTP, SNMP, and DHCP.

The first Ethernet-APL infrastructure and field devices that support EtherNet/IP are expected to be available in 2021. Continuous enhancements to EtherNet/IP are both planned and underway to meet future industrial communication and control needs across discrete, hybrid and process applications. Recent EtherNet/IP process enhancements include the addition of NE 107 diagnostics, HART integration, IO-Link integration, and device description enhancements.

With EtherNet/IP, NAMUR NE 107 diagnostic information can be easily transported to a DCS for an operator's review or to an edge device mapping for predictive maintenance. Seamless information sharing with broad usage of EtherNet/IP in process automation, even better than what is now possible between HART and EtherNet/IP and between IO-Link and EtherNet/IP devices, will enable a more efficient and interconnected infrastructure. ODVA is continuing to expand the EtherNet/IP ecosystem with the next generation of digitized device description files, including FDT, FDI, and xDS, to simplify integration into process asset management tools. The end goals of the device description efforts are to provide a standard, robust and detailed description of device information, implement secure device description artifacts, and prepare for a future driven by Industry 4.0 and the industrial IoT.

IEEE Ethernet standard compliance provides users with a choice of network interface speeds — e.g., 10, 100 Mbit/s, 1 Gbit/s and beyond, installation options including copper, fiber, fiber ring and wireless, and topologies including star, linear and ring. EtherNet/IP provides support for functional safety with CIP Safety™, device defense with CIP Security™, with parallel redundancy protocol (PRP) and Device Level Ring (DLR) for fault tolerant redundancy. ODVA is committed to ensuring that EtherNet/IP meets all requirements of Industry 4.0 and IIoT.

EtherNet/IP is a proven industrial automation network that is multivendor interoperable, and highly standardized. Ethernet-APL along with process specific enhancements will open the door to the advantages of EtherNet/IP within process automation for network and device health monitoring, built in security and safety, and remote device configuration.

Ethernet-APL value for end users

Ethernet-APL will open the door to widespread use of industrial Ethernet in process automation. Process end users can now leverage Ethernet-APL as a single Ethernet physical layer for long distance field devices, intrinsic safety, and application-layer industrial protocol support to optimize production while maintaining the safety, security, and ease of use from prior solutions.

Additionally, usage of gateways will be significantly reduced. Conformance tested products will be released soon to enable the start of the Ethernet to the field revolution in process plants. Ethernet-APL offers new possibilities including enhanced remote commissioning, asset management, control, analytics, and diagnostics/prognostics, which will help drive adoption of this new technology. It's not hyperbole to say that Ethernet-APL is the future of process automation given that it meets the requirements of the process industry, including enabling the NAMUR Open Architecture (NOA) second channel.

Steven Fales, Director of Marketing, ***ODVA.***

Visit Website

TSN technology: basics of Ethernet Frame Preemption

Ethernet Frame Preemption is a new extension to Ethernet. Part of Time-Sensitive Networking (TSN), it guarantees a constant cycle time for industrial applications. Why this extension is necessary, and the way it works is described in two articles. Look for Part 1 online in the June issue of the Industrial Ethernet Book.

IN THE FIRST ARTICLE ON FRAME PREEMPTION (see our June issue), we described how frame preemption can chop a message in smaller fragments, and the receiver assembles them again to re-create the original (long) message. This looks simpler than it sounds, as it is a fundamental change to the Ethernet implementation as it has been for 35 years.

Basic terminology

We have seen that in order to keep the real-time requirements, some messages must have the guarantee that they can be sent in time. In Ethernet terminology, these are called the "Express" messages. All messages not being express messages are labelled "Normal" messages (we called them 'acyclic' earlier). Depending on the available time in a cycle, the normal messages can be subject to fragmentation due to preemption. The first fragment of the preemption procedure is called the "Start Fragment", after which a number of "Continuation Fragments" can follow, followed by the "Last Fragment".

Changes to the message format

The Ethernet message format hasn't changed much in 35 year, except for the introduction of the VLAN/QoS (4-byte) field. For frame preemption, a much larger change is necessary, needed to store the additional administrative fields. These fields contain the data that the receiver needs to properly handle fragments (first/intermediate/last) in the right order, and detect errors.

The original Ethernet message format is shown in figure 1. Each message starts with a 7-byte "Preamble", each byte with value 0x55 (binary 01010101). Following the preamble comes the 1-byte field "SFD" (Start Frame Delimiter), with the fixed value 0xD5. Next comes the sender's MAC-address (6 bytes), receiver MAC-address (6 bytes), Type field (2 bytes), and up to 1500 bytes of data. The message ends with a 32-bit CRC

For use with frame preemption, the following changes are made (the SFD byte is now called SMD):

- Transmission of "Express" messages. The SMD has value 0xD5 (unchanged).
- Transmission of "Verify" and "Respond" bookkeeping messages. The SMD has value 0x07 or 0x19.

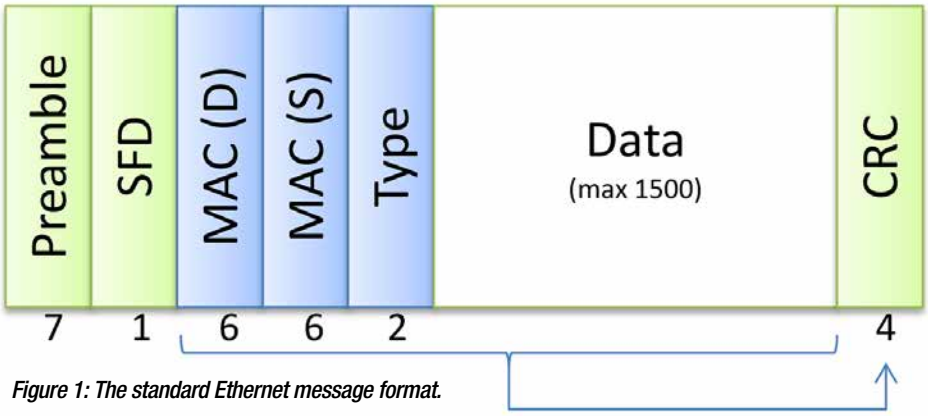


Figure 1: The standard Ethernet message format.

- Transmission of the first fragment of a message. The SMD has value 0xE6, 0x4C, 0x7F or 0xB3

A different message format is used for the continuation fragments (2..n-1, if any) of a message, and the last fragment. This requires some additional administration, so the receiver knows how to recognize what it receives. Additionally, it also allows the receiver to detect errors (such as a missing fragment). The SMD-Cx has value 0x61, 0x52, 0x9E or 0x2A (see below for an explanation).

The IEEE has decided to shorten the preamble by one byte; it is now only 6 bytes long. Next comes the SMD, followed by a new field called "fragment counter". This makes the initial fields (preamble, SMD, fragment counter) again 8 bytes long.

Next comes the data, which is always at least 60 bytes (to satisfy Ethernet timing requirements). Finally we have the CRC field. As usual, the CRC field (in 802.3br renamed to "mCRC") is calculated over all bytes following the first 8 bytes. Note that the SMD-Sx, SMD-Cx, and the fragment counter, are not covered by the mCRC; therefore additional measures are necessary to detect any errors in these fields.

The least significant 16 bits of the mCRC are inverted just before transmission. However, for the last fragment, the original CRC is used, and the last 16 bits are not inverted. This difference allows the receiver to detect that the last fragment has been received.

Backwards compatibility

For any new extension to Ethernet, there is always the question: is it interoperable with older Ethernet equipment? The IEEE has always striven to remain backwards compatible as much as possible. This policy has undoubtedly been fundamental to the popularity of Ethernet, an there is thus also backwards compatibility with equipment that doesn't support frame preemption (read: almost all Ethernet-devices in the world today).

When two devices do not both support frame preemption, communication errors result. Due to the changed implementation of the message header, and the changed CRC, a receiver would not accept these messages as being valid (and just discard them).

Therefore, when frame preemption is intended to be used, two devices must negotiate this with each other. This is done via a different mechanism than used for auto-negotiation. Here, two specially crafted Ethernet message are used, called a "Verify" and a "Respond" message.

A device that wants to send frame preempted messages first sends a "Verify" message to the other device (at the other end of the cable). When this device sends a "Respond" message back, it states that it also supports frame preemption, and from that moment on it may be used.

Fragment Indication

The most difficult part in frame preemption algorithm is the error handling; any fragment can be lost while 'in transmission' on the cable. It must be assured that this is always properly detected.

The receiving device must have some intelligence in recognizing the fragments, as they must be concatenated in the right order.

In order to detect this, each fragment is given a "Fragment Counter" (2 bits in size). Following the start fragment (S), the next fragment gets value 0, subsequent fragments increment this counter modulo 4: S,0,1,2,3,0,1,2,3,0,1… etc.

When the receiving device notices the wrong sequence, for example S,0,1,2,0,1,2,3… a fragment has gone missing (3) in this case. Even two fragment may be missed, for example S,0,1,0,1… is still seen as wrong. In case three subsequent fragments are missed this is still detected: S, 0,0,1,2,…

Should 4 subsequent fragments be missed, this is no longer detectable with the fragment counter (S,0,1…), because the receiver does not know the total number of fragments. The only way to detect the missing fragments is that the CRC of the reconstructed message does not match.

When one (or more) fragment(s) are lost, it is not possible to reconstruct the original message. The receiver will wait for the first fragment of the next message. Higher-level protocols (like TCP) will detect the missing message and repair it.

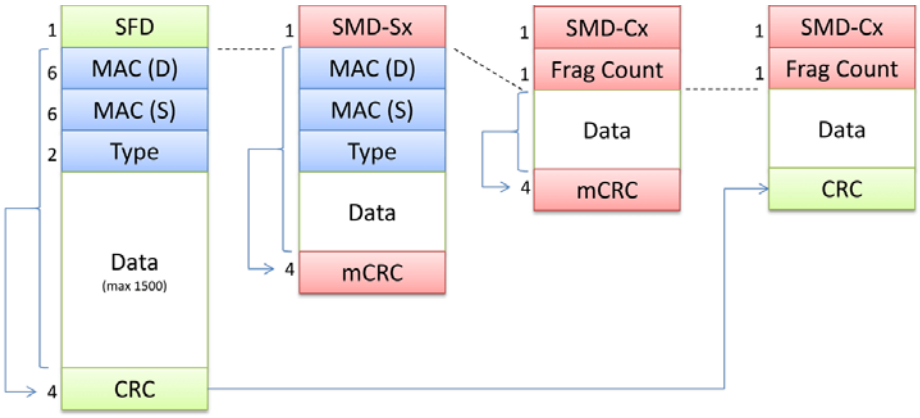


Figure 2: The different three types of fragmented messages as compared to the original Ethernet message format (left). Green and blue fields retain their original value; red fields have different values. The "data" field is not shown to size.

One byte for two bits?

Even though the fragment counter has only 4 possible values, in the Ethernet message it occupies 8 bits. The four possible values are not sent as-is (00,01,10,11) but as 8-bit values 0xE6, 0x4C, 0x7F and 0xB3, respectively. Why is this done? Remember that the fragment count field is not covered by the mCRC. When using only 2 bits, a bit error in transmission could therefore (unknowingly to us) change one valid fragment counter value (say, 01) into another valid bit pattern (11 or 00). This is of course very dangerous.

The 4 values 0xE6, 0x4C, 0x7F and 0xB3 are chosen because of their mathematical property called "Hamming Distance 4". Changing any of the 8 bits never produces one of the other three values. For example when taking value 0xE6: changing one bit produces either 0x66, 0xA6, 0xC6, 0xF6, 0xEE, 0xE2, 0xE4 or 0xE7, none of which is one of the other three. Even 2 or 3 faulty bits never produces one of the other values. Only when at least 4 bits of any value are inverted one of the listed numbers can result. And even then there is only a ¼ chance that the value for the expected fragment count is produced.

The first fragment

The first fragment of a message is indicated by a special value in the SMD field: a "SMD Start" value SMD-S. When the receiver sees an SMD-S, it knows that it can discard any previously received fragments (if present) and start the assembly of fragments for a new message.

Actually there are four values defined for SMD-S: SMD-S0 (value 0xE6), SMD-S1 (0x4C), SMD-S2 (0x7F) and SMD-S3 (0xB3), values again with HD4. The sender cycles through these four values for every new first fragment. The reason is that the receiver can unambiguously detect that a new first fragment (for a new message) is received.

If a fragment is received which does not contain an SMD-S0, S1, S2 or S3 it is ignored.

Continuation fragments

Continuation fragments of a message are sent according the new message format (figure 2). The SMD field contains a so-called "SMD Continuation" value SMD-C.

Which SMD-C is used depends on the original SMD-S. When it was value SMD-S0, the continuation fragments contain use value SMD-C0; when it was an SMD-S1, the continuation fragments use an SMD-C1, etc. This assures that the receiver always knows to what network message the continuation fragment belongs. This is needed in case of a complete loss of a fragment.

Suppose that in normal circumstances the following fragments are transmitted: (1) SMD_S0, (2) SMD-C0 (first fragment), (3) SMD-C0 (2nd and last fragment), (4) SMD-S0, (5) SMD-C0 (first fragment), (6) SMD-C0 (second fragment), etc.

There are several different error scenarios.

(1) Suppose that message (3) is completely lost. The receiver now gets an SMD-S again, so it knows a new message is started without the previous message completely having been received. The two fragments are discarded. Ethernet proceeds with processing message (4) and beyond.

(2) Suppose that messages (3) and (4) are lost. The receiver gets two fragments, both with the same fragment counter. This is not allowed, all received fragments are discarded, processing continues with the next SMD-S in message (7) or later.

(3) Suppose that messages (3) and (4) and (5) are lost. The receiver gets two fragments with succeeding fragment counters 0 and 1. This is as it is supposed to be! But it is still wrong, as fragments from two different messages are now concatenated.

In order to detect scenario 3, Ethernet gives the second group of fragments a different SMD_S value, i.e. SMD_S1 in our example. On the line we would then see: (1) SMD_S0, (2) SMD-C0 (first fragment), (3) SMD-C0 (2nd and last fragment), (4) SMD-S1, (5) SMD-C1 (first fragment), (6) SMD-C1 (second fragment), etc.

If messages (3) and (4) and (5) are now lost, the receiver gets an SMD-C0 (first fragment) followed by an SMD-C1 (second fragment), so now sees that they belong to two different messages (C0 and C1). The error is now detected.

The last fragment

The number of fragments is not known to the receiver, so how does it know that it has received the last fragment? The fragment counter cannot be used for it, it just counts 0,1,2,3,0,1,2,3… etc. The last fragment is indicated by the 16 least-significant bits of the CRC not being inverted. The receiver can detect this, and so knows it has received all fragments.

Fragment assembly

The receiver concatenates all received fragments as long as the fragment counter (in the message) corresponds to the expected fragment counter. If there is a mismatch, the most likely reason is that a fragment has been lost while in transit, usually caused by data corruption. The receiver then simply discards all received fragments, and starts waiting for a new first fragment (with an SMD-Sx).

With the original CRC in the last fragment, it can also be checked that the concatenation of all received fragments is identical to the original message. If not, the message is discarded.

Rob Hulsebos has been in industrial networks and cybersecurity for more than 30 years.

View Complete Article

New standard for PROFINET cables on robots

Ethernet cables have to cope with a lot when used in industrial robots. However, common Ethernet cables have usually been unable to cope with the challenge of horizontal linear movements combined with torsion. A new ETHERLINE ROBOT PN Cat.5e now complies with the type R standard for PROFINET cables on robots.

ROBOTS ARE GAINING GROUND IN AUTOMATED manufacturing processes and the number of industrial robots is constantly growing.

Today, robots are a fixed part of a modern factory's symbol. For a long time, robots have been able to do more than just monotonous movements. Thanks to their connection to the data network, they also allow access that is necessary for monitoring processes or remote maintenance, for example.

Feedback loop communication

Industrial protocols such as PROFIBUS and PROFINET are used to ensure seamless feedback loop data communication between the sensors on the robot arm, the robot system/control system and their connection to the control level. Flexible ETHERLINE® data cables provide the cabling that is necessary for network communication.

However, the robot arms' rapid movement sequences in a three-dimensional space often cause a significant mechanical load for the cabling from when the robot is commissioned right up to the final completed cycle.

This puts Ethernet data cables to the test: they are some of the most technically sophisticated cables, with their twisted pairs of cores, double shielding and transmission parameters that are critical for successful data communication.

In many cases, robot application designers must choose between data cables that are designed for linear, horizontal travel paths – typically used in cable chains – and data cables that are designed for torsional movement sequences. The main reason is that the cable types have a different interior structure. Lay lengths within the core pairs must be strictly adhered to and matched to one another. Core pairs next to each other must not obstruct each other and interference signals must be prevented.

While relatively short lay lengths are preferred for cables for horizontal travel distances to achieve lower bending radii in the cable chain, long travel lengths are a priority for torsion cables. The problem is that, in their movement sequence, robot applications combine horizontal linear movements with torsional load. A large number of conventional Ethernet cables have not been able to properly cope with this combined challenge.

SOURCE: LAPP

Sophisticated cable design

The challenge when creating a sophisticated cable design has been the lack of standardised industrial standards for robot-compliant Ethernet data cables. This resulted in a wide range of incompatible and proprietary understandings of what "robot suitability" means for Ethernet cables on the market. The PROFINET user organisation responded to this situation and worked closely with AIDA (the Automation Initiative for German Motorists) to come up with the necessary specifications.

After exchanging ideas with leading companies in the industrial cabling field, the stringent PROFINET type R data cable specifications were created. Well-known manufacturers were not the only ones involved in the process of developing the new guidelines: opinions and suggestions from users, for example from the automotive industry, were also taken into account.

The new "type R" describes two-pair Cat.5e industrial data cables, which must withstand numerous electrical and mechanical requirements and provide longevity when used in industrial robots. The latest version of the "Cabling and Interconnection Guideline", Version 4.11 not only includes "type A" (fixed installation), "type B" (flexible installations) and "type C" (cable chain and special applications) but also includes "type R" for the first time.

But what makes a data cable a PROFINET-compliant type R robot cable? The mechanical requirements are at the top of the list. And there are not just a few: A type R-compliant cable must be able to endure all of these tests before it is ranked as a robot-compliant cable according to PROFINET: 5 million vertical torsion cycles at ±180° per metre, 5 million cycles in the horizontal cable chain at accelerations of up to 10 m/s² and speeds of 3 m/s over a travel distance of 5 m, an additional 1 million bends in the alternating bending test according to EN 50396 at a bending radius of just 7x outer diameter.

LAPP has developed the new ETHERLINE® ROBOT PN Cat.5e for this field. It is suitable for industrial data cabling within or on a robot and can be used in cable assemblies or laid freely. It offers a high load capacity, longevity and data communication reliability with data rates of up to 100 Mbit/s. Even challenging welding robot applications are no issue for LAPP's all-rounder. The LAPP developers placed particular emphasis on choosing the right cable design.

Thanks to the filling elements and reliable materials, such as the robust PUR outer sheath, the ETHERLINE® ROBOT PN Cat.5e not only covers the mechanical load requirements, but also complies with important certifications and standards such as UL compliance as per AWM Recognized. This enables it to be exported to the North American market.

The new all-rounder has been put through its paces in the high-tech LAPP test centre, which has state-of-the-art test equipment and devices and has many years of experience handling data cables. For example, it continuously monitors the electrical transmission parameters according to IEC 61156-6 during the lengthy cable chain test procedure. Here, highly flexible ETHERLINE® data cables are tested fully automatically at defined intervals – usually every 20,000 to 50,000 cycles – and changes are identified in over 20 critical transmission parameters.

Particularly in the test phase of prototypes, this makes it possible to fully trace design weaknesses, which are eradicated and improved in the next stage of development. At the end of the test phase, the robot cable did not have any damage to the outer sheath and no adverse effects were documented in the transmission-critical electrical parameters.

*Technical article by **Lapp**.*

Visit Website

TSN: evolving for continuous improvement of Ethernet

Arno Stock, Business Development Manager at CC-Link Partner Association (CLPA) member Renesas Electronics, looks at what Time-Sensitive Networking (TSN) can offer and the latest achievements that are shaping the future of industrial Ethernet.

TIME-SENSITIVE NETWORKING (TSN) IS preparing industrial Ethernet to support tomorrow's industrial communications needs by providing innovative, highly beneficial features. Companies are well aware of this potential, and a lot is happening to fully realise the TSN-driven Connected Industries of the Future.

TSN is an extremely promising technology that will allow industrial Ethernet to reach new levels. Operating at Layer 2 of the Open Systems Interconnection (OSI) model, it enhances standard Ethernet as we know it by making it deterministic by design. This characteristic, in turn, will benefit end users in a variety of industries by offering the ability to merge different types of data traffic, leading to more flexible and collaborative environments. At the same time, this creates simplified, more economical network architectures as well as unified hardware and software systems.

Therefore, the crucial role of TSN in the Connected Industries of the Future is clear. This technology is the precondition needed to support key Industry 4.0 applications and trends, such as Edge and Cloud computing.

A smooth transition

In addition to these most obvious advantages, an instrumental feature of TSN is its continuity with existing network technology. In effect, while it offers unprecedented capabilities, it does so by evolving conventional Ethernet rather than by substantially disrupting the status quo. As a result, businesses can seamlessly transition towards TSN-compatible industrial Ethernet systems.

This also means that TSN is compatible with legacy standards. Furthermore, it can be combined with additional solutions that are already available for conventional industrial Ethernet, such as gigabit bandwidth, which is key to support ever-increasing data throughput. In addition, it can accommodate the higher number of network devices and nodes resulting from converged architectures.

Additional advantages of mixing TSN and gigabit Ethernet include the ability to shorten cycle times, increase the accuracy and precision of control loops as well as strengthening the ability of a network to transfer various types of data, such as video.

Such a solution can also reduce the complexity of distributed control systems, as it is possible to reliably move more functions to a single controller, also making the intended applications more robust as well as easier to set up and maintain.

End users are ready for TSN

The multiple benefits of TSN are evident to machine builders and end users. In particular, Renesas is noticing a high level of interest from its customers, who are aware the technology will be a must in the years to come. A key aspect that is extremely appealing to most of them is the standardisation/simplification of protocols, enabling the connection of all parts within an enterprise.

In order to successfully implement TSN, it is necessary to use a network technology with higher-level protocols, as these are needed to complete the OSI reference model and support TSN applications. An example is the open industrial Ethernet CC-Link IE TSN. In addition, companies require suitable hardware that can utilise this Layer 2 technology, such as Renesas' R-IN32M4-CL3 large scale integration (LSI) that leverages CC-Link IE TSN. Driver-level support is also important, as real-time TSN-compatible systems require a close interaction between low-level driver software and hardware equipment.

To address these aspects with leading solutions, automation vendors need to team up to deliver devices with TSN capabilities that meet customers' expectations and needs. Being part of an extensive partnership network, such as the CLPA, is thus extremely beneficial, as it offers a forum where solution providers come together to drive the development and consolidation of key automation products.

A look at the future of industrial communications

A number of major milestones have been reached to support the use of TSN. In particular, the IEEE 802.1 standards defining the technology are now complete and accessible. Also, the first network solutions have been released to the market, namely CC-Link IE TSN – the first open Ethernet that combines gigabit bandwidth and TSN capabilities.

Finally, the first prototypes and complete

SOURCE: RENESAS

Arno Stock, Business Development Manager, Renesas Electronics

products have already appeared, with actual devices available and ready for use now. More testbeds are also ongoing or planned to take place in the short term. These contribute to making the technology more mature and support its large-scale implementation.

The sector is working towards the finalisation of IEEE profiles, particularly for industrial automation as well as the development of new applications for wider use, not confined solely to industrial settings. To support the global adoption of TSN, it will soon be essential to set up unified conformance testing to make sure that different solutions are interoperable, hence truly leveraging the full potential of TSN. Open technologies, such as CC-Link IE TSN, are therefore likely to be favoured.

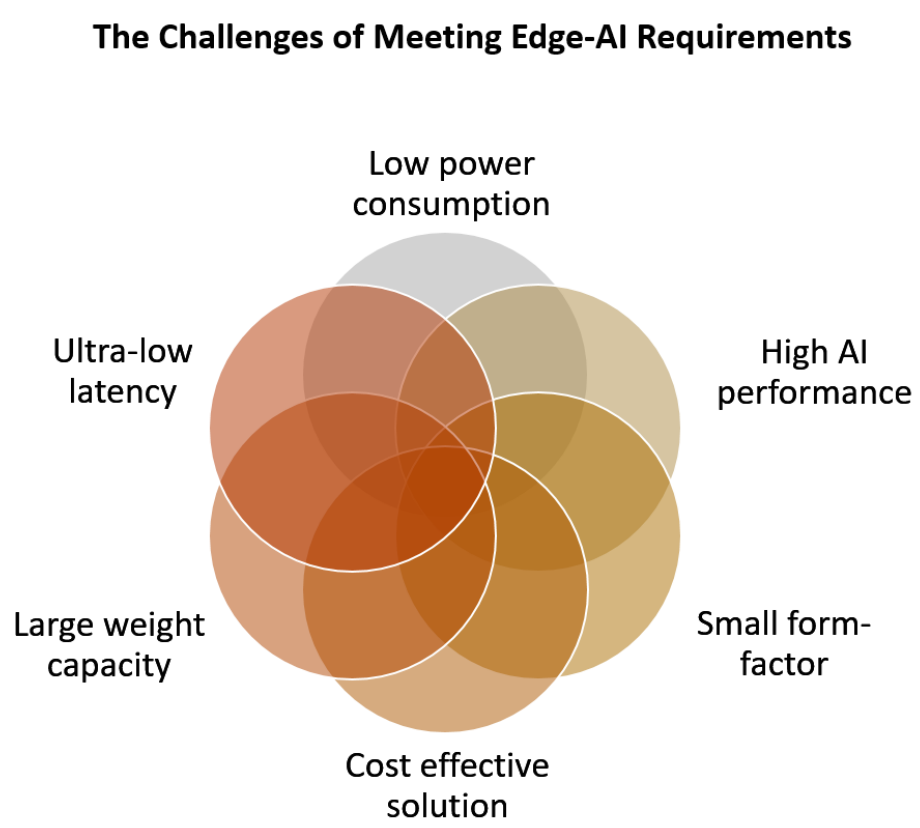
The transition towards TSN will be particularly exciting, as it is a natural evolution of Ethernet that will support its continuous improvement. Ultimately, we will be able to benefit from more and more building blocks that will open up new functions and higher performance while supporting existing, still functioning systems.

*Technical article by **CLPA**.*

Visit Website

Transforming industries and challenges with Edge-AI

Analog compute-in-memory takes advantage of high-density flash memory to enable compact, single chip processor designs. It dramatically reduces power consumption and, by reducing the barriers of cost, size, power and performance, companies can truly rethink what's possible with AI.



SOURCE: BECKHOFF

New AI technology companies are removing hurdles with implementing artificial intelligence in industrial automation applications by providing a complete inference solution – high performance and low-power hardware in a small form factor, along with ready-to-deploy DL algorithms.

TODAY COMPANIES HAVE ONLY SCRATCHED THE surface of what AI is capable of at the edge. The full potential of AI is being constrained by a number of different factors. One challenge has been the limited compute capabilities of edge devices, at least until recently.

Additionally, edge inference, what enables a neural network to perform different functions when encountering real-world data, has been a major technical challenge. The good news is that advancements in edge-AI processing are working to solve these challenges and open up a new world of AI-powered possibilities.

Let's take a look at the top five industries that will be transformed by edge-AI.

Industrial Automation

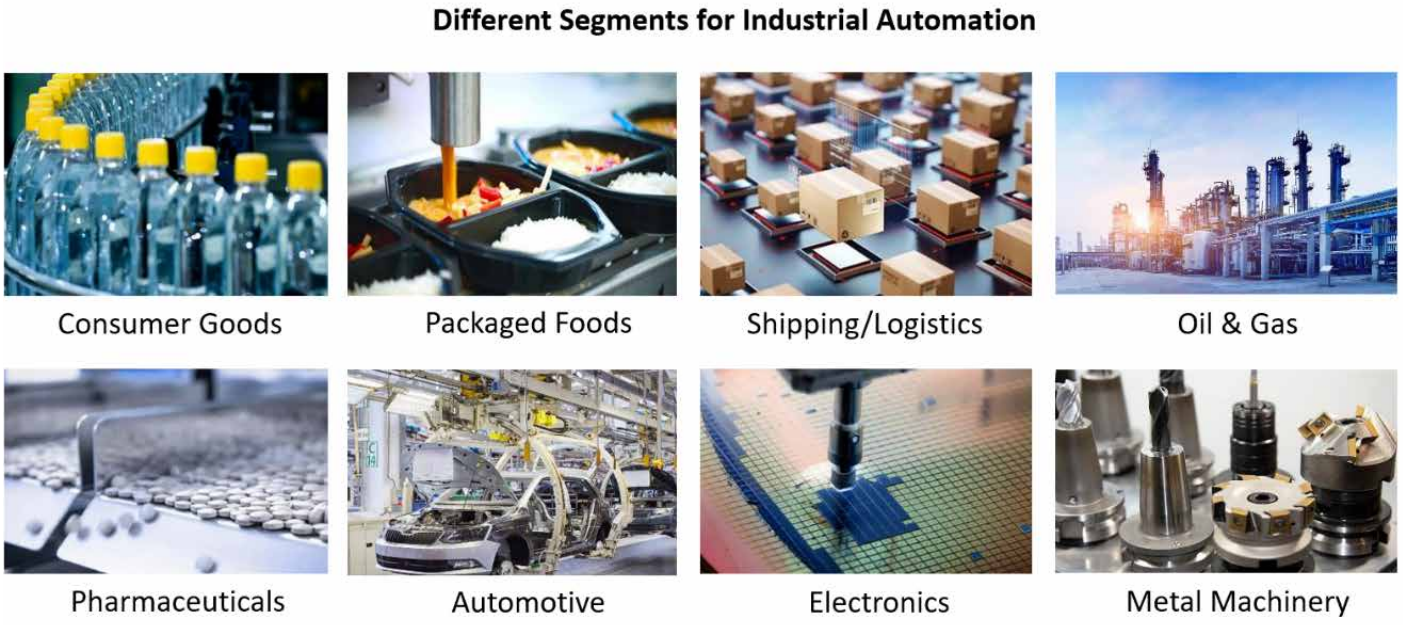
Over the past few decades, factories have become more and more automated, bringing efficiency to new heights and driving down the costs of the goods that consumers use every day. While factories have already deployed computer vision (CV) to optimize production lines, factories can now take advantage of new edge-AI processing technologies to combine the power of CV with AI, especially deep learning (DL).

This will significantly improve factory throughput and quality, two essential metrics for an efficient production line. As factories become more automated with interactive human-to-machine processes, AI is also being used to deliver a new level of workplace safety. Just imagine a food processing factory with AI-powered collaborative robots to inspect cereal boxes on the production line in real time.

Deploying AI solutions for industrial automation is a challenge. Automation engineers in the manufacturing field don't have the expertise to develop effective AI/DL algorithms. However, several AI technology companies are removing these hurdles by providing a complete inference solution – high performance and low-power hardware in a small form factor, along with ready-to-deploy DL algorithms. We'll see more investment being poured into this area as more factories want to take advantage of powerful edge-AI processing to improve efficiency and workplace safety.

Aerospace/Drones

Edge-AI processing is also enabling many different types of physical surveillance applications for drones. Drones are being outfitted with ultra-high definition cameras that can be used for many CV applications, including monitoring agricultural yields, inspecting critical infrastructure such as



power lines, cell phone towers, bridges and wind farms, inspecting fire damage, examining coastline erosion, and much more. These tasks often require running complex AI networks locally to provide immediate and relevant information to the control station, so it's important to have powerful AI processors that are also extremely power-efficient.

Smart Home

AI voice applications have already reshaped the home as we know it, bringing intelligence to all sorts of devices from speakers to TVs and refrigerators. The next smart home revolution will be powered by vision applications. One of the most interesting AI capabilities is human pose estimation – when a camera sensor can detect and track movement of your body parts – which can be used for a wide variety of applications.

Take AR/VR gaming, for example, where AI could track gamers' movements from head to toe and then instantly render those movements as their character on the screen for a truly immersive gaming experience. AR/VR requires instantly processing information from cameras and LiDAR, time-of-flight (ToF), and audio sensors, so edge-AI processing is a must.

Smart fitness is another exciting use case. There are already some popular fitness applications that use pose estimation to monitor users' movements and then provide corrections and recommendations. Instead of going to the gym, consumers can learn from an AI trainer right in their living room.

We'll also see AI-enabled robots become increasingly popular in the smart home. The idea of smart home robots was popularized in the Jetsons TV series with the robot maid Rosie which could talk, clean and take care of other household tasks. That vision for a truly smart robot is getting closer to reality. In the coming years we'll see robotic vacuums that see and avoid obstacles with AI to clean faster and more efficiently, unlike the ones of the past that would wander around the home aimlessly. Autonomous lawn mowers are another type of CV robot that will become mainstream in the years ahead.

Data Centers

When you think of data centers you might not think about edge-AI computing. However, edge-AI processing can enable data centers to run neural networks at scale across all of their data streams. Companies can use AI processors to support a broad range of neural networks, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and dense networks.

This makes it possible to process high resolution data accurately across neural networks to perform inference across live data. Since neural network inference is compute-intensive and power-hungry, traditionally it has required costly hardware, advanced cooling infrastructure, and kilowatts of power. New technologies have made it possible for processors to be extremely powerful and power-efficient, while also being scalable so they can easily fit into companies' existing infrastructure.

Physical Security

Having security cameras can make a big difference in catching criminals and keeping people safe. However, there has been a lot of debate about cameras providing safety monitoring.

AI seems to be adding to this anxiety, even though it can actually be used to better protect people's privacy – if AI is applied appropriately. In current systems, cameras capture images of people and objects and send that information to a command center for visual analysis; this is where the uneasiness comes with being monitored constantly. A better alternative is to have cameras that use trained AI algorithms to detect specific sequences – accidents, crimes, or other events – and only send the footage of potential security incidents for analysis.

This approach delivers the safety and security the public desires while providing the privacy all of us expect. Cameras today are already equipped with computer vision techniques. To reach the next level of safety and privacy, high performance edge-AI capabilities in the camera will be required for traffic monitoring, incident detection, facial recognition, and many more applications to come in the future.

AI processing at the edge requires silicon that can meet demanding requirements for size, performance, and power consumption. A new approach – analog compute in flash memory – promises to solve these challenges and make it possible to widely deploy powerful edge-AI. Digital AI processors are extremely expensive to deploy and are very complex to develop, which has restricted innovation to the biggest technology companies.

Analog compute-in-memory takes advantage of high-density flash memory to enable compact, single chip processor designs. Perhaps even more importantly, analog compute-in-memory dramatically reduces power consumption, making it 10X more efficient than digital systems while still enabling extremely high performance computing. By reducing the barriers of cost, size, power, and performance, companies can truly rethink what's possible with AI.

David Kuo, Sr. Director Business Development and Product Marketing, ***Mythic.***

Visit Website

Variation for ix Industrial connector

Right angle plug variation to the IEC Standard Compliant (IEC 61076-3-124) ix industrial connector.

HIROSE ELECTRIC has added a right angle plug as a new variation to the IEC Standard Compliant (IEC 61076-3-124) Industrial Ethernet Interface ix Industrial Connector Lineup. The ix Industrial connector was released in 2017 in collaboration with German-based development partner, Harting Technology Group, and has been used in a variety of industrial markets such as Factory Automation, robotics and machine vision.

The ix Industrial has been adopted by several large industrial application manufacturers for Ethernet connectivity, due to its space-saving and durable design. Hirose has released the new right angle plug variation in response to market needs for space-saving routing, free of stress on the connector resulting from cable bending when space on the interface connection side of the device is limited.

SOURCE: HIROSE

New right angle plug variation released in response to market needs for space-saving solution.

While straight plugs are already a part of the ix Industrial lineup, the right angle type allows the cable to be pulled out at a right angle in respect to the mating axis, reducing the height of the equipment interface connection and making it easier to route the cable in tight spaces. The ix Industrial lineup provides more wiring flexibility, with two cable assembly options of solder and IDC, 2 keying options, and both downward cabling and upward cabling right angle plug variations for use based on the application.

Features include: IEC standard compliant (IEC 61076-3-124); ix Industrial offers a reduced size of 75% compared to conventional RJ-45 modular solutions. Receptacles allow 10mm parallel pitch mounting and HIROSE's unique shell design withstands shock and vibration. Connector offers 5,000 mating cycles to ensure excellent durability.

HIROSE Electric

Visit Website

First industrial 5G router

Scalance router connects local industrial applications to public 5G, 4G, and 3G mobile wireless networks.

The Scalance MUM856-1, the first industrial 5G router from Siemens, is available now. The device connects local industrial applications to public 5G, 4G (LTE), and 3G (UMTS) mobile wireless networks. The router can be used to remotely monitor and service plants, machines, control elements, and other industrial devices via a public 5G network – flexibly and with high data rates.

Demand for this type of solution is growing in industry. In addition, the device can be integrated into private 5G networks. The Scalance MUM856-1 therefore supports future-oriented applications such as mobile robots in manufacturing, autonomous vehicles in logistics or augmented reality applications for service technicians. Thanks to a robust IP65 housing, the router can also be used outside the control cabinet, for example under harsh conditions in production or in outdoor facilities in the water industry.

To ensure the powerful connection of Ethernet-based subnetworks and automation devices, the Scalance MUM856-1 supports Release 15 of the 5G standard. The device offers high bandwidths of up to 1000 Mbps for the downlink and up to 500 Mbps for the uplink – providing high data rates for data-intensive applications such as the remote implementation of firmware updates. Thanks to IPv6 support, the devices can also be implemented in modern communication networks.

SOURCE: SIEMENS

The Scalance MUM856-1 supports Release 15 of the 5G standard.

Various security functions are included in order to monitor data traffic and protect against unauthorized access: for example, an integrated firewall as well as authentication of communication devices and encryption of data transmission via VPN.

Siemens

Visit Website

Long-reach Industrial Ethernet offerings

Goal is to achieve last mile connectivity in process, factory and building automation.

Analog Devices expanded its ADI Chronous Industrial Ethernet portfolio with solutions that bring long-reach Ethernet connectivity from the edge to the cloud and enable real-time configurability, lower energy consumption, and increased asset utilization.

The new ADI Chronous offerings support the 10BASE-T1L physical layer Ethernet standard allowing new data streams from edge nodes in remote and hazardous locations across process and building facilities. This previously unavailable data can now be seamlessly accessed across the network and used to assess factors such as asset health, raw material usage, and process parameters enabling cleaner manufacturing.

The newest ADI Chronous offerings enable customers to reduce energy consumption in buildings as well as their overall carbon footprint through improved control of building parameters. The ADI Chronous ADIN1100 and ADIN1110 Industrial Ethernet solutions can transfer data over 1.7 kilometers or more than a mile (a significant increase from previous Ethernet standards) through a single twisted pair of Ethernet cables, which helps reduce space, weight, and cost. These cables are lighter and more malleable than traditional Ethernet cables, and can support reuse of existing cabling infrastructure, reducing commissioning cost and complexity.

SOURCE: ADI

New offerings support 10BASE-T1L physical layer Ethernet standard allowing new data streams from edge nodes.

The new Industrial Ethernet solutions are offered in two flexible options: MAC PHY and PHY. The MAC PHY (ADIN1110) enables the industry's lowest power systems, which simplifies retrofitting for Ethernet in field sensors or actuators and preserves existing investment in software and processor technology.

Analog Devices

Visit Website

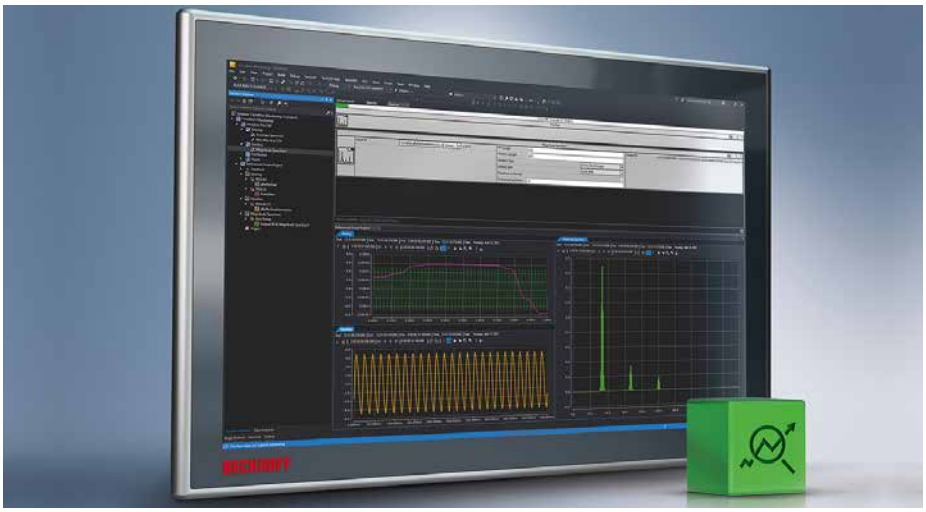
Frequency analysis without programming

TwinCAT Analytics expanded with easy-to-configure condition monitoring functions.

TwinCAT Analytics software from Beckhoff offers a complete workflow from acquisition of data through to its storage and analysis to dashboards for continuous machine monitoring.

Traditional condition monitoring algorithms are now also available in TwinCAT Analytics using simple configuration with no programming requirements. This addition optimizes both the standard workflow and spontaneous measurements, such as during machine commissioning or service.

Beckhoff presented the TwinCAT Condition Monitoring library as early as 2010. This library includes numerous algorithms that support Moment Coefficients, Discrete Classification and Vibration Assessment according to the ISO standard, in addition to functions such as Magnitude Spectrum, Envelope Spectrum, Zoom FFT, Power Cepstrum and multiple RMS calculations. All functions are available as standard PLC function blocks, which means that condition monitoring functions, for example, for permanent monitoring of bearings or gearboxes, integrate directly and easily into the machine controller.



SOURCE: BECKHOFF

Machine operators and service engineers have a solution with the TwinCAT Analytics Service Tool.

In the past, commissioning staff and service engineers had to invest significant time and effort to calculate a frequency spectrum that would allow selective inspection of machine components, for example. This is precisely where TwinCAT Analytics can help by reducing a programming task to a simple configuration task. All condition monitoring algorithms are available in the toolbox and can be dragged to the Analytics editor and configured.

Beckhoff

Visit Website

Flowmeter integrates cloud connection

Promag W 800 flowmeter provides battery-powered flow measurement with integrated cloud connection.

The extraction and transport of water often takes place in remote areas where there is no possibility to supply measuring instruments with power or to transmit data via wired connectivity. It is precisely for such applications that Endress+Hauser has developed the innovative Promag W 800 flowmeter with battery-powered operation. It provides maintenance-free operation for up to 15 years, as well as worldwide secure data transfer via cellular radio.

The Promag W 800 electromagnetic flowmeter ensures not only reliable monitoring of water supply networks, but also efficient and time-saving maintenance. Leaks can be located reliably, and non-billable water losses (non-revenue water) can be avoided.

Promag W 800 is suitable for measuring lake, river, spring, or groundwater flows for drinking and process water, as well as distribution networks subject to fiscal metering. Consumption measurements when irrigating the frequently agricultural areas in climatic dry regions are also important.

Promag W 800 has a backlit display, making it quick and easy to read measured values. Endress+Hauser's SmartBlue app can be used to interact with the flowmeter for operations, and to provide more comprehensive data retrieval on site. It is also available with various drinking water approvals such as KTW/W270, WRAS BS6920, ACS, or NSF 61.

SOURCE: ENDRESS & HAUSER

Promag W 800 electromagnetic flowmeter ensures reliable monitoring of water supply networks and maintenance.

For future-oriented communication and connectivity, the Proline 800 transmitter includes everything needed within its minimal footprint: measuring electronics, batteries, data logger, and a cellular radio module to send and receive data worldwide via LTE Cat M1, LTE Cat NB1, or EGPRS.

Endress & Hauser

Learn More

ix Industrial new PROFINET interface

A 70% smaller Ethernet interface offers miniaturisation potential for PROFINET users.

The new PNO guideline Profinet Cabling and Interconnection Technology - Guideline for PROFINET Version 5.0 specifies the ix Industrial mating face as a new standard for Ethernet applications.

The guideline was officially published on June 29, 2021, and provides PROFINET users with a reliable set of rules for industrial cabling. Thanks to the ix Industrial® PROFINET are benefitting from an Ethernet interface that is significantly more compact and more robust than previous RJ45 solutions, a path to the miniaturised future.

On June 29, 2021, the PROFINET User Organization (PNO) published the PROFINET Cabling and Interconnection Technology - Guideline for PROFINET Version 5.0 , a new set of rules for PROFINET-compliant cabling in industrial equipment, systems, and plants. The ix Industrial mating face for Ethernet transmission represents a new component in SPC "Specific Passive Components".

Consequently, manufacturers of PROFINET-compliant devices are now able to develop more compact devices on a secure and reliable basis and thereby save valuable installation space in the control cabinet. Given the 70% smaller ix Industrial device socket compared to known RJ45 connections, the number of ports can be doubled for the same device size or, conversely, a device can be designed that is significantly more compact.

SOURCE: HARTING

ix Industrial® - 70% smaller in device. Certified according to the new PROFINET directive since June 29, 2021.

The HARTING ix Industrial interface offers device manufacturers and users a high-performance, reliable, and industrial-grade connector.

HARTING

Visit Website

CAN communication via Wi-Fi/Bluetooth

The Anybus Wireless Bolt CAN features CAN-based communication to the host equipment.

The new Anybus Wireless Bolt for CAN enables CAN-based, heavy-duty machinery and applications to ransfer CAN data over a robust wireless link. Wireless communication is established either over a fast Wi-Fi connection or a reliable Bluetooth link. The CAN data is transported over a TCP/IP link which enables other standard Wi-Fi infrastructure to also connect to the wireless link if desired.

Wireless access to J1939 CAN-based vehicle data A typical use case is wireless access to CAN data from an industrial vehicle, such as a bulk material transport truck. For example, with the Anybus Wireless Bolt CAN, J1939 CAN data is easily communicated to a handheld tablet which gives the operator full control and visibility of the ongoing bulk material filling process.

Anybus Wireless Bolt CAN is fully transparent when it comes to transporting CAN data, meaning that it works with any CAN-based protocol, including CANopen. This opens the possibility to create mobile automation islands in any manufacturing process – the Anybus Wireless Bolt CAN will bridge the CANopen line wirelessly.

In addition to the new Anybus Wireless Bolt CAN, the Wireless Bolt product family includes other versions which can connect to the host equipment using serial and industrial Ethernet connectivity. On the wireless side of the Wireless Bolt, the Wi-Fi and Bluetooth options were recently complemented with a version that supports the new LTE standards NB-IoT and CAT-M1, targeting IoT applications.

SOURCE: HMS NETWORKS

New products offer a wide range of wireless connectivity options for industrial networks and IoT applications.

Use cases vary from warehouse installations and AGVs to manufacturing of food, underground mining or rough outdoor applications.

HMS Networks

Visit Website

Industrial safety with HMI tablets

Unique way for operators to use modern tablet interfaces with industrial machinery and equipment.

IDEC Corporation has developed the HT3P Safety Commander to address a growing need for users who want to incorporate modern tablets into their industrial automation systems, but also need to include hardwired emergency stop (e-stop) and enabled functionality.

The Safety Commander makes it easy to hold a tablet securely in an industrial setting, for applications like machinery, robotics, automatic guided vehicles (AGVs), and production lines.

Traditionally, industrial operations personnel have needed to stand in front of fixed control panels, or use dedicated handheld touch panels or teaching pendants. Each method has its place, but many operators need more detailed human-machine interface (HMI) capabilities at their fingertips.

Industrial internet of things (IIoT) initiatives and capable HMI options are now prompting designers to select mobile tablets as visualization and control devices because of their convenience and productivity benefits.

Tablets offer high display resolutions, powerful computational abilities, extensive memory, Wi-Fi networking, and Bluetooth wireless connectivity—all at a low cost.

IDEC has developed a unique device for adding industrial-grade safety to typical tablets. The Safety Commander is a hand-held device with a slider and adjustable grippers to accommodate tablets ranging from 8- to 11-inch diagonal size.

SOURCE: IDEC

The LioN-X family is housed in a strong design for durability and reliability even in the harsh environments.

IDEC Corporation

Visit Website

Isolated system-monitoring solution

Size shrinks by 40% and tightens accuracy by 50x to improve system uptime for automated substations.

Maxim Integrated has expanded the MAXSafe Technology line with the MAX22530, an isolated, field-side self-powered 12-bit system monitor. Featuring 4 channels, the MAX22530 provides isolated system monitoring to improve accuracy 50x and to reduce solution size by 40 percent by integrating five components into a single IC.

Automation system designers continually seek ways to save board space, increase channel density and improve the accuracy of monitoring voltage and current inputs, so operators can monitor the system with finer precision and reduce system downtimes. The MAX22530 delivers a 50x improvement in monitoring measurement accuracy (from +/- 50 percent to just +/- 1 percent) compared to the standard linear optocoupler isolation solutions made from discretes.

It uses Maxim's isolation technology that combines a 12-bit ADC, a DC-DC converter, user-settable threshold detection levels and chip-level diagnostic capabilities. This combination enables 50x greater stability in current transfer ratio performance to achieve an ultra-stable sense resistor voltage. By achieving better measurement accuracy across four voltage and current inputs, it allows end users make better real-time decisions to improve performance and enhance productivity. The integration also allows a 250mm² solution size, which is 40% smaller that the 420mm² size for the closest competitive discrete solution.

SOURCE: MAXIM INTEGRATED

Design simplicity includes integrating five ICs into one 12-bit ADC to ease system design.

MAXSafe products combine integrated and isolated micropower DC-DC converters and communications lines.

Maxim Integrated

Learn More

Operator terminals, wider choices

Two new Graphic Operation Terminals are latest addition to Mitsubishi GOT2000 Series wide model lineup.

Mitsubishi Electric has launched two new Graphic Operation Terminals (GOTs), which come as the latest addition to its GOT2000 Series Wide Model lineup. The 12.1-inch widescreen models, which feature narrow bezels and come in frame colors of smart silver (GT2512-WXTSD) or cool black (GT2512-WXTBD), will help meet customers' needs for a wider screen to show more information in factory, process, utility and other automation applications.

These new widescreen GOTs are also ready to support remote connection in cases where user access may be restricted. Remote connection functions such as SoftGOT enable remote maintenance via access to the local GOT screen while operators can obtain live data using GOT Mobile.

New models also feature two Ethernet ports, facilitating the connection of Ethernet cables.

Antiviral protection sheets

In further enhancements to support safe-working practices, there are also new antibacterial, antiviral protection sheets as options for standard GT27 and GT25 GOTs in 12.1, 10.4 and 8.4 inch sizes. These sheets help reduce disinfection work by adopting "SIAA" certified sheets with anti-virus and anti-bacterial features. The sheets, which use RIKEN TECHNOS' RIKEGUARD, are proven to inactivate 99.99% of viruses and reduce bacterial growth to less than 1/100, with 10+ years of performance in typical environments. This product uses RIKEGUARD®, which is registered with SIAA.

SOURCE: MITSUBISHI

By using GOT Mobile, operators can monitor the screen from computers and tablets in a remote location.

Mitsubishi

Visit Website

Wireless add-on module for MXview

New module overcomes the Wi-Fi network management challenges in smart manufacturing.

Moxa has released the MXview Wireless add-on module for its MXview industrial network management software.

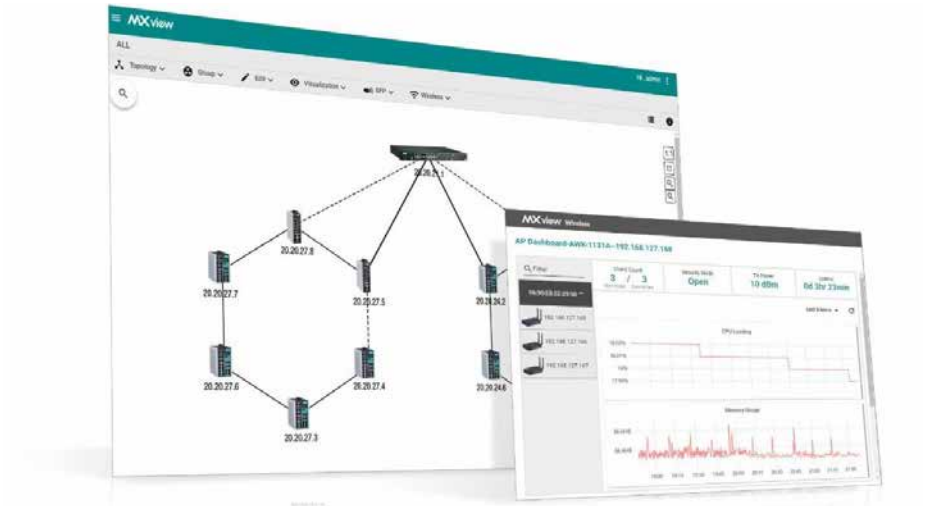
This software has helped customers from in different industries such as in power, intelligent transportation, and manufacturing. Today, with the rise of smart manufacturing, intelligent and reliable industrial network communication has become the cornerstone for nearly every smart application.

In response to the transformation of the industrial environment and increasing number of Wi-Fi applications, the new MXview Wireless add-on module fulfills the different requirements of both static and dynamic wireless applications in smart manufacturing. With reliable network communications as a foundation and real-time network management from a single pane of glass, business owners can focus on improving operational efficiency and achieving maximum system uptime.

Intelligent process control is a typical static wireless application in smart manufacturing where customers use Wi-Fi to establish the communication between the clients installed at production lines and the control center.

However, an unstable wireless connection might lead to wrong decision-making due to incomplete on-site information or dropped connections, affecting optimal production processes. It's often difficult to know the exact status of the Wi-Fi connection and fix issues immediately the moment they occur.

The MXview Wireless add-on module simplifies network management by allowing users to get detailed device information and performance indicator charts for individual AP and client devices from the device dashboard.



SOURCE: MOXA

MXview streamlines management by visualizing networks, helping non-IT staff increase network uptime.

Moxa

Visit Website

Secure remote access platform

Red Lion platform allows allows users to easily access, monitor and manage remote equipment

Red Lion's Secure Remote Access Platform, in partnership with MB connect line GmbH, is now available in United Kingdom, Ireland, Iceland, Norway, Sweden, Finland, and France. This next-generation remote access solution meets the most demanding security requirements of modern industrial applications.

The platform centralizes the management of routers, allowing users to quickly respond to and act on their most crucial assets from anywhere, at any time. The ability to remotely access, monitor and manage diverse equipment helps to lower operational costs and downtime by reducing site visits and dramatically improving response times.

Remote access routers and software provide flexible capability with unyielding security. The RLConnect24, a remote service portal, provides a simple centralized site to monitor and manage deployed assets and users. It provides data visualization, geographic mapping, data logging, and alarms based on operational or system-generated data. The RLDialUp client software enables operators to securely connect their PC to remote assets for tasks, just as if they were plugged into it locally. The routers are industrial-grade gateways offering optional LAN, WAN, serial, USB, Wi-Fi or 4G LTE connectivity.

Red Lion also launched the RA10, a compact industrial firewall, which provides OT-cybersecurity. This intelligent firewall can learn and self-configure to help secure older assets, avoid address conflicts, and/or logically isolate machines or groups of machines.

SOURCE: RED LION

The ability to remotely access, monitor and manage diverse equipment lowers operational costs and downtime.

Red Lion

Visit Website

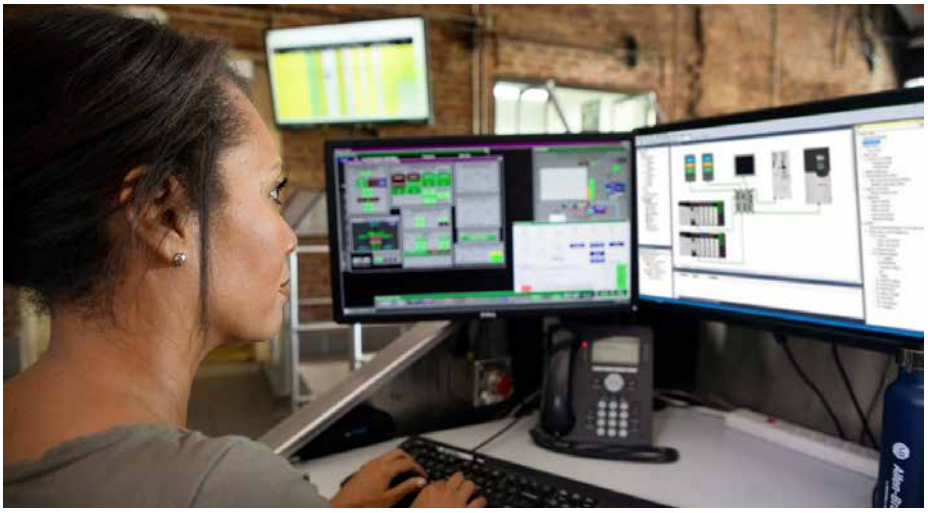
Enhanced FactoryTalk Linx software

Rockwell Automation increases productivity, security with enhanced FactoryTalk Linx software.

Engineers on the plant floor can be more productive with the latest release of FactoryTalk Linx software from Rockwell Automation. The latest release helps ease system recovery, increases upload and download speeds, and helps bring new devices online more efficiently. These enhancements free up time for plant engineers so they can focus on other priorities.

To help protect an organization, the latest FactoryTalk Linx software adds new security measures, including communications integrity/confidentiality, credential authentication, audit tracking, and configuration backup and restore. These extra layers of security can help reduce unplanned downtime due to security concerns and issues.

The release also adds backup and restore capabilities that allow users to save configuration settings. This helps improve administrator efficiency by eliminating the need to manually reconfigure the entire system during recovery. A reconstructed interface increases online performance for Studio 5000 and ControlFLASH Plus software with faster upload and download times. This increases efficiency by providing better performance for design tools and communication services.



SOURCE: ROCKWELL AUTOMATION

FactoryTalk Linx Gateway includes user-specified tag groups and access to Logix structure and array definitions.

Additionally, users bringing a new device online can now assign IP addresses based on a range or load a preset configuration. This helps improve productivity by bringing new machines and devices online more quickly.

The FactoryTalk Linx OPC UA Connector has been enhanced to provide access to more types of data. It can also now pick up data from a secondary server if a redundant server is shut down, which can improve system uptime and increase data access.

Rockwell Automation

Visit Website

RTI Connext connectivity software

RTI's Connext enables real-time connectivity and reliability between MAESTRO and AMR platforms.

634AI, aMushashiAI spin-out company, has selected RTI Connext DDS for real-time connectivity between its MAESTRO system, a Robot-as-a-Service software solution, and its Autonomous Mobile Robot (AMR) platforms. Connext allows for real-time connectivity between systems, supports fast, reliable communication, and enables 634AI to offer a central control tower that can streamline the management and control of AMR tasks on an industrial floor.

As the automation landscape advances rapidly, more suppliers are replacing forklifts with AMRs to complete a wide variety of tasks including navigating around factories and warehouses, and guiding autonomous cargo ships across oceans. However, AMRs tend to run unique or proprietary operating systems, navigation systems and fleet management systems.

634AI created its MAESTRO solution to give customers control and management of AMRs in one centralized AI-based system. RTI Connext DDS software supports fast, reliable communication between the MAESTRO system and AMRs with near-zero latency for critical data, while providing fuel-proof, real-time connectivity over Wi-Fi networks.

SOURCE: RTI

ConnectX allows for real-time connectivity between systems and supports fast, reliable communications.

Connext enables easy deployment, while allowing 634AI to avoid investing unnecessary time in building out robust, scalable connectivity systems. With Connext as the underlying communication framework, 634AI is able to add new messaging and devices seamlessly, with zero latency and minimal effort.

Real-Time Innovations

Learn More

Condition monitoring digital service

ABB launches condition monitoring digital service, tailor-made for predictive maintenance of conveyor belts.

ABB Ability Condition Monitoring for belts collects and tracks data from conveyor belts to provide real time information about the health of the equipment, enabling planned and timely maintenance.

The service helps mine operators to track speed, misalignment, damage, thickness and wear, slippage and temperature of conveyor belts in real time, and therefore anticipate maintenance, avoid unplanned downtime and improve belt reliability and lifetime.

Belt damage can cause significant production time loss in mines and processing plants with in-person inspections typically carried out to determine the condition of conveyor belts. T

he new ABB Ability Condition Monitoring for belts offers a complete overview of the assets' condition through continuous monitoring of belt health, generating alarms and warnings in the event of deterioration.

By moving from preventative to predictive maintenance, operators can avoid costly failures that occur between physical inspections and personnel can be removed from dangerous areas. The technology is based on sensors installed in strategic points of the conveyor belt equipment and is specifically designed to withstand harsh environments while monitoring asset health and condition.

SOURCE: ABB

Solution can work as a stand-alone option or can be integrated into any control system

ABB Ability Condition Monitoring for belts provides easy access to informative dashboards. Fault trend analysis, event alarms, data logs and reports can be monitored for single or multiple conveyors and by remote connection, SMS text message and email.

ABB

Visit Website

Digital twin for intralogistics

Using Digital Enterprise Portfolio for machine builders and plant operators along intralogistics value chain.

The intralogistics industry is facing new challenges. The Covid 19 pandemic has changed markets and requirements and the industry must cope with a rapidly growing e-commerce. Growing inventory turnover rates with evershorter storage periods, small order quantities with fast delivery times, increasing return rates, and increased delivery quantities on short notice all require flexible, scalable intralogistics processes.

The new demands can be met with the help of digitalization and automation. Siemens brings together the data generated in the process in a continuous loop between the real and digital worlds. This enables intralogistics companies to better understand and use data. Traditional silos between previously separate areas break down and new opportunities for sustainable and flexible processes are created. Accordingly, employees in intralogistics companies can make appropriate decisions based on data and react faster to changes.

With the Digital Enterprise Portfolio, Siemens supports machine builders and operators of logistics centers on the path to digital transformation. The end-to-end portfolio consists of software-based, seamlessly integrated automation and drive systems that can be used to equip central logistics center technologies such as automated guided vehicles (AGV), conveyor technology and automated storage systems. In addition, the concept of the digital twin provides a closed loop between the digital world of planning and the real world of operations and performance.

SOURCE: SIEMENS

Digitalization in intralogistics can create a decisive competitive advantage.

Siemens

Visit Website

Handheld operating panel

Use the OPC UA-capable handheld panel to operate, teach-in, test and service machines.

The HGT 1053 mobile operating panel comes with a capacitive 10.1-inch multi-touch screen and thanks to the EDGE-3 technology quad-core processor, 2 GB DDR4 RAM and 8 GB eMMC memory, it provides the best conditions for demanding applications and (web) visualizations.

With the OPC UA-capable handheld panel, it is possible to operate, teach-in, test and service machines, systems and robots directly on-site.

The integrated safety elements emergency stop and confirmation switch, as well a key switch provide the required safety for the user and machine (SIL 3, PL e). Communication is established via Gigabit Ethernet communications. The HGT 1053 also has a USB 2.0 Type A interface.

The mobile solution scores with a high-resolution multi-touch display in portrait format (WXGA 800 x 1280 pixels) and therewith, intuitive operability as well as an optimal user experience.

The cable-connected, ergonomically designed operating panel in IP54 protection fits well in the hand and with a weight of only 1,250 g, enables fatigue-free use.

SOURCE: SIGMATEK

The 10.1“ HGT 1053 mobile panel offers a multi-touch screen, high visualization power and safety elements.

Visualizations are created in LASAL SCREEN or in the web-based VISUDesigner. With current web standards such as HTML5, CSS3 and JavaScript, the user has a high degree of freedom in (web) visualization design using the LASAL VISUDesigner.

Predefined display/operating elements support the user and svg files, individually designed graphics, controls as well as animations, videos and audio files can be easily integrated.

Dimensions: 226 x 264 x 76 mm

Sigmatek

Visit Website

M12 X-Code cable assembly

M12 X-Code cables are a type of category 6A cable (CAT6A), standardized twisted pair cables for Ethernet.

New M12 X-Code cable assembly from TE Connectivity is equipped to handle maximum Ethernet speeds for more reliable, high-quality data transmission. The M12 X-Code cordset can transfer 10Gbps of data with separate channel pairs and increased shielding.

TE Connectivity is launching the M12 X-Code cable assembly as it continues to build a complete M8/M12 connector portfolio. This portfolio adds to TE's current offering, focusing on sensor applications, data supports, and industrial communication.

M12 X-Code cables are a type of category 6A cable (CAT6A), standardized twisted pair cables for Ethernet and other network layers that can handle up to 10Gbps of data. The demand for these high speeds will continue to drive advances in connector design, especially in applications with a need for extremely accurate data. These applications include data acquisition, vision systems and cameras — the latter of which require the ability to capture and transmit very precise data of a moving force in order to operate productively.

In order to withstand the high data speeds, and the subsequent heat created by those speeds, CAT6A cables have significant shielding and cable twist requirements. The M12 X-Code connector was designed to handle these requirements by separating channel pairs and increasing the amount of shielding within the connector itself.

Equipment manufacturers are beginning to utilize the increased bandwidth CAT6A cables like the M12 X-Code can afford — up to 10 Gbps.

SOURCE: TE CONNECTIVITY

The M12 X-Code cordset can transfer 10Gbps of data with separate channel pairs and increased shielding.

TE Connectivity

Learn More

Edge controller and computer

Devices for edge of network computing provide low latency control and connection with Cloud based services.

WAGO is combining the advantages of decentralized Cloud computing with local control networks by debuting their new Edge Controller and Edge Computer. These devices for edge of network computing provide low latency control and simplified connection with Cloud based services providing interfaces for connection to field devices and monitors.

The Edge Controller (752-8303/800-002) is designed for edge network applications where deterministic PLC control can be combined with machine learning, data aggregation, Cloud services, predictive maintenance and other analytic algorithms. It allows users to run high speed and complex applications with its quad-core processor as well as applications through Docker Containers with its Linux-based real time operating system. This controller supports e!COCKPIT runtime for control and visualizations via onboard HTML-5 webserver and industrial protocols such as MODBUS, Ethernet/IP adapter, EtherCAT and BACnet. IIoT protocols such as MQTT, OPC UA and Sparkplug are also supported.

For Linux-savvy users that want an industrial grade computer to run Node RED, Grafana or edge applications such as AWS IoT Greengrass, our Edge Computer (752-9400/752-9401) is the optimal device to use. It comes with a Debian Linux operating system, a quad-core ATOM processor, 64 GB flash memory and either 4GB or 8GB RAM with memory able to be expanded via SSD HDD memory card. Control engineers and software developers can leverage the device's openness to operate their edge of network applications.

SOURCE: WAGO

Solution allows users to run high speed and complex applications through Docker Containers.

WAGO

Visit Website

IoT network kit enables "proof of value"

Positioning technology enables total asset visibility in all environments using narrow-band technology.

Wittra is pleased to announce the launch of their *IoT Network Kit* which is redefining the IoT landscape by taking customers straight to 'Proof of Value'. Wittra's solution provides a simple, practical approach for tracking and monitoring assets, their groundbreaking positioning technology enables total asset visibility in all environments never considered possible using narrow-band technology.

Reducing the complexities in any IoT project Wittra offers unique pre-integrated, pre-tested and pre-secure products for immediate deployment. Based on open standards to ensure interoperability and ease of integration users can collect, communicate, and control assets. Devices run on a 6lowpan IP-based true mesh radio network which uses the sub-GHz spectrum providing long range and good penetration of structures for robust and reliable data delivery in any setting.

The Network Kit contains the Wittra Gateway, Sensor Tags, Mesh Routers and all the associated accessories ensuring an IoT project is up and running in hours; deploying the solution via the cloud-based API is simple and intuitive offering a true 'IoT Out Of The Box' experience across many market sectors.

Each tag contains several sensors which include temperature, accelerometer, gyroscope, magnetometer, and positioning. Additional sensors can be added via a plug on sensor approach covering humidity, ambient light, and air pressure. The mesh network is extended in range by the addition of Wittra's Mesh Routers creating a multi-hop self-forming and self-healing true mesh network.

SOURCE: WITTRA

Network Kit contains the gateway, sensor tags, mesh routers and all the associated accessories for an IoT project.

Wittra

Visit Website

Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

Offering the 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