10.2019 Issue 114
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking and IoT

Next generation IIoT gateways transform manufacturing 8

SIEMENS

Ingenuity for life

Making the most of air

Industrial Wireless LAN – SCALANCE W

With increasing digitalization, industrial communication networks are becoming more and more important. Particularly with wireless data transmission, demands on network components are high. Our comprehensive IWLAN portfolio offers the right solution for every application – whether in harsh industrial or moderate environments. When it comes to your wireless applications, choose performance and reliability with SCALANCE W from Siemens.
Expertise in industrial networks.

siemens.com/iwlan

PDPA-A10249-00-7600

Edge and gateway computing...

The goal of Factory Automation IoT projects is to send data from control systems that monitor and control the physical world within smart manufacturing plants to information technology (IT) data processing systems.

To achieve these IIoT goals, there is not only a need to connect the world of machine sensors and control hardware to the IT world but there is now a bigger issue of how to handle potentially much larger masses of data and how to efficiently settle on an effective system architecture.

In this issue of IEB with our focus on Factory Automation, we also are highlighting next generation IIoT gateway solutions and new edge controller architectures that are transforming smart manufacturing.

Edge intelligence is helping to advance digital transformation by enabling manufacturers to increase productivity, reduced downtime and increase product quality. But the key is an ability to bridge the gap between the worlds of operations and information technology.

In the article "*Next-generation IIoT gateways transform smart manufacturing*" on page 8 of this issue, Matthew Lee of Moxa discusses how a new generation of IIoT Gateways are helping companies reap the benefits of the IIoT.

"A new generation of IIoT gateways that are optimized for industrial applications are revolutionizing the manufacturing landscape," Lee writes. "Built around an open Linux-based platform, these IIoT gateways are secure, industrial-grade computing platforms that support multiple communication interfaces and run on low power."

The article goes through the technology benefits of new edge computing platforms, and how applications are leveraging these types of solutions.

Another article on this topic, "*New controller technology works effectively in edge applications*" (page 13) summarizes a new kind of edge controller that simplifies and secures factory automation IIoT applications.

The article concludes that edge technology not only gives automation engineers real-time control for all kinds of traditional automation applications, but it also positions them to be able to provide the IIoT and database-driven tasks that companies want to implement now.

The technology frees engineers to focus on connecting to legacy systems, transforming data into actionable information, visualizing it and performing real-time control.

These technologies are a continuing fulfillment of the potential that machine networking, powered by Industrial Ethernet, began to realize when this magazine was founded more than 20 years ago. The goals are largely the same, but the beat goes on ...

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **November 2019**
Deadline for editorial: October 4, 2019 **Deadline for artwork:** October 25, 2019

Product & Sources Listing

All Industrial Ethernet product manufacturers (not resellers) are entitled to free of charge entries in the Product locator and Supplier directory sections of the Industrial Ethernet Book. If you are not currently listed in the directory, please complete the registration form at **www.iebmedia.com/buyersguide/** to submit your company details.

Update your own products

If you wish to amend your existing information, login to the Editor section **www.iebmedia.com/buyersguide/register.htm** and modify your entry.

Do you want to receive issues of Industrial Ethernet Book? Call, mail or e-mail your details, or subscribe at **www.iebmedia.com/service/**

Editor: Al Presher, editor@iebmedia.com
Contributing Editor: Leopold Ploner, info@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +49-8192-994-9928 · Fax: +49-8192-994-8876
Online Editor: Adela Ploner, info@iebmedia.com
Circulation: subscriptions@iebmedia.com

Published by IEB MEDIA
IEB Media, Bahnhofstrasse 12, 86938 Schondorf am Ammersee, Germany
ISSN 1470-5745

Machine vision model based on OPC UA released by VDMA

The OPC Foundation vision for creation of globally harmonized information models via OPC UA Companion Specifications reaches its first milestone and demonstrates path forward to true semantic interoperability.

THE OPC FOUNDATION HAS ANNOUNCED the release of the first global OPC UA Machine Vision Part 1 Companion Specification whose development was hosted by the VDMA Machine Vision Initiative. The OPC Foundation is also proud to announce that this is the first OPC UA Companion Specification developed via close international collaboration between multinational Machine Vision related standards bodies including the American AIA, Chinese CMVU, European VDMA and EMVA, and Japanese JIIA.

The value of the OPC UA Machine Vision Part 1 Companion Specification is that it describes an abstraction of a generic vision system via a common digital representation (digital twin). This enables other systems to easily and seamlessly interact with any given physical vision system without having to deal with the challenges 'custom' information models and interfaces create.

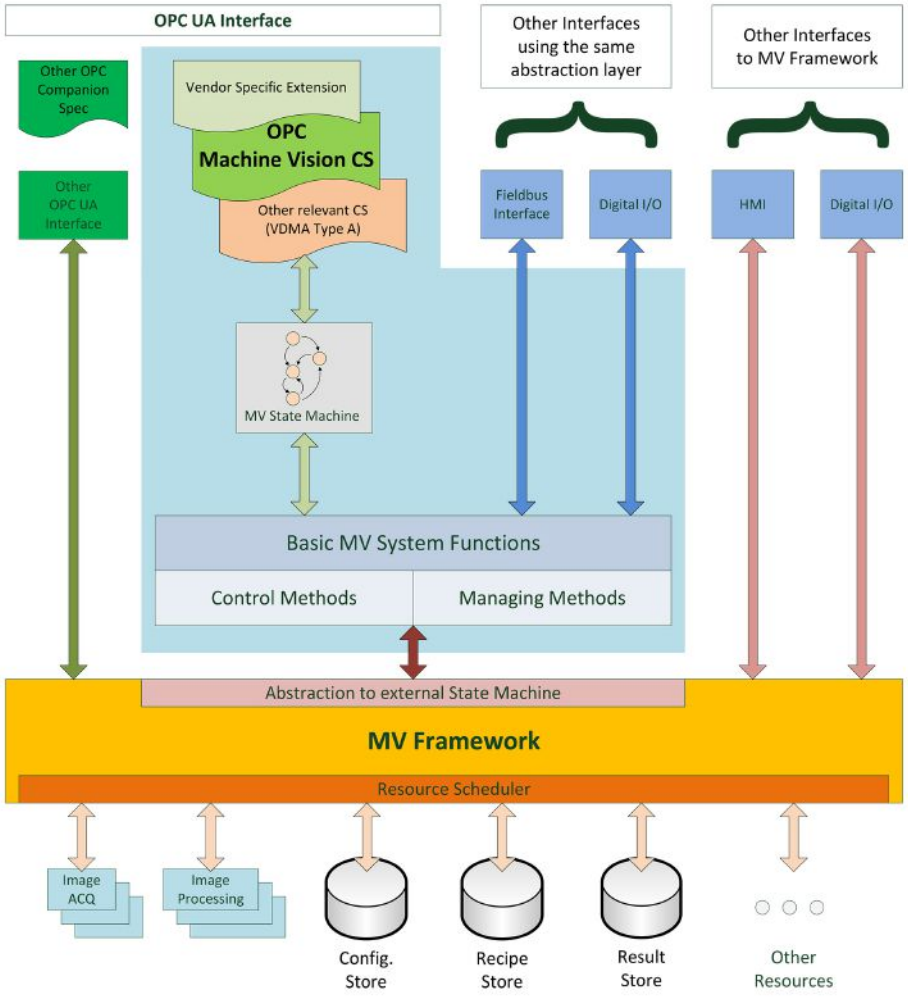
In addition, the value of the OPC UA companion specification being internationally accepted is that it enables 3rd Party systems from around the world to work seamlessly together across the shop floor and vertically throughout the enterprise.

This common OPC UA based model:

- Helps make semantic interoperability possible
- Provides end-users with maximum choice for finding best-fit components and solutions
- Creates new opportunities for vendors looking to expand their markets.

A test implementation of the OPC UA companion specification was successfully completed and was presented to a large audience of automotive engineering experts at a major OPC UA automotive industry event in Germany. A hardware demonstrator is being developed and will be soon showcased at major trade shows in Germany.

Sharing his views on interoperability, Dr. Horst Heinol-Heikkinen, Managing Director of ASENTICS and VDMA board member said: "Wouldn't it be great, if machines could communicate in a direct way with each other? This idea is at the core of the Industry 4.0 movement to create the smart factory of the future. This goal of reaching "interoperability" is the new core competence that must distinguish our future products in a connected world of Industrial IoT – but even more, the acting people and organizations involved."



SOURCE: VDMA

System model of OPC Machine Vision.

Heinol-Heikkinen concluded, "I am proud that Machine Vision plays a pioneering role and as one of the first VDMA divisions, is presenting the release of an OPC UA Companion Specification to the public, thanks to the extraordinary commitment and cooperation by the core working group members who worked very hard and made it possible."

Stefan Hoppe, President and Executive Director of the OPC Foundation commented: "The OPC Foundation truly appreciate the results of the joint VDMA Machine Vision Initiative working group – Machine Vision has taken a decisive step forward into the Industrie4.0 era that is second to none."

"Beyond the work done to adopt OPC UA as the interoperability platform for Machine Vision, we applaud the joint working group for embracing the spirit of inter-organizational collaboration on a global scale with G3. This 'big thinking' aligns well with a key OPC Foundation focus on encouraging organizations to work together to reduce the vast number of overlapping 'custom' information models into a harmonized set of OPC UA Companion Specifications which will benefit end-users and vendors around the world by lowering the barriers to true interoperability," he added.

The OPC Foundation encourages organizations to work to reduce the vast number of overlapping 'custom' information models into a harmonized set of OPC UA Companion Specifications which will benefit end-users and vendors around the world by lowering the barriers to true interoperability.

*News by **OPC Foundation.***

Minimum size for maximum versatility

The C6015 ultra-compact IPC: 82 x 82 x 40 mm

www.beckhoff.com/C6015

With the C6015 ultra-compact Industrial PC, Beckhoff is expanding the areas of application for PC-based control. In situations where a conventional PC-based control solution is out of the question for space or cost reasons, the C6015 offers an optimum price-performance ratio with a very compact design. With up to four cores, aluminium zinc die-cast housing, low weight and different mounting options, the C6015 can be used universally for automation, visualisation and communication tasks. The C6015 is also ideally suited as an IoT gateway.

- processor: Intel® Atom™, 1, 2 or 4 cores
- interfaces: 2 Ethernet, 2 USB, 1 DisplayPort
- main memory: up to 4 GB DDR3L RAM

Ultra-compact

C6015 C6017

Ultra-high performance

C6030 C6032

New Automation Technology **BECKHOFF**

New initiatives announced by Industrial Internet Consortium

A series of liasons, testbeds and challenges focussing on the IIoT in action are targeting vertical markets including global mining, geospatial applications, smart buildings and a new negotiation automation testbed.

The Industrial Internet Consortium (IIC) working with other trade groups have announced a series of programs to help further the development of the industrial internet.

Under the agreements, the IIC will work together with industry partners to align efforts designed to maximize interoperability, portability, security and privacy for the industrial internet.

Global Mining

Under an agreement, the IIC and the Global Mining Guidelines Group (GMG) will work together to align efforts to maximize interoperability, portability, security and privacy for the industrial internet.

Joint activities between the IIC and GMG will include:

- Identifying and sharing IIoT best practices
- Collaborating on standardization
- Collaborating on interoperability in mining through the two organizations respective committees, working groups and task groups
- Collaborating in IIoT adoption by co-creating reference architectures, methodologies and guidelines
- Participating in a joint workshop to exchange ideas and information

"Emerging technologies are changing the way centuries-old industries operate," said Dr. Mark Dunn, IIC Liaison Officer and Principal Research Engineer, Coal Mining Research Program, CSIRO Energy. "In the mining domain, adding sensors and internet connectivity to vehicles, machinery and people is increasing mine safety, enhancing productivity and improving our use of global natural resources."

Open Geospatial Consortium

The Industrial Internet Consortium (IIC) and the Open Geospatial Consortium (OGC) announced they have agreed to a liaison to work together to advance their shared interests.

"OGC recognizes the important work the IIC is doing in industries such as smart cities, energy, government and others," said Nadine Alameh, CEO, OGC. "We are looking forward to our collaboration with the IIC as together we explore ways geospatial information can help to further the adoption of the industrial internet."

SOURCE: IIC

System model of OPC Machine Vision.

"Through its liaison program, IIC is accelerating the digital transformation and its adoption by building industry ecosystems across verticals," said Wael William Diab, Chair of the IIC Liaison Working Group and Secretary of the IIC Steering Committee. "We are excited to partner with the OGC who bring a tremendous expertise in the application of geospatial data across industries."

Smart Buildings Challenge

The Smart Buildings Challenge, a program designed to give smart building technology suppliers the ability to collaborate with customers to create targeted, outcome-based solutions for smart buildings. The Challenge presents contestants with a set of smart building problems faced by building operators and investors, as well as a set of parameters required of the solutions.

Technology suppliers will develop solution proposals, alone or with partners, and compete to deploy pilot implementations to fulfill the requirements outlined by the challenge. A jury will select the winners from the pool of entries at the end of the Challenge. Prizes for winners will include the opportunity to deliver a live Proof of Concept in a shopping mall supported by Deka and ECE.

The Smart Buildings Challenge is one of the IoT Challenges co-organized with the Trusted IoT Alliance. The Challenges are open to the industry vendors, organizations, teams and individuals worldwide and are designed to advance and validate industrial IoT applications and solutions.

Negotiation Automation Testbed

A Negotiation Automation Platform Testbed is being led by IIC member NEC Corporation with support from IIC members Kabuku Inc., Fraunhofer IOSB and Korea Electronics Technology Institute (KETI).

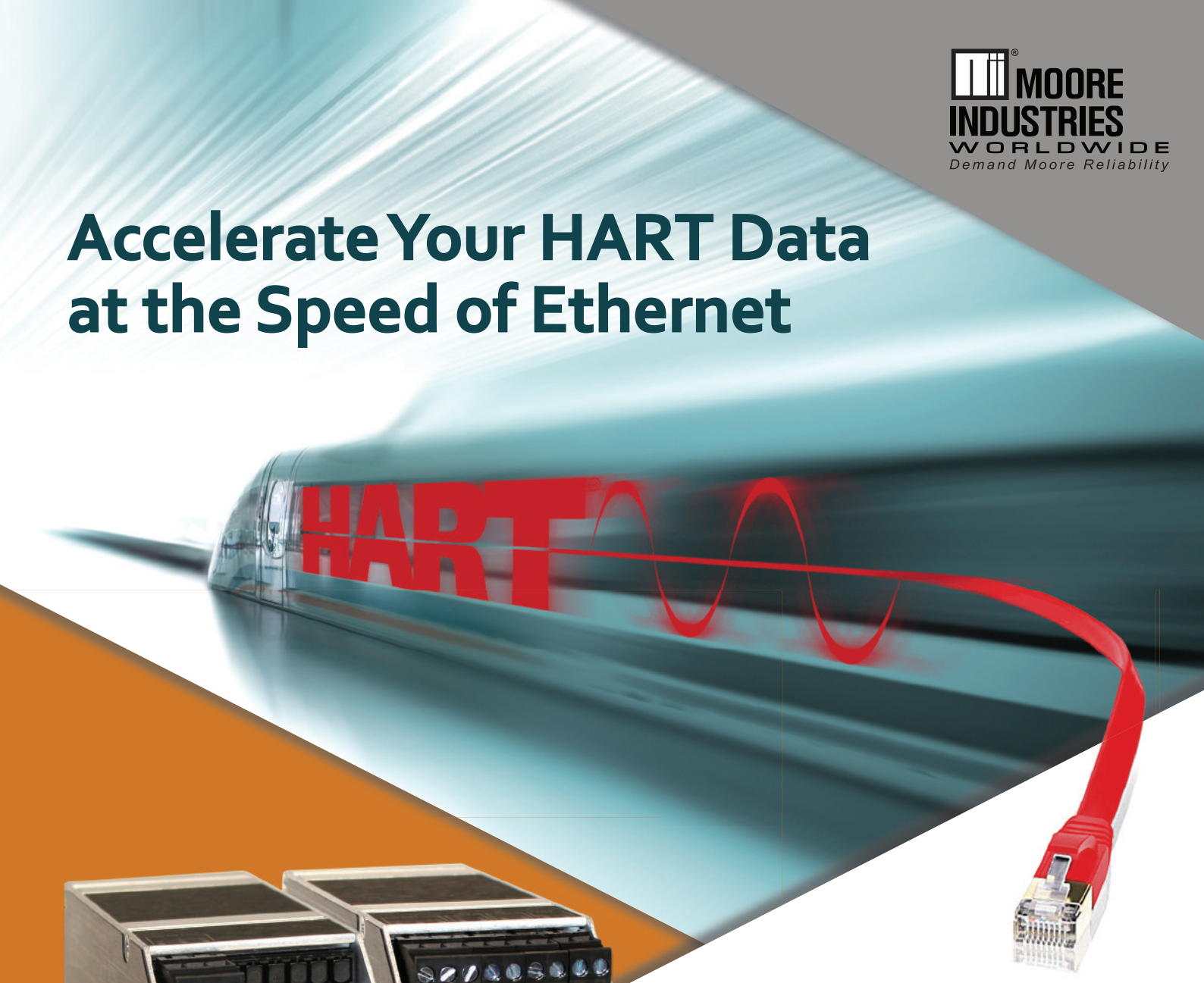
The IIC Negotiation Automation Platform Testbed will use a variety of AI infrastructure technologies, which automatically negotiate with each other, in order to find mutually agreeable contract terms. In the future, the testbed aims to promote standardization activities that support the growth of AI throughout society.

"In a manufacturing use case, automatic negotiation on conditions for the trading of products benefits both buyers and sellers," said IIC Testbed Lead Dr. Satoshi Morinaga, Research Fellow, NEC. "It enables buyers to be flexible with their demands by expressing their procurement requirements within a range and sellers can expand opportunities for orders and profits by making full use of their assets.

*News by **Industrial Internet Consortium**.*

MOORE INDUSTRIES WORLDWIDE
Demand Moore Reliability

Accelerate Your HART Data at the Speed of Ethernet



Get the process detail you need from your Smart HART devices to MODBUS/TCP and HART-IP based monitoring and control systems at the speed of Ethernet with the **HES HART to Ethernet Gateway System**.

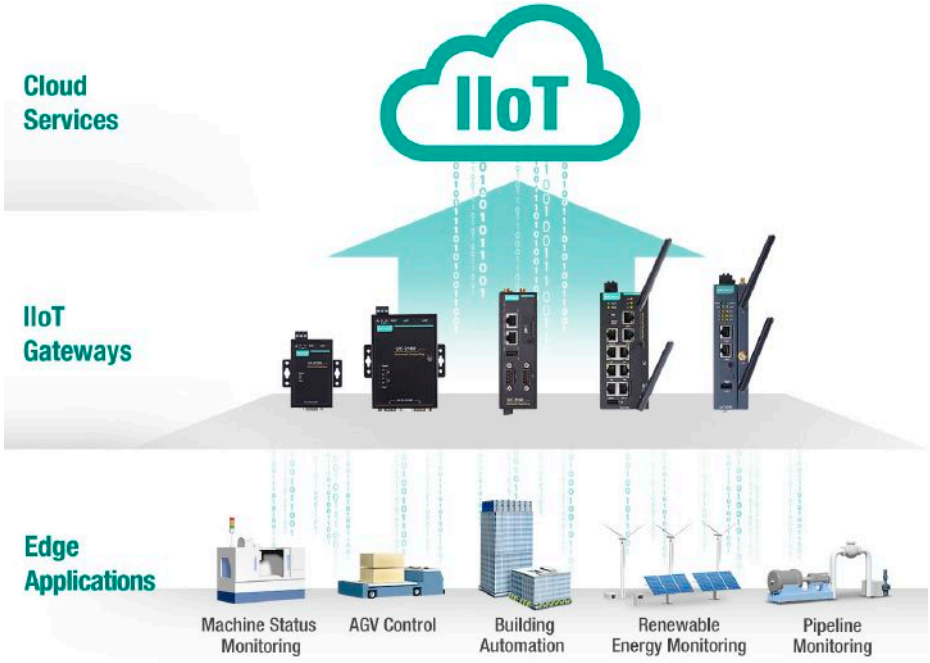
Connect up to 64 Smart HART devices and collect the Dynamic and Device Variables, along with diagnostics, from each device that delivers critical information needed to address process and device problems before they turn into unplanned downtime. Plus, the built-in web server lets you easily monitor all HART device data via any web browser.

To learn more about the Moore Industries
HES HART to Ethernet Gateway System
Call **800-999-2900**
or visit **www.miinet.com/HES**

Next-generation IIoT gateways transform smart manufacturing

Manufacturing companies have a great opportunity to benefit from the IIoT trend, powered by the benefits of new IIoT gateways. Intelligent edge-computing solutions are providing a mechanism to bridge the worlds of OT and IT, and offer new ways to increase productivity, reduce downtime and increase product quality.

SMART MANUFACTURING AND DIGITAL transformation, coupled with edge intelligence, are enabling manufacturers to increase productivity, reduce downtime, and increase product quality. A key factor in the success of this transformation is the deployment of intelligent edge-computing solutions that can bridge the gap between the operation technology (OT) and the information technology (IT) worlds by providing a number of benefits. In this article, we discuss what manufacturers need to benefit from the IIoT trend and how a new generation of IIoT Gateways are helping them reap the benefits of the IIoT, thereby transforming their businesses.



SOURCE: MOXA

Key benefits of IIoT gateways combine industrial-grade Linux, low power consumption and secure operation into solutions that support multiple interfaces/protocols and provide easy connectivity from the edge to the cloud.

Reduced latency

Manufacturers are expected to be more responsive to customer needs by providing customized products and services on a global scale. In addition, time-sensitive applications need immediate processing of device data to be able to take timely corrective actions and facilitate quick decision-making. Edge intelligence can facilitate quick decision-making at the field sites as opposed to sending all the device data from the edge to the cloud for processing.

Independent remote operations

An edge-computing platform enables remote locations to reduce downtime and operate independently when the central system is inaccessible. For example, if there is a network outage and connectivity to the cloud system is lost, field sites can use local computing power to process and analyze data. Processed data can then be sent to the cloud for long-term storage when the connection is restored.

Data security

Sending sensitive operational data from the edge to the cloud puts data and edge devices at risk. Multiple levels of security need to be put in place to ensure that the data is securely transferred from the edge device to the cloud. Processing data at the edge helps prevent data breaches and enables faster responses.

Reduced data-transfer costs

Transferring large volumes of data from the edge of the network to a cloud server can be prohibitively expensive. Furthermore, the cost of transferring this data on a daily basis could lead to unsustainable communication costs in the long run.

Manufacturers are looking for optimized computing solutions for their industrial-automation applications to intelligently process large volumes of data received from the sensors and field monitors, and send only critical data or a summary of the data to the cloud. Compact-sized, ruggedized industrial Arm-based computers, designed for low power consumption, are at the heart of these solutions and make edge-side computing more reliable and cost-effective.

Benefits of Arm-based Linux

Arm-based Linux IIoT Gateway solutions provide industrial-grade security, manageability, performance, and reliability while still maintaining extensibility. They typically combine the hardware, OS, and software functions listed below to provide an optimized edge-computing solution for IIoT applications.

Longevity: Industrial products are usually in place for 10 to 15 years. To meet this requirement, Arm-based CPUs typically come with a minimum lifespan of 15 years. In addition, Arm's commitment to long-term support and access to their future enhancements, make Arm- based solutions an ideal choice for industrial applications.

Low Power Consumption: Low-power processing is a requirement in many industries to ensure that the equipment does not overheat and pose a potential hazard. Fanless equipment are also preferred so as to mitigate the effects of dust in industrial environments. Arm Cortex-A processors are highly optimized for performance and power efficiency.

Scalability: Linux is eminently scalable and is able to run on a variety of platforms. The basic functionality of a Linux platform—command line tools, configuration, and code—are compatible with any Linux-based device. This flexibility allows for easier upgrades and compatibility between different systems.

Enhanced Security: While manufacturers are reaping the benefits of digitization, they are also faced with data security risks and software-integrity issues. A Trusted Platform Module (TPM) can be deployed to guarantee

YASKAWA

Let's Get Connected

Introducing the GA800 Variable Frequency Drive

Need your variable speed drive to have an easy and problem-free connection to your favorite Ethernet or Fieldbus network? Yaskawa takes your desire for control and data seriously.

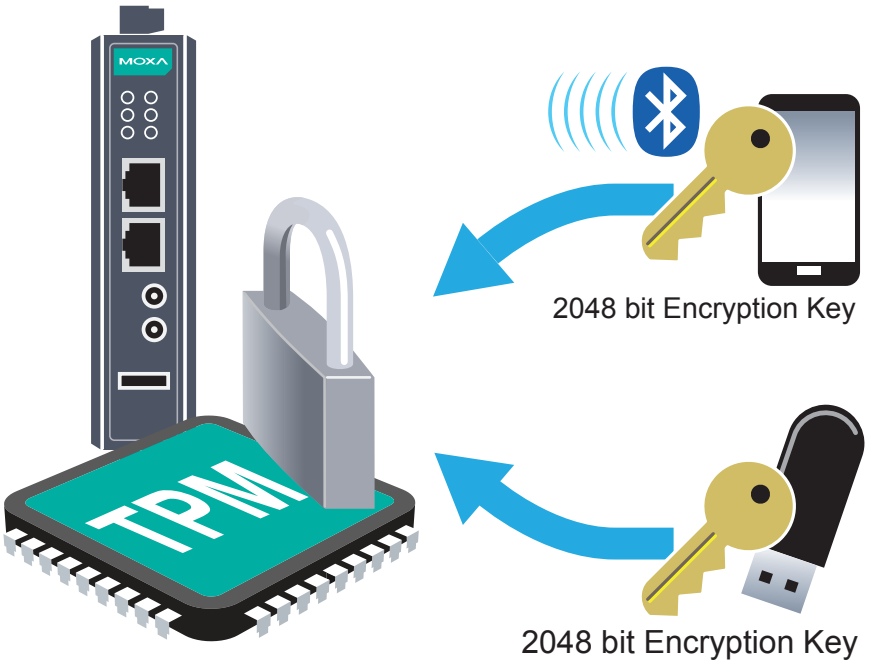
Our new GA800 is no exception. It provides data-rich connectivity with all major industrial networks. The Industrial "Internet of Things" is here. Let Yaskawa help satisfy your appetite for it.

Your days are complicated enough. Let us help simplify them.
Call Yaskawa today at 1-800-927-5292.

SUSTAINABLE
FLEXIBLE
EASY

Yaskawa America, Inc. Drives & Motion Division 1-800-YASKAWA **yaskawa.com**

For more info: http://go.yaskawa-america.com/yai1321



SOURCE: MOXA

TPM and Arm-based computers give system integrators and engineers powerful new tools in their security arsenal.

the physical security of edge devices. In addition, Arm's TrustZone can be used to create an isolated secure world, which can enhance security and maintain the integrity of edge-computing solutions.

Ready-to-run IIoT gateways

A new generation of IIoT Gateways that are optimized for industrial applications are revolutionizing the manufacturing landscape. Built around an open Linux-based platform, these IIoT gateways are secure, industrial-grade computing platforms that support multiple communication interfaces and run on low power.

Industrial-grade Linux

IIoT gateway solutions that include a high-performance industrial-grade Linux distribution and long-term support are better equipped to meet the growing needs of manufacturers. Currently, long-term support (LTS) offered on a Linux kernel is five years. In most industrial establishments, especially in critical systems such as energy, water, transportation, and communication, it is not feasible to update the software systems every 5 years. Software vendors should commit to long-term maintenance of the Linux platform. A long-term commitment (10 years or more) to support a Linux kernel, which includes security patches and bug fixes will address the needs for extended lifecycle of computing systems in industrial automation applications, making industrial projects secure and sustainable.

Projects, such as the Civil Infrastructure Platform (CIP), aim to speed implementation of Linux-based civil infrastructure systems, build upon existing open source foundations and expertise, establish de facto standards by providing a base layer reference implementation, and contribute to and influence upstream projects regarding industrial needs. CIP's kernel will be based on Linux kernel 4.4 and will include security patches and features backported from newer kernels.

CIP is driven by some of the world's leading manufacturers of civil infrastructure systems and industry leaders including Codethink, Hitachi, Plat'Home, Renesas, Siemens, Moxa, and Toshiba. This project is hosted by The Linux Foundation to create an open-source platform for managing and monitoring IoT-enabled civil infrastructure and make it safe, secure, reliable, scalable, and sustainable.

Other related projects include the Core Infrastructure Initiative (CII) and the Kernel Self Protection Project.

Low power consumption

It is a well-known fact that when it comes to low-power systems, Arm-based systems are a natural choice. Intel based x86 IIoT gateways consume on an average 30 W of power while their Arm-based counterparts, for example, gateways build on the Arm Cortex-A processor, can provide industrial-grade performance in power budgets under 10 W. Low power computers and devices help substantially reduce your operational costs. They consume less power and hence generate less heat, which means no cooling systems are required.

Secure platform

Operational networks were simply not built for connectivity to the Internet/cloud. The key focus of these networks is quick data access for industrial processes. Manufacturers feel that implementing multiple security levels is a huge drain on network resources and may impact productivity. However, in the IIoT age, where the trend is towards more connectivity for edge device, which may otherwise never be connected to the Internet, there is a quantum increase in possible attack points for malicious attackers.

Security threats can extend to even low-level devices. Cyber attackers can target anything that is exposed to the Internet, including a thermostat in the field to a wireless device. Manufacturers can longer take this threat lightly. Information security, system hardening, security fixes, and ability to backport fixes to existing cores without having to change the software helps organizations better fight cyberattacks.

One example is Arm-based computers that support TPM v2.0. Bringing TPM and Arm-based computers together gives system integrators and industrial engineers a powerful new tool in their security arsenal. By creating a specific cryptographic key for each individual device, which is hardcoded within the platform itself, the data stored on the computing system is secured and protected from being read by an unauthorized party. Moreover, the OS on the system can be locked from being overwritten to secure edge devices and data in distributed areas. Security utilities and tools that can conveniently build up the protection mechanism on the software platform to meet your cybersecurity requirements are other ways to secure industrial systems.

Multiple interfaces and protocols

IIoT Edge Gateways should come with multiple interfaces such as serial, CAN, Ethernet, Wi-Fi, and NB-IoT. 4G LTE-ready. IIoT gateways with carrier (Verizon/AT&T) certifications and industrial-grade CE/FCC/UL certifications enable reliable connectivity for edge devices.

An edge-side software that accelerates mass configuration of devices, easy device management, and data acquisition can speed up system deployment. Modbus connectivity for data acquisition and processing and MQTT support for lightweight edge-to-core data transmission reduce development efforts. RESTful APIs and Modbus APIs for implementing gateway software functions enable easy integration with existing systems and with new-age IIoT applications.

Easy connectivity to the cloud

Edge intelligence and connectivity to the cloud are two faces of the same coin. Depending on the IIoT applications, connectivity to a private cloud, public cloud, or both may be required. To enable cloud connectivity and edge intelligence, generic Modbus and EtherNet/IP protocol support, MQTT /HTTPS and RESTful/ C/Python API support are required.

240 power budgets on any assignable port

NT24K FULL GIGABIT POE

Red Lion NT24k advanced PoE management allows quick and easy allocation of the switch's 240 Watt PoE power budget to any of its 16 ports (up to 30 Watts per port). Additional comprehensive features include: auto IGMP configuration, advanced redundant technologies, RSTP, advanced monitoring systems, CIP messaging, SNTP, IEEE802.1x and Radius remote server authentication. IP67 – M12 versions for harshest environments are available.

sps
smart production solutions
Nürnberg, 26.–28.11.2019

WWW.REDLION.NET

EUROPE
+31 (0) 33 4723-225 | europe@redlion.net

AMERICAS
+1 (717) 767-6511 | info@redlion.net

EXCELLENCE. REDEFINED.

Built-in clients for AWS, Azure, Ignition Edge (Sparkplug), and Wonderware Online services may also be necessary, depending on the cloud services that are required for your IIoT applications.

The following two cases illustrate how new-age IIoT gateways help speed up IIoT deployments and transform operations based on intelligence from field data.

Machine Data Acquisition (PLCs)

Traditional machine tool builders are now willing to invest in new IIoT trends so that they can provide more value with their products and improve the quality of machine status data collected for post-sales management and services.

The data acquisition system must be capable of acquiring data from different brands of PLCs with their own proprietary protocols, send the data to backstage control server, and display the data on a dashboard remotely and locally. Furthermore, a compact and reliable device for data acquisition is required without having to changing the structure of machines which means the system should be small enough to fit in existing control cabinets.

System Requirements

- Computing solution to collect data from PLC to monitor the status of the stamping press remotely and locally through Wi-Fi
- The solution should work with a vareity of Mitsubishi, Delta, and Allen-Bradley PLCs
- Compact-sized and vibration-proofed systems for reliable operation in the cabinet of the stamping press

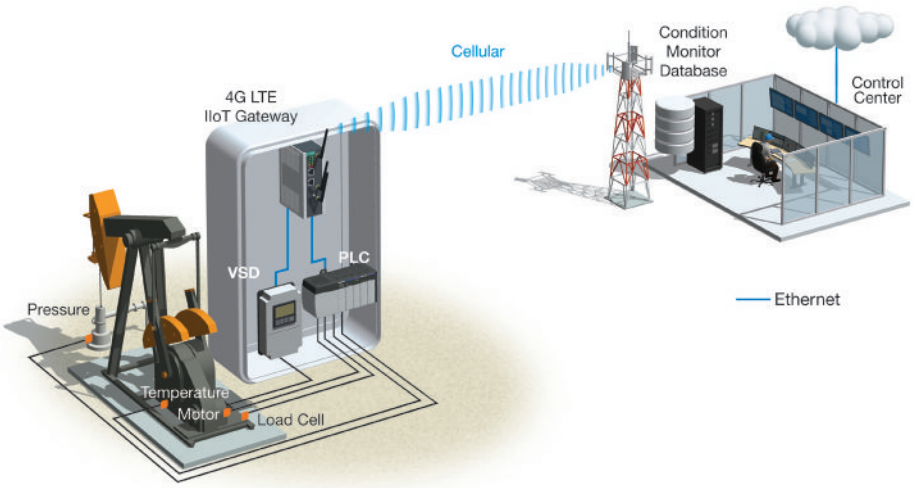
Artificial lift monitoring systems

A leading oil and gas service company is building telematics solutions for its customers to run smooth operations and conduct predictive maintenance for artificial lifts in oilfields. With the trend of oilfield digitization, telematics has been tremendously useful in understanding equipment status so as to avoid problems, also called predictive maintenance.

The data generated by the manufacturing equipment during the operations is the key to achieving this goal. As a result, this oil and gas service company needs a reliable and secure solution to ensure that the data needed is brought back to the control center for further analysis.

A wireless-enabled Arm-based open computing platform that acts as a secure IIoT gateway, allows oil companies to aggregate data from variable speed drives (VSDs) and PLCs for their pumping systems and to transfer the data back to the control center through LTE communication in the harshest environments.

A built-in Trusted Platform Module (TPM) in the IIoT gateway can ensure that each individual device is hardcoded by a cryptographic key to ensure the data is only accessible by authenticated parties.



SOURCE: MOXA

A reliable and secure solution ensures that needed data is brought back to the control center for further analysis.

System Requirements

- Low power consumption because oil wellheads are often located in harsh environments where powering is sometimes difficult
- Reliable 4G LTE connectivity in high operating temperatures for constant data aggregation
- Computers must feature Trusted Platform Module (TPM) to ensure data integrity
- Open Linux platform for flexible application development

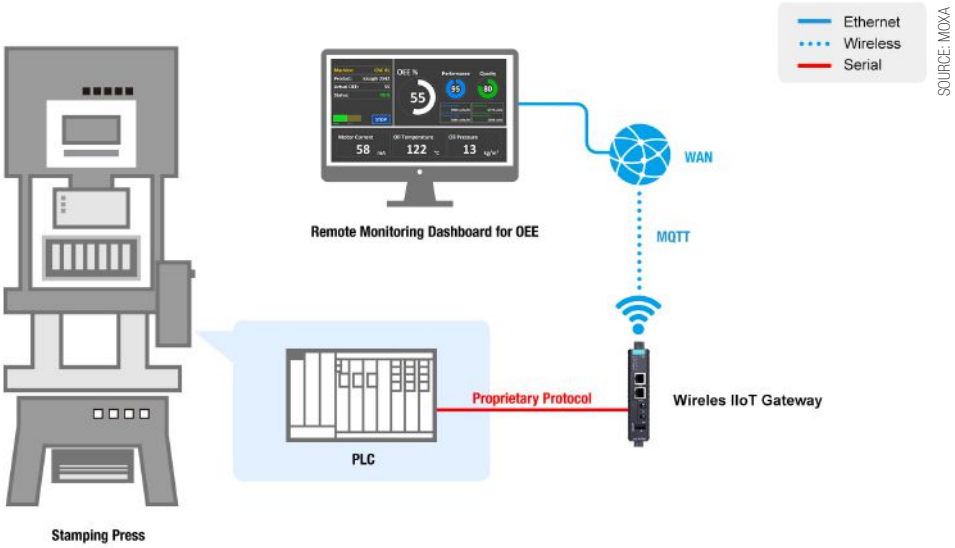
Wireless IIoT gateway solutions

UC series IIoT edge gateway technology offers industrial-grade, wireless-ready Arm-based computing platforms that are designed to operate reliably in a wide temperature range of -40 to 85°C. These gateways are built around the Arm Cortex-A processor and come with Moxa Industrial Linux (MIL) to address the need for extended lifecycles in computing systems for sectors such as solar/wind power, water and wastewater, oil and gas, transportation, and factory automation. Key benefits include:

- Industrial-grade Linux
- Low power consumption
- Secure platform
- Multiple interfaces and protocols
- Easy connectivity from edge to the cloud

The UC series IIoT Edge Gateways are the first Azure IoT Edge certified Arm-based computers. Integrating Azure IoT Edge with the gateways benefits customers, especially those operating on Linux platforms, in a number of ways. The benefits include secured remote connections to enable deployment in remote locations, connectivity to allow existing brownfield applications to share data with the cloud, and device management and product longevity to ensure customers can deploy, scale, and maintain their IIoT applications.

Matthew Lee, Product Manager, ***Moxa.***



SOURCE: MOXA

Solution collects data from PLC to monitor the status of the stamping press remotely and locally through Wi-Fi.

Controller technology works effectively in edge applications

A new kind of industrial controller simplifies and secures automation and IIoT projects, reducing costs and complexities. The technology frees engineers to focus on connecting to legacy systems and smart systems, getting data and transforming it into actionable information, visualizing it, and performing real-time control.

A GLASS PRODUCTS MANUFACTURING COMPANY presented their automation engineers with a new project last year. Data from manufacturing lines needed to appear in a web-based user interface (UI) the company's supervisors already used.

Solving the UI problem

The UI showed production goals and sales from the company database. Supervisors needed to see real-time production figures in order to compare them to goals and sales and adjust production accordingly. How hard could it be? Almost everything was on premises.

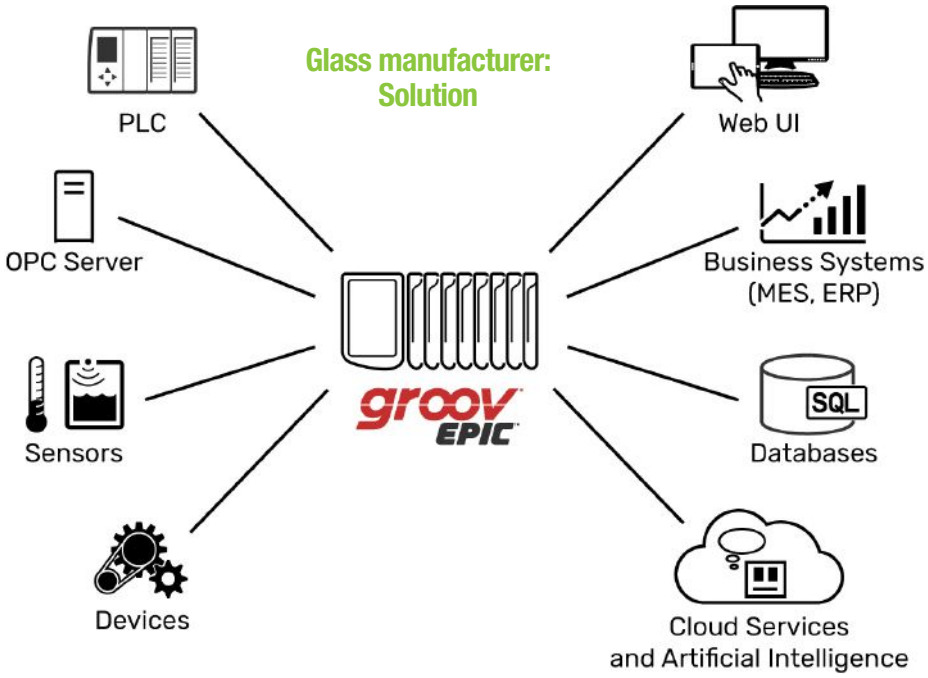
Field devices on the manufacturing lines were wired to local programmable logic controllers (PLCs), with field device values in counts. Getting data from the PLCs required device-specific communication drivers. The engineers purchased and installed them, chose the desired points, and mapped the points in a spreadsheet. Data in counts had to be converted to engineering units.

Next, the PLC data was networked to a PC-based HMI (human-machine interface) and a SCADA (supervisory control and data acquisition) system. These systems required the engineers to configure data tags, drivers, and polling rate assignments.

Then, working with their information technology (IT) department, the engineers also configured the HMI and the SCADA system to transport the data into the company database. Additional programming was required to make the data available to supervisors.

Though expensive and complicated, it worked. The engineers and the IT personnel could finally get back to other projects they'd had to put on hold while figuring this one out. They wished there had been an easier, less costly solution.

And then the company realized that their supervisors needed more information from the manufacturing lines, as well as a way to control some process elements. In addition, new production lines were being planned to manufacture a different kind of glass. The new lines would require control and a similar complex architecture to share data with the supervisors' interface.



SOURCE: OPTO 22

New controller technology eliminates middleware and shrinks the steps required to collect data—reducing complexity, lessening security risks, and decreasing the time and expense required for installation and maintenance.

OEM machine designer

At about the same time, an original equipment manufacturer (OEM) in California was rethinking its machine design. The OEM built ovens that were suited for a wide variety of industrial and commercial applications, and the company wanted to differentiate its ovens from those of its competitors in order to increase sales.

Feedback from customers pointed to three ways they could improve:

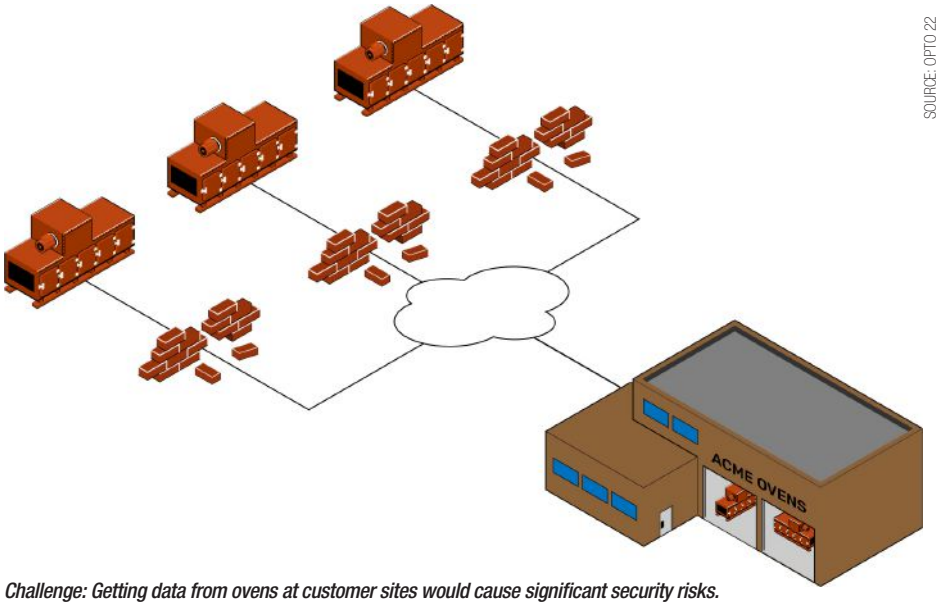
- Make it easier for customers to integrate the oven with process control systems
- Add human-machine interface (HMI) options, so customers could more easily monitor and control the oven's operation
- Reduce customer costs, especially for operation and maintenance

The OEM's engineers explored a number of ways to achieve these customer requests.

They thought about ways to simplify integration with popular process control systems—for example, drivers for an OPC UA server. But because control systems are proprietary, a driver would have to be developed separately for each system. Since

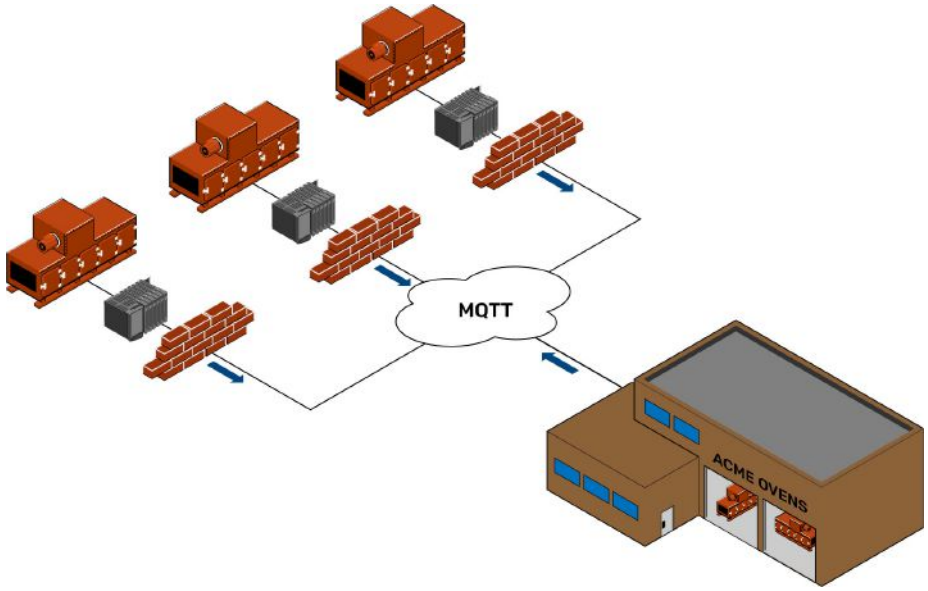
SOURCE: OPTO 22

Most control systems use protocols and networks specific to automation— computers/mobile devices use standard Ethernet, wireless networks, open protocols and standards.



SOURCE: OPTO 22

Challenge: Getting data from ovens at customer sites would cause significant security risks.



With an EPIC device, the OEM can use a pub/sub communication method, like MQTT, to acquire data from ovens at customer sites, without compromising security.

the company's ovens were used with many types of systems, a one-at-a-time approach would not be cost effective.

Integration with existing HMIs would run up against the same problem. The engineers considered other options for an HMI, including an improved interface on the machine itself and even a mobile app. These ideas sounded possible but expensive to develop.

Reducing customer costs seemed even more difficult. All their ideas depended on data. If they could get operational data from in-place ovens at customer locations, they could analyze it to improve their products' efficiency. Data like that could also reduce customer costs by providing a new level of service.

For example, the OEM could track burner ignitors, anticipate failures, and call the customer in advance to avoid unplanned downtime. Scheduled maintenance would likely be reduced as well, replaced by preventive maintenance and even predictive maintenance, to determine the likelihood of failures before they occur.

Customers would appreciate these cost reductions and new services. But to get oven data from a customer's site, the OEM would have to gain access to the customer's network. The customer's IT department would have to open incoming firewall ports and allow the OEM to request, or poll, the data. IT departments would never allow such a potential breach to their network security.

How could the OEM redesign their ovens to meet their customers' wishes and differentiate their products in the market, without spending so much time and money and causing major security problems?

Challenges of the IIoT

These two projects touch on three of the main challenges most automation engineers find today with the Industrial Internet of Things: complexity, security, and expense. Usually the extent of these challenges is not obvious before a project begins; the challenges become clearer once the project is underway. Any IIoT or data-intensive automation application seems to end up involving far more complexity, many more security risks, and much greater investment in time and money than many companies want to expend or can afford.

Getting data from the edge of the network—from the sensors and actuators in factories, commercial buildings and remote sites—to the databases and people who need to use that data can be daunting. Bi-directional communication, for control as well as monitoring and data acquisition, can be even tougher.

Most control systems and equipment use protocols and networks that are proprietary or specific to automation such as EtherNet/IP, Modbus, PROFIBUS, serial and OPC. But computers and mobile devices use standard Ethernet or wireless networks and open protocols and standards like TCP/IP, HTTP/HTTPS, JSON, and RESTful APIs.

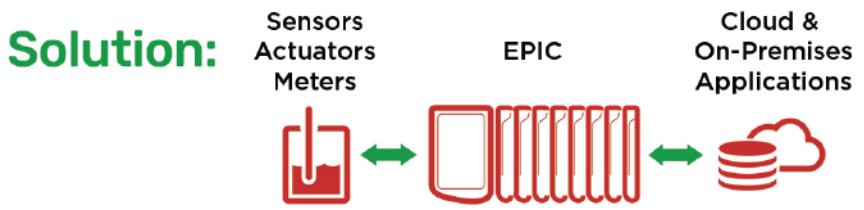
Translating data between these systems and moving it to where it's needed involves a lot of expense and middleware: computers, gateways, drivers, parsers, custom software, licenses. As soon as data moves outside its immediate network or off premises—for use in the company computer network, or remote locations, or on a tablet or smartphone connected to the internet—middleware increases and security concerns balloon. A typical setup includes many steps.

New approach to IIoT Automation

Controls engineers are familiar with PLCs (programmable logic controllers) and PACs (programmable automation controllers). Both have been used and improved over many years, incorporating capabilities that used to be found only in SCADA systems, adding communications with Microsoft Windows-based HMIs, running on standard Ethernet networks, and so on.

But now, for the kinds of applications companies want to do currently and in the future, there is a need for a new approach that simplifies connections and communication—a new approach that does much more than a PLC or even a PAC. There is also a need to shrink or eliminate the middleware and move data from where it's produced to where it needs to be in many fewer steps.

New controller technology called EPIC (for Edge Programmable Industrial Controller) provides a device that eliminates middleware and shrinks the steps required to get the needed data—reducing complexity, lessening security risks, and decreasing the time and expense required for installation and maintenance. By looking at each part of the acronym, it is possible to learn what this technology means for automation applications.



SOURCE: OPTO 22

Edge controller provides hardware and software interfaces to simplify communication between devices and cloud.

Edge

All data acquisition starts at the edge, because that's where data is produced. A manufacturing line or shipping department in a factory, refrigerated rooms or barcoded containers in a warehouse, pumps and pipes and storage tanks at remote sites: all are at the edge of the network and all have data that could be used to improve processes and profits.

If that data is obtained directly from the source, then it's accurate. So an EPIC device sits at the edge and connects directly to sensors and actuators through its I/O, the inputs and outputs that gather sensor data and send control commands. It can also connect to existing PLCs or other devices to gather their data and issue commands, if needed.

An EPIC device at the edge of the network actively works on the data as well, filtering out anomalies, labeling, storing and transmitting only by exception to reduce unnecessary volume, and converting values from one protocol to another. All this preprocessing makes operations, enterprise, and business cloud applications far more efficient.

Because it is the single source for data, an EPIC device can also securely share this data with software and equipment, including other control systems, building management systems, databases, cloud services, and others.

An edge device like this has integrated hardware and software that can perform control, monitoring, data acquisition, operator interface, edge data processing, and analytical functions. Key features include quad-core processing power using a real-time, open-source operating system, along with two or more independent Ethernet network interfaces to segment a trusted network (for example, an internal automation network) from an untrusted one (for example, a network with internet access)

Gateway functions and a configurable internal firewall enable access control for all network interfaces. Authentication and encryption is built into all communications, to eliminate default usernames or passwords.

User account creation and management should be based on required access to specific software on the system, with support for modern security standards like PKI-standard certified connections to servers and clients using SSL certificates.

Standard Ethernet network interfaces and standard modern computer ports like USB and HDMI should be utilized for communications. Multiple methods may be implemented for communicating via standard automation and internet protocols, with multiple software options available for programming and data communications.

An integrated, user-configurable, web-based HMI that runs in a web browser (independent of device screen size, manufacturer, or operating system) can be used to implement an integrated high-resolution color touchscreen for local configuration of I/O and networks, troubleshooting, and system visualization.

The controller's open-source operating system and quad-core processing provide the intelligence and speed of a computer. Programming and communication options, PC-like ports, solid-state drives, and file space

SOURCE: OPTO 22

The glass products manufacturer already used PLCs to control their existing manufacturing lines.

offer options not available on a PLC or PAC. For example, users can store project files (like panel drawings, P&IDs, installation notes) on an EPIC device, so they can be accessed in the field by authorized technicians.

For visualization, an EPIC device includes software for building a web-based, mobile-ready HMI. The HMI is not limited to data and controls from one manufacturer only, but can let authorized users see and send data and manipulate controls, if required, for multiple automation systems, software, and cloud services. Visible on the EPIC's touchscreen, this HMI is web-based and therefore also available to authorized users on computers, laptops, tablets, and smartphones.

Other options may also be available such as open-source Node-RED for wiring together devices, databases, cloud applications, and APIs (application program interfaces) with simple logic flows.

Programmable

An EPIC device is not a PLC, not a PAC, and not a PC, but like them it must be programmed for control. An EPIC device provides several programming options, some of which reflect traditional automation tools and others that come from PC and internet backgrounds.

Users can program control using familiar automation tools like flowcharting or any IEC 61131-3 compliant language, including:

- Function Block Diagram (FBD)
- Structured Text (ST)
- Sequential Function Charts (SFC)
- Ladder Diagram (LD)

Users more familiar with higher level languages can gain access to the controller's open-source OS and choose to build custom programs in languages such as C/C++, Java, Python, or others. The device does not limit programming options like PLCs and PACs that may force users to learn a new programming language in order to use it. Instead, it leverages what the user already knows to help build control, data exchange, and HMI programs more quickly.

Industrial

Engineers often have to place controllers in severe environmental locations. One problem with PCs in industrial automation is that an off-the-shelf PC cannot be trusted to stand up to harsh environments. In contrast, EPIC technology grew from real-world automation experience and is designed to withstand tough conditions.

Industrial-grade components and processors are designed for long life. UL hazardous locations approval and ATEX compliance are standard. Operating temperature ranges are wide, for example, -20 to 70 °C and its I/O is hot swappable. THe stainless-steel chassis comes in different sizes to fit enclosures or machine designs and can be DIN-rail or panel mounted.

Controller

At heart, an EPIC device is a real-time industrial controller designed to run control applications. Programmed with standard automation tools, like flowcharting, structured text, and even traditional ladder logic, it works just like a PLC or PAC in a control system. But the device is more than just a controller.

For example, its I/O modules offer multiple channels. Modules with isolated channels are available. Analog and discrete I/O accept a variety of signals, with each channel usually software configurable.

Because EPICs were designed by control engineers, they include features that simplify commissioning and troubleshooting:

- A built-in touchscreen is usable with a finger, a stylus, or while wearing gloves.
- A web-based system management application can configure I/O and networking on touchscreen in the field, or using a computer or mobile device.
- I/O module specs and wiring diagrams are viewable in the field, on device itself.
- Spring-clamp terminals and integrated, covered wireways accommodate a variety of wire sizes.
- LEDs on each I/O module indicate module health and discrete channel status.

Taken as a technology group, edge control systems technology offers significant options for automation and IIoT projects that help future-proof a company's technology investment. And in the area of security, unlike older automation controllers, an edge device includes tools to help make the system as secure as possible.

So how could an EPIC device help the glass products manufacturer and the OEM with their projects?

The Glass manufacturer

The glass products manufacturer already uses PLCs to control their existing manufacturing lines. An EPIC device can connect to these existing PLCs and communicate their data. The manufacturer won't need to purchase PLCs for the new lines they're going to add, however. EPIC processors can be used instead, connecting directly to sensors and actuators to provide control, while communicating data wherever it is needed.

Because the EPIC provides data in standard engineering units, no conversion software is required. Once configured with plain-language names, I/O channels are available automatically as tags in all EPIC software, so no spreadsheets are needed to keep track of points.

Incorporating production goals and sales from the company's database is simpler with an EPIC, which includes software such as Node-RED to acquire that data through pre-built nodes. Data from all sources—PLCs, sensors and devices wired to the EPIC, and the company database—is easily made available to authorized users in the EPIC's HMI software.

Using EPIC devices also makes future changes or expansion easier and more secure. In addition to providing connections to PLCs and databases, an HMI, and real-time control, an EPIC can also move data among OPC servers, business systems like MES and ERP, and cloud services and software.

Data from new sources can be added to the system without middleware. IIoT connections are encrypted and authenticated. New data,

controls, and authorized users can be easily added to the HMI, with changes pushed out to users.

The OEM machinery builder

The OEM's engineers discovered the solution to both their security and cost. An edge controller in the oven replaces the PLC or industrial PC—or both—that used to be required. It is wired directly to sensors and actuators in the oven and provides control, monitoring, data processing, communication, and visualization in a single unit.

For control programming, the OEM can use flowcharting, IEC 61131-3 languages, or Secure Shell access (SSH) for a custom program running on the Linux OS. For an improved HMI, the OEM has choices:

- On smaller ovens, the built-in touchscreen can provide local visualization.
- On larger ovens, an industrial monitor can be added, plugged into the unit's HDMI port.
- For all ovens, the OEM can build a secure web-based HMI for use on computers and mobile devices. This HMI can be used by customers and also by the OEM.

Because the technology's system management software is web-based, the OEM can apply software updates and manage the oven from their location, rather than having to go to the customer's site.

Secure data from customer sites

Perhaps the greatest advantage of edge control for the OEM, however, is the ability to get the data they want from their ovens at customer sites, without causing security issues for the customer. In addition to the usual request/response method for data communication, the technology offers another method: publish/subscribe.

Publish/subscribe, or pub/sub, works by setting up a central broker, either on premises or in the cloud. The broker handles all data communications. Each data source sends data to the broker only when it changes (report by exception). Equipment and software that need data subscribe to only the data they need, and they receive it from the broker only when it changes.

Most important from a security standpoint, all communications are device-originating, outbound-only connections from the EPIC to the broker over secure, encrypted connections. (Secure, device-originating, outbound connections are normally permitted by most IT departments.)

Once initiated, data can flow in both directions. Firewalls allow outbound communications, so there's no need to open unsecure ports in firewalls. Security is maintained and IT involvement is reduced.

Because it greatly reduces network traffic and maintains security, a pub/sub communication method is well-suited for remote locations. With an EPIC controller in their ovens, the OEM can set up a pub/sub broker at their facility or in the cloud and transfer data from ovens at customer sites, via outbound communications, anywhere they need to use it.

For example:

- In the HMI for monitoring and controlling
- In a database for analysis to improve oven design
- In software for tracking individual customer service
- In online artificial intelligence and machine learning services for analyzing wear and determining preventive maintenance schedules, or predicting when failures might occur to reduce or eliminate downtime.

SOURCE: OPTO 22

Edge controller technology gives automation engineers tools for both real-time control along with IIoT and database-driven tasks.

Looking ahead

As we've seen, edge controller technology not only gives automation engineers real-time control for all kinds of traditional automation applications, but it also positions them to be able to provide the IIoT and data-based tasks companies want to do now.

The technology frees engineers to focus on what needs to be done: connecting to legacy systems and smart systems, getting data and transforming it into actionable information, visualizing it and performing real-time control.

Because systems are scalable, they can be applied to smaller applications and then expanded with virtually no limitation. Users can see how the technology works before committing significant resources.

It also offers a simple, secure, maintainable, and cost-effective solution for data communication. If solving the latest challenge involves complex steps, expensive middleware, or security issues, take a look at edge controller technology. It may very well shrink those steps, reduce costs, and help provide the security needed.

Technology report by ***Opto 22.***

Trade-offs selecting a wireless instrumentation protocol

The larger wireless landscape has changed since the introduction of WirelessHART and ISA100.11a. These two standards have changed the process manufacturing landscape, but some companies are still trying to decide which protocol to adopt. What considerations should guide a facility choosing between the two today?

IT'S BEEN OVER A DECADE since the introduction of the two most comprehensive and widely adopted wireless instrumentation protocols: ISA100.11a (IEC 62734) and WirelessHART (IEC 62591). Given the tens of thousands of wireless instrumentation networks in use globally, there should be no question that these protocols work as advertised when deployed correctly with a high degree of cyber security. The question as to which protocol to choose is less clear.

Those wanting to argue the selection question on technical minutia are welcome to do so, but for purposes of this article, we will focus mainly on the issues of network topology and network management, which are the key differences in the context of how the larger industrial wireless landscape is changing.

Similarities vs. differences

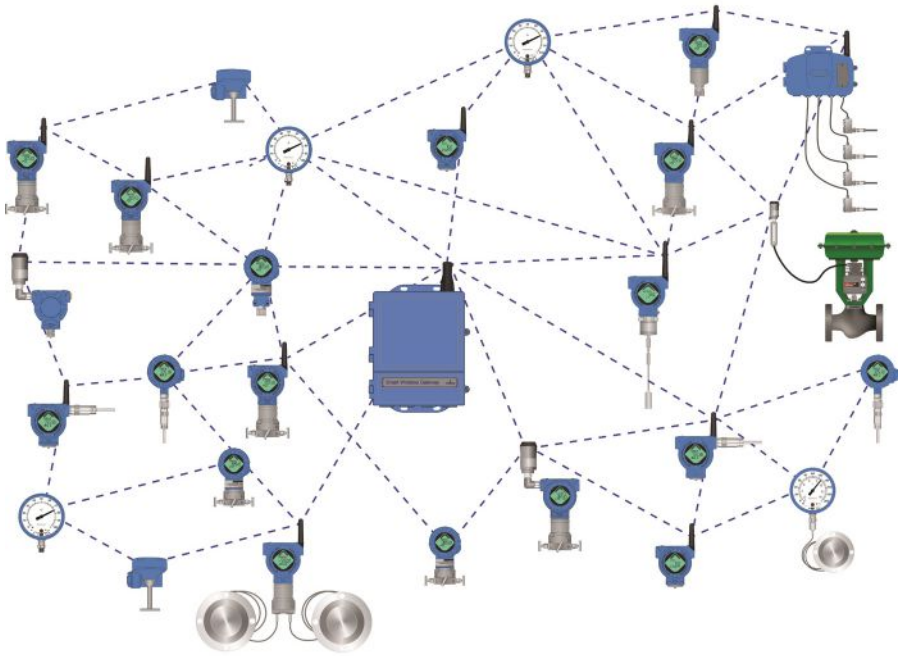
To begin, it is important to keep in mind that ISA100.11a and WirelessHART are alike in many ways, although still incompatible:

- Both are open standards maintained by independent industry organizations and recognized by the IEC.
- Both specify end devices that have similar battery life estimates.
- Both use the IEEE 802.15.4 radio (as do Zigbee, MiWi and other wireless protocols).
- Both are designed for communication of low-data rate devices over short distances with low power consumption.
- Both use AES-128 encryption and a secure network joining mechanism.
- Both have extensive catalogs of compatible process instruments, actuators and accessories provided by multiple vendors.
- Both provide multi-vendor interoperability with certified devices.

The overall operational scope of both is very similar and, in that respect, they compete head-to-head in process manufacturing environments. Where differences emerge is in user implementation.

Differing network topology

Companies implementing ISA100.11a typically use a star topology where groups of individual end devices cluster around a router which collects their data and sends it to a central gateway. Multiple routers can communicate with a single gateway. Routers are normally externally powered and can therefore have more powerful transmitters than end devices. They are helpful for gateway communications with a over longer distances and with greater bandwidth but have the potential to limit throughput into and out of a single subnet.



SOURCE: EMERSON

ISA100.11a uses a star topology where groups of individual end devices communicate with a router, which sends data to and from the gateway.

While this approach minimizes the need for meshing between individual end devices, there can be side effects. Due to typical ISA100.11a network topologies, communication is line-of-sight and devices need to be visible to a router. This means routers need to be mounted in relatively high locations where they can communicate with individual end devices while maintaining a clear path to the gateway.

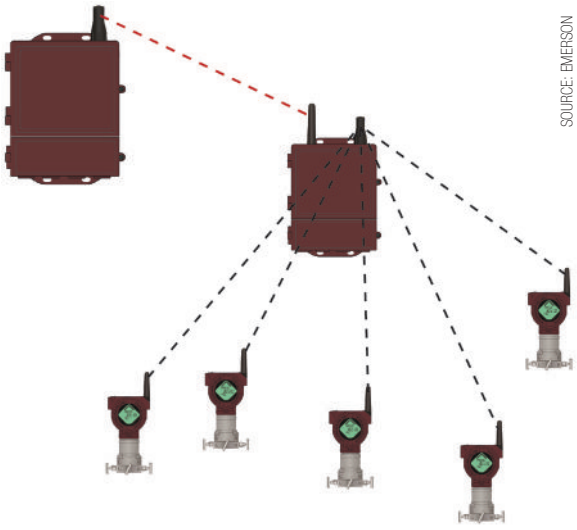
WirelessHART takes a different approach and embraces the meshing concept, using it to create a dynamic self-organizing and self-optimizing network where end devices can communicate directly with the gateway when possible, or via hops from device to device where they are out of range. While meshing can introduce some latency, it is typically a minor consideration and does not affect the overall performance of the network. Network management software constantly monitors network traffic and adjusts meshing patterns automatically as necessary to avoid bottlenecks and transmission delays.

This is one of the biggest differences between the two networks, and while its effect is nuanced, it can still have a major effect on implementation and day-to-day use.

Network management

Hand-in-hand with the difference in networking topology is the difference in network management. ISA100.11a requires manual network management to the extent that when a new end device is added, it needs to be assigned to a given router and configured to follow specific communication paths as primary and backup. Network management personnel have the tools to control these interactions, and diagnostic software can indicate performance as desired.

WirelessHART, on the other hand, is self-organizing and self-optimizing. When a new end device is added to a network, the management software automatically determines how it will communicate, without the need for any manual management or



SOURCE: EMERSON

WirelessHART uses a self-organizing mesh network which adjusts communication paths automatically and continuously when necessary.

adjustment. Someone watching network traffic can see communication paths and what is talking to what, but the network management software automatically determines how devices communicate within the network.

To a prospective user 10 years ago, this must have represented a major difference. An engineer considering WirelessHART had to understand the whole concept of industrial wireless networking, and how the software was able to control network management. The idea of a self-organizing network likely sounded great, but to some the manual management of ISA100.11a may have had an appeal.

All this was going on a decade or so ago in a context where many process plants were cautiously considering wireless in a variety of ways. Maybe new users were unsure, but it didn't take long for them to find out that WirelessHART's self-organizing and self-optimizing capabilities worked extremely well, providing easier implementation as compared to ISA100.11a in many instances.

Watching WirelessHART network activity using software tools verified correct communications and showed how the data found its way from instrument to gateway. If there were weak areas of communication in a network, best practices with instructions were provided to evaluate antenna position and determine where an additional relay point might need to be added to provide alternate paths. With some very basic monitoring and adjustment, usually necessary only in a small number of cases, mesh networks could hum right along all by themselves.

Changing wireless landscape

These days, we deal with self-organizing networks everywhere. Nobody has to tell their smartphone to use the best network, whether cellular or Wi-Fi, to complete a call or send a text message. It's all automatic. This is more important than ever with industrial networks. The original designers of ISA100.11a and WirelessHART probably saw these as a mechanism to support process instruments using largely static networks. Manual management would be tolerable because network changes would be infrequent.

Such is not the case anymore. The sophistication of self-organizing network management software has improved, making it more effective than ever. At the same time, the range of natively wireless process instruments has grown, plus, whole new classes of wireless condition monitoring sensors (bearing temperature, motor vibration, acoustic transducers, etc.) have exploded onto the market. As these proliferate, the attractiveness of high-performing, self-organizing networks becomes all the more apparent. The easier it is to deploy these devices, the more they will find their way into everyday use where they can deliver improved performance and cost savings.

Not a binary choice

For someone deciding between ISA100.11a and WirelessHART today, considerations should not fixate on the past but look to the future. Whichever protocol is adopted, it is likely to be around for many years to come and it is important to project how it will fit into tomorrow's implementations. Wireless instrumentation networks will undoubtedly become more integrated into industrial internet of things (IIoT) deployments.

For these more integrated deployments, wireless Ethernet (Wi-Fi) has become the common denominator in most plants due to its ability to support mobile workers and a host of other high-bandwidth applications. Major Wi-Fi infrastructure providers can now incorporate ISA100.11a and WirelessHART into their industrial routers, allowing all three networks to come together on the Wi-Fi backhaul. The self-managing characteristics of WirelessHART make it highly adaptable and easy to integrate in these contexts. This ability combined with its overall ease of use and broad product offering has kept WirelessHART the leader in number of networks installed.

Process plants are running on wireless networks to an increasing degree and the networks are becoming more integrated. This provides plants and facilities with more options, allowing them to choose the best solution for their applications.

Eric Braun, engineering director for wireless applications & gateways, ***Emerson Automation Solutions.***

TwinCAT OPC UA connects research to innovation

Flexible communication across building and mobility applications at Empa rely on the OPC UA standard to interconnect its research infrastructure. Data communication, from control traffic between devices to data analysis in the cloud, is handled by embedded PCs running TwinCAT 3 OPC UA software.

EMPA (SWISS FEDERAL LABORATORIES for Materials Testing and Research) conducts interdisciplinary energy research in the building and mobility sectors inside an actively used living and working environment on its campus.

Empa relies on the OPC UA communication standard to interconnect its research infrastructure: three large-scale projects named "NEST," "ehub" and "move" plus all components involved in producing, storing, transporting and converting energy. Data communication, from control traffic between devices to data analysis in the cloud, is handled by embedded PCs running TwinCAT 3 OPC UA software.

Empa, an interdisciplinary research institute and member of the ETH Domain, composed of university and research institutions, is working to bridge the gap between the lab and real-world applications. One primary focus of its work is on energy and sustainable building technologies based on research and technology transfer platforms called demonstrators.

These include the Next Evolution in Sustainable Building Technologies (NEST), the Energy Hub (ehub) and the demonstrator for future mobility (move). Working in close collaboration with research and industry partners, Empa uses these largescale building, mobility and energy projects to deliver market-ready solutions in those sectors.

SOURCE: BECKHOFF

East view of NEST with the Urban Mining & Recycling unit illuminated in the center and the striking Solar Fitness & Wellness unit at top right.

Open, clearly defined interfaces

Given that Empa's demonstrators are available to a wide range of users, it was essential to create an open, manufacturer-independent platform with clearly defined interfaces, according to Philipp Heer, ehub Group Leader at Empa: "The units have just a single physical link to the NEST backbone that connects them with the thermal and electrical systems.

Each unit operates independently and incorporates its own automation solution, which communicates via Ethernet. The challenge here is to integrate new units into the demonstrator infrastructure with as few limitations as possible so that systems can be maintained by service technicians and used safely and to their fullest potential for research purposes as well. From an integration point of view, flexibility is essential because the system boundaries shift whenever we add a new unit."

Enabling flexible access from outside the Empa campus was another challenge. To achieve this, the process control level was implemented in the cloud rather than on internal servers. This called for a specialized control system software architecture to ensure safe system operation yet allow actuator override where necessary for research purposes.

For Philipp Heer, Open Platform Communications Unified Architecture (OPC UA) was the ideal communication technology to meet the requirements for a highly complex and flexible system of this kind: "We use OPC UA across the board, for everything from device-to-device communication at the control level all the way up to data analysis in the cloud and research integration.

We developed an OPC UA information model specifically for this purpose. This model lets us integrate new units and components based on standardized specifications. To keep the integration effort as low as possible and ensure consistency, we incorporated parts of the software architecture into the OPC UA information model itself. This approach also allows us to implement new Internet of Things (IoT) software and services without having to adapt the system."

Embedded PCs / TwinCAT OPC UA

Ten CX5140 Embedded PCs running TwinCAT OPC UA software (TF6100) control the communication among Empa's three demonstrators. Philipp Heer explains: "We have seven CX5140s operating on the NEST backbone as TwinCAT OPC UA servers and clients that we use to connect heating, ventilation and room automation systems.

The other three Embedded PCs work as central management systems in NEST to hook up the micro grid and integrate the units. The system as a whole monitors some 60,000 OPC UA objects, including a number of data point instances needed for building automation or to provide researchers write access.

Around 6,000 relevant sensor signals from these objects are logged straight to a database. Despite the scale and scope of the system, there have been no performance issues so far. The TwinCAT OPC UA Gateway offers a distinct advantage here: It provides a central point of access to the entire information model, where each sensor is mapped to a corresponding structure. With this setup, all of the information contained in the database and

from integrated systems such as LabVIEW can be accessed easily through a single interface."

Another valuable feature from Heer's perspective is that the classic building automation system, implemented using the TwinCAT Building Automation Library, can be manipulated directly over OPC UA: "We can override any individual actuator to suit the needs of specific research projects. TwinCAT OPC UA lets us create new instances elegantly and easily within the information model's tree. Researchers are only able to see their own particular tree – in much the same way as the building automation system can only see its own tree for normal operating purposes. We can choose and apply the requisite permissions via a selector implemented in the Beckhoff control system. This is both extremely flexible and fast, which is a huge advantage."

NEST, ehub & move demonstrators

NEST is a building with a modular, flexible structure consisting of a central core, the backbone, and three open platforms. Individual research and innovation modules can be installed on these platforms, which serve as building floors, according to a large-scale plug-and-play principle. These modules, or units, serve not just as dwellings or places of work but also as test labs operating under realistic conditions. The units are connected via thermal and electrical networks, across which they can interact withone another.

The ehub energy research platform connects the other two demonstrators – NEST and move, which are located in separate buildings. However, it can also control all energy infrastructure components individually in line with specific research requirements. Rather than treating NEST as a single entity, ehub sees the various NEST units as separate buildings. In conjunction with the NEST and move demonstrators, ehub can be used to combine energy flows in the areas of mobility, housing and work, to test new energy concepts under real-world conditions, and to explore the potential for increasing efficiency and reducing carbon emissions. Empa's Philipp Heer explains: "The Energy Hub is a typical energy center, complete with the usual physical components like heat pumps, geothermal probes and batteries, serving a total of 15 buildings. More interesting, though, is how it works at the control level: It operates as a virtual platform for control and energy management projects."

The demonstrator and technology transfer platform for mobility research, move, supports the development and trial of new types of vehicle drives designed to produce significantly lower carbon emissions. Excess power from photovoltaic or hydroelectric plants serves as an energy source for charging electric vehicles and producing hydrogen and synthetic methane for fuel cell and natural/biogas-powered vehicles. The connection between ehub and move allows a shift of renewable energy from the building sector to the mobility sector, where it is either used as fuel or stored in the form of hydrogen.

SOURCE: BECKHOFF

Research units can be added to NEST easily using a large-scale plug-and-play principle.

Empa's OPC UA in detail

The OPC UA transport layer: the Empa demonstrator park is modular in structure. Separate controllers operating as OPC UA servers and clients control various subsystems on the NEST backbone, in the NEST units, and in the ehub and move demonstrators.

The subsystems communicate with one another and with the TwinCAT OPC UA Gateway in the cloud over OPC UA; all the OPC UA servers can access the gateway as a shared server. The latter also serves as an access node for higher-level databases, research templates and SCADA systems. Empa implemented device-to-device communication between CX5140 Embedded PCs using OPC UA client PLCopen function blocks.

OPC UA information model: The NEST information model is based on object types defined for every device and sensor group. These object types differentiate between read and write operations, and contain all key data points. There is one object type per device group; the object types can be instantiated to objects as often as required. This establishes a hierarchical structure in which the objects can be queried via OPC UA server namespace with different resolutions.

Machine-to-machine communication: The plants at Empa's demonstrator park use a wide variety of controllers. All measured values and control outputs from the plants are processed by their respective controllers, which are connected over I/O or bus systems, then made available via the objects defined in the OPC UA namespace.

Machine-to-human communication: Each plant can operate in normal or research mode. In research mode, the control system logic is overridden. A function block was created for each actuator to make this possible. Each function block can be accessed via two OPC UA write instances for the two operating modes.

Flexibility – the core advantage

Empa began using PC-based control technology from Beckhoff in 2013 to automate a research building equipped with a large number of different interfaces. Says Philipp Heer: "One important factor besides the compact design was the variety of interfaces, which went well beyond the usual array of building technology standards like DALI, KNX or M-Bus.

The building relied on additional industrial communication protocols, which we also had to accommodate. The project called for a mix of Bus Terminals and EtherCAT Terminals, which was not a problem with Beckhoff technology. The outstanding communication performance of EtherCAT is another big advantage for us, especially in situations that require exceptionally precise measurements."

A benefit of PC-based control is that it allows seamless integration of energy measurement technology. Empa uses around 25 EL3403 and EL3443 EtherCAT three-phase power measurement terminals to record and analyze key electrical data in its supply network. TwinCAT Scope also makes work even easier, as Philipp Heer explains: "With TwinCAT Scope's ease-of-use and powerful analysis capabilities, we can test controllers using high-resolution data and evaluate disturbance inputs exceptionally well."

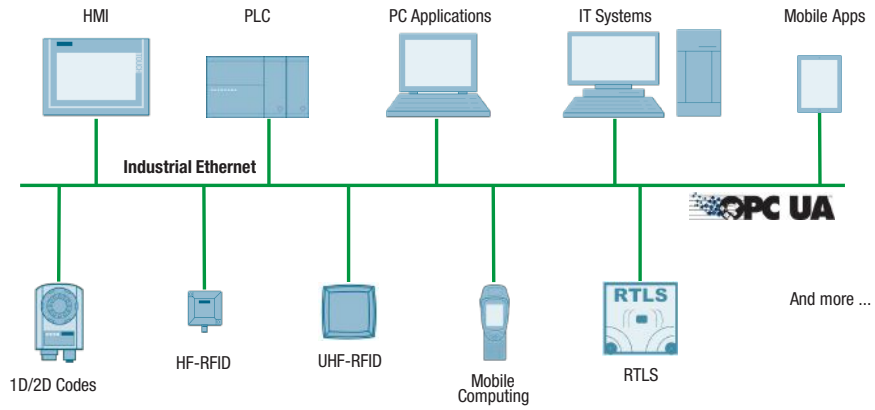
Stefan Ziegler, ***Beckhoff Automation.***

One communication standard: OPC UA for AutoID devices

AutoID devices continue to differ depending on the manufacturer, with all devices having sufficient differentiation options. Only the data exchange is standard across all of them, which simplifies integration of AutoID technology and built-in security is now accelerating the expansion of automation to Industry 4.0.

AIM-D LAUNCHED A NEW COMMUNICATION STANDARD for AutoID devices in 2016, in cooperation with the OPC Foundation. At the last SPC IPC Drives trade show, it became clear that this standard is being embraced by many device manufacturers across the entire AutoID spectrum. What's more, demand for OPC UA as the communication standard in the industry is also consistently rising.

In 2014, the AIM System Integration working group motivated by Siemens and HARTING decided to define a new, forward-looking, technology-independent and manufacturer-independent communication standard for the AutoID industry. Until now, many devices communicated via proprietary interfaces, and there were often various communication standards for various technologies. Regardless of whether it was via barcode or UHF RFID had an impact on the programming of the communication interface software to be connected. These circumstances evolved historically.



SOURCE: HARTING

OPC UA is one of the standards for implementing state-of-the-art communication architectures that is also listed in the RAMI specifications for Industry 4.0.

AutoID the technological base for Industry 4.0

Containers, printed circuit boards, car bodies, hospital beds and much more – today these can all be automatically identified thanks to AutoID technology. This is generally something that happens entirely passively and without maintenance work on the object, making the technology essential in the driving forward of automation in general.

With UHF RFID (also known as RAIN RFID), the object itself has a memory. Information like the date of manufacturing and the firmware version of a printed circuit board can be saved directly on the printed circuit board in this example. There is no need for a power supply, accessibility is wireless and updates can be implemented easily.

Today, AutoID technology is a self-explanatory tool for implementing an overall solution, for example, an automatically functioning warehousing logistics centre. Communication barriers are unwanted. The AutoID technology used should also be decided on the basis of the application and not by the communication interface of the AutoID device. Classic communication structures – keyword automation pyramid – are also broken open. Today, an RFID Reader communicates directly with an ERP system and with a control unit on the production line.

Motivated by these ideas and requirements, the AIM working group decided to define a communication interface based on OPC UA technology. OPC UA is one of the standards for implementing state-of-the-art communication architectures and is also listed in the RAMI specifications for Industry 4.0 by the government. Moreover, OPC UA is already supported by many control units and software systems. Communication with the machine and with the database system in the Cloud is simple to implement. OPC UA is the communication standard of the automation industry. There is virtually no provider for this industry and virtually no machine manufacturer that does not already offer an OPC UA interface today.

Thanks to its object-oriented structure, OPC UA was highly suited to the development of a common communication standard for the various AutoID technologies. Commonalities such as a scan method for simple detection of an ID can be defined in higher-level classes. Specific characteristics can be implemented in classes derived from these for the individual AutoID technologies. Thanks to this mechanism and on the basis of the standard, manufacturer-specific updates can be performed without affecting the common basic functionality.

Integrated security

Communication security is another important issue. Isolated communication systems are becoming increasingly rare in production and logistics. As already explained, the vertical and horizontal integration of AutoID systems is crucial to be able to develop an overall solution. OPC UA already offers diverse integrated security mechanisms and this was also investigated by the Bundesamt für Sicherheit in der Informationstechnik (BSI) – the Federal Office for Information Security. The BSI confirmed that OPC UA already offers integral mechanisms for implementing secure data communication. According to the BSI, "OPC UA was developed taking security aspects into account and does not have any systematic security gaps."

For AutoID systems, this aspect should not be disregarded. Ultimately, complete machines and processes work more or less autonomously on the basis of the data communicated by the AutoID system.

The topic of security, not just from the perspectives of communication with the control unit or computer system, was rated as important by the members of the AIM association. For this reason, AIM Deutschland founded its own working group AutoID & Security in 2018. This working group issues recommendations on how to securely use the AutoID technology. Further information on this working group can be found at www.aim-d.de.

In 2016, AIM Deutschland introduced the new OPC Unified Architecture for AutoID Companion Specification at the Hannover Messe. The first RAIN RFID devices launched on the market by Siemens and HARTING were presented in a demo application at the trade fair stand of the OPC Foundation. Direct communication, e.g. to the Microsoft Azure

Cloud, is not a problem. The interface specification is available free of charge upon request from info@aim-d.de. The interface can be directly integrated by all control units and backend systems.

OPC UA has become even more important since 2016. The Volkswagen Group's membership of the OPC Foundation in 2018 is testament to the importance placed on OPC UA by one of the key industries in Germany and Europe, the automotive industry. On 21st May 2019, the AIDA Automatisierungsinitiative Deutscher Automobilhersteller (the Automation Initiative of the German Automotive Industry) together with the VDMA Verband Deutscher Maschinen- und Anlagenbauer (Mechanical Engineering Industry Association) and in cooperation with the OPC Foundation held an OPC UA information day for car manufacturers at Volkswagen in Wolfsburg. This also shows that users of the AutoID technology are demanding OPC UA.

One for all

Meanwhile, the *OPC Unified Architecture for AutoID Companion Specification* published in 2016 has been integrated into devices by many AutoID manufacturers. As was evident at the OPC Foundation trade fair stand at the SPS IPC Drives in November 2018, barcode, HF and UHF devices are now available with an OPC UA interface. Many different AutoID technologies but one common communication standard. Standard, secure data communication with various devices from different manufacturers is now a reality – and it is based on OPC UA, the future-proof communication standard in the automation industry.

Of course, AutoID devices continue to differ depending on the manufacturer, with all devices having sufficient differentiation options. Only the data exchange is standard across all of them, something that simplifies the integration of AutoID technology. The "inbuilt security", if used correctly, increases the security of communication, which is accelerating the expansion of automation to Industry 4.0.

However, the work of the System Integration working group did not come to a stop in 2016. The participants continue to work on extending and improving the interface specification. Their tasks here are multi-faceted. A core issue is the simplification of the interface for – from the AutoID perspective – simpler application scenarios. The purpose here is to accelerate implementation and interface integration and remove unnecessary obstacles. Thus, simple scanning of an individual object via variables alone is possible in the newest version. Function calls are no longer required and implementation work is reduced to a minimum.

Another important topic is the integration of sensor data. The RAIN RFID technology, in particular, is increasingly being used to transfer sensor values. This enables an object to be uniquely identified, additional data to be read out and written and the current status of the object to be queried. Information on whether the drive is too hot, the body is wet or the container is locked can be directly requested. There is often no need for a battery even – i.e. passively and without additional maintenance work.

The individual technologies are merging more and more here and classic sensors and AutoID are growing together.

AIM Deutschland also looked at this aspect in 2018 in an additional working group "RFID & Sensors". The results and recommendations of this working group are, needless to say, being taken into account in the extension of the OPC UA-based interface. There is also an international exchange on the RAIN or AIM North America Association.

The Hannover Messe 2019 saw the introduction of the latest release of the OPC Unified Architecture for AutoID Companion Specification from AIM Deutschland in cooperation with OPC Foundation. Initial results of work packages discussed above have already been included. The System Integration working group is naturally also active beyond the Hannover Messe 2019 in cooperation with the OPC Foundation.

Olaf Wilmsmeier, Business Development Manager RFID, ***HARTING IT Software Development.***

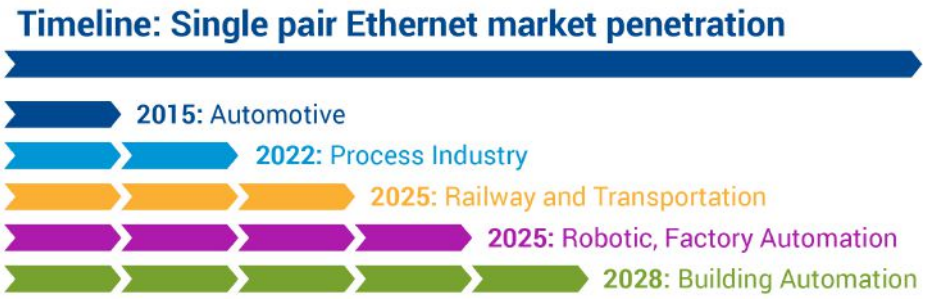
Single Pair Ethernet gears up to impact industrial automation

With Single Pair Ethernet technology and Time Sensitive Networking, industrial automation is poised for a leap forward in precision and productivity. With the new, unique SPE protocol for encoding and scrambling data, industrial networks will gain lower EMI, lower cost, reduced cabling weight and higher bandwidth.

IN THE WORLDS OF INDUSTRIAL AND PROCESS automation, and the networks that enable technology advances, tremendous progress has been made in recent decades. Over the years, more smart devices, more bandwidth, more determinism, along with more precision and sophistication, have been added to the work at hand – whether that work is automotive or semiconductor manufacturing, electrical power delivery or natural gas extraction.

Intelligent equipment uses sensors and actuators that can be connected over one common network. The data captured and conveyed to the data center for analysis and prediction is vital. But with this, many sensors and actuators that accommodate space, packing density, costs, infrastructure, and ease of installation and service, have become all the more important.

Proprietary and legacy fieldbus systems including Profibus, AS-Interface, Modbus, CANOpen, DeviceNet, CC-Link, and IO-Link are generally too bulky or resource-intensive for the best Industrial Process implementations. Remember, complexity breeds cost and space in control system layout is not unlimited. Order, structure and reliability with these legacy systems are not what it should be. But now, we are on the cusp of reversing that entropy. Two wires, a single twisted pair, are enough.



SOURCE: BELDEN

The benefits of Single Pair Ethernet is expected to gain wide market acceptance. One network from the sensor to the cloud guarantees control over all network components. Thinner, lighter cables enable more orderly, defined cabling.

Industrial Ethernet breakthrough

One Ethernet network in compliance with IEEE 802.3 from the sensor to the cloud is arriving. Now, with the coming of Single Pair Ethernet (SPE) technology in the Industrial Field together with Time Sensitive Networking (TSN) capability, our sector is poised for a leap forward in precision and productivity. With the new, unique SPE protocol for encoding and scrambling data, industrial and process networks gain lower electro-magnetic interference (EMI), lower cost, reduced cabling weight, and higher bandwidth.

One lighter, thinner cable that is still capable of Power over Data Lines (PoDL) and that will have a signal and power reach up to 1000 meters is arriving now. This will be one cable and one network type that any sensor or actuator can get power from, and any sensor or actuator can talk to.

Germany's PI International Organization and ODVA (US) have begun their work to adopt the IEC single pair Ethernet cable and connector standards and the various IEEE 802.3 SPE protocols. With this development, "the stars are aligned," as the saying goes. System integrators and field application engineers truly have a pathway to functionality gains without increases in their costs for installation, operation and repair.

With the right partners and the right application of these new standards and the engineering expertise it took to ratify them, there will very soon be one global common network type from the sensor through to I/O modules and switch devices, and up into the cloud backbone. All of this is possible if the right systems engineering is applied.

Automotive Ushered in SPE

Single Pair Ethernet is being used successfully in the automotive environment today. Vehicle harnessing systems and in-vehicle networks have greatly benefited from the work that key automotive engineering teams did in partnership with their cable and connector partners. That work included the time and energy put into getting the IEEE 802.3bw technology standard for 100BASE-T1 for Automotive in-vehicle networks published in 2015.

IEEE 802.3bw was driven primarily by the needs of the global automotive industry and it perfectly illustrates how Ethernet can expand into new application areas and bring about innovation. Advanced driver assistance systems and compute-intensive displays created the need for cost-effective, high-bandwidth connectivity. But, importantly, it fell to the component and cabling ecosystem to give automotive engineers a way to build that better network inside a very tight weight and space envelope. Enter, Single Pair Ethernet. Where once four wire pairs were necessary, now there can be just one.

Advanced automotive electronic systems require faster communication networks as today's vehicles share an enormous amount of real-time data, firmware and software between electronic control units (ECUs). IEEE 802.3bw (100BASE-T1) came to be because engineers developed a new physical layer (PHY) communication protocol that could make single pair work. This PHY was developed by automotive manufacturers in collaboration with leading integrated circuit (IC) manufacturers and the ecosystem of suppliers around them.

The 100BASE-T1 standard was based upon, and is interoperable with, the existing OPEN Alliance Broad-Reach automotive specification. 100BASE-T1 is the first in a family of Single Pair Ethernet standards to address new applications.

100BASE-T1-PHY performs all necessary scrambling and encoding prior to transmission over an unshielded twisted pair cable up to 15 meters. 100BASE-T1 is transparent from the media access control (MAC) device's point of view, as the existing Media Independent Interface (MII) does not change.

100BASE-T1 is a physical full-duplex interface, which means that the data is sent and received on the same pair of conductors. The physical full-duplex transmission is achieved according to the principle of superposition.

100BASE-T1 PHYs have integrated hybrid circuits and use echo cancellation to remove

their own transmitted signal and extract the information received from the remote station. In contrast, 10BASE-T and 100BASE-TX have their own pair of conductors for each transmission direction. This PHY approach was a true networking engineering breakthrough.

The use of one transmission medium for both directions reduces the total weight of the cables installed in the vehicle, so we have not only reduced material costs but also reduced fuel consumption. Using superposition and special coding and scrambling techniques, 100BASE-T1 reduces electro-magnetic interference (EMI), weight, cost and footprint compared to existing 10BASE-T and 100BASE-TX Ethernet standards.

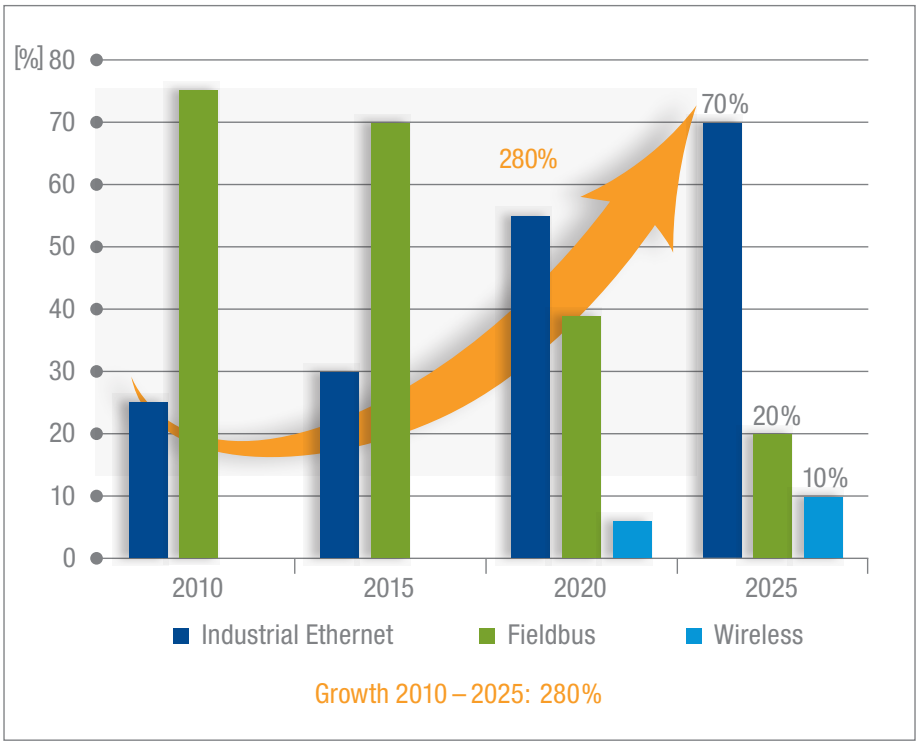
100BASE-T1 enables the transmission of audio, video, connected car, firmware/software and calibration data in vehicles using Ethernet protocols for Audio Video Bridging (AVB) via unshielded single twisted-pair cable. The AVB protocols developed by the IEEE Time-Sensitive Networking Task Group offer low deterministic latency, synchronized nodes, and traffic shaping. These aspects are important for the communication of different types of information in automotive systems and give 100BASE-T1 the ability to transmit different types of data with different priorities (low data rate with high priority, or high data rate with low priority and time synchronization).

The Industrial and Process Automation world took note of automotive's accomplishments with Single Pair Ethernet. Manufacturing and process engineers know that operational efficiencies will be gained with a common, higher bandwidth network encompassing much more of the power and data-carrying requirements manufacturing software calls for. The question was, "How do we get there?"

The 4th industrial revolution could be realized with the two-wire solution. So, the Ethernet standard IEEE P802.3cg, 10Mb/s Single Pair Ethernet Task Force group, formed. This group of companies and engineers took up the task of understanding everything that industrial fieldbus technologies do today to complete communication to the edge of the network, and they took up the task of building a unified Ethernet program that could replace them.

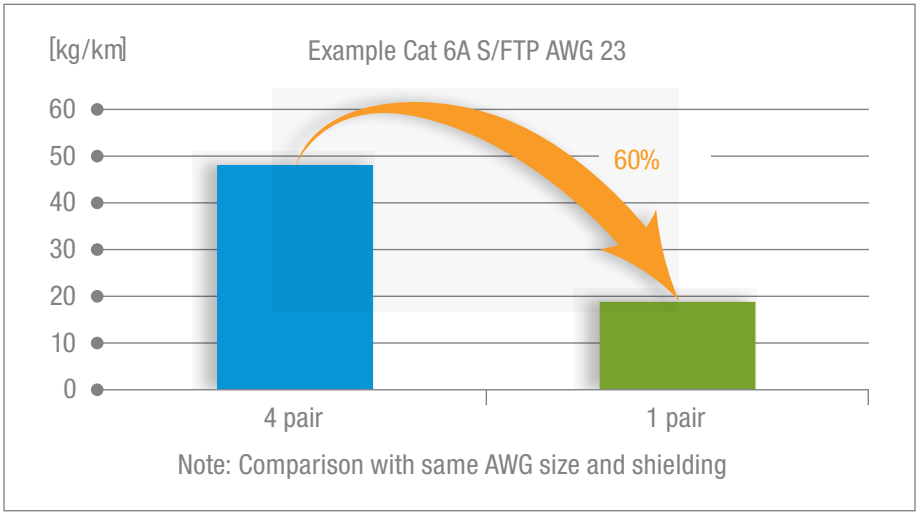
With the new SPE technology, it is possible to connect devices over a full 1000 meters at 10 Megabits per second throughput and even have PoDL technology as an option. Any of the fieldbus technologies with data rates from hundreds of kilobits per second up to 10Mbps can be replaced. The long reach of 1000 meters is the key. Now, SPE can come into hazardous environments, because remote powering will be possible. And now, SPE can be used in power generation and transmission, in oil and gas exploration and extraction processes, in mining environments and in chemical and wastewater processing.

Industrial Ethernet Market Shares



SOURCE: BELDEN

Weight Reduction through SPE



New cable standards from IEC

To be certain the long-distance applications come to be for these Industries, two new cable standards are currently being developed. The new cable standards, IEC 61156-13 and IEC 61156-14, describe symmetrical single pair cables with transmission characteristics up to 20 MHz over a distance up to 1 kilometer (km) to support 10Mbps for mainly industrial applications.

The cable type is intended to be used for shielded channels, and they may also support remote powering. Part 13 can be used for horizontal floor wiring, thus the specification for it to have a solid, annealed copper conductor, and a nominal diameter between 0.64 and 1.7 mm. Part 14 is intended for work area wiring and stranded wire, so it is in flexible materials.

We see our role and our responsibility to customers as insuring the Single Pair Ethernet cables fulfill the standards. We are completing all of the necessary electrical and transmission characteristic documentation and tests, mechanical and dimensional documentation of requirements, and insuring the environmental characteristics are met for bending, elongation, and tensile strength. When these things are done, we will have the solution for SPE for remote and hazardous

environment automation and instrumentation.

PROFIBUS & PROFINET International (PI), ODVA and the FieldCommGroup are working equally hard to support SPE for customers. They have specified an Advanced Physical Layer (APL) to connect power and data over a shielded twisted pair line to field devices and support the familiar trunk-and-spur-topology. With that, Ethernet in the Field really should be ready by 2021/2022.

APL is the ruggedized, two-wire, loop-powered Ethernet physical layer that uses 10BASE-T1L. It enables a direct connection of field devices to Ethernet-based systems in a way that process industries can benefit. With this, they can converge their IT and OT systems. Utilizing a switched architecture, the design intent is eliminating interference between devices connected to the same network.

Single Pair Ethernet in field

With the success of SPE in Automotive, the advanced standardization work on IEEE 802.3cg for the process industry, and the first jointly developed specifications from the user organizations PI and ODVA culminating in the APL, Single Pair Ethernet will move into the Industrial markets and replace current fieldbus technology, we have talked about.

The benefits over current solutions are too big to ignore. In 2016, the IEEE 802.3bp standard 1000BASE-T1 for higher data rates and the SPE standard IEEE 802.3bu for Power over Data Lines (PoDL) of Single Balanced Twisted-Pair Ethernet were published. This was a watershed moment in SPE's evolution.

"The IEEE 802.3bu project was initiated due to the increased utilization of Ethernet in automobiles in a single pair configuration. It also holds a good deal of promise for further applicability across a wide range of industries and within a rapidly growing Internet of Things ecosystem," said Dan Dove, chair of the IEEE P802.3bu Task Force.

"The standard defines a power delivery protocol that supports multiple voltages, and multiple classes of power delivery at each voltage, with assured fault protection and detection capabilities for identifying device signatures, as well as communicating directly with devices to determine accurate and safe power delivery."

As we have said, this remote and safe power delivery engineering is key. The question now moves to connectors.

Meanwhile, the standards for SPE cables and connectors have been pushed from international and national standardization groups. Now, cable standards for applications for long distances with transmission characteristics up to 20 MHz (IEC 61156-13 and -14) and also for applications with higher data rate and transmission characteristics up to 600 MHz and distances up to 40 m

(IEC 61156-11 and -12) for both horizontal floor and work area wiring are on the way.

Six new proposal connector standards for the various applications are in progress. Four of these SPE connectors in accordance with IEC 63171 parts 1 to 4 are designed for the office environment (IP20), thus mechanical, ingress and protection, climatic and chemical and electromagnetic (abbreviated as "MICE") level 1, or M1I1C1E1.

IEC 63171-5 and IEC 63171-6 are specified SPE connectors for the industrial environment (IP65/67). These 2-contact connector types can be used for levels 2 and 3, or M2I2C2E2/ M3I3C3E3 environmental conditions.

All of these connector variants have to fulfill the general requirements and tests for all shielded or unshielded free and fixed connectors for balanced single-pair data transmission with current carrying capacity. These connectors are intended to be used for Single Pair Ethernet according IEEE Ethernet standards: 10BaseT1 (IEEE802.3cg), 100Base-T1 (IEEE 802.3bw), 1000Base-T1 (IEEE 802.3bp) and PoDL (IEEE 802.3bu).

In addition, the Information Technology standard "Generic Cabling for Customer Premises ISO/IEC 3WD TR 11801 part 9906 – technical report: Balanced 1-pair cabling channels up to 600 MHz" describes balanced one-pair channels for the support of Single Pair Ethernet applications according the IEEE 802.3 SPE standards. This document clearly lays out that all of the standards – 1000 Mbps (IEEE 802.3bp) up to 40 m, 100Mbps (IEEE 802.3bw) with unshielded cable up to 15 m or 10Mbps (IEEE 802.3cg) up to 1000 m – are achievable, with cable design and wire diameter determining the reach that is possible.

With these standardization and specification activities for SPE in the Industrial field happening together and with them making the progress they have, we recently reached the point where "all of the oars were pulling the boat in the same direction."

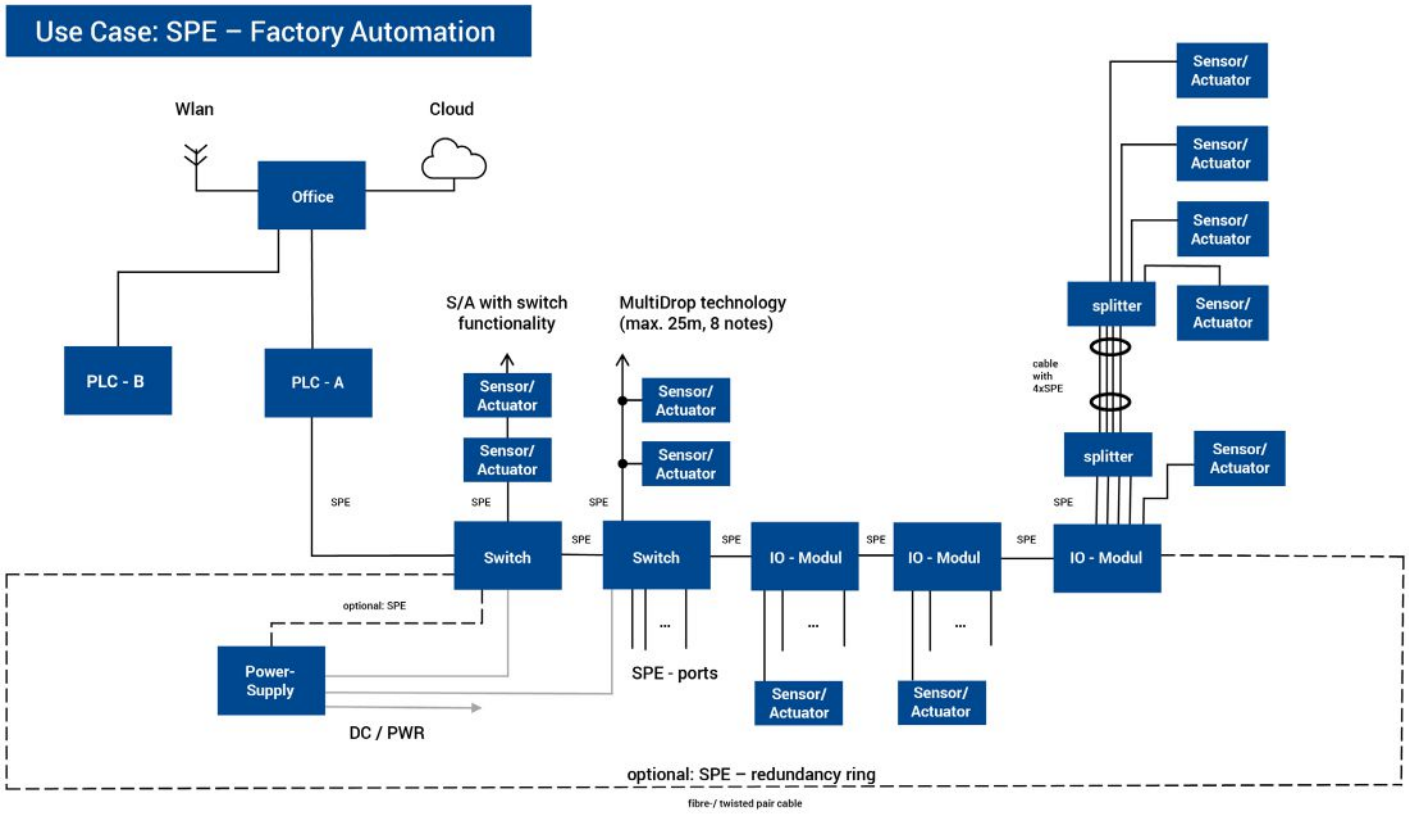
Now, a complete range of components, devices and applications for Single Pair Ethernet technology will bring Industry 4.0, the fourth industrial revolution, to the world with scalability, determinism and interoperability.

Ethernet Shielded Twisted Pair Cable

Year	IEEE 802.3 Standard		Max Distance	Speed	Bandwidth	Category*	Pairs
1990	IEEE 802.3i	10BASE-T	100 m	10 Mb/s	10 MHz	CAT 3	2
1995	IEEE 802.3u	100BASE-TX	100 m	100 Mb/s	100 MHz	CAT 5	2
1999	IEEE 802.3ab	1000BASE-T	100 m	1 Gb/s	100 MHz	CAT 5e	4
2006	IEEE 802.3an	10GBASE-T	55 m	10 Mb/s	250 MHz	CAT 6	4
			100 m		500 MHz	CAT 6A	4
					600 MHz	CAT 7	4
					1000 MHz	CAT 7A	4
2015	IEEE 802.3bw	100BASE-T1	15 m UTP	100 Mb/s	66 MHz	SPE	1
2016	IEEE 802.3bp	1000BASE-T1	40 m 15 m UTP	1000 Mb/s	600 MHz	SPE	1
2019	IEEE 802.3cg	10BASE-T1 10BASE-T1S	1000 m 25 m UTP	10 Mb/s	20 MHz	SPE	1
2020	IEEE 802.3ch	Multi-Gig	(15 m)	(2.5/5/10Gb/s)	---	SPE	1

SOURCE: BELDEN

** -- Category according to ISO/IEC TR11801- ...*



SOURCE: BELDEN

Single pair Ethernet technology in facotry automation example application.

Thriving IEEE 802 ecosystem

To better address the needs of all of these areas, IEEE 802 standards are constantly evolving and expanding. The success of IEEE 802 standards – from their inception about 30 years ago through today – has been due to the fair, open and transparent IEEE 802.3 development process.

Now, a new IEEE P802.3ch task force group for Multi-Gig Automotive Ethernet has been founded and research projects are underway to make this standard suitable for the industrial and building sector, too.

Belden teams throughout Germany and around the world embody our core competence in physical, electrical and electronic network infrastructure. When we meet with customers and fellow suppliers in standardization groups, the exchange of ideas and the challenges we put to one another make the end products better.

We have found this process for single pair Ethernet technology in new Industrial applications has gone just the same. Our customers are already seeing the benefits from that and in the next three to five years, they definitely will see it.

One network from the production process at the field level up to the control level (in PLCs) and up to the process management (MES) and enterprise level (ERP) truly can be a reality: one network from the sensor to the cloud.

Single Pair Ethernet will become the backbone of the fully digitized factory. Cost-effective, reliable cables, connectors and active components adhering to SPE mean all factory subsystems can get smaller and the amount of space and accommodation for power and temperature control go down. Simpler cabling and installation of components are going to drive materials and labor costs out of new factory floor builds.

We believe that focus on these details, engineering for plug and play installation and repair, fast-connection technology between connector and wire and between connectors, low cable weight, and systems for monitoring the complete network are going to turbo-charge the deployment of the IIoT in the near future.

Think about how Single Pair Ethernet will look on the automated, connected factory floor:

- One network from the sensor to the cloud guarantees control over all network components.
- Thinner, lighter cables enable a more orderly, defined cable infrastructure, but with more Ethernet channels in existing cable ducts.
- Single Pair Ethernet connector standard for M2I2C2E2 /M3I3C3E3 industrial environmental with universally known M8 and M12 connector designs well-established in industrial environments (IP65/67).
- SPE standard enables cable sharing (four SPE channels in one cable) and allows simple and cost-effective passive line distribution.
- Possibility of connecting network components via multi-drop bus technology in which all components are connected to one cable for short distance.
- Higher reliability through simpler cable and connector designs because there is only one channel.

Further in the future, there will be a globally uniform Ethernet network for every market and application area. There may continue to be a heterogeneous network infrastructure for certain system requirements. But the common thread through them all will be Ethernet that global suppliers agree on.

Fiber cables for long transmission distances and shielded CAT 7 copper Ethernet cables for high data rates with 4-pair for 10 Gigabyte per second will continue to be required. Still, when sensor and actuator and PLC data can be gathered and passed up to these trunks without translators and without proprietary interfaces, the industry will benefit.

Now, new single pair Ethernet components as switches, IO modules, connectors, splitters, and cables are starting to be developed for future IIoT requirements.

Part of our expertise is doing that alongside the work of insuring compliance to the standards and directives of the various end-markets such as fire protection for buildings or low smoke, halogen free cable for railway applications.

Technology report by ***Belden Corporation.***

Variable frequency drive design simpifies smart manufacturing

Variable Frequency Drives (VFDs) store a plethora of information that can be easily accessed. Regardless of the connection method, traditional fieldbus or Industrial Ethernet, the main objective can be to retrieve that production data and use it to create information that helps transform and drive business strategies.

PICK THE TERM THAT SUITS YOU BEST for the fifth industrial revolution – Industrial Internet of Things (IIoT), Industrie 4.0, and Smart Manufacturing are just to name a few. When you dig deep into each term, they all vary slightly on what they mean and the pathway to the fifth industrial revolution. But if you take a high level view of all different terms, they all revolve around three things: (1) connectivity of industrial devices; (2) acquiring data from industrial devices, and most importantly; (3) using the data to drive your strategy.

SOURCE: YASKAWA

Variable Frequency Drive designs have evolved over time to make Smart Manufacturing simpler for users.

Connectivity

When it comes to discussing connectivity, it mainly revolves around connecting a device to an Ethernet network. One of these industrial Ethernet protocols could be PROFINET, EtherNet/IP, Modbus TCP/IP, or EtherCAT to name a few. But if you take a look at the machines in your facility, you might discover that there is a lot of installed equipment that either do not support or cannot be made to support any of these protocols.

The thought of getting your plant to partake in the fifth industrial revolution has suddenly become an overwhelmingly daunting task, because of all the various devices on your machines that will need to be changed out and the capital that is required to make this all happen. However, this type of mindset is like trying to eat the whole elephant in one sitting. In reality, you may already have things in place that can get you moving in the direction that you're trying for, i.e. eating the elephant in small sizeable chunks over a period of time (sorry to elephant lovers that may be offended by the analogy).

One step is taking a look at the devices that are currently installed on your machine. Of primary interest would be if your machine has a variable frequency drive, or VFD, installed. A VFD is responsible for the prime mover, i.e. motor, that is used to run your machine. Its ability to vary speed of machines through electrical means has allowed machines to have fewer mechanical components, hence less wear component to worry about.

Its inherent energy saving capabilities are an added bonus. But when it comes to the fifth industrial revolution, a VFD can provide a plethora of information. It's just a matter of accessing all the information and putting it to use. A VFD that has an embedded protocol like Modbus RTU installed can take advantage of that with no additional cost. It would just be a matter of adding a Modbus RTU master that can be used to retrieve the data from the VFD. Or perhaps your machine was already designed using an existing fieldbus protocol like PROFIBUS or DeviceNet, in which case you're already connected to a network and the ability to gather more data is available.

Data

As mentioned previously, a VFD has a plethora of information contained. Regardless of the connection method, traditional fieldbus or Ethernet, the main objective is to be able to pull that information out of the VFD and be able to use it to your advantage. One such example is reading the VFDs output current.

When read instantaneously, the output current from the VFD could provide information on whether or not the machine is overloaded due to the process or a mechanical failure that is present. But if the output current is recorded and monitored over time, the data could be analyzed to provide deeper insight into the machine. If the operating current has steadily increased over time, this could indicate that there are mechanical components that are starting to wear and will eventually fail. With this information, you can proactively plan to change out the offending components at the next scheduled downtime, or face costly downtime if the component fails while in operation.

In addition to being able to implement preventative maintenance measures, another large advantage is being able to analyze and correlate different pieces of data to achieve different objectives. Perhaps you want to be able to maximize how efficiently your machine is producing a component (i.e. energy used per part). Recording the power output of a VFD over time and the number of parts produced, which would be a data point from a different part of the machine, you can achieve a quantitative value. This will allow you the ability to experiment and vary the throughput of the machine to find this value. Or perhaps you are trying out a new process and want to get insight on how the machine reacts to the new process. Being able to read various data points from the VFD like current, output frequency, output power, plus other values from sensors that are mounted on the machine, can give users a bigger picture look and determine if additional tweaks are needed or not.

Getting your factory to join the fifth industrial revolution shouldn't be a daunting task. Taking a careful look at what you have available and taking on various tasks as small chunks will go far. You may be surprised to find that you already have things available to help you along the way. Perhaps it is a VFD that isn't currently connected to a network, but can easily be put onto a network using the embedded protocol, like Modbus RTU. Or perhaps an existing fieldbus is already in use. It's just a matter of taking advantage of this. You might be surprised by how quickly and easily it is for you to join IIoT, Industrie 4.0, Smart Manufacturing … pick a term.

Edward Tom, Drives Product Manager, ***Yaskawa America, Inc.***

industrial ethernet book

Reader Service Card

IEB issue 114 - October 2019

IMPORTANT: You must update your subscription annually to continue receiving your free copy of Industrial Ethernet Book magazine.

Return by mail to:
IEB Media
Bahnhofstr. 12
86938 Schondorf
Germany

Or use our online reader service at:
www.iebmedia.com/service

Please enter your contact details below:

Name: _____
Position: _____
Company: _____
Address: _____
_____
City: _____
State: _____
Zip Code: _____
Country: _____
Phone: _____
Email: _____

I want to:

☐ **Start** a new subscription
☐ **Update** my subscription
☐ **Digital** edition or ☐ **Print** edition
☐ **Change** my address
☐ **I do not want** to receive promotional emails from Industrial Ethernet Book
☐ I want to be **removed** from the subscription list

Signature: _____

Date: _____

Company Activity (select one)

☐ Aerospace/Defence
☐ Electronics Industrial/Consumer
☐ Instrumentation/Measurement/Control
☐ Manufacturing Automation
☐ Metal Processing
☐ Mining/Construction
☐ Oil & Gas/Chemical Industry
☐ Packaging/Textiles/Plastics
☐ Pharmaceutical/Medical/Food & Drink
☐ Power Generation/Water/Utilities
☐ Research/Scientific/Education
☐ System Integration/Design/Engineering
☐ Telecomms/Datacomms
☐ Transport/Automotive
☐ Other: _____

Job Activity (select one)

☐ Engineer - Instrumentation & Control
☐ Engineer - Works/Plant/Process/Test
☐ Engineer - Research/Development
☐ Designer - Systems/Hardware/Software
☐ Manager - Technical
☐ Manager - Commercial or Financial
☐ Manager - Plant & Process/Quality
☐ Scientific/Education/Market research
☐ Other: _____

Looking inside the real-time capabilities of Industrial Ethernet

Behind every Industrial Ethernet protocol lies an organization that advances the standardization and popularization of the respective protocol. Each of these organizations has formulated a Time Sensitive Networking strategy. Consequently, we will see nearly all existing protocols again with TSN.

REAL-TIME INDUSTRIAL ETHERNET has experienced a huge upswing over the last few years. Although classic fieldbuses are still running in large numbers, they have passed their prime. The popular real-time Ethernet protocols extended the Ethernet standard to meet the requirements for real-time capabilities. Time Sensitive Networking (TSN) now provides a new route to real-time Ethernet.

Real time and communications

In the context of factory automation and drive technology, real time means safely and reliably reaching cycle times in the range of less than ten milliseconds down to microseconds. For these real-time requirements to be satisfied, Ethernet also had to gain real-time capabilities.

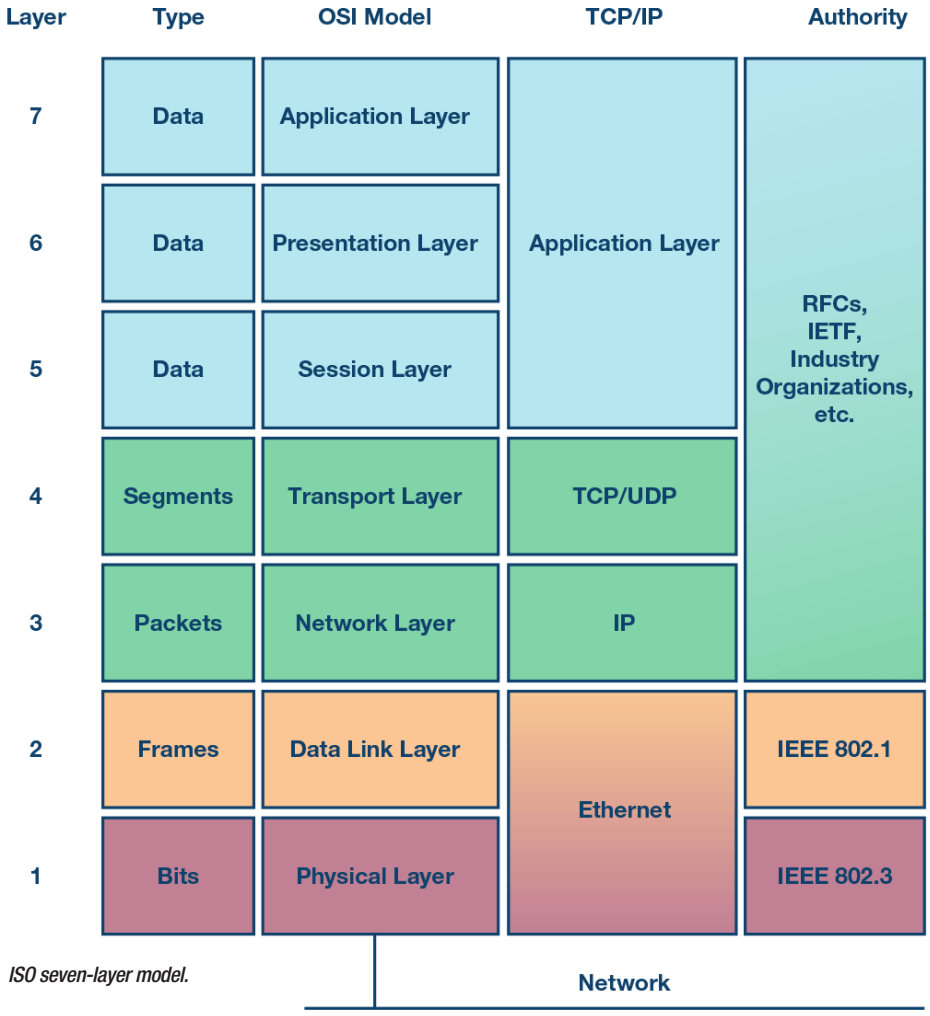
Ethernet is a lot faster than a fieldbus—so what?

For the real-time requirements of automation to be satisfied, both transmission bandwidth and transmission latency need to be guaranteed. Even if these bandwidths are usually decidedly small (a few dozen bytes per device), this transmission channel must be available in every I/O cycle with the required latency.

However, the guarantee of latency and bandwidth is not provided with classic Ethernet. On the contrary, an Ethernet network may discard frames at any time if this is necessary for operation. What does this mean?

Ethernet is a so-called bridged network. The frames (Ethernet frames) are sent from one point to another: From the endpoint to the switch (bridge), from there possibly to other bridges, and finally to the other endpoint. This architecture is largely self-configuring. The bridges first completely receive frames before forwarding them. And this is where multiple problems arise:

- If at peak times there are more frames to store than the buffer memory in the bridge can hold, then the newly incoming frames are discarded.
- Because the frames differ in length, they are delayed as a function of their lengths. This leads to fluctuating latencies (jitter).



ISO seven-layer model.

SOURCE: ANALOG DEVICES

- Because the port through which the switch is supposed to send a frame may already be occupied by other frames up to the full frame size, additional delays come into play. The sending of a large Ethernet frame (1522 bytes) takes about 124 µs at 100 Mbps.

We can argue that Ethernet normally works well and is somehow fair. However, by doing so, we use two words that make no sense in connection with hard real time. It is not enough if a real-time condition is only normally met. It always has to be met.

Anyone who lives next to a chemical plant or a refinery can appreciate this. And industrial communications aren't fair either: The most important thing, the control/closed-loop control application, always has priority.

Real-time extensions illustrated using PROFINET and EtherCAT as examples

Because no solution to the problem was available in the IEEE, which is responsible for Ethernet standardization, the industry developed its own solutions—once again demonstrating its innovativeness. The solutions all have their strengths and weaknesses, and ultimately address different markets.

PROFINET: universally applicable

With PROFINET, two complementary solutions are offered. PROFINET RT is a factory automation solution with a cycle time of up to 1 ms. RT is directly based on standard Ethernet. The possibilities of

iManufacturing

Intelligent Manufacturing & Integrated Solutions Expo

亚洲智能集成及智能制造解决方案展

2019.11.25-27

Shanghai New International Expo Center

10,000 Trade Visitors

40 Presentations

200 Industry Leaders

www.asia-iMan.com

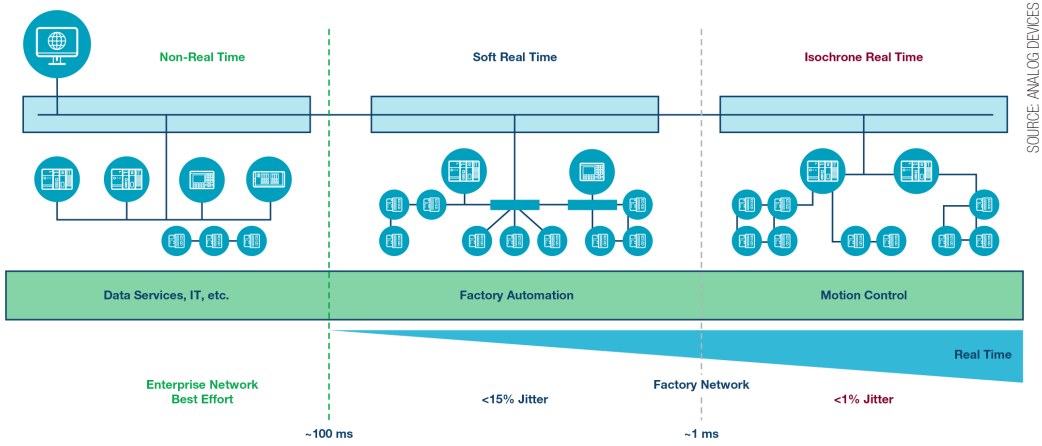
Visitor Registration

Website

Organizers

中机国际 SINOMACHINT

Messe Düsseldorf Shanghai



SOURCE: ANALOG DEVICES

Real-time communications in automation.

Ethernet (for example, quality of service (QoS, prioritization)) are utilized to give real-time traffic priority. That helps, but QoS does not completely solve the resource and latency problem. That's the reason for restriction to soft real time. The good compatibility with other protocols (such as HTTP, SNMP, and TCP/IP) used in the network is a clear strength of the technology.

For hard real time, PROFINET offers the isochronous real-time (IRT) extension. Here, part of the Ethernet bandwidth is reserved exclusively for IRT traffic through an extension to standard Ethernet hardware. This is made possible by precise synchronization of the clocks in the IRT nodes. As a result, a channel (the red phase), can be blocked for normal traffic in every cycle. Only IRT frames in the red phase reach the network. In addition, the network participants send the IRT frames exactly at pre-calculated times, enabling maximization of efficiency within the red phase. The IRT frames move almost without slip through the network. One advantage of this is that it limits the length of the red phase, in which all other traffic must wait, to the bare minimum. The red phase can occupy up to 50% of the bandwidthl.

As already mentioned, a full length (1552 byte) Ethernet frame needs about 124 µs on the wire. If PROFINET IRT occupies a maximum 50% of the bandwidth, the fastest cycle time is 2 × 124 µs = 248 µs, or 250 µs when rounded up. Only in this way can other protocols (like HTTP) coexist in unchanged form with it.

Even faster cycle times of down to 31.25 µs are possible due to PROFINET 2.3 for IRT's optimizations, including fast forwarding, dynamic frame packaging, and fragmentation.

EtherCAT

In the development of EtherCAT, there were other requirements in the beginning. EtherCAT is a fieldbus based on the physical Ethernet—that is, layer 1. Even layer 2 is optimized for fieldbus applications and high throughput. EtherCAT doesn't have the classic Ethernet bridge. It uses a summation frame telegram, which makes data transmission efficient.

Instead of normal Ethernet, in which a separate frame is sent by each device involved in communication between devices, EtherCAT sends one frame per cycle. However, this frame contains all data for the addressed devices. While the EtherCAT frame is being forwarded by a device, the data for that particular device are inserted into and taken out of the frame live. Through this, very short cycle times of even less than 31.25 µs, in the extreme case, can be achieved.

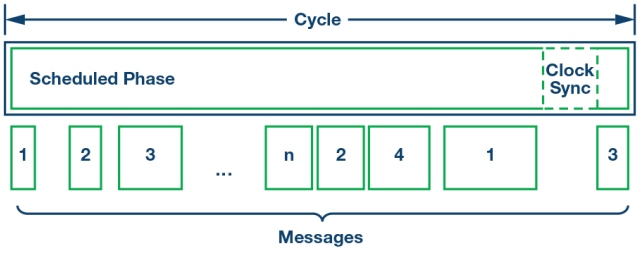
EtherCAT also has time synchronization. Effort was put into enabling not always ideal Ethernet interfaces on a PC to be used as EtherCAT masters. Traffic such as web or TCP/IP traffic can only be transported in small portions in piggyback style over EtherCAT; direct coexistence on the wire is not possible.

Unscheduled Network

- Cycle Times Down to 1 ms
- CIP Sync Provides 1588v2 Time to Nodes
- PROFINET RT (Class B) Has No Time Sync Mechanism for Nodes

EtherNet/IP

PROFINET (RT)

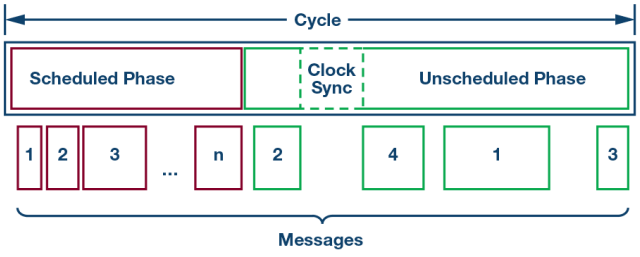


Scheduled Network

- Cycle Times Down to 31.25 µs
- PROFINET IRT (Class C) Time Sync in Unscheduled Phase
- SERCOS Scheduled Phase Encapsulated in 1 Message

PROFINET (RT)

sercos international

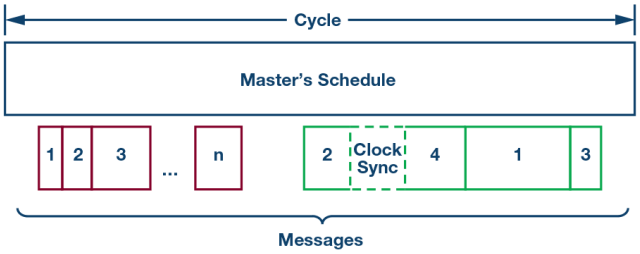


Master/Slave Network

- EtherCAT
  - Cycle Times Down to 12.5 µs
  - Encapsulated in 1 Message
- POWERLINK
  - Cycle Times Down to 100 µs

EtherCAT

ETHERNET POWERLINK Standardization Group



SOURCE: ANALOG DEVICES

Overview of EtherNet/IP, sercos and Ethernet Powerlink protocols.

What about the others?

POWERLINK takes the same basic approach that EtherCAT does; it assumes complete control over the Ethernet and transports IP applications by piggyback to the nodes. But that's the only thing they have in common. POWERLINK does not employ a summation frame protocol. Nevertheless, it performs similarly well in practical applications.

Like IRT, SERCOS has a reserved bandwidth, but uses a summation frame protocol within it. SERCOS allows other protocols to coexist.

It's time for TSN

IEEE approached the topic of real time within the scope of the audio/video bridging (AVB) protocol. In the improvement of the protocol, the more challenging real-time communications of industry were also considered.

The original name for the set of standards, AVB2, was hereupon changed to TSN (for time-sensitive networking). With these standards, it is now possible to use a unified, deterministic version of Ethernet.

This actually makes many things easier. Well-known industrial networks are nearly all defined for 100 Mbps. Today, however, gigabit Ethernet and 10 Mbps Ethernet have become the focus of attention in special applications. The TSN standards cover all speeds. With TSN, the wheel does not have to be reinvented: if it weren't for TSN, all of the existing standards would have to be redefined for gigabit—which would result in costs for hardware development and in market fragmentation.

Real time with TSN

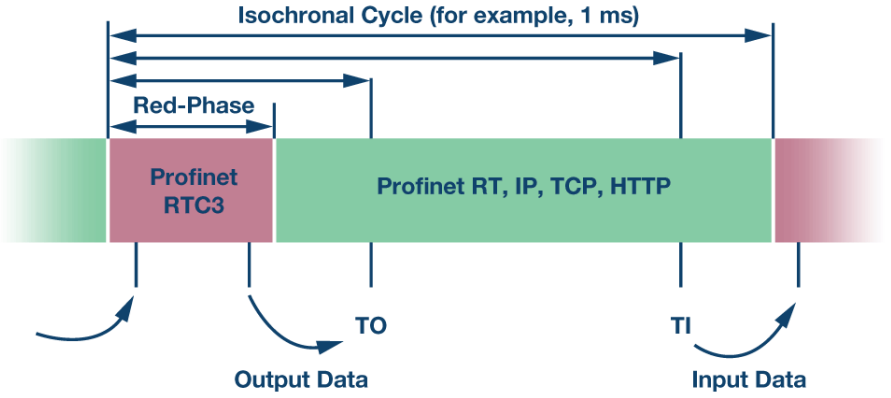
TSN extends layer 2 of Ethernet to include a series of mechanisms needed for real-time operation:

- 802.1AS/802.1AS-Rev provides for extremely precise synchronization of the clocks in the network.
- The time-aware shaper (TAS) option enables Ethernet to be operated with hard scheduling. With it, one or more queues of the QoS model can be blocked/released at specific times.
- The preemption (interspersing express traffic) option enables long frames to be broken up into smaller parts so that delays are minimized for higher priority frames. It can be used to optimize the guard band for TAS or replace TAS at speeds of above 100 Mbps.
- The frame replication and elimination for reliability option can be used for the definition of redundant paths through the network; for example, in rings.

Use of software-defined networking means that frames are no longer forwarded to the destination by means of the hardware MAC address of the destination node, but are rather forwarded through a combination of special MAC addresses (locally administered multicast MAC) and VLAN IDs. How these frames are routed through the network is no longer automatically determined, but rather configured by software. This combination of multicast MAC and VLAN ID is called the stream ID and all TSN frames with the same stream ID are called the TSN stream. A TSN stream always has just one sender, but it can have several recipients.

The TSN streams can now be set up in consideration of the existing resources in such a way that no frame has to be discarded anymore. The bridges now use their resources for loss-free forwarding of the TSN streams.

The best effort traffic (standard Ethernet, IP, web) takes place completely normally with the remaining resources (memory/bandwidth).



SOURCE: ANALOG DEVICES

PROFINET IRT.

What happens above Layer 2?

Behind every Industrial Ethernet protocol lies an organization advancing the standardization and popularization of the respective protocol. Each of these organizations has formulated a TSN strategy. Consequently, we will see nearly all existing protocols again with TSN—in one form or another. Staying with our examples:

For PROFINET, the path to TSN is a relatively short one because there is already a wealth of experience with time-aware shaping available (it is already done very similarly to IRT) and the coexistence of industry and IT protocols has always been supported. Much remains the same for the user, so a familiar environment can yield new performance.

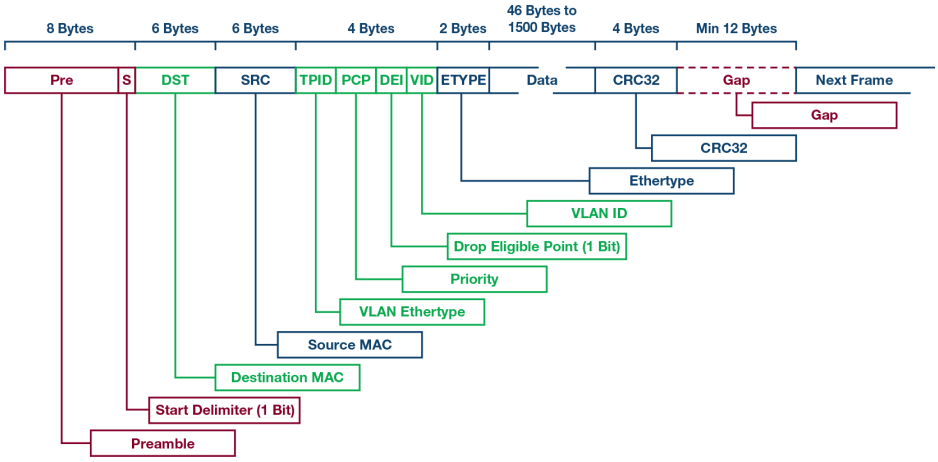
EtherCAT and, similarly, SERCOS will make TSN accessible above the field level. For example, the EtherCAT automation protocol (EAP) is very suitable for networking classic EtherCAT segments via TSN at a low overhead.

However, there are also new players in the field. There is a group that is defining a completely new industrial Ethernet protocol. OPC UA is being used as the application layer. TSN is seen as a means for making this protocol real-time capable. However, work still has to be done here. A new transport layer for OPC UA, the so-called OPC UA PUB/SUB protocol, is needed for the transport.

Does a lot help a lot?

Today we are using 100 Mbps Ethernet in industrial automation and soon gigabit Ethernet will be available. However, higher speed does not automatically mean guaranteed latency and guaranteed transmission. Hence, for hard real time, special mechanisms are always necessary. With TSN, they are now standardized.

Volker Goller, systems applications engineer, ***Analog Devices.***



An Ethernet frame, with parts relevant to TSN data stream identification shown in green.

Cyber security in the oil and gas industry: preparation for risks

By following federal and industry standards and implementing a defense-in-depth approach to cybersecurity, hydrocarbon professionals in the oil and gas industry will be better prepared to prevent the financial, informational and physical risks that can result from a cyber-attack.

THE OIL AND GAS SUPPLY CHAIN IS A GLOBALLY interconnected environment, moving millions of barrels of crude oil and billions of cubic feet of natural gas on a daily basis. Due to the increasing demand in global energy, the oil and gas industry faces many disputes and challenges in the service sectors of exploration and production (upstream); processing, storage and transport (midstream); refining and processing (downstream); and oilfield applications. One of these challenges is the growing risk of cyber threats.

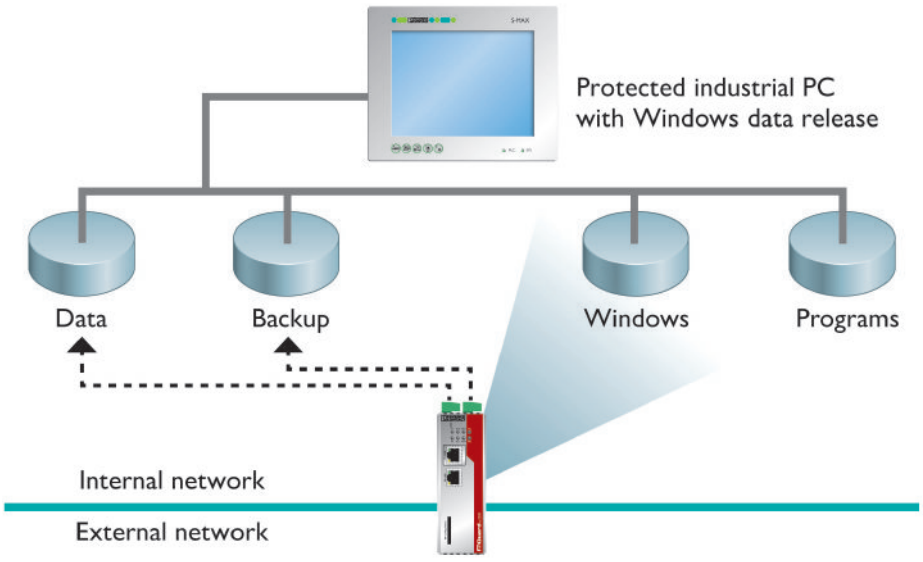
Today's industrial Ethernet and wireless technologies have made it easy for oil and gas professionals to share data faster and more efficiently – whether they are on an offshore platform or back in the main office. All of these far-flung locations, spread throughout the globe, are connected via complex, enterprise-wide networks transferring critical data between all areas of production and processing and to the corporate headquarters for planning and scheduling purposes. Connecting control systems with the business world optimizes operations.

However, these complex communication networks distribute data in all directions and to multiple applications, increasing the risk of cyber threats. An accidental virus infection could shut down production, costing millions of dollars in lost revenue. The global supply chain infrastructure is susceptible to numerous risks and threats; any intentional or accidental disruption anywhere along the communication path could result in a catastrophe.

This susceptibility of the communication path begins at the wellhead and ends at the distribution point at the other end of the supply chain. Hackers have a long path on which to find a small back door that allows them entry to inflict potential damage. This is not a simple violation of the companies' privacy or security.

Cybersecurity guidelines

According to a news release from Tripwire, 82 percent of oil and gas industry respondents said their organizations have seen an increase in successful cyberattacks over the past 12 months. The study, by Dimensional Research in November 2015, included more than 150 IT professionals in the energy, utilities, and oil and gas industries. The study also found that 69 percent of oil and gas respondents said they were "not confident" their organizations were able to detect all cyberattacks. Unfortunately, there are numerous examples of cyber risks and threats to the oil and gas industry.



SOURCE: PHOENIX CONTACT

CIFS Integrity Monitoring is an alternative to traditional anti-virus methods.

One of the biggest threats appeared in 2012, when the Shamoon virus attacked Saudi Aramco, the world's leading oil and gas production company. The virus erased data in at least 30,000 of Aramco's corporate computers. Aramco reported that the objective of the attack was to stop the company's production, which represents more than 10 percent of world oil supply.

Shamoon is just one example of a threat to strike the industrial world. Other well-known malware includes Stuxnet, Flame and Duqu, but others are likely lurking undetected. A hydrocarbon system could come under cyber-attack for multiple reasons:

- Financial gain: providing insider information
- Intellectual property theft
- Supply disruption from environmental activists
- Supply disruption from political activists
- Disgruntled employee
- Gaining unlawful access to technology related to production and processing
- Terroristic threat
- Cyber warfare by a rogue nation

The owner-operators must address all of the above points as they begin designing and maintaining a "cyber-secure" control and communications network infrastructure throughout the entire supply chain, from the wellhead to the final distribution point. How will an owner-operator develop, implement and maintain a corporate-wide, global-yet-local cybersecurity strategy of this magnitude?

In the new cyber world order, everyone should be involved in the design and engineering of cybersecurity guidelines for existing systems. This represents a huge challenge for owners and operators. They now need to locate and map out the entire supply chain network and determine what technologies, best practices and programs are suited for the specific system without any production interruptions. Meanwhile, they must meet the cybersecurity guidelines that government agencies have imposed for the specific industry.

Protection of critical process data

Hydrocarbon production, processing and distribution systems have evolved and

developed based on a safety culture. Most owner-operators have already implemented a common health, safety and environmental (HSE) culture to ensure that their facilities meet the industry's needs. The next step is integrating measures and procedures into this existing system from day one.

Protecting the entire digital network infrastructure must become a part of the norm. It is important for the global oil and gas industry to protect its valuable assets. This means that there is an informal security interest for the protection of the flow of oil and gas, which benefits both producing and consuming nations. Supply chains all over the world are regulated by the country of origin. In the United States, for example, the supply chain network is part of the critical infrastructure and is regulated by the Department of Homeland Security and its Chemical Facility Anti-Terrorism Standards (CFATS).

Hydrocarbon companies acknowledge that hackers and malware will get into their systems. Knowing this, these organizations must take a proactive approach, focusing on the protection of critical process data. Owners and operators need to point out the location of the critical data, identify the characteristics of the systems that carry the data, understand the vulnerabilities of those systems and detect changes in activities that signal potential cyber-attacks.

Cooperation-control engineers & IT

Network security is the highest priority of IT staff, but it is low on the radar for most control engineers or plant managers. The discovery of the Stuxnet worm, however, forced industrial plant managers to bring a higher level of attention to the operational risks that chemical, oil and gas, and other critical plants face. Since then, control engineers have realized that they need to take an active role in security, and not leave it entirely in the hands of IT.

To create a secure network, control engineers and plant managers must work together with the IT department and the technology they use. They face the difficult task of placing protective measures around and within existing systems and still maintaining the flexibility of multiple protocols and technologies. A good first step is to completely know and draw your existing network plant and if needed, place it behind the current IT infrastructure. Recommended best practices include:

- Insulate and isolate communication between the corporate and the plant networks with a router
- Filter data coming in and out with a firewall; this also promotes network segmentation
- Avoid accidental, unauthorized access by blocking and managing access controls
- Mitigate viruses and malware that come into your systems with integrity monitoring scans and detection tools
- Use virtual private network (VPN) technology to send and receive encrypted data from remote locations.

SOURCE: PHOENIX CONTACT

Today's industrial security devices can provide a defense-in-depth option for critical applications.

Rugged industrial security devices

In the industrial world, productivity drives business. When the Internet started growing, control systems evolved from isolated islands to highly interconnected systems. The concept of "security by obscurity" as a tool to protect control systems from cyber-attacks is not realistic. However, network architectures can be protected and guarded by specific devices coded with the same IT secure technology, but designed to meet the rugged, hazardous conditions that may be present in a hydrocarbon plant.

Today, there are security devices with industrialized hardware and advanced configuration options that can provide defense-in-depth for critical applications. These devices have security capabilities including firewalls with integrated router and VPN. The Common Internet File System (CIFS) is the standard way that users share files across corporate intranets and the Internet.

Some industrial security devices include CIFS Integrity Monitoring, an antimalware tool used in industrial PCs to scan Windows-based systems for files that have been manipulated by malware, without the need of updating the database of signatures. Industrial devices can also save and store logs from data packets and information coming in and out of the network for audits with the corresponding federal regulatory agency.

Secure, cloud-based portals

A defense-in-depth approach to cybersecurity incorporates multiple layers of protection to keep unwanted traffic off the industrial network.

It is proven that diverse layers of protection within industrial networks are a better approach than a single, monolithic one. This defense-in-depth method of protection delays, more than prevents, access from unwanted users. These measures not only connect and protect, but can also be easily integrated into production environments and industrial systems.

No matter what security measures the owner of the hydrocarbon plant takes, there is always a possibility of a breach, so a disaster recovery plan is still critical. This plan should be tested and practiced. Defensive strategies must be monitored and active at all levels of possible attacks: detection, isolation, containment and elimination.

Taking this protection one step further, there are now secure, cloud-based portals that can integrate industrial devices and automated systems directly into the network without modification or planning. A professionally hosted service can give oil and gas system operators easy access to fast and secure remote support, offering complete encryption of data and stateful firewall protection for every site.

Conclusion

Oil and gas companies understand that cyber-attacks have increased over time and that they need to take a more comprehensive and proactive approach to protect their critical systems. In the constantly changing cyber world, protecting control systems will be an ongoing responsibility that everyone – from the owner-operator to the control engineer to the IT staff – must share.

Mariam Coladonato, Product Marketing Specialist Networking and Safety, ***Phoenix Contact USA.***

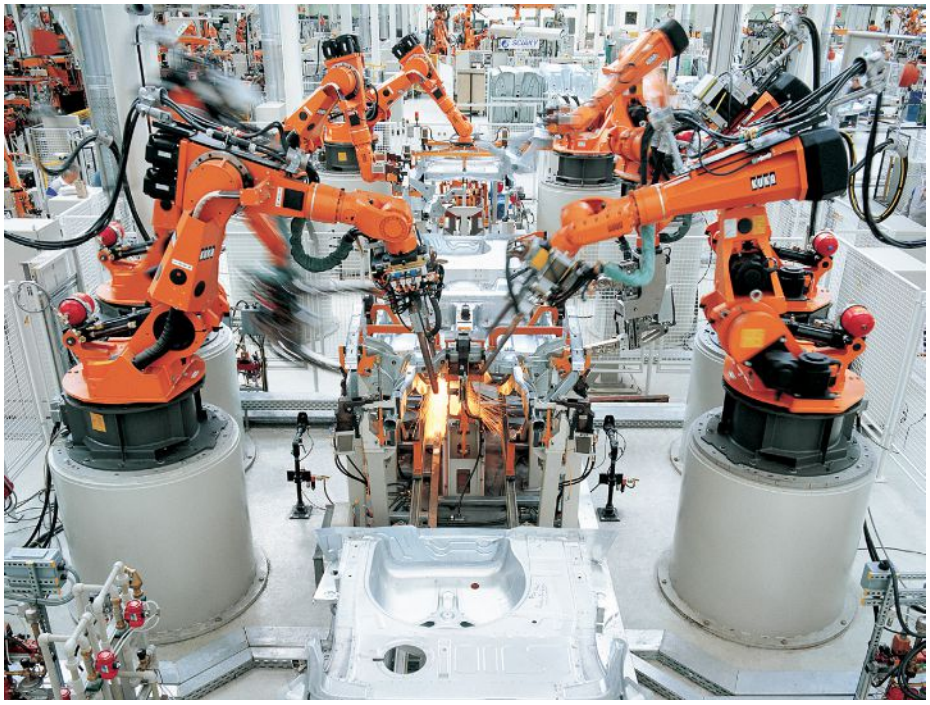
Business impact of TSN for industrial systems

Time Sensitive Networking enables the convergence of networks and systems that were previously separate for reasons of operational integrity, real-time performance, safety or security. Breaking down communication barriers between critical and noncritical systems is a foundational concept of the IIoT and Industry 4.0.

THE EMERGENCE OF THE INTERNET OF THINGS (IoT) is driving the need for networked, time-aware systems in all sectors of the economy. In the industrial market, evolution of the Industrial Internet of Things (IIoT) will increase the amount of data harvested through distributed networks, requiring new standards for managing and transferring critical and non-critical information. There will be a demand for higher levels of reliability and security than what is provided by today's numerous specialized and segregated industrial communication standards. The latest set of IEEE 802.1 Time Sensitive Networking (TSN) standards represents the next evolution of standard Ethernet technologies, targeted to meet these new market demands.

Industrial control applications require consistent and deterministic delivery of data from sensors to controllers and to actuators. The data exchanged between these components is critical in controlling any manufacturing process and it is imperative that interference or hindrance of this exchange is minimized. Historically, this has not been problematic for most automation systems, as control data has been physically segmented from information data over separate networks. However, moving forward, the Industrial Internet of Things (IIoT) proposition changes that paradigm because manufacturers are looking to glean insights and analytical information from the same sensors and devices that are also controlling the process.

Therefore, the total amount of data communicated over the same network increases. Some of that data is critical for control systems, while other data is needed for both the information and analytical systems. TSN is one way to ensure that this control data traffic is delivered in a timely manner by securing bandwidth in the network infrastructure, while simultaneously allowing non-critical forms of data traffic to coexist on the same network. TSN provides the tools to enable the convergence of different data traffic on the same physical network, reducing the infrastructure cost.



SOURCE: AVNU

With TSN's intelligence, systems becomes more automated and less dependent on human intervention and error.

What is TSN?

Time Sensitive Networking (TSN) is a collection of Ethernet standards introduced by IEEE, which defines a new set of mechanisms for managing traffic. TSN standards define new functions for Ethernet networking such as traffic shaping, frame pre-emption, traffic scheduling, ingress policing, and seamless redundancy. When all parts of a network are running with the same sense of time, traffic can be coordinated based on a schedule, one method that allows for better control of critical traffic. These new features provide a whole new layer of control for managing Ethernet traffic; but from a business perspective, is it worth the investment?

The legacy of Ethernet

Since its inception in the 1970s, Ethernet has morphed from a CSMA/CD technology where hubs were used for connecting multiple segments together. Over the years, hubs and collision detection methods have given way to switches and switching technologies. Prioritization mechanisms were introduced to give preference to critical traffic over non-critical traffic, and traffic shapers provided further control to help ensure reliability for data delivery.

As new technologies and features have been introduced to "standard Ethernet," the number of mechanisms added to the control plane has expanded, and today's switches carry all these functions in order to be backwards-compatible for any application. The majority of today's switches carry nearly 50 years of technology, most of which is not used in any single application.

A drawback to this phenomenon of "feature accumulation" is the multitude of control functions that has left the switch and the network itself fundamentally unpredictable and incapable of being modeled. As various prioritization mechanisms are enabled and weighting mechanisms are applied, and as traffic shapers are employed and more switches are arranged into increasingly complex topologies, the ability to know when data will arrive or if it will arrive has become murky at best.

Most networks today are designed with an empirical sense: If a certain design worked on a previous system with 'X' amount of data over 'N' nodes, then this design should work with a few extra nodes and a few more bytes of data. But the difference between should work

and will work can be an installation that goes in smoothly, or one that requires additional hardware or extra conduit – at a point in the commissioning cycle when such additions can be extremely expensive.

Historical network configuration

Traditionally, network configuration has been managed on a component-by-component, switch-by-switch, and node-by-node basis. The software used for such configuration has been similar to DOS in its presentation, utilizing such interfaces as CLI (command line interface) where hierarchical precepts are often inferred and knowing where one is in the command hierarchy is often not intuitive or clear.

Furthermore, if the configuration of one switch or router requires a complementing configuration in an adjacent router or switch, any configuration error in either of the adjoining components would cause problems in the network. Essentially, there is no system-level knowledge at the component level for configuration. Both the CLI interface as well as the PuTTY (terminal emulator) interface are cryptic and difficult to navigate. Closer inspection of the command lines themselves begs the following questions: "What set of skills must I hire to manage my networks?" and "Is this really necessary in the year 2019?"

TSN network configuration

If TSN represents yet another layer of new standards added to an already complex system, how can TSN create a simpler system for the end user?

TSN standards were specifically designed to facilitate system-level configuration and were created with a system view in mind, rather than from a component perspective. TSN enables end-stations to publish their requirements on the network and allows bridges and switches in the system to announce their capabilities to the wider network. As an example, the "P802.1Qcc Stream Reservation Protocol (SRP) Enhancements and Performance Improvements" specification is one of the mechanisms designed to allow the network infrastructure to be more intelligent at a system level and to convey the information necessary to transition the control plane from a manual configuration workflow to an automated process.

In the future architecture pictured above, the user is provided a view of the system that allows for the configuration of the I/O and control devices as well as for the layout of the topology and the infrastructure devices. A core principle of the TSN value proposition is that all network communications are managed so that performance and data delivery are guaranteed. To accomplish this, all devices need to participate in traffic planning by publishing to or notifying the system of its traffic requirements and of its capabilities for managing traffic.

In this example, a Centralized Network Configuration engine, or CNC, is used to configure the system. In this future reality, the CNC is an intelligent tool, enabled by the information collected and conveyed from TSN standards; it will calculate the best possible solution to accommodate all the traffic flows between all connections in the network. The system sees the available bandwidth and configures the infrastructure components in the network (i.e., the bridges) to accommodate the traffic flows. If the system is not able to solve for a configuration that meets the performance requirements and loads of the traffic streams in the subnet, it will notify the user so that topology, performance requirements, or loading can be modified.

TSN makes it possible to run the calculations that can help the implementor predict if a network design will be successful for a given application. This wasn't possible in previous generations.

With TSN's intelligence in the network, the system can become more automated and less dependent on human intervention and subsequent error.

Meaning for businesses?

The industrial market currently requires two types of networking professionals: informational technology (IT) and operational technology (OT). The current industrial control and associated enterprise-wide systems require many IT and OT personnel to manage and configure network infrastructure and control system parameters. Now, with TSN and its potential for smart software, there is an ability for the smart system to configure the network infrastructure. With TSN's intelligence in the network, it becomes more automated and less dependent on human intervention and subsequent error.

The costs for highly-trained personnel could be mitigated using intelligent systems and devices capable of participating in a wider, self-configuring ecosystem. Software Defined Networking (SDN) type tools can enable system-level configuration software, as well as diagnostic and monitoring tools. These new mechanisms would allow the end user to finally manage the network from the manufacturing floor to the business systems.

System modeling & network design

TSN is expected to bring a holistic approach to network management, enabling new tools for system-level configuration. In this new paradigm, payload, sampling frequency and maximum latency might be managed from a system-wide view and then used to calculate flows and configure bridges and infrastructure to meet the application demands.

This approach to network management would dramatically change the workflow for designing and planning networks. TSN provides the foundation for network calculus and planning as part of the solution toward managing traffic and guaranteeing performance. If designs prove inadequate or a solution is not achievable given system constraints, then network design could be modified to accommodate the system requirements.

Through TSN's modeling methods, system designers could proactively answer questions about the network capability before the system is integrated, which allows them to plan for the traffic that needs to be managed.

In addition to understanding the capabilities of the network today, users want to know about possible future capabilities to support business growth. Today, there is no reasonable capability for predicting network success or outcomes; empirical system designs can help managers to baseline their designs, but the system may not work for every application. TSN helps manage the configuration and modeling of these systems, enabling the software-designed environment for predictable system design and advanced planning systems. Offline and online predictive tools that can mathematically simulate network traffic and allow for predictable design could provide more detailed understanding of the system's success prior to hardware acquisition or commissioning of equipment.

Smart modeling in this way will maximize the life of the system and future-proof the components to facilitate, adding switches to the infrastructure to scale with the system needs. When systems are built with future scalability in mind, huge reductions in cost and time can be made. Fixed cabinet space and previously poured concrete, and existing conduit make changes and additions to the system's incredibly expensive endeavors. Modeling capabilities made possible with TSN will bring predictability to the success of the future system.

Modeling and Industry 4.0

Industry 4.0 is underpinned by the idea of digitization and cloud computing for virtual modeling of cyber- physical systems through real-time data. In order to create a digital twin for that kind of cyber-physical modeling, there must be a clear pathway to collect, process and control the data in real-time. TSN ensures guaranteed latency, which means the pathways between the process sensors collecting the data and the analytical computers processing the data are unimpeded – enabling guaranteed data delivery.

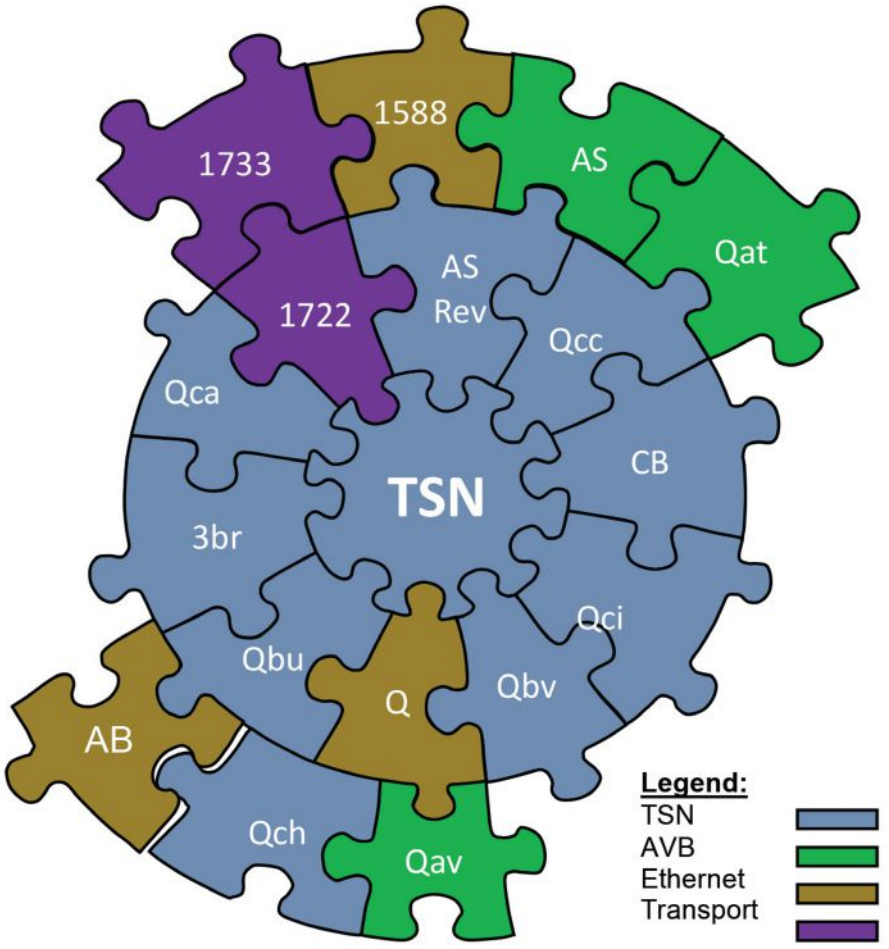
The benefits of common time

Digitization and its benefits require a time-stamped data collection to provide a chronology of events, time-based analysis,

time-series analytics, and finally, a model for predictable outcomes. The analysis of time-stamped data can allow system managers to see exactly what went wrong, as well as where and when.

TSN provides a common reference of time in which to do this. The same clocks that are required for traffic scheduling on the network can be synchronized with other time domains to provide a wider view of system events or faults. Essentially, "TSN time" can be correlated with time in the enterprise systems so that events and conditions on the plant floor are chronologically comparable to events within the company's business systems.

Consider a case where more precise understanding of when a product was completed is needed in manufacturing, with respect to the distribution systems that will move such product to the consumer. In the supply chain, there could be a tighter understanding of when products are completed against when the material to produce such products needs to be reordered. What if the cause and effect of faults on the plant floor could be more easily viewed at a system level through a sequence of events capability, where time is common across the entire manufacturing facility? Such capabilities present an opportunity for higher efficiencies that, ultimately, are reflected in a company's financial success.



SOURCE: AVNU

TSN has leverage both AVB (Audio Video Bridging over Ethernet) and Ethernet technologies.

The benefits of TSN

Digital technology powered by TSN infrastructure may enable shorter operational lead times, more visibility over systems and more efficient asset utilization. These benefits could be realized in industrial systems soon and can pave the way for improvements by "future-proofing" systems and include:

Ease of Network Configuration: Today, technicians have to configure each network device manually on conventional networks, but TSN can allow for automatic configuration via intelligent configuration tools. The network understands what must happen to achieve the desired performance and will turn specific services on and off as necessary. Standardized methods for network-wide configuration and commissioning required by TSN also create the avenue for offline simulation and modeling of the network and the architecture.

Secure Networks: For industrial automation and control networks, security is critical. Because TSN is standard Ethernet, control networks can take advantage of best-practices for security that have been developed into Ethernet for decades. TSN also adds a layer of security to the data with the precise timing mechanism that facilitates early detection of a network breach.

Reduced System Costs: TSN allows the convergence of different traffic classes on a single network and reduces overall system costs significantly. Hardware and maintenance costs may also be reduced since the system needs fewer devices and cables.

Future Enhancements: As TSN is part of the Ethernet family, it naturally scales with Ethernet, which means that the technology will not be limited in terms of bandwidth and other performance criteria. New nodes can be easily added to the network and discovered via standard networking protocols.

TSN enables the convergence of networks and systems that were previously kept separate for reasons of operational integrity, real-time performance, safety or security. Breaking down communication barriers between critical and noncritical systems is a foundational concept of the IIoT and Industry 4.0.

With TSN and time synchronization, insights from real-time data at the edge arrives on time from anywhere, no matter how demanding the environment. Choosing TSN changes the industrial model and workflow with fewer workers for a more converged and deterministic network built on platforms to protect investments long- term.

Ecosystem approach

Today, many of the underlying systems for Industry 4.0 applications are based on proprietary standards and could present integration challenges. A lack of a broader industrial networks ecosystem perspective in terms of business systems, platforms and standards as well as interoperability could present a significant challenge for the adoption of industry 4.0 into modern workflows. Consortia, industry and government bodies as well as standards associations are working to establish standards, associated profiles and tests. It is incumbent upon everyone involved in the ecosystem to work with partners to stay current on evolving standards, make them interoperable and coexist to maximize the value delivered by Industry 4.0.

Since TSN provides a standards-based foundation, system designers and engineers would be able to architect a network that will stay current with evolving use cases. Avnu's reference test tools and test plans support vendors with rapid adoption of the TSN standards. As the need for time-synchronized communications continues to grow, Avnu Alliance works to ensure that TSN is successfully implemented to realize the maximum possible benefits of configuration, data use, and cost savings in industrial settings and beyond.

*Anil Kumar and Denzil Roberts, Ph.D., **Intel** and* Steve Zuponcic, ***Rockwell Automation***.

IoT security system integrity, protection and verification

IoT security is an umbrella term that includes network, internet, endpoint, API, cloud, application, container security and more. It's about establishing a set of security strategies that work together to help protect your digital data. Security is an ongoing process that includes continuous monitoring and a clear response plan.

PROTECTING AND VERIFYING THE INTEGRITY of Internet of Things (IoT) systems is critical. A key element of system integrity is ensuring that a system has not been modified or corrupted. This is especially important for IoT gateways and edge servers that are directly attached to networks and to the Internet.

Ideally, it is best to prevent a system from being compromised in the first place. In many cases, it is better to prevent a system from operating at all if it has been corrupted or modified without authorization. No matter what, it is vital to protect information on the system and especially critical secrets like crypto keys.

Effective tools

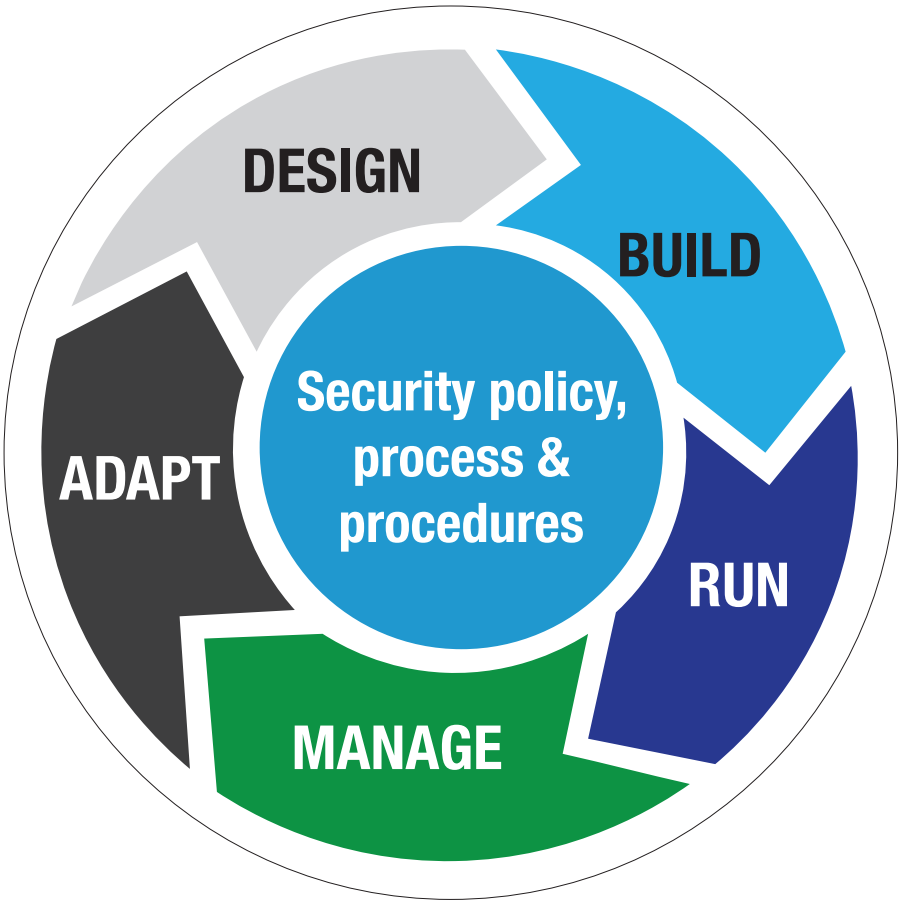
A variety of tools at the operating system level help verify the integrity of software. These include storage encryption, cryptographic signing of software packages, checksums of files, and tools for checking the system. But what can be done to make sure that the underlying system has not been compromised, to verify the hardware, BIOS and other firmware, and the bootloader? And what can be done if problems are detected?

Let's consider what can be done using a Hardware (HW) Root of Trust and recent developments in the Linux operating system that provide a view into the integrity of the underlying system.

The first factor is Linux Unified Key Setup (LUKS), a robust storage encryption capability built into Linux. LUKS encrypts everything from disk drives to USB drives, SD cards, and network storage. LUKS encrypts at the volume level, and Linux systems can be configured as either a single volume or multiple independent volumes on a single drive or multiple drives. This gives considerable flexibility and power for configuring and improving the protection of information on an IoT system.

One of the use cases for LUKS is to encrypt the system drive. When this is done, the LUKS password must be provided to boot the system. With systems like laptops this is commonly done by typing in the password. Network Bound Disk Encryption (NBDE) is a Linux package that uses a network service or a HW Root of Trust to provide the LUKS key to boot the system.

NBDE is a flexible crypto framework that uses various pins or crypto engines to encrypt and decrypt secrets such as LUKS keys. NBDE is designed to be extended - it currently supports two pins: a network tang server and a Trusted Platform Module (TPM) 2.0 HW Root of Trust. NBDE also implements policies which allow multiple pins to be combined.



SOURCE: RED HAT

An effective security program includes continuous monitoring, so users always know what's happening, along with a clear response plan to efficiently handle surprises when they do happen.

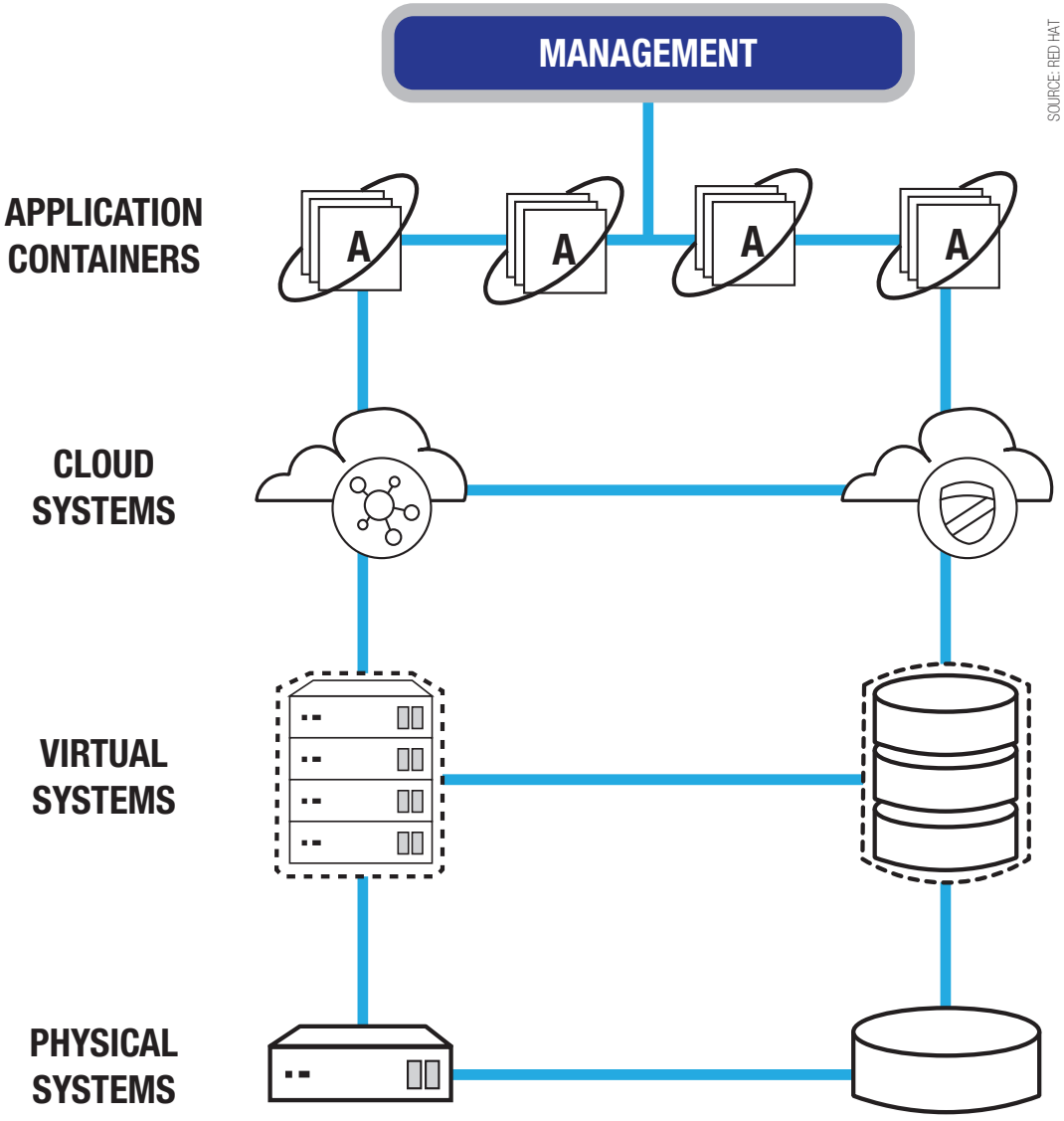
NBDE with TPM2 is a good choice for IoT systems in remote locations without secure network connections or complete physical security. This ensures that the system will only boot if the operating system (OS) disk is in a system with a properly configured TPM2 module and it has been bound to that TPM2 module.

Secure boot

The next element to consider is secure boot. This is implemented in the Unified Extensible Firmware Interface (UEFI) firmware and requires that the bootloader and operating system are signed with a known and approved software key before it will allow the system to boot. Secure boot is a good tool for ensuring that the operating system is valid. Industry standard secure boot keys are commonly installed in the UEFI firmware at the factory. These keys can be used as is, custom keys can be added, or the standard keys can be deleted and only custom keys used.

Secure boot is an effective tool and should be used. However, secure boot can't verify the underlying hardware, the firmware, or that secure boot itself is running. This is where TPM2 and measured boot come into play. Measured boot is sometimes referred to as Trusted Boot.

Measured boot works at multiple levels. The TPM2 module contains a set of 24 Platform Configuration Registers (PCRs). Software, such



SOURCE: RED HAT

Technical controls are the heart of cloud security. Centralized management makes technical controls easier to implement. Some of the most powerful technical controls in the toolbox are encryption, automation, orchestration, access control, and endpoint security.

as UEFI firmware, is hashed using an algorithm like SHA-256 and the hash is stored in a PCR. However, the hash isn't written directly into the PCR. Rather the hash is extended into the PCR using cryptographic operations inside the TPM2.

Multiple measurements can be combined into a single PCR. The final value in the PCR depends on the hash of each file and the order the files are evaluated. This process is deterministic - given a set of files and an order of measurement, you get the same results each time. These measure and extend operations can be replicated outside of a TPM - you can determine in advance what the final value in a PCR should be.

Measured boot updates the PCRs in a sequence of operations: a very low level software routine, essentially part of the hardware, measures the UEFI firmware and option roms such as network interface cards (NICs) and storage controllers. The UEFI firmware measures the Master Boot Record and bootloader. The bootloader measures the kernel and related files. Other tools, such as Linux Integrity Measurement Architecture (IMA) can then measure the rest of the system. Measurement can include both files and configuration. Eight of the PCR registers are pre-defined for system use and eight are available for custom use by applications.

The TPM and PCR model is designed to make it impossible to modify PCR measurements without detection and very difficult to interfere with the measurement process without detection.

PCR measurements can be used for a variety of purposes, including local and remote attestation of the integrity of the system. They can also be used for sealing operations inside a TPM. In TPM sealing a TPM protected secret is further protected by a TPM policy that checks PCR values against approved values before decrypting the secret.

As a concrete example, using NBDE you can seal the LUKS password against PCRs 0, 2 and 7. This would measure the UEFI bios (PCR0), firmware on other devices in the system (PCR2), and secure boot (PCR7). The LUKS password would only be provided if the UEFI firmware had not been modified, other device firmware had not been modified, and secure boot were still enabled. Note that these checks are done inside the TPM. These measurements ensure that the firmware has not been corrupted and that no rootkits have been added. While not absolute protection, it can significantly improve the integrity of the system.

Note that this approach also protects from live image attacks where you boot from a live image, mount the existing system disk, and read information off of it. In this case the TPM2 sealing would detect the presence of new hardware in the system and refuse to provide the LUKS key.

In this example the operating system and applications can be updated without touching the TPM. Firmware can still be updated - this would require resealing the TPM with the new values.

As previously mentioned a set of PCRs are available for user applications. User applications can extend values into these PCRs which can then be used to verify application level integrity and used to seal secrets.

Any secrets can be protected using the approaches described here. SSL keys, SSH keys, software license keys and device access codes can all be protected by TPM. Crypto keys can be loaded directly from the TPM2 into memory and then wiped as soon as they are no longer needed; there is no reason for them to persist on disk.

In the case of a system compromise the entire TPM can be immediately wiped by issuing a TPM_reset command, making TPM protected secrets unavailable. Full details on the range of protections available using TPM2, PCRs, and sealing is available from the Trusted Computing Group at trustedcomputinggroup.org. Details on NBDE and the clevis framework are available at github.com/latchset/clevis.

Russell Doty, Product Manager for Emerging Technologies, Red Hat Enterprise Linux, ***Red Hat.***

Migrating to TSN-based networks of the future

Looking at the impact of Time Sensitive Networking, two key points clearly come out. First, industries should consider what open network technologies are available to help them migrate current industrial Ethernet systems to TSN compatibility. Second, any assessment needs to combine TSN and gigabit Ethernet.

THE IMPLEMENTATION OF A SMART FACTORY concept is designed to deliver ever-increasing efficiency and productivity. By providing a continuous stream of data flowing across an entire enterprise and beyond, it is possible to monitor and manage manufacturing processes in real-time. Time-Sensitive Networking (TSN) technology is bringing what was on the horizon for Smart Manufacturing closer by offering an increasingly holistic approach to industrial communications today.

Connectivity is a crucial requirement in the digital transformation that is currently being experienced in the industrial landscape, and its role will continue to become increasingly prominent. Standard industrial Ethernet has served manufacturing industries well for a long time, evolving over the years to address new challenges and requirements in industrial communications. However, some of its features are becoming increasingly obsolete, hindering businesses in adopting Industry 4.0.

Only a new technology, built around the needs of Smart Manufacturing, the Industrial Internet of Things (IIoT) and Big Data, can successfully address this issue. TSN, as defined by IEEE 802.1, provides a migration path to the future for current industrial Ethernet.

SOURCE: CLPA- EUROPE

TSN as defined by IEEE 802.1 provides a migration path to the future for current Industrial Ethernet implementations.

What TSN can do for business?

Fundamentally, the creation of a responsive and transparent cyber-physical enterprise requires high-level systems to monitor, control and make decentralised autonomous decisions on all process operations. The most elegant way to achieve this is by using one single industrial network to provide the necessary convergence of information technology (IT) and operational technology (OT). In practice, only a few companies have this luxury. Typically, any given plant will have many different types of networks, as installations take place over time and according to different needs. TSN can address this issue by offering the possibility to unify multiple different industrial Ethernet protocols on the same network infrastructure.

These capabilities are enabled by the set of IEEE 802.1 standards that define TSN. Key amongst them are 802.1AS and Qbv. These define the synchronisation of devices on a network and control the prioritisation of traffic respectively. TSN ensures that vital process data is handled in a reliable and deterministic manner, while allowing lower priority traffic to co-exist on the same network. Hence, not only does TSN offer productivity benefits, but it also lowers cost of ownership associated with the network infrastructure.

The removal of any physical separation between critical and non-critical data sharing, simplifies network planning as well as reducing capital expenditure (CAPEX) and operating expenses (OPEX) associated with cabling and network administration.

Attention has been focused on the fact that TSN allows "standard" Ethernet to be deterministic. While this is true, TSN only addresses the data link layer of Ethernet. It does not consider higher level functions addressed by industrial Ethernet protocols, such as safety and motion control. Users looking for a migration path to future communications need to consider how TSN can be combined with these needs to ensure high performance and functionality.

Moreover, as a series of open IEEE technical standards that device makers can currently pick and mix, TSN ensures openness and future interconnectivity among technologies adhering to the same IEEE 802.1 sub-standards. The IEC/IEEE 60802 working group is currently building on this by creating a set of profiles for using TSN in automation to ensure standardisation.

Revolutionising smart manufacturing

These opportunities have the potential to contribute to improving manufacturing processes and increased competitiveness for businesses that adopt TSN. In the long term, they will transform global manufacturing. Major players in the factory automation business have already introduced a range of products that support TSN, so the concept isn't a theoretical tomorrow's world, but very much a solid step in the evolution of industrial networking. The level of connectivity offered by TSN will help to connect different 'islands of automation' within a production plant into one independent and self-coordinated 'living system' responsive to many variables including both fluctuating inputs and scheduled events.

Cyber-physical systems that TSN can support are not confined to automation but can be extended to asset management and predictive maintenance. When combined with OPC UA, TSN provides an efficient and reliable network for the transfer of high-quality, real-world data on the performance of physical machines and their virtual counterparts. As a result, it is possible to create highly accurate and responsive real-time digital twins.

Consider adopting TSN technology?

As a key enabler for Industry 4.0, TSN will likely become a must for industrial communications. Development teams from different disciplines from IT and engineering, to manufacturing and logistics, should start researching and planning the implementation this technology into their industrial communication networks. Looking at TSN is a chance to assess in-house systems and look for a migration path to address future needs. A parallel emerging trend is the growing need for increased bandwidth to handle the "explosion" of data that Industry 4.0 is generating.

John Browett, General Manager, ***CC-Link Partner Association (CLPA) – Europe.***

Real-time, high performance TSN networks & future standards

Leveraging the combination of a real-time-capable communication technology (TSN) and real-time-capable language (OPC UA PubSub) makes it possible to realize real-time capable applications in an industrial environment based on standards and 5G technology.

DATA COMMUNICATION IN NETWORKS can be illustrated like the synchronization between ants in a colony. Whether small, simple or large and complex structures – only a reliable and structured collaboration of all units ensures the preservation of the respective colony. However, the more complex the linkages, the more important are the mechanisms that are available in order for the ant collective to function reliably.

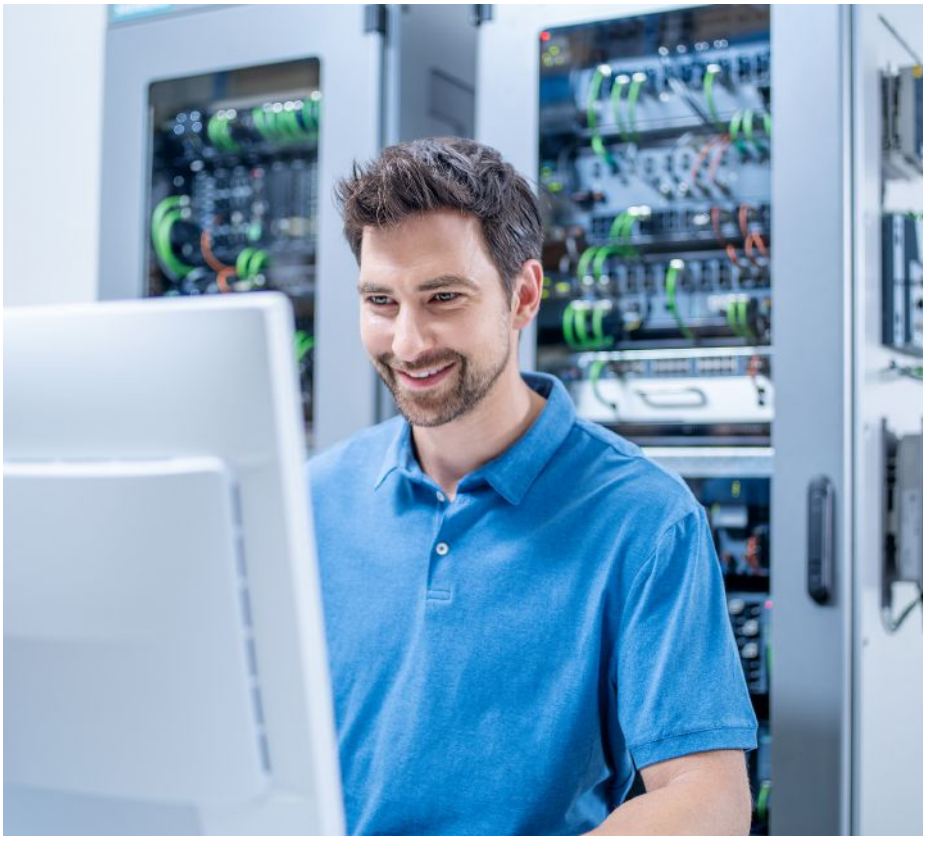
Industrial networks utilize globally defined standards for this, whereby only now protocols are specified that guarantee real-time capability even with complex structures. Time Sensitive networking (TSN) technology, together with OPC UA PubSub, forms the basis of innovative and future-proof communication, which promises lots more thanks to 5G communications technology.

Seen from the outside, an ant colony appears quite unstructured. The collaboration of many ants, which seem to organize a wide variety of activities in an uncoordinated manner, is not really comprehensible to us humans. And yet, over time, a small hill becomes a big mountain. Each ant in the collective knows its place and task in the "network" to maintain and enlarge the colony.

Like an ant, communication data fulfills a specific purpose and must be sent by the sender to the recipient. This must work reliably even as networks become larger and more complex. Like an ant hill, information is distributed both horizontally and vertically in a network.

High-performance communication structures are therefore indispensable as more and more intelligent individual components exchange data with each other. The performance of a network is also key to the amount of data that can be transported. The network components used must therefore also meet these requirements, and this across all network structures all the way to the cloud.

As part of digitalization, the network plays an essential role particularly in industry. The so-called industrial backbone is the backbone of an end-to-end digital infrastructure. And it is the deciding factor that transforms a plant into a smart plant, turns things into the industrial Internet of Things, and makes digital connectivity possible with an intelligent network.



SOURCE: SIEMENS

Robust, reliable, and secure industrial network components as well as high-performance network management software are the "Alpha and Omega" in discrete manufacturing and the process industry.

TSN real-time capable Ethernet

While confidentiality and integrity are paramount in traditional corporate networks, functions such as real-time capability play a decisive role in industry alongside protection for people and the environment. Just like ants respond to unforeseen events at lightning speed, data also needs to reach its destination in a predictable time for the rapid triggering of actions.

New technologies such as Time-Sensitive Networking (TSN) will enable this in the future based on international standards. TSN is the further development of Ethernet incorporating standardized real-time mechanisms and, in conjunction with Gigabit switches, enabling the deterministic data exchange via extended Quality of Service mechanisms (e.g. bandwidth reservation with predictable latencies) as well as time synchronization and seamless redundancy.

With TSN, multiple real-time protocols in parallel and large amounts of data can be transmitted without collision. TSN, specified in IEEE 802.1 by the Institute of Electrical and Electronics Engineers, consists of several IEEE standards that extend the scope of the Ethernet standard.

Depending on the industry sector and area of application, different individual standards are needed. While in motor vehicles IEEE 802.1DG is used for the internal communication between the individual components, the real-time-capable transmission of audio/video data is important, for example, in public transportation. This is made possible by the IEEE 802.1BA standard, among others.

In industrial networks, real-time-capable communication has priority and here, a number of new sub-standards have been added to the IEEE 802.1Q standard. But to explain all of them here would result in too much detail.

With the new 5G mobile communications standard, ultra-short latencies now make industrial applications such as mobile robots feasible.

If you are interested, all current Time Sensitive Networking sub-standards of the specification can be found at this website: https://1.ieee802.org.

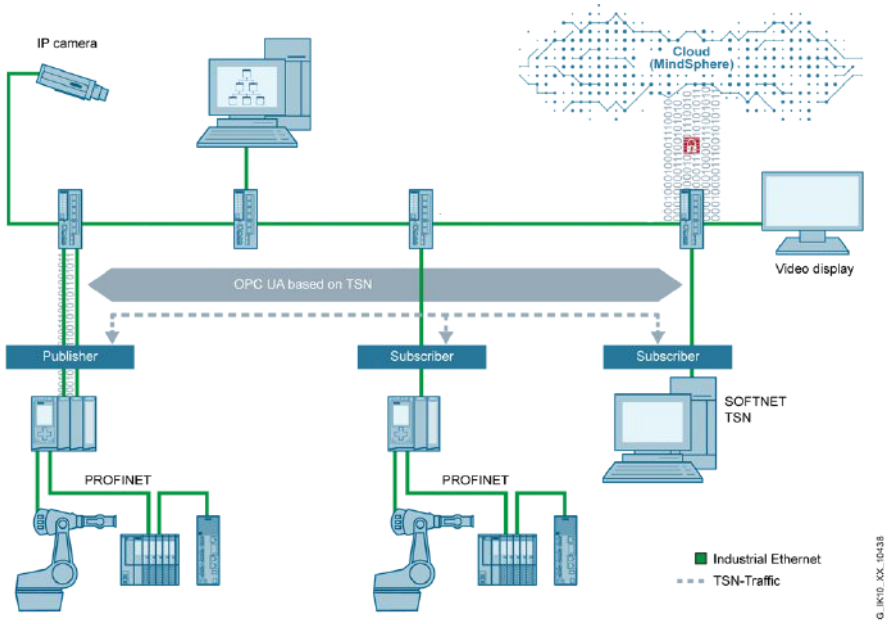
Real-time capable protocols

In the following, we limit ourselves to IEEE 802.1Qcc, which describes the stream reservation with TSN. Using the example of the ant colony, this can be clearly illustrated: Here, many workers must simultaneously transport building material, food, and more within the ant hill, without obstructing each other and thus losing valuable time in building up the colony. With regard to the industrial network and the data transmitted therein, this is accomplished with TSN transporting multiple – now also real-time capable – protocols on different paths (so-called streams), but on one and the same line, in parallel without collision. This enables real-time capability in the medium, which however only provides an advantage for the communication if the transport protocol is real-time capable as well.

In the standardization committees of the IEEE, IEC, and OPC Foundation, of which Siemens is a member, OPC UA in general was initially agreed on for the automation starting from the control level. OPC UA was specified a few years ago by the OPC Foundation and combines the OPC protocols OPC DA, OPC HDA, and OPC A/E existing at the time. Among other things, OPC UA is used for exchanging data between devices from different manufacturers and in the vertical communication.

This protocol (often provided with the affix Client/Server) utilizes TCP/IP mechanisms, but with the major disadvantage that TCP/IP is not real-time capable. Therefore, another protocol was introduced with OPC UA PubSub that compensates for this disadvantage. At the field level, too, PROFIBUS & PROFINET International (PI) has recently specified V2.4 PROFINET as a real-time-capable protocol in combination with TSN. However, it will take years before products and an entire ecosystem based on PROFINET over TSN will be available for the field level.

Hence OPC UA PubSub over TSN and thus the control and operator level will be discussed below. With OPC UA PubSub, a publisher continuously sends data – i.e. deterministically – to a TSN network, which is distributed to the subscribers in the TSN network. The combination of real-time-capable communication technology TSN and real-time-capable language OPC UA PubSub



Real-time-capable machine-machine communication for increased productivity and higher reliability.

makes it possible to realize real-time-capable applications in an industrial environment based on standards.

M2M communication

One of these applications with TSN and OPC UA PubSub is reflected in the real-time-capable machine-machine communication, as already demonstrated by a demo application from Siemens. A TSN talker and several TSN listeners (e.g. SIMATIC controller with communication processors) establish a connection to the associated TSN bridges (e.g. SCALANCE X switches) via standardized IEEE protocols.

The TSN talker sends a request (advertise) to the connected TSN bridge and receives a confirmation (ready) from it after connection establishment. The same process is repeated for each connected TSN listener.

If the connection of all TSN subscribers has been successfully established, a predefined stream will be set up with a timestamp over IEEE 1588v2 between talker, in-line TSN bridges, and listeners. The TSN network has thus been created. So that a deterministic exchange of productive data between TSN talker and listeners can take place, OPC UA PubSub is used.

Through it, the TSN talker continuously sends data (publisher) in the predefined stream, which is received by the TSN listeners (subscribers). The result visible to the observer: The end devices (e.g. robots) connected to the TSN talkers and listeners exhibit a mutually synchronized behavior.

The synchronization remains even if the network becomes loaded. To prove that, a load generator is switched in the demo application that "floods" the network with a large amount of data. All communication in the network except for TSN talker and listener experiences a downtime. In the demo application, this becomes apparent through the connected camera, whose video stream no longer arrives on a monitor connected to the TSN network; ultimately, the monitor image "freezes".

However, as the data exchange of TSN talker and listener takes place over the predefined stream, this communication is unaffected by the extra load.

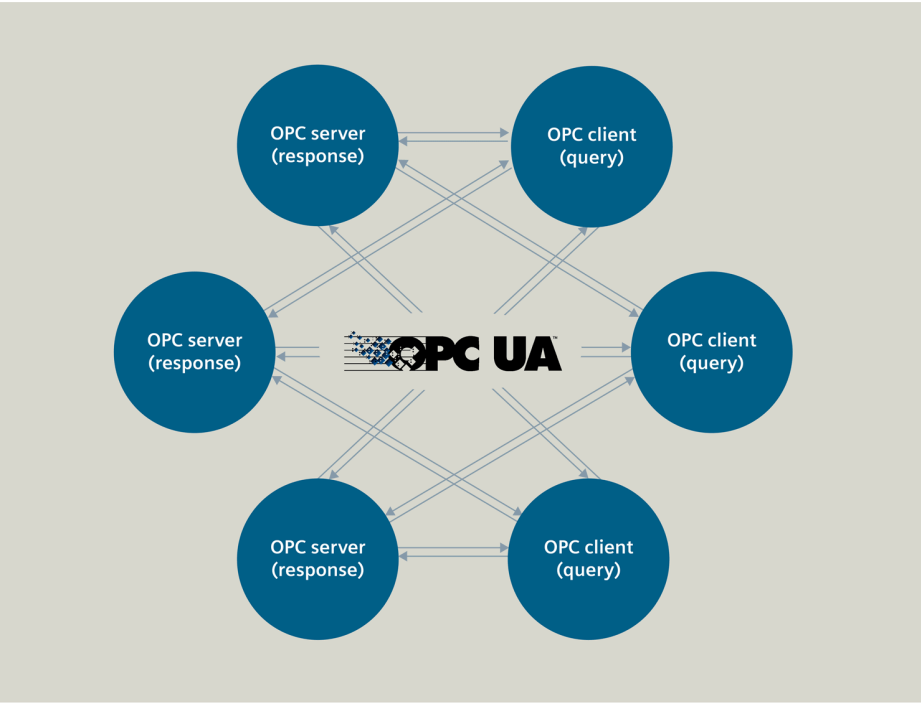
A real-time-capable productive data exchange is therefore a given at any time – even under unfavorable constellations. In order to be in control of the network at all times and to be able to respond to undesirable effects early on, the TSN network is also monitored via a network management software.

Complementary: TSN and 5G

The realization of a real-time-capable machine-machine communication is not new and could already be executed with Industrial Ethernet mechanisms such as PROFINET with IRT functionality. But only Ethernet with TSN now makes it possible to provide real-time capability on the basis of globally accepted technology. And this acceptance is the reason why other technologies can now take part in the advantages of TSN.

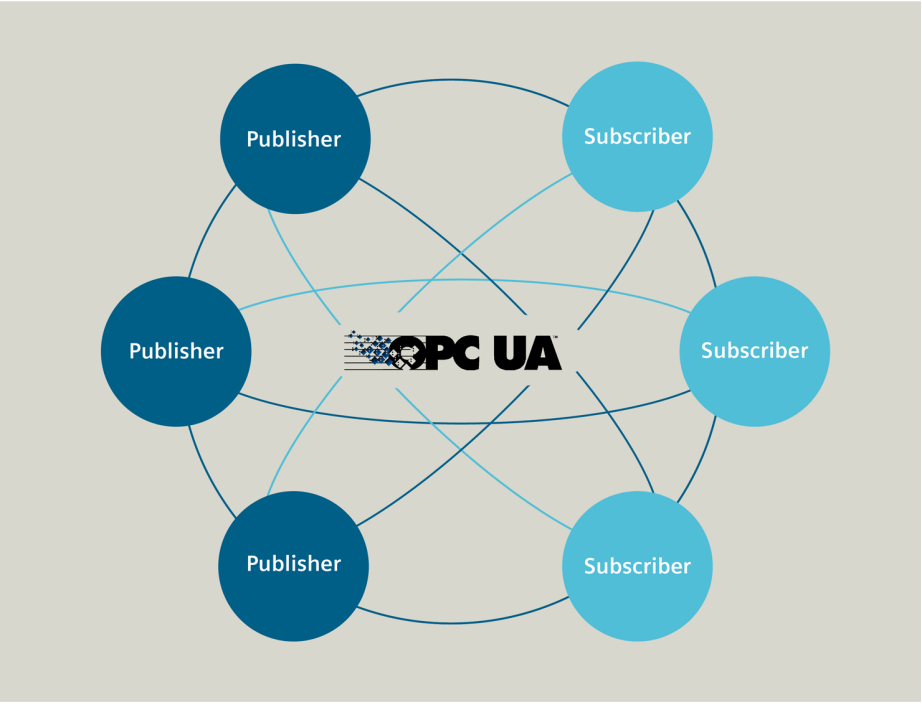
One of them is the new 5G mobile communications standard, which enables the secure and reliable implementation of future-proof industrial applications. In addition to full-area coverage and high data rates, ultra-short latencies also play a crucial role in the realization of applications such as mobile robots in manufacturing, autonomous vehicles in the transport and logistics sector, and virtual reality operations. So, what could be better than combining TSN and 5G – TSN for real-time wired, and 5G for real-time wireless networks. The future sounds promising, and we can all go on a journey to discover new concepts and fields of application – like flying ants swarming to establish new colonies.

Manfred Wolf, Marketing Manager, ***Siemens.***



SOURCE: SIEMENS

Operating principles of OPC UA Client/Server (above) and OPC UA PubSub (below).



Compared to OPC UA Client/Server, the data with OPC UA PubSub is continuously available in the network, i.e. only OPC UA PubSub is real-time-capable.

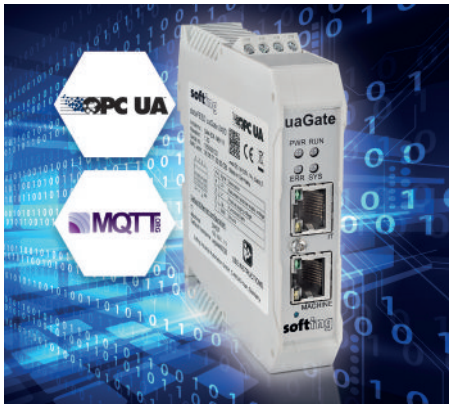
Industrial video surveillance

Phoenix Contact: The company's first comprehensive solution for wired or wireless IP video surveillance in industrial applications includes an extensive product portfolio of connection and automation technology for use between the camera and video server.

Industrial Ethernet components, power supplies, surge protection, connectors, cables, lines, terminal blocks, and 19" components ensure secure connection between the camera and video server. The required components are available individually, as modules or as ready-to connect boxes. The products are suitable for industrial use and therefore enable high network availability even in critical applications.

The IP video surveillance solution is suitable for small installations through to large systems with high security requirements. In addition to providing security for property in buildings and on company premises, the solution can also be used for technical system monitoring. Phoenix Contact also provides extensive advice for the configuration and planning of video networks.

Edge gateway



Softing: The new uaGate 840D gateway allows users to access the complete data from SINUMERIK 840D machine tools via the OPC UA standard, and use it directly in Industrie 4.0 applications.

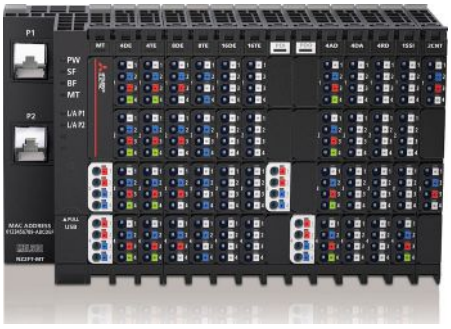
The SINUMERIK 840D sl CNC controller from Siemens is used in a variety of machine tools for implementing milling, turning, grinding, nibbling and punching technologies. Here, a central requirement is the further processing of both the control data as well as the NC and drive data within an integrated overall application.

In the context of increasing digitalization, the use of open and standardized communication technologies is becoming increasingly important.

So far, however, only the data from the integrated SIMATIC S7 controller could be reused outside the machine tool, while the NC and drive data could not be accessed from outside. Softing's new uaGate 840D gateway now closes this gap and for the first time provides access to the complete machine tool data. This allows important spindle and axis data, such as torque and power consumption, to be read out and processed outside the Siemens world using the OPC UA and MQTT communication technologies.

Together with the associated alarms, this data for instance becomes available for condition monitoring, predictive maintenance, data logging or analysis tasks. In addition, this gateway allows to generally integrate the SINUMERIK 840D sl CNC controller into Industrie 4.0 applications.

Remote I/O modules



Mitsubishi Electric: The latest slice type I/O modules offer helpful features for PLC users in addition to saving space and helping reduce costs. Commissioning is made easier and quicker with fast-fit connections and hot-swap installation, plus, online and onboard software for settings.

Each slice offers a clip-in mounting system, while status LEDs help with visual diagnostics. A width of 11.5 mm means space is saved on the rack, allowing for larger systems to be wired into a smaller panel, up to 64 modules can be connected per row, potentially saving on hardware costs.

Wiring is made much faster and easier thanks to push-in spring clamp terminal blocks. The terminal block itself is detachable, allowing components to be wired-in and then simply plugged in to the I/O block while it is in position, adding convenience and saving time.

Set-up is accessible and flexible using the proprietary software GX Works3 or a dedicated onboard settings tool built into the communication module. The tool includes features such as monitoring/diagnostics and functional tests, helping to reduce engineering time and machine costs.

Communication modules provide connectivity to main network protocols and can also be used to provide power to a row of I/O modules. Power does not have to be manually wired-in as it is supplied discretely through each slice and there is the option for an extended power supply module. The modules are also hot swappable for fast installation and reduced downtime during system changes.

Wi-Fi connectivity cloud kit

Renesas Electronics: The RX65N Cloud Kit features onboard Wi-Fi, environmental, light and inertial sensors, and support for Amazon FreeRTOS connected to Amazon Web Services (AWS). The kit gives embedded designers a fast start and secure connection to AWS. Using Renesas' e2 studio Integrated Development Environment (IDE), IoT applications are easily created by configuring Amazon FreeRTOS, all the necessary drivers, and the network stack and component libraries.

The RX65N Cloud Kit provides an evaluation and prototyping environment, enabling embedded designers to create secure end-to-end Internet of Things (IoT) cloud solutions for sensor-based endpoint equipment. Employing Renesas' browser-based software, users can visualize their sensor data using a smart device cloud dashboard to monitor a wide range of applications including networked smart meters, building, office, and industrial automation systems, as well as home appliances.

High-performance HMIs

IDEC: Newly upgraded 5.7", 8.4", 10.4" and 12.1" human-machine interface (HMI) touchscreen models offer high performance, making them a great fit for both new and retrofit applications.

In retrofit applications, the High-Performance Series HMIs are direct replacements for previous models, offering a seamless upgrade path and fitting into the exact same panel cutouts. All HMI

programming can be converted from existing to these new models, so no new programming is required.

All updated models use TFT-LCD screens displaying a wide range of vivid colors, with the three larger-sized HMIs improving the resolution to 1024x768 pixels, while the 5.7" model remains at 640x480 pixels.

The entire range of HMIs in the series offers brightness, in this case ranging from 600 to 800 cd/m2, to deliver greater visibility, even in high-glare locations such as direct sunlight. Backlight life ratings are 100,000 hours minimum.

Gyroscope sensor module

SIGMATEK: New in the company's S-DIAS portfolio is the highly precise BC 031 gyroscope sensor module. The module provides rotation rates and linear acceleration information in 3 individual axes, so position and inclination can be exactly determined at any time.

The compact solution is based on a MEMS sensor and ensures high-precision rotation rate measurement. The resolution for the acceleration is 0.061 mg/LSB. For the rotation speed, it is 4.375 mdps/LSB. Even in harsh environments, with strong impacts and vibration, the robust module delivers reliable measurement results. For filtering raw data, the high-resolution sensor module has a microcontroller. In addition, an Ethernet and RS485 interface for reading e.g. Sick laser sensors are integrated.

The BC 031 is used in applications where precise measurement of acceleration or rotational movement is required. The sensor module is therefore especially suited for automated guided vehicles (AGV), logistics, lifting platforms, industrial robots and many other areas of application.

Edge computer

HARTING: The industrially-suited MICA Edge Computer is now available with a secondary Ethernet interface. It can be used to easily exchange and process data between two

Ethernet networks, including wired-to-wireless gateway applications.

With many Industry 4.0 applications, it is necessary to separate networks and send data back and forth between Ethernet protocols without permitting external applications direct access to a corporate network. As a result, HARTING has added a second interface for these applications to its MICA Edge Computing device. An additional USB interface can also be used for adding further capabilities or a USB storage device. This is because, unlike a router, MICA can also carry out complex data transformations and aggregations.

The secondary Ethernet interface is provided via the functional circuit board and expands the modular system of the MICA platform. In particular, MICA Wireless with WLAN, BLE and LTE connectivity with an additional Ethernet interface is an easy to manage and compact solution for many projects in the areas of industry and transportation.

Virtual appliance

Rockwell Automation: Manufacturers seeking to virtualize smaller applications now have a solution that is sized for them. The new VersaVirtual appliance provides all the computing, networking and storage capabilities needed to deploy and maintain up to 15 virtual machines in one ready-to-use appliance.

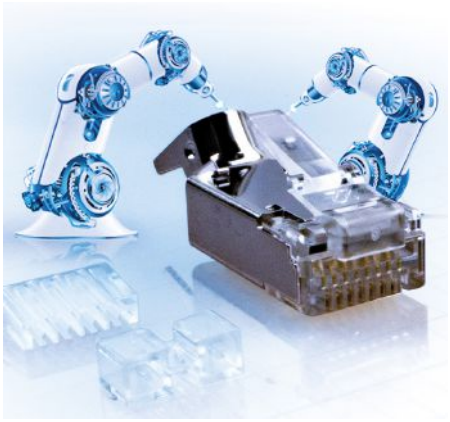
The VersaVirtual appliance helps save time and money when virtualizing applications in two key ways.

First, it avoids the potential pitfalls of a do-it-yourself virtualized architecture. Homegrown solutions can take weeks to deploy and require working with multiple vendors. The pre-engineered VersaVirtual appliance arrives at a user's location preconfigured, where it can be deployed in mere hours. And instead of dealing with multiple vendors, VersaVirtual appliance users have one number to call for support.

Second, the VersaVirtual appliance provides similar capabilities as an Industrial Data Center but with scaled down cost and complexity for smaller applications. This can break down barriers to virtualization for companies that are challenged by solution complexity, lack of skills or resources, and infrastructure costs.

The VersaVirtual appliance comes with one-year remote monitoring and administration so that users receive around-the-clock system monitoring to help prevent downtime. Customers will also receive support from certified IT/OT professionals who have an average response time of three minutes to help resolve technical issues.

Connector for 10GB data transmission



Yamaichi: A new CAT6A RJ45 connector supports 10 Gigabit data transmission according to the ISO/IEC 11801 standard. The development was necessary due to higher data transmission demands in the industrial area. Gigabit Ethernet is required by more and more applications.

The RJ45 cable connector is designed with integrated cable guide, EMC shielding made of nickel-plated brass and a rectangular cable crimp that prevents cable rotation. The tested life is more than 1,000 mating cycles and the operating temperatures range from -40°C to +120°C for extreme operating conditions in the field or the plant.

Within the Y-ConRJ45 series, the described component can additionally be protected against external mechanical environmental influences according to the protection classes IP69K, IP68, IP67 and IP20. Reliable protective covers made of high-grade materials such as PBT or zinc die-cast are part of the series. This gives the customer the flexibility to choose the right component for different applications.

NIC module

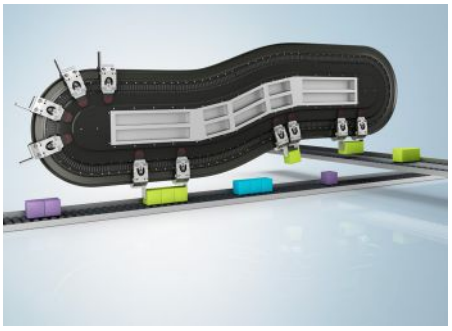
Lanner: This PTCRB-certified Wi-Fi/3G/4G/LTE NIC module is designed for operators and device manufacturers located in regions where PTCRB interoperability/compatibility (cat-3 & cat-6) is a requirement.

The NCS2-MINIPCIE02 incorporates Wi-Fi/3G/4G/LTE wireless network connectivity and is designed to work with Lanner network appliances via a Gen2 PCIe*8 interface, enabling

wireless network connectivity to compatible Lanner network appliances and delivering wireless connectivity for enterprise network management and convenience.

This module comes with three nano sim card sockets, two mini-PCIe sockets and one M.2 socket, together not only allowing users to install Wi-Fi/3G/4G/LTE compatible modules and SIM cards, but also making available a wider variety in network interface options in terms of both wired and wireless Internet connections. The NCS2-MINIPCIE02 comes with four antenna inputs, allowing greater signal receptions.

Linear transport system



Beckhoff: Now available in the U.S., XTS combines the advantages of rotary and linear drive principles into a linear transport system that provides capabilities for packaging machines and smart factories.

This mechatronic solution enables intelligent material flow, exceptional precision, real-time robotics integration and efficient self-reconfiguration based on lot, recipe or other product specifications. Highly customizable and durable motor modules, mechanical guide rails and wireless movers integrate the necessary power electronics, EtherCAT communication and position measurement in a compact form factor, reducing machine footprint up to 50%.

XTS movers can be controlled with high dynamics at velocities reaching 4 m/s and acceleration exceeding 100 m/s^2. Modular linear motors and rails can create circles, clothoids and S-curves as well as straight, open segments. Supporting installation horizontally, vertically or at angles, tracks can be combined to dynamically manipulate or transport parts with multiple movers. Flexible mass production down to lot size 1 is possible through XTS along with EtherCAT networking, PC-based control hardware and TwinCAT 3 automation software.

The universal TwinCAT engineering environment and runtime permit vision system programming and implementation using languages that controls engineers are familiar with, such as those standardized in IEC 61131-3. With a fully integrated vision solution, TwinCAT offers an end-to-end software platform complete with PLC, motion control, robotics, high-end measurement technology, HMI, IoT and machine learning.

Digitally advanced CNC system

Bosch-Rexroth: With the latest software version of the CNC system MTX, Bosch Rexroth is expanding and simplifying the digital engineering of machine tools right through to 3D machining simulations as part of everyday operations. In parallel to the increase in digitalization and connectivity, the engineering and functions of the CNC system have evolved into a practical and proven IoT solution which is already capable of meeting future connectivity requirements today.

Based on the highly effective hardware which is scalable in three stages, the CNC system MTX controls up to 250 CNC axes in up to 60 channels with one control, including the PLC functionality. The latest software version contains software packages both for all popular metal-cutting processes and for beam cutting and hybrid machines.

Engineering is consistently carried out via the central engineering software IndraWorks for planning, parameterizing and testing CNC, PLC and HMI. Manufacturers have already virtually and automatically commissioned several hundreds of machine tool types with the MTX's digital twin and the integrated software tools. Machine manufacturers can reproduce their know-how in the fully open architecture, safe in the knowledge that it is protected. Furthermore, thanks to realistic 3D machining simulations, end users can identify errors in advance and digitally optimize the machining processes.

Digital enterprises portfolio

Siemens: Xcelerator unites the core Siemens Digital Industries software portfolio with Mendix multi-experience application development platform to power digital transformation and make it possible for anybody to easily build, integrate and extend existing data and systems.

It also enables rapid innovation and validation of products during design, manufacturing and use through creation of an accurate digital twin.

This integrated portfolio of software, services and application development platform can be personalized and adapted to fit customer and industry-specific needs to help companies of all sizes become digital enterprises. Xcelerator combines the full portfolio of Siemens' software for design, engineering and manufacturing with an expanded Mendix low-code, multi-experience application development platform. The Mendix platform now includes cloud and app services for digital engineering and Internet of Things (IoT) powered by MindSphere, in addition to Mendix's market-leading unified low-code and no-code development environments.

IIoT-ready controller

Schneider Electric: The new Modicon M262 controller is IIoT-ready for logic and motion applications. It offers intuitive, scalable and reliable machine integration into Industry 4.0 environment, machine to device, machine to human, machine to machine, machine to plant or machine directly to cloud.

The M262 controller embeds cybersecurity features and encryption protocols to provide direct cloud connectivity and digital services thanks to its two ready-to-work and independent embedded Ethernet ports.

Five Ethernet ports enable users to create separate networks and cyber-secured cloud connectivity that can be integrated plant using open protocols including OPC UA, PackML, SQL or integrated with cloud services using MQTT, JSON or HTTPs requests (API).

With four to 16 synchronized axes with scalable cycle time down to one millisecond and a three nanosecond to instant processing speed independent from communication tasks,

Modicon M262 Controller answers performance demanding motion applications. Modicon M262 Controller helps simplify machine architecture and field bus wiring. And with Machine Assistant (webserver technology), no software is required for device discovery, commissioning and diagnostics.

Model-based simulation tool

B&R: A new simulation tool for model-based machine development has been integrated into the Automation Studio engineering environment. The 3D simulation software greatly simplifies model-based machine development. Developers can import CAD data from machine components or entire machines directly into the simulation tool. Then they can quickly and easily generate a digital twin for developing and testing the machine software.

Digital twins are the key to efficiency when it comes to software development and the virtual commissioning of a machine. industrialPhysics generates digital twins from CAD data. The data is imported in STEP format, which makes it possible to utilize important properties of the CAD design, such as mass and density.The tool makes it possible to view physical behavior of the machine in real time. Developers can simulate flow of materials and identify potential collisions early to make easy corrections.

With no additional effort, the machine model can also be viewed using virtual reality or augmented reality headsets. Free from any distractions, developers can work directly with the simulated machine. Processes can be evaluated with the simulation running. Augmented reality offers the added benefit of being able to view the model on-site in the real environment.

Digital electricity cables

Belden: Available in copper and copper/fiber hybrid versions, this new cable is designed to take advantage of VoltServer's Digital Electricity technology. Cables in copper and hybrid copper/fiber constructions can transmit power and data over long distances in a single cable run.

Tailored specifically to the demands of Digital Electricity, this new cable line delivers power to applications that Power over Ethernet (PoE) and remote DC power can't support due to distance limitations. Belden's Digital Electricity Cables deliver up to 20 times more power or distance than PoE: up to 2,000W across a reach of up to 2 km in indoor and outdoor applications.

Twisted pairs in the copper cable maintain flexibility and performance during installation, improve electrical performance, speed up installation and reduce confusion by offering easy identification of cable pairs. Made of tinned copper, the cable features anti-corrosion properties for improved longevity.

The copper/fiber hybrid version helps installers reduce cable inventory (because a hybrid construction requires only one cable to stock and manage) and reduces labor costs with only a single cable to pull.

Plug and play connectors

Panduit: The TX6A, Category 6A UTP Field Term RJ45 Plug is a simple-to-attach plug for field termination of 4-pair unshielded twisted pair cable for Category 6A,Category 6 and 5e systems.

Designed for quick and easy termination in the field, the simple-to-attach TX6A Field Term Plug is ideal for connecting networked devices such as wireless access points, LED lighting, IP cameras and motion sensors, building access modules and display panels.

The plug's unique design enables quick and easy termination to cabling while at the same time being compact enough to fit in similar spaces as traditional modular plugs. Available in straight and angled versions, it is designed to be connected to common plug attached network devices.

Wireless Ethernet gateway

WAGO: A new wireless Ethernet gateway (WEG), is equipped with an external omnidirectional antenna providing more flexible mounting options for optimal wireless connectivity for multi-directional communication via Bluetooth 4.0 or Wireless LAN at 2.4Ghz or 5GHZ. Multiple communication configurations add to the WEG's

versatility for industrial applications.
The WEG is packaged in IP65 housing and easy to mount directly on equipment, making it ideal for use in harsh environments. It can be configured using a button on the front of the unit or via a web browser.

EPIC controller firmware update

Opto 22: The release of firmware update 1.4.1 for the groov EPIC Edge Programmable Industrial Controller expands the capabilities of this next-generation industrial control system. Engineers and developers will find helpful new networking options and tools, plus new software choices for their automation and industrial internet of things (IIoT) applications.

For secure remote access to the groov EPIC, the system now offers VPN (virtual private network) client technology to connect to an OpenVPN-based VPN server. This option is a rare feature in programmable controllers and a key to creating secure data communication architectures, particularly with geographically dispersed systems.

For example, an original equipment manufacturer (OEM) embedding groov EPIC in their machine design could benefit from establishing a remote connection to their equipment using industry-standard, IT-friendly VPN technology for diagnostics and predictive service. Likewise, a system integrator could use the VPN technology to provide continuing integration services after equipment is installed at a plant or location.

Also with the new release, users can choose between Inductive Automation's Ignition Edge or the full Ignition platform, whichever edition is better suited to their application. Choosing

the full Ignition option allows groov EPIC to serve as an industrially hardened OPC-UA server to legacy PLCs—like Rockwell Automation, Siemens, Modbus, and more—eliminating the need to purchase, configure, and deploy Windows-based computers to perform this function. This option can also significantly reduce the need for IT involvement in many cases.

Network management tool

EtherWAN: The launch of eVue, a network configuration and monitoring tool, offers a software tool that complements the effective deployment and quick management of EtherWAN managed devices while fulfilling user expectations on managing complex networking environment and optimizing user experience.

In order to provide a time-saving and simple method to address configuration and complicated monitoring tasks, eVue is designed with an integrated web-based interface, which is fully compatible with the most commonly used web browsers so that there's no worry with compatibility. The eVue application discovers and lists EtherWAN devices on the network to perform a visualization of the network topology, network monitoring, bulk configuration deployment, event and device status, and firmware upgrade scheduling, with an intuitive and easy-to-use layout.

To reveal network status, eVue continuously monitors for events of EtherWAN devices, and records them for later review at any time. Furthermore, with the ability to send notifications by email, SMS, and SNMP trap based on selected levels of severity, eVue provides up to the minute information on critical systems. Administrators can receive alerts instantly when an event occurs, becoming aware of network issues long before users are impacted, saving time and resources. Last but not least, security is not left behind, with multilevel account authentication that maintains the desired level of network security as needed.

Industrial gateway

ORing: A new industrial dual 4G LTE M2M IoT gateway has numerous features, including Ignition Onboard and Ignition Edge Onboard. The industrial-grade design is compliant with requirements of IEC 61850-3.

The new gateway has built-in 8-port Gigabit

Ethernet with 4x10/100/1000Base-T(X) and 4xGigabit SFP Combo ports. It also includes Ignition Onboard and Ignition Edge Onboard, for easy use of the powerful, web-based Ignition platform for human-machine interface (HMI), supervisory control and data acquisition (SCADA), and the Industrial Internet of Things (IIoT). Node-RED is also onboard, along with support for MQTT and other protocols. The Gateway is AT&T-certified and can be purchased with a bundled SIM card and LTE data plan.

ORing has extensive experience in switch and wireless product design. ORing's products have been deployed in surveillance, rail transport, industrial automation, power substations, renewable energy, and marine applications.

Software library

HMS Networks: CODESYS Control Win SL from 3S-Smart Software Solutions GmbH now supports the Ixxat PC/CAN interfaces from HMS.

The Ixxat PC/CAN interface portfolio from HMS Networks is available for all common PC interface standards, such as USB, Ethernet, Bluetooth, PCIe, PCIe Mini and PCIe 104. Now, this comprehensive range of interfaces is directly supported by CODESYS.

The library required for operation is included within CODESYS version 3.5.14.0 or newer. In addition to the CODESYS installation, only a VCI-V4 driver installation is required to use all Ixxat PC/CAN interfaces under CODESYS. The VCI-V4 driver can be downloaded for free from the Ixxat website.

Using the integrated library, it becomes very easy to access the CAN bus via CODESYS Control Win SL controller applications. For accessing the CAN network, the user can choose between different Ixxat hardware solutions, e.g. a compact Ixxat PCIe Mini CAN interface, which is integrated directly in the controller application, or an external Ixxat CAN interface, which is accessed via USB or Ethernet.

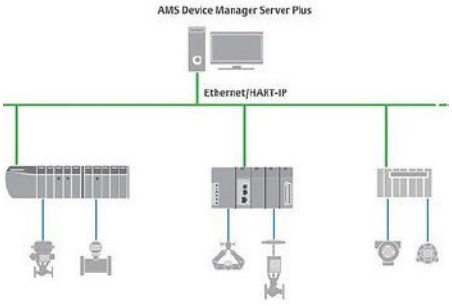
Industrial gateways

Pepperl+Fuchs Comtrol: A new product family within the DeviceMaster industrial gateway lineup allow communication between EtherNet/IP controllers and Modbus master controllers.

The new EIP-MOD gateways enable EtherNet/IP controllers—such as CIP complaint controllers that support Class 1 and Class 3 connections, including PLCs, HMIs, SCADA systems, and OPC servers—to connect to Modbus master controllers. This includes serial Modbus RTU/ASCII interfaces, Modbus TCP interfaces, and Modbus RTU/ASCII over Ethernet TCP/IP.

DeviceMaster EIP-MOD gateways offer EtherNet/IP to Modbus communications. They also provide highly flexible EtherNet/IP interfaces, advanced Modbus gateway functionality, and a built-in data mapping feature that provides a Modbus Concentrator and direct EtherNet/IP controller to Modbus device communication.

HART-IP support



Emerson: An expanded AMS Device Manager with HART-IP support, making it easier to connect with devices and control systems and potentially eliminate hundreds of thousands of dollars in project hardware and engineering.

AMS Device Manager is used by thousands of facilities across the globe to streamline installation of field devices during capital projects, increase safety system uptime, and quickly and safely test devices from the control room. By eliminating multiplexers, organizations can more easily use AMS Device Manager to configure, calibrate, validate, and document more of their HART-enabled field devices and systems.

A look at cool and connected bicycle technology

The steel-frame, single-speed cycling traditionalists may not like it, but today's bicycles are becoming more and more connected. Modern bikes come with built-in computer and wireless hardware, but basically any bike can be upgraded to offer better navigation, tracking and training metrics.

WITH COMPUTERS AND WIRELESS connectivity becoming ubiquitous, advanced bicycle companies are starting to integrate these features into their products. But thanks to smartphones, older bikes can be upgraded, too.

Integrated theft protection

Innovative bicycle manufacturers are starting to integrate onboard computers in their bikes. One example is Dutch company VanMoof.

Their Electrified S2 e-bike comes with a clever battery management system and a unique user interface. 166 LEDs are integrated in the top tube and show vital information like ride speed or battery status.

PICTURE: VANMOOF

In certain situations it will even display a skull gnashing its jaws. That happens when anyone tries to steal the bike. The skull image on the display is a last warning to would-be thieves before an earsplitting alarm sounds. The bike will then automatically disable its motor, flash an SOS signal with the head- and taillights, and notify its legitimate owner via a push message. It also sends out a tracking signal to help the owner locate his or her bike.

www.vanmoof.com

Intelligent retrofit

To upgrade existing bicycles with smart mobile technology, COBI offers a package consisting of a smartphone case, a thumb controller, lights and dedicated cycling software.

To work as the bike's dashboard, the phone is placed in a weatherproof case, which is attached to a hub on the handlebars. This hub includes a battery pack to keep the phone charged during the ride. The hub also has an integrated accelerometer. It senses when someone tries to move the bicycle and sounds an alarm.

A six-button thumb controller mounted on the handlebar is used to control the different COBI apps on the phone. These include navigation, speed, weather forecasts, music streaming, and even control of the front and rear light. Thanks to Bluetooth connectivity, COBI can also integrate additional sensors for heart rate, cadence, and more.

cobi.bike

Smartphone mounts

If you don't need a wireless light switch and trust a robust chain lock for theft protection, then many of the intelligent features of a smart bike are also available through different apps on your smartphone. The only problem here is that it is rather impractical to carry the phone in your hand while cycling. This is where dedicated bike mounts come in.

PICTURE: COBI

These come in various shapes and sizes, some designed for certain smartphone models, with or without protective case, some even with an integrated battery pack.

We like the Quad Lock system because it works with any phone and is not as bulky as many other designs.

PICTURE: QUAD LOCK

Quad Lock uses a strong 3M VHB adhesive to attach an adapter directly to the rear of a phone. This adapter connects the phone to a stem or handlebar mount with a secure dual-stage lock. The phone is firmly held in place even on rough terrain, yet it is easily detached if you want to take a photo or make a phone call.

www.quadlockcase.com

Leopold Ploner

Win a Quad Lock bike mount

The Quad Lock Universal Adaptor uses a strong adhesive on the rear of a phone or case, which then allows your smartphone to be securely attached to the bike mount. For a chance to win one, enter our contest at: **www.iebmedia.com/quiz**
The winner will be announced November 7.

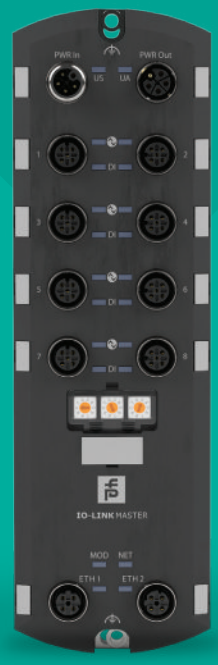
Contest sponsored by:

COMTROL
Pepperl+Fuchs

Pepperl+Fuchs Comtrol
www.comtrol.com

HEY PLC,

DON'T MIND ME.



Monitor, collect, exchange, and analyze data for reliable predictive maintenance with Pepperl+Fuchs Comtrol IO-Link masters. Unique MultiLink™ technology allows simultaneous data access from PLCs and OPC UA clients, so you can collect and deliver sensor data where you need it—to on-site systems, mobile apps, or the cloud. This helps you unlock the benefits of IO-Link and IIoT / Industry 4.0 without having to replace or interfere with your PLC.

www.pepperl-fuchs.com/comtrol

COMTROL
Pepperl+Fuchs

CODESYS

Node-RED

ssh

groov VIEW

Ignition! by Inductive automation

Sparkplug MQTT

OPENVPN™

***groov* EPIC**: it's **real-time control, connectivity, data handling,** and **visualization** in one industrial package. And it's ready for your industrial automation and IIoT applications today—and tomorrow.

- Program using tools you know: flowchart, ladder, function block, Python, C/C++, and more
- Integrate with other systems, including PLCs, databases, HMIs, cloud services, and IoT platforms
- Reduce unnecessary middleware to securely and efficiently get data where it needs to be
- Protect with built-in security, including configurable firewalls, encryption, and user accounts
- Install on plant floors and at remote sites—UL Hazardous Locations approved; ATEX compliant

Learn more now at **op22.co/thisisEPIC**

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
The Future of Automation.