02.2021 Issue **122**
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking & IIoT

Visit for the Latest Updates ■ www.iebmedia.com

TECHNOLOGY
Edge computing and AI create Industrial AIoT applications
Trending
Latest Updates
PC and EtherCAT-based control for Magellan telescope
10BASE-T1L extends Big Data analytics to edge of networks

Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

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

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

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

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

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

industrial ethernet book

Industrial Networking & IIoT

GET CONNECTED…

Visit our new website at: www.iebmedia.com

Software is the future ...

In this issue of the Industrial Ethernet Book, we take an in-depth look at the Industrial Internet of Things, starting with our IIoT Progress Report starting on page 8 but also through a series of articles authored by industry experts on topics ranging from Industrial 5G to cybersecurity.

As we look to the future for the Industrial Internet of Things, the overarching theme that comes back again and again is the increasing need for a software-centric approach. Software will be the determining factor in the future of industrial automation, in contrast to the discrete automation systems that use hardware focused architectures today.

In a recent article, Stan Schneider, CEO at Real-Time Innovations (www.rti.com), argues that the future belongs to software.

"Historians will look back on our time and wonder how we got by without smart machines," Schneider wrote in a piece for *Electronic Design*. "The transition will not be smooth—product lines, companies, and entire national economies are at stake."

"So, software excellence must join the manufacturing technology mix. In the next 20 years, manufacturing system performance will not improve by a factor of 10,000. Interoperability will not become 10,000X more valuable. But software will become 10,000X more important. That's the inevitable result of exponential computing growth. Any architecture that doesn't target using compute power as its primary goal is already obsolete," he stated.

Certainly, what we are finding with the Progress Report is a series of enabling technologies that will be shaping the future of the IIoT and its use in industrial automation and control networking. While developments such as the emergence of Single Pair Ethernet address hardware issues, the future will be shaped by software.

As the IT and OT worlds grow closer together, IoT systems in the cloud and edge computing environment will continue to develop. Technologies such as Industrial 5G will continue to expand connectivity options, and cybersecurity will be more important than ever.

Given that the IIoT is already ten years in the making, it's ironic that we are in a huge change process rght now. The influence of IIoT is already great today, both for industrial automation and smart manufacturing, but it's clear that industry's biggest needs today will be best addressed with digital initiatives. Digitalization of products and systems opens opportunities to deliver new and enhanced software solutions, and enable new digital services and business models.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2021.**
Deadline for editorial: March 15, 2021 **Advertising deadline:** March 20, 2021

View Industrial Ethernet Book website for latest news: www.iebmedia.com.

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

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

Technology to spur Industrial Ethernet market expansion

Global Market Insights reports that the Industrial Ethernet market may expand to more $100 billion (USD) by 2026, based on Industrial Ethernet enabling more communications across enterprises.

SOURCE: GLOBAL MARKET INSIGHTS

Industrial Ethernet software segment is likely to record a CAGR over 20% over the forecasted timeframe.

WITH EFFICIENT NETWORK INFRASTRUCTURE being installed across industrial settings, Global Market Insights, Inc. reports that the Industrial ethernet market is expected to procure commendable growth by 2026 in a new study, based on Industrial Ethernet enabling communication across enterprises.

Industrial Ethernet offers the availability of scalable communication performance whenever necessary using switching technology, and also encompasses advanced capabilities like high speed and enhanced connectivity across distance as well as the ability to connect multiple nodes.

Given to growing application and demand in the industrial sector, companies specializing in Industrial Ethernet products are developing advanced solutions and services. For example, in 2020, supplier of industrial communications equipment Advantech announced the launch of its latest series of 10G Industrial Ethernet switches that enable higher flexibility and bandwidth for heavy data transmission.

In view of such advancements, Global Market Insights, Inc., reports that the industrial ethernet market may register over USD 100 billion by 2026.

In terms of components, the Industrial Ethernet software segment is likely to record a CAGR of more than 20% over the forecasted timeframe. Industrial Ethernet software solutions also llow network management through the monitoring of Industrial Ethernet networks with different number of nodes.

Through these solutions, multiple devices can be configured at the same time. Industrial Ethernet diagnostic software solutions allow efficient topology recognition and support different devices including switches/hubs, WLAN devices, routers, as well as end devices.

Noteworthy advancements in the electrical and electronics sector is slated to offer substantial boost to the industrial ethernet market in the upcoming years. The implementation of Industrial Ethernet has enabled the usage of latest networking products such as firewalls, routers, hubs, switches, and gateways.

Geographically, the Europe Industrial Ethernet market is expected to hold over 25% of the global industry share during the forecast period. Presence of major companies like Robert Bosch GmbH, ABB Ltd., and Siemens AG is offering a considerable impetus to the regional market. Firms in the region are working on innovative platform solutions could offer support to customers demanding for enhanced Industrial Ethernet.

On a global scale, major companies operating in the industrial ethernet market are Rockwell Automation, Robert Bosch GmbH, Cisco Systems, Inc., Schneider Electric SE, and ABB Ltd. These organizations are focused on developing advanced, modern Industrial Ethernet components.

*Samikshya Borse, **Global Market Insights**.*

Moxa partners with Xilinx on advanced TSN technology

MOXA ANNOUNCED A COLLABORATION WITH Xilinx that focuses on development of time-sensitive networking (TSN) technology to realize a truly unified network for industrial automation and mass customization. The collaboration holds promise for enhancing network flexibility and interoperability on different levels of a TSN system.

Considered the new paradigm of industrial automation, TSN introduces deterministic, time-critical features on standard Ethernet and empowers the delivery of critical data to the right place at the right time in a converged and large-scale industrial network.

The partners plan to showcase preliminary success of their collaboration with a demonstration of a unified Ethernet infrastructure with guaranteed Quality of Service and in deterministic low-latency conditions.

The promising features of TSN make it compelling for a variety of industries including semiconductor, automobile manufacturing, machinery, food and beverage, chemical, electric power generation, and more. However, each TSN application has its specific requirements, and a substantial gap exists between TSN standards and application-specific TSN systems.

Because of this challenge, both Moxa and Xilinx want to fill the gap between the diverse TSN application requirements and TSN standards with the best possible real-time control and communications, advancing TSN to create leading edge platforms and infrastructure for industrial automation.

The TSN standards, like any popular industry standards, keep evolving, and most TSN implementations based on dedicated chipsets have limited future-proof capabilities to address customers' needs. Xilinx's FPGAs are designed to fix the flexibility issues brought by the ongoing evolution.

The combination of adaptable, high-performance Xilinx FPGAs and Moxa's TSN bridge solutions offer significant upgradability and reconfigurability to support the evolving standards and customer needs in the expansion of future applications.

*News report by **Moxa and Xilinx.***

| AT11-19E |

XPlanar®: Levitating, contactless, intelligent!

Free 2D product movement with up to 6 degrees of freedom

Levitating planar movers
kg
Scalable payload
360°
360° rotation
5°
Tilting by up to 5°
Lifting by up to 5 mm
Velocities up to 2 m/s

www.beckhoff.com/xplanar

XPlanar enables new degrees of freedom in product handling: Levitating planar movers float over individually arranged planar tiles on freely programmable tracks.

- Individual 2D transport at up to 2 m/s
- Processing with up to 6 degrees of freedom
- Transport and processing in one system
- Wear-free, hygienic and easy to clean
- Free arrangement of planar tiles enabling customized machine layout
- Multi-mover control allowing parallel and individual product handling
- Fully integrated into the powerful PC-based Beckhoff control system (TwinCAT, PLC IEC 61131, Motion, Measurement, Machine Learning, Vision, Communication, HMI)
- For use across all industries: assembly, food, pharma, laboratory, entertainment, …

New Automation Technology **BECKHOFF**

UWB Alliance & omlox partner on ultra-wideband technology

UWB Alliance focuses on UWB ultra-wideband technology, advancing updates of UWB rulesets in the U.S. and global ruleset and spectrum management harmonization. omlox focuses on real-time locating services.

THE OMLOX COMMUNITY OF PI (PROFIBUS & PROFINET International) has signed a joint liaison agreement to work together with the UWB Alliance in areas of mutual interest.

Within the liaison, UWB Alliance focuses on matters arising from the promotion of UWB technology and advancing updates of the UWB rulesets in the United States, EU as well as furthering global ruleset and spectrum management harmonization. omlox (the open location standard) focuses on the definition and promotion of the UWB technology, to provide cost-efficient real-time locating services for the industry, in an open and interoperable manner.

The UWB Alliance was established in 2018 to foster the use of UWB technology solutions, promote industry growth and advocate favorable regulatory developments worldwide. In addition to promoting the adoption of UWB technology, the alliance works with public policy officials around the world to further the understanding of UWB capabilities, use cases and promote advantageous UWB rulesets. Most recently the UWBA was successful in advocating for changed duty cycle measurements in the EU.

omlox, was also established in the same year to develop open and interoperable standard for real-time locating services in the industry based on UWB (amongst other locating technologies). Today, omlox is an award-winning standard, driven by a large ecosystem of software and hardware vendors, as well as system integrators and research labs, and hosted by PI (PROFIBUS & PROFIBUS International).

SOURCE: PI INTERNATIONAL

Focus is on unlocking more innovative use-cases and augmenting the huge adoption curve for UWB technology.

"In-line with our expectations, last year UWB achieved the milestone of widespread acceptance in consumer electronics," said Timothy Harrington, Chairman of the UWB Alliance. "Three of the top-ten smartphone vendors adopted it in conjunction with the IEEE 802.15.4z standard in their latest smartphone products. It also made the significant jump to laptops, mass-market wearables and smart home products. Through our partnership with the omlox community, we can enrich and inspire the already thriving environment in which innovation for UWB products, applications, technologies and use cases drive forward the global UWB ecosystem to take the market for UWB to the next level."

UWB Alliance and omlox

IO-Link over Single Pair Ethernet (SPE) working group

A new IO-Link over Single Pair Ethernet working group formed by PI International will examine the potential and feasibility of combining these two technologies through a concept study.

In common factory automation applications, IO-Link easily meets most application requirements. But smart Factory developments driven by Industry 4.0 are creating new challenges. The portfolio of IO-Link devices is also growing, which in turn is expanding potential areas of application. For example, there is indeed demand for transferring IO-Link over greater distances than the 20 m currently specified.

SPE (Single-Pair Ethernet) promises a number of advantages. This is why the IO-Link Steering Committee has recently created a working group intended to examine the potential and technical feasibility of a published "IO-Link over SPE" concept study. Karim Jamal of Texas Instruments has been named head of the working group.

"Our goal isn't to replace IO-Link, but rather to expand it with a new interface where it makes sense" said Jamal in summarizing the task. "We place great value on existing IO-Link integration standards like IODD and will keep compatibility in the foreground of our technical considerations."

IO-Link over SPE will retain the protocol and data model of IO-Link and expand it with a physical interface. With SPE and a potential combination with PoDL (Power over Data Lines), terminals – i.e. sensors or actuators – can also be operated on the lower field level with sufficient data bandwidth.

With IO-Link over SPE, IO-Link messages are transferred over a single-pair line – without TCP/IP or UDP – instead of being transferred as pulse-encoded telegrams over the classic 3-lead cable at 24 V. The advantage is that the core components of IO-Link communication, the implementations of the protocol layer and the functions remain unchanged.

In other words, IO-Link is still IO-Link. IO-Link over SPE isn't another Ethernet-based bus system, but rather a point-to-point connection with no IP addressing.

All the defined interfaces and functions are retained. Established IO-Link integration standards like IODD, the OPC UA Companion Standard, JSON mapping and fieldbus integration can still be used in the exact same way.

PI International.

Prefabricated data centres enable rapid edge deployments

New edge computing facilities will complement the cloud, not replace it. The idea is to handle as much of the now enormous quantity of data as close to where that data is generated as possible.

WITH THE INTERNET OF THINGS, ARTIFICIAL intelligence, and 5G networks gaining momentum, much more data will be processed much closer to its source. The infrastructure necessary to shorten these distances must be flexible, modular, and quick to deploy at many sites on the edge of the network. Prefabricated, all-in-one data centers may provide an attractive alternative solution.

The dawn of the cloud era went hand-in-hand with the advent of the hyperscale data center. A lot of data moved from on-premise enterprise facilities to cloud. The advantages of having massive storage and compute resources concentrated at a single physical location include cooling efficiency and the ability to balance loads across many servers. But not every application can operate up to its potential given the latency and bandwidth limitations of the internet.

SOURCE: DELTA ELECTRONICS

Edge computing carried in the form of modular data centers may be an answer to managing overwhelming IT loads.

Enter the edge

Edge computing and the IoT will not make enormous, hyperscale data centers obsolete. Even though the trend is moving towards distributed data processing and storage, these new edge computing facilities will complement the cloud, not replace it. The idea is to handle as much of the enormous quantity of data as close to where that data is generated as possible.

By limiting distances and hops between devices and the cloud resources that serve them, edge computing facilities reduce latency. They also ease the bandwidth constraints within which traditional cloud solutions must operate and provide additional compute resources. There are a host of new technologies on the horizon such as autonomous driving, augmented reality (AR), and virtual reality (VR) that will benefit greatly from edge infrastructure.

In VR applications, inputs such as hand motions, photons, and controller inputs need to be processed extremely rapidly to mimic reality. At the same time, many complex rendering processes are necessary to generate the virtual (or augmented) environment for the user.

With processing loads this high, it´s difficult to include the required compute power inside the device itself. The answer is split processing, with part of the computational or rendering load handled in the edge-powered cloud instead of the AR or VR device itself.

First wave: telecommunications & IT

As New Radio (5G) mobile communications networks are deployed around the globe, preparations for a massive increase in data traffic are also underway. There will be so much data, it will be impossible to process all of it from centralized data centers. That´s why telecommunications operators will be the first vertical to start deploying edge data centers at scale. In many major mobile networks, for instance, there are only a handful of wireless network interconnects for an entire country. Data can travel extremely long distances before it even gets an IP address. The ensuing latency would limit many of the services that 5G is being built to support.

The future of telecommunications infrastructure may therefore involve some RAN functions moving to data centers in areas where low-latency 5G services are available. This convergence with mobile edge compute could lead to a more unified approach to 5G architecture. Even with more edge computing capacity, more fiber will still be needed.

The IIoT and other verticals

In addition to telecommunications, many other industries will also be investing in edge computing. Manufacturing is currently experiencing a revolution that includes smart factories, the IIoT and Big Data. In many cases, existing manufacturing facilities are not equipped to handle the amount of IT hardware necessary to power those increasingly essential applications. Most factory floors are no place for dust-sensitive servers and power equipment. Cloud solutions may not provide the ultra-low latency (ULL) required in a manufacturing context.

Edge computing carried in the form of modular data centers can be the answer to managing otherwise overwhelming IT loads. Instead of building an entire datacenter at a different location, a container can quickly be set up in a parking lot next to the factory, for instance. Healthcare, utilities, transportation, smart buildings, and smart cities are other fields in which edge computing enabled by prefabricated data centers makes sense. In most cases, improving application performance will be the main motivator behind the decision to invest. But many will also deploy compute resources to the edge to take advantage of real-time analytics or utilize streaming data.

Making edge computing a reality

Edge data centers serve to cache and aggregate data at points between users and larger data centers. Often, the goal is to push the edge out closer to users across a wide geographic region. Consequently, network operators and enterprises need affordable, reliable, and quick-to-deploy infrastructure, much like Delta´s new SmartNode Tier II and Tier III modularized data centers. It´s their agility and speed that allows prefabricated data centers to start contributing to revenue generation almost immediately. Break-even is reached much faster when compared to a conventional data center construction project.

*News from **Delta Electronics**.*

Industrial Internet of Things Progress Report

A broad set of IIoT-enabling technologies from Industrial 5G to OPC UA, cloud and edge computing, Time Sensitive Networking and Single Pair Ethernet, to name just a few, are continuing to emerge and will empower and drive new levels of innovation for companies implementing IIoT applications.

The system is always greater than the sum of its parts, and IIoT-enabling technology is emerging that will provide new levels of connectivity in manufacturing.

NEW INDUSTRIAL INTERNET OF THINGS technologies are creating a richer and richer ecosystem of connected devices, controllers and subsystems, from the sensor to the cloud, enabling new levels of digital innovation that is rippling through and transforming global manufacturing.

The rate of change may not always seem to be profound, but when you stack all of the significant areas of technological change related to the IIoT together, we see a different picture.

Major initiatives including development of Industrial 5G, Edge Computing, IT/OT Convergence, Time Sensitive Networking, Single Pair Ethernet, Cybersecurity Standards and OPC UA provide an impressive array of developing new possibilities that will drive the IIoT forward for the foreseeable future.

Even though we already have a decade of IIoT development in the books, in many respects we are still early in the process and the best is yet to come.

IIoT progress report

For this IIoT progress report, IEB reached out to major players in the development of the Industrial Internet of Things to get their perspective on the megatrends shaping and enabling development of the IIoT in 2021 and beyond. We wanted to know what specific benefits these enabling technologies will provide versus what is possible with typical applications today—along with the challenges that these technologies address.

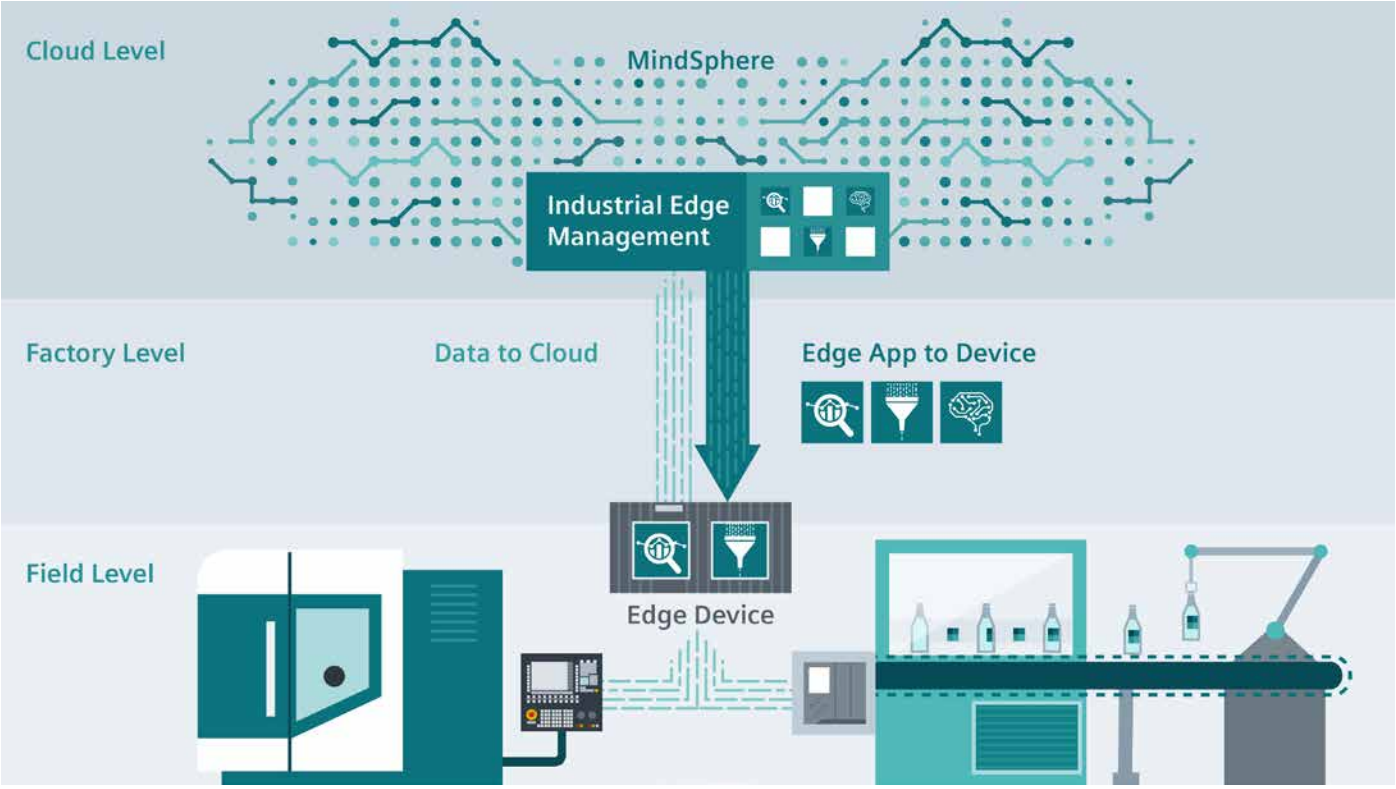
And finally, given that the IIoT is already ten years in the making, we asked for their assessment of the progress and overall impact of the IIoT on industrial automation and smart manufacturing to date, and what are the key next steps and/or technologies that will enable more rapid development of IIoT applications.

Cloud, edge and Industrial 5G

Key IIoT enabling developments are continuing refinements of cloud, edge and Industrial 5G technology solutions with a focus on the needs of IT/OT convergence. The reality is that the potential of the IIoT depends on tight integration between operating machines, on one hand, and business information systems, on the other.

Katrin Kunz, Head of Marketing for SIMATIC IPC/HMI/IoT Products at Siemens said she expects the convergence process to continue to develop, aided by new cloud and edge computing solutions along with the emergence of Industrial 5G.

“I expect the OT and IT worlds to grow even closer together,” Kunz said. “This will result in a greater degree of networking of IoT devices. At the same time, the data volumes to be handled will continue to increase. IoT systems in the cloud and edge computing environment will continue to develop,” Kunz stated. “The number of cloud and edge apps available on the market will explode. And I am sure we will see more and more virtual reality and artificial intelligence installations.”



SOURCE: SIEMENS

Creating IIoT solutions that work from the sensor to the cloud is requiring new system architectures that enable higher levels of data accessibility.

She added that industrial security will certainly become increasingly important in connection with these developments. In addition, open IoT ecosystems will form, from which device manufacturers, app developers, and service providers will benefit massively in the coming years. In industrial communications, she also expects Industrial 5G to become increasingly established on the market over the next few years.

"This focus not only on the technology is needed but also on the business change required. I am sure many enterprises will realize that investing in an IoT solution is only one step to solving the business problem and integrating it into the business processes that it seeks to impact," Kunz added. "Vendors and service providers need to find ways to adjust the messaging to talk about the business process change and how the technology will support it."

IIoT: unprecedented flexibility

First of all, Kunz wanted to emphasize that traditional implementations and IIoT implementations with cloud and edge computing will coexist. Most applications can be implemented traditionally or with IoT technologies. From her point of view, IoT technologies result in unprecedented flexibility and agility. The price companies have to pay as a basis is standardization.

"With edge computing and in our case Industrial Edge evolving as open ecosystem of solutions, devices and apps, customers are able to flexibly realize IoT solutions close to machines - best integrated into industrial automation," she said.

Companies can introduce applications like data analytics or AI to the shop-floor close to the machine in less time to increase the productivity of machines & plants even further. Furthermore, shop-floor users are empowered to manage machine parks and plants by choosing and centrally deploying best-in-class applications from an open app store.

"With cloud computing and, in our case MindSphere, IoT solutions are powered from the edge to the cloud with advanced analytics and AI. Customers can connect and analyze data from connected products, plants and systems to optimize operations, create better products, and enable new business models. Built on the Mendix application platform, MindSphere empowers customers, partners and the Siemens organization to quickly build and integrate personalized IoT applications."

Challenges for automation & control

Kunz stated she thinks the biggest challenge for automation and control engineers is to embrace the new/unknown. Company leaders, automation and control engineers, but also employees need to be open, trained in IoT technologies and industrial security. Especially in IoT projects, it is important to understand that the technology is one thing, and the implementation of processes and change in the minds of the workforce is another. Everyone who ends up working with IoT technologies needs to be aware of what he/she is doing, and also what can be done in the process.

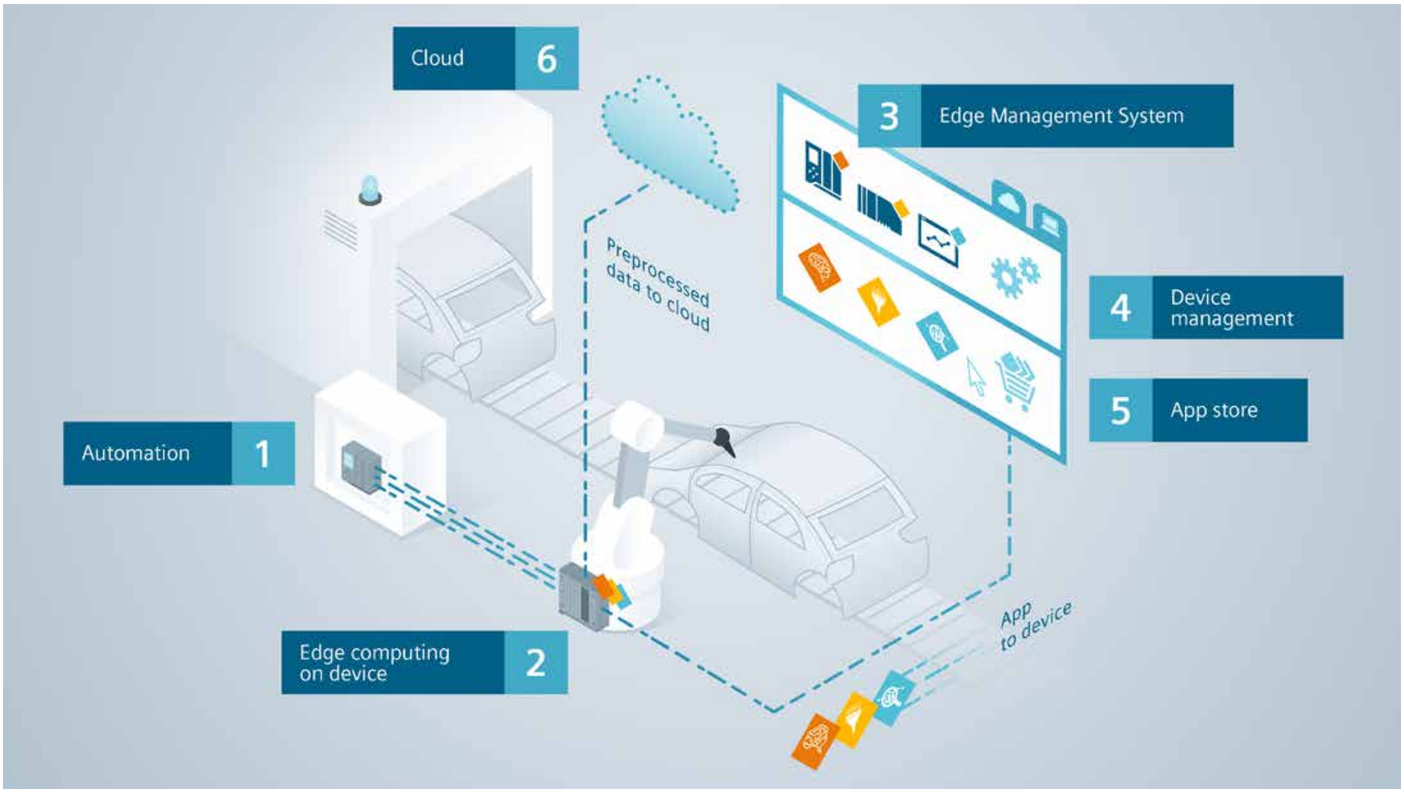
Standardization is the foundation for any digitization project. But what is also becoming increasingly important is to understand the company data and its semantics in detail because, without that, it will be difficult or impossible to implement artificial intelligence.

"We are all in a huge change process right now. I believe that the influence of the IIoT is already great today, for industrial and process automation as well as for smart manufacturing," Kunz said. "Its importance will increase massively in the coming years and decades."

She cites low code programming and Siemen's low-code application platform (all-in-one-platform) that is making it possible for anyone to be empowered to build, integrate and extend applications 10x faster, with 70% fewer resources. Customers are enabled to increase operational efficiency, modernize core systems, launch new products and create digital experiences, backed by the Mendix developer community and industry-leading, low-code capabilities as well as cloud services, and industrial and business services.

IIoT: data in the forefront

One key trend with the emergence of the IIoT is the ability for companies to better use and leverage large amounts of data. This ranges from better remote access to equipment, use of data for more resilient operations, and simulation and emulation tools to reimage



SOURCE: SIEMENS

Industrial Edge allows user to analyze all data at the machine or preprocess it quickly and instantly. The optimized data points can then be transferred more quickly to the cloud where, for example, you have access to more computing power and larger storage capacities.

machine operation and workflow.

"Industrial companies have accelerated their adoption of remote access at blazing speeds during the pandemic. With onsite access for equipment experts, limited use cases for remote access have expanded, such as for equipment demonstrations, factory acceptance testing, and troubleshooting and maintenance," Jessica Forguites, Product Manager at Rockwell Automation told IEB recently. "This is made possible with a foundation that includes a network architecture based on standard and unmodified Ethernet, and high-performance smart devices with gigabit speeds and security features."

Another trend is the use of IIoT data to create more resilient operations. Supply chain issues that emerged during the pandemic and other challenges like the skills gap and limitations of people inside of facilities have created a need for companies to improve resiliency enterprise wide. They're doing that by using newer innovations like closed-loop scheduling, self-aware systems and smart objects. They're also making investment in MES and analytics solutions to drive labor efficiencies, tighten integration between production and material planning, and meet quality and regulatory requirements.

Tools like simulation and emulation software are also using digital twins to help reimagine work, from iterating designs before steel is cut, to testing the controls for a machine before it's bolted to the floor, to creating experienced workers before they touch live controls.

Remote access technologies

Forguites said that secure remote access is helping keep workers safe by allowing them to do their jobs from home. But companies are also using it to transform and improve how those jobs are done. OEMs, for example, can combine remote access with other technologies like a digital twin and augmented reality (AR) to do remote virtual demos of new equipment. Production workers can also connect with remote experts to more quickly resolve problems, without waiting for the expert to fly in. Using AR technology, remote support can even be enhanced with drawings and overlays that are placed directly on the machines in front of the production workers.

"Meanwhile, IIoT applications that strengthen resiliency can simplify jobs and optimize operations. Closed-loop scheduling can automate and optimize daily schedules," Forguites added. "Self-aware devices can automate device configuration and ease maintenance. And innovations in control system designs like smart objects can greatly simplify data science by allowing data to be automatically organized, modeled and consumed by IoT systems, with little to no effort from a programmer. In one case, a company estimated it would have taken a developer one month to do what smart objects enabled in only six hours."

Working through the pandemic

The pandemic has changed work as we know it in the industrial world. For some companies, this has led to new and better ways of working. At one chemical company, secure remote access helped employees remotely deploy two new facilities during the pandemic. This helped keep employees safe, improved overall efficiency because of reduced travel needs and improved system support coverage. The company now plans to use this approach to start-up and commission all of its facilities.

Forguites said that the skills gap is another top challenge facing industry. Retirements of skilled employees are mounting, and technologies and processes in production facilities are becoming increasingly complex. Analytics software that turns raw production data into useful, real-time information can give less experienced workers helpful insights into production and answer their pressing questions. What's more, companies can use analytics software for real-time workforce performance monitoring. This can help them understand how long a process is taking an operator and uncover ways to improve productivity.

Innovations like smart objects also reduce the demands put on engineers and data scientists by streamlining data preparation. And self-aware devices help simplify device integration and maintenance.

"Digital transformation has forever changed how people make things. And it's clear that industry's biggest needs today are best addressed with digital initiatives," Forguites said. "Companies that are well underway on their digital journeys are already discovering

Industrial 5G Impact on the IIoT

One of the main differences between 5G and previous generations of cellular networks lies in 5G's strong focus on machine-type communication and the Internet of Things (IoT).

The capabilities of 5G extend far beyond mobile broadband with ever-increasing data rates. In particular, 5G supports communication with unprecedented reliability and very low latencies, and also massive IoT connectivity.

In manufacturing in particular, 5G may have a disruptive impact as related building blocks, such as wireless connectivity, edge computing or network slicing, find their way into future smart factories.

In order to ensure that the specific needs and requirements of a particular vertical industry are adequately understood and considered by the telecom industry and, likewise, the capabilities of 5G are fully realized and exploited by the vertical industries, close collaboration is required between all relevant players.

With this in mind, the 5G Alliance for Connected Industries and Automation (5G-ACIA) has been established, which serves as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. Review white paper for an overview of 5G's basic potential for manufacturing and relevant use cases.

Read White Paper

what's possible and demonstrating value of these investments back to their organizations. One company facing a skilled worker shortage established a new center to provide support and collaboration for its hundreds of global production facilities using remote monitoring and predictive analytics. In another case, AI-driven predictive maintenance and asset optimization helped global mining operations save hundreds of thousands of dollars in unnecessary spend."

As companies undergo digital transformation, they should remember that it's an ongoing journey. They should try to learn from early successes and failures, not only in their digital initiatives but also those of organizations. Make sure initiatives incorporate what have proven to be the best practices of digital transformation, executive sponsorship, a roadmap, a change-management plan, comprehensive cybersecurity and a partner that can bridge internal gaps.

Importance of cybersecurity

Cybersecurity is a non-negotiable component of any digital transformation. But companies must make sure they tailor cybersecurity to the unique risks, network activity and requirements of operations environments. Visibility and threat detection software should be able to explore the deepest level of industrial network protocols to identify even the smallest of anomalies. The software should also use a passive monitoring approach to inspect traffic without the risk of disruption.

Using control products with CIP Security is a way to tailor cybersecurity to the operations environment. CIP Security is the only standard designed to secure communications between industrial control systems and other devices on an EtherNet/IP network. Companies should also make sure that they and their suppliers comply with global security standards, such as ISA/IEC 62443 and ISO 27001.

"Companies should map out their process workflows. That's important from a security standpoint, Forguites said. "But it can also help keep track of the many system and data point connections, especially as those connections grow over time. Software tools and services are available to give companies visibility into their network connections."

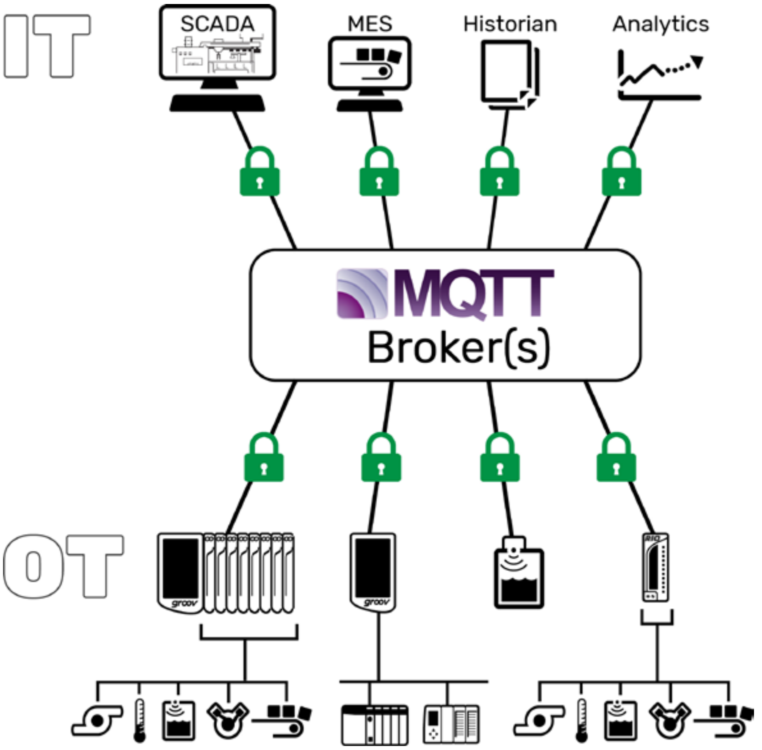
Emergence of edge computing

Traditional industrial communication systems address data processing from a hierarchical perspective, as with the classic Purdue model. One good feature of this hierarchy is the clarity it provides with regard to where data can originate, be stored, undergo processing, and be delivered.

However, the task of transporting data and processing it in context is often quite difficult, because so many layers of equipment and software are required to connect devices and applications.

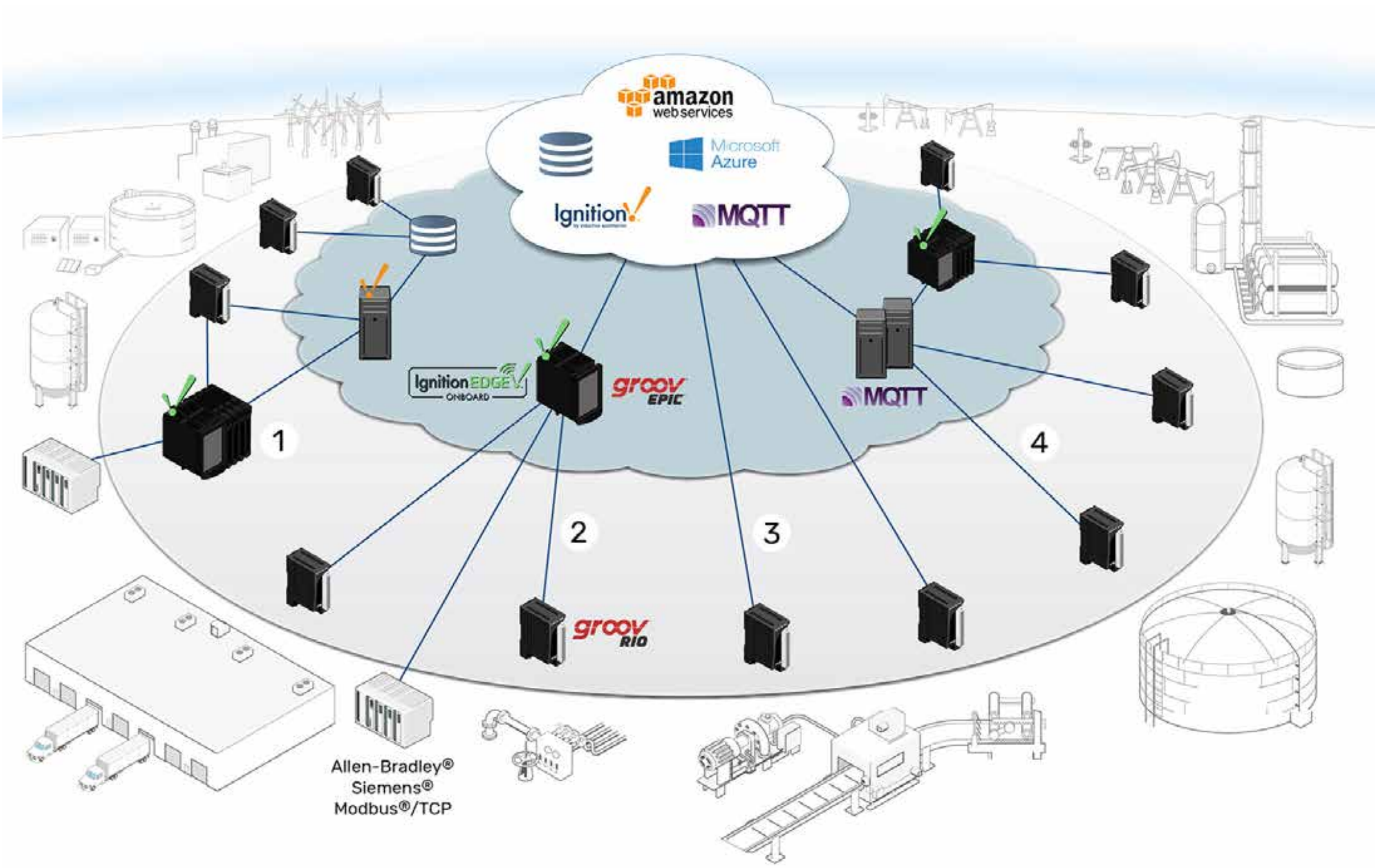
"The hierarchical approach was necessary when computing capability, network bandwidth, and security features were much less available," Josh Eastburn, Director of Technical Marketing for Opto 22 told IEB. "Each step up the hierarchy from a basic hardwired sensor to cloud computing systems was required to access greater computing and networking resources. It also clearly delineated the security measures networks required around unsecured field equipment."

"Now, industrial edge computing is changing the relationship between field assets and the systems that collect and use their data. Complementary to this, MQTT/Sparkplug B is gaining traction as a potential industrial standard, enabling large-scale interoperable IIoT communications. Together the two technologies are laying a foundation for widespread IIoT."



SOURCE: OPTO 22

The basic structure of an MQTT network, clients from OT and IT communicating through an MQTT broker.



SOURCE: OPTO 22

Four examples of new architectures that are possible with industrial edge devices: 1) Shared infrastructure with edge data processing; 2) Legacy device integration with edge controller as IoT gateway; 3) Direct-to-cloud I/O network; and 4) Many-to-many MQTT infrastructure.

Benefits of edge technology

Traditional industrial devices are designed for a narrow scope of operation with limited software/firmware tools and protocols outside of I/O and control networks. Specifically, they lack functions that would make them compatible with other parts of the enterprise, most notably standard IT security and communication formats. They also lack the computing capability to deal with large and complex data volumes.

According to Eastburn, industrial edge devices provide general-purpose computing, networking, and storage directly to the process, sensor network, or field of operation, enabling them to overcome these traditional limitations. Opto 22's groov family of edge devices, for instance, implements centralized user authentication, device firewalling, TLS data encryption, certificate management, VPN, and so on. They also support data processing and communication directly to databases, cloud services, and other applications using tools like Node-RED.

"Within that infrastructure, MQTT can provide communication that is 80-90% more efficient than traditional poll-response protocols because of its lightweight format and brokered report-by-exception communication pattern," Eastburn added.

"And because client connections are outgoing (device-originating), edge device firewalls can completely block outside connection requests while still providing bi-directional communication. Building on top of this, Sparkplug B defines an interoperable data exchange format for MQTT communications with a data-rich payload structure that supports a unified namespace where IIoT communication can happen across the organization."

Flexible, scalable architectures

IIoT growth requires, first and foremost, scalable architectures. Scalability is a combination of cost-efficiency, driven by the efficiency of the underlying communication mechanisms, and the quality of cybersecurity and other factors affecting data integrity (You can't scale if it costs too much or isn't safe).

Unfortunately, the traditional, multi-layered Industry 3.0 technology stack inflates integration costs and reduces efficiency because of the complexity required to introduce new connections between applications and devices.

The connectivity and data processing embedded in industrial edge devices provide simple, comprehensive integration options that reduce the cost of expanding the network. Rather than navigating layers of infrastructure, they can send process data directly to business applications, cloud services, and so on.

They can further flatten the architecture by assimilating automation functions typically given to PCs, like hosting database, communications, and HMI servers; running custom applications; or bridging disparate automation networks. They can also provide secure gateway functions to integrate legacy control systems and equipment.

MQTT overcomes similar challenges, improving data security and reducing bandwidth consumption without requiring investment in new infrastructure, because it is built around scalable architectural concepts. Rather than focusing on point-to-point connections, MQTT traffic is routed through an MQTT broker, which handles distribution to all clients. It creates a one-to-many relationship between clients that is much easier to scale up than many direct connections.

Early days for IIoT

"These are still early days for the IIoT. These projects have largely been taken on by well-funded industry players and are only recently becoming a possibility for the typical system integrator, manufacturer, etc. as we put forward technologies that are efficient and effective," Eastburn said.

Key next steps and/or technologies that will enable more rapid development of Industrial Internet of Things applications in the future include:

1. *Considering alternative architectures:* IIoT is prompting an evolution in technology, but if you don't grasp the concepts behind that evolution, you can misapply the technology and fail in your IIoT goals. Trying to do the same thing bigger or faster is not what IIoT is about. Understand what it could mean to reorient your infrastructure for scalable communication across the entire organization.
2. *Having a conversation with your IT group about security:* Security is a traditional sticking point between IT and OT personnel. Edge computing with MQTT makes it possible to resolve this disconnect but you may still encounter a lot of skepticism. Make the effort to understand best practices and demonstrate to your IT counterparts that you can meet those requirements. Then you can proceed with a conversation about what is possible when your networks are safely connected.

IT/OT Convergence

One trend that is driving the IIoT forward is the primary need for convergence between Information Technology (IT) and Operations Technology (OT) within the smart factory.

Digitalization of products and systems opens the opportunity to deliver new and enhanced software solutions and enables new digital services and business models. But the implementation of these concepts is made more difficult because of the heterogeneity of communication protocols at the field level.

According to a technical paper from the OPC Foundation, although most of today's fieldbus systems and real-time Ethernet protocols are standardized by IEC in the 61784/61158 series, automation devices supporting different protocols are not interoperable with each other and often cannot coexist in a common network infrastructure. In addition, device information is structured using different information models, which makes data analysis a labor-intensive and time-consuming task that is also vulnerable to errors, especially in multi-vendor and multi-protocol environments.

However, the trend of moving to seamless interoperability accelerated by the dawn of the Industry 4.0 and Industrial Internet of Things (IIoT) era requires industrial system integration to become vendor-independent and to support end-to-end interoperability from sensor to cloud, including field level devices for all relevant industrial automation use-cases, including real-time, motion, and functional safety.

"Standardized communication from sensor to cloud will support the digital transformation across all industries, including factory automation and process automation," the report states. "End users, machine/skid builders and system integrators will benefit from easier system integration and cross-vendor interoperability. Seamless access to production data and process conditions will facilitate availability and optimization of production processes."

This approach requires standardization to take place on multiple levels: semantics, information modeling, communication protocols, data link layer and physical layer – all embraced by a common cyber-security framework.

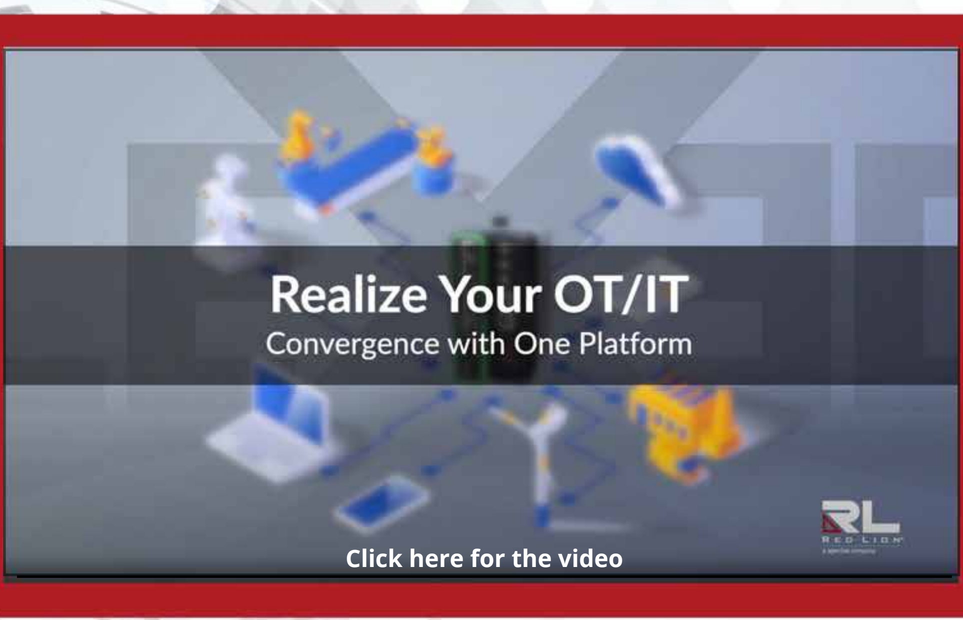
An important aspect is the convergence of information technology (IT) and operational technology (OT) allowing a common network infrastructure to be shared by IT and OT traffic while guaranteeing different levels of quality of service (QoS) demanded by diverse IT and OT applications.

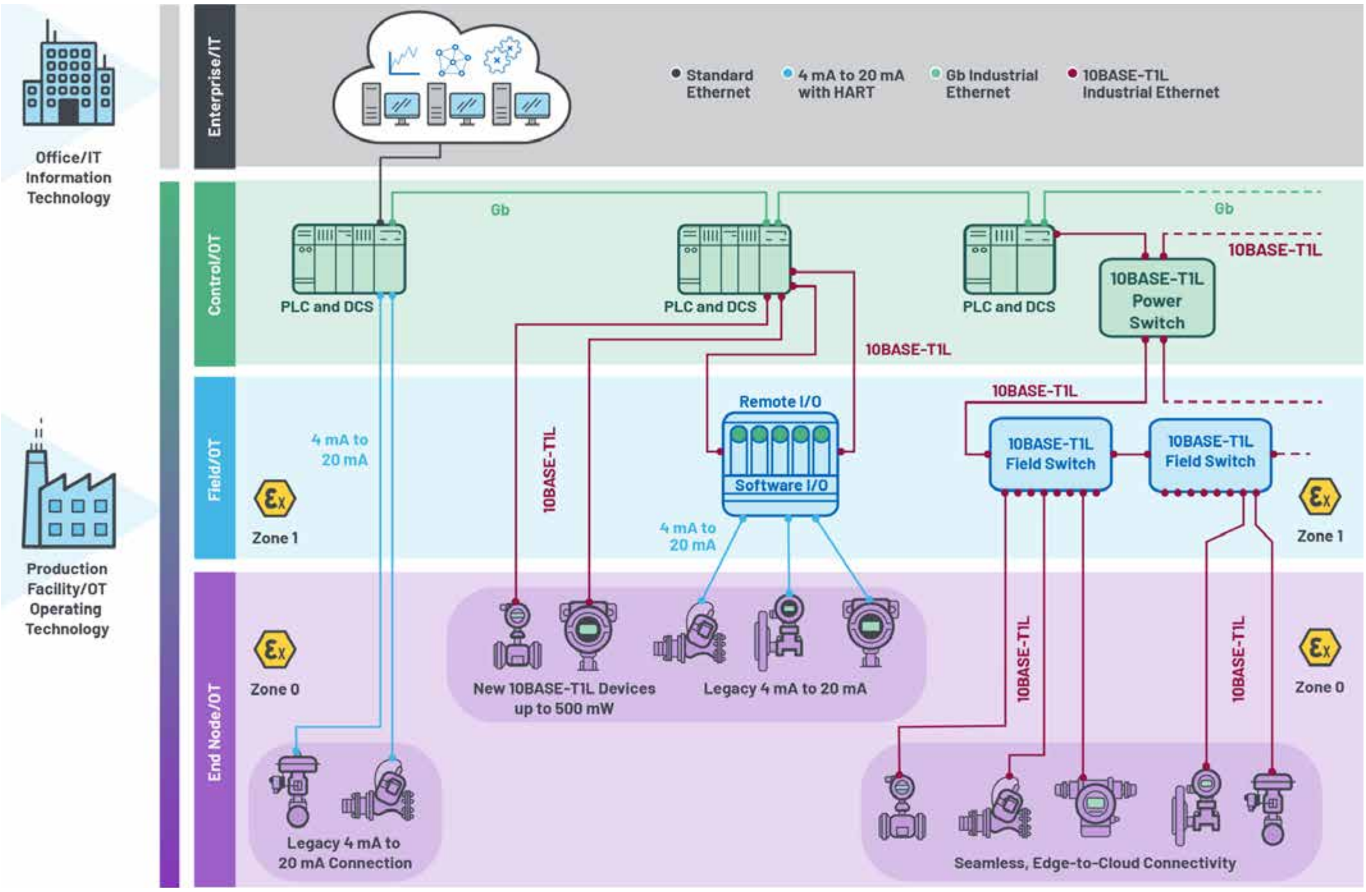
APL and TSN technologies

Technologies that the OPC Foundation report singles out as having particular importance are the Ethernet Advanced Physical Layer (APL) and Ethernet Time-Sensitive Networking (TSN). APL facilitates seamless Ethernet connectivity down to the field level, including long cable lengths and explosion protection via intrinsic safety with power and communication over two wires.

TSN enables deterministic communication on standard Ethernet, allowing IT and OT protocols to coexist in a common network infrastructure.

The OPC Foundation's Field Level Communications initiative was established in November 2018 to specify extensions to the





SOURCE: ANALOG DEVICES

The deployment of increased numbers of Industrial Ethernet connected edge nodes across both factory and process facilities will result in operations managers having data at their fingertips to optimize operations and inform decision making.

OPC UA framework in order to standardize the semantics and behaviors of controllers and field devices from different manufacturers. The main use cases covered by the initiative are controller-to-controller, controller-to-device, and device-to-device including support for IIoT connectivity for both controllers and devices (controller-to-compute and device-to-compute).

The technical work is being performed in OPC Foundation multi-vendor working groups that define the technical concepts and specify the different mechanisms to achieve these goals.

Horizontal/vertical connectivity

"The goal of digitalization is to foster the integration of IT technologies with OT products, systems, solutions and services across their complete value chains, which stretches from design and production to maintenance. Once implemented, digitalization of products and systems opens the opportunity to deliver new and enhanced software solutions and enables new digital services and business models."

The Internet of Things (IoT) brings together a broad range of technologies to those OT products, systems and solutions that have traditionally not been connected via today's near ubiquitous IP-based networks. While Ethernet provides the ability for things to 'reach' each other, they still need a common way to communicate. Standardized data connectivity and interoperability addresses this need.

The report says that, in simple terms with standardized data connectivity at its core, the Industrial IoT (IIoT) can be looked at from two perspectives: horizontal and vertical data connectivity. An example of horizontal communications is to be clarified: controller-to-controller (C2C) data connectivity between shop floor systems.

An example of vertical communications is device-to-cloud data transfer. In both cases, the OPC Unified Architecture (OPC UA) standard from the OPC Foundation provides a secure, reliable, and robust foundation to facilitate standards-based data connectivity and interoperability.

For years, many companies and partner organizations have openly worked together under the umbrella of the OPC Foundation to make this a reality and will keep doing so as it continues to expand its collaboration activities.

"A key aspect of improving horizontal and vertical data connectivity is network convergence supporting a common network for IT and OT-related communication. Ethernet Time-Sensitive Networking (TSN) according to IEEE 802.1 supports communication with bounded latency and jitter," the report added.

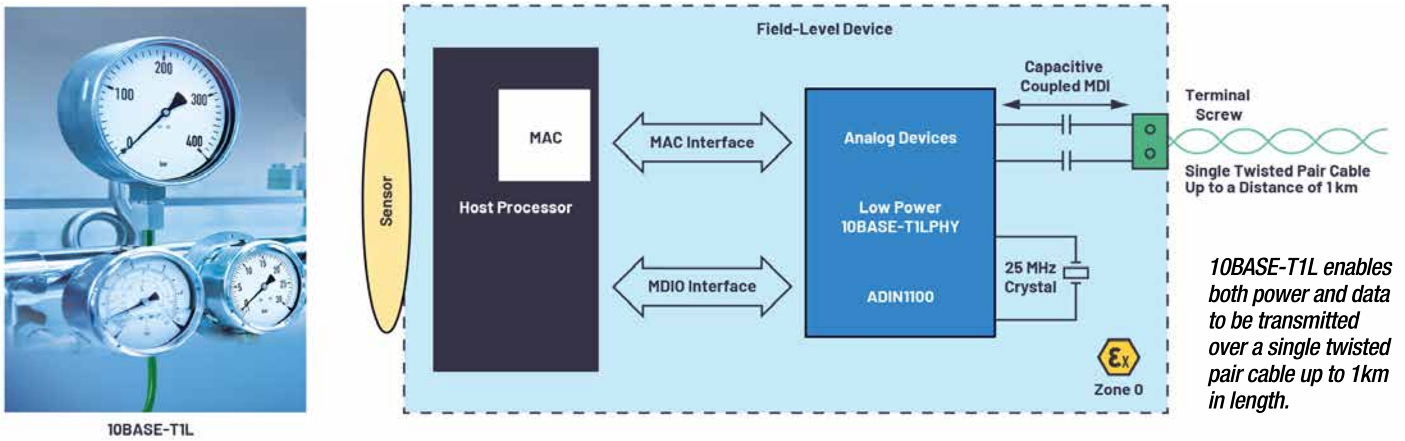
"In addition, various data streams, and traffic types can be transmitted over a common network infrastructure, while at the same time guaranteeing the various bandwidth, latency, jitter and reliability requirements of the different applications. Therefore, TSN plays a key role in supporting the convergence of IT and OT. The Ethernet Advanced Physical Layer (APL) is another key technology to drive network convergence as APL delivers seamless Ethernet connectivity to sensors and actuators in process automation – including hazardous areas."

Field Level Communications

The OPC Foundation announced recently that its Field Level Communications Initiative has accomplished a significant milestone in the ongoing project by completing their initial release candidate with the focus on the Controller-to-Controller (C2C) use case. In addition, a technical paper has been published that explains the technical approach and the basic concepts to extend OPC UA to the field level for all use cases and requirements in Factory and Process Automation.

For more information, download the "OPC Foundation FLC Initiative Technical paper".

Read Technical Paper



10BASE-T1L enables both power and data to be transmitted over a single twisted pair cable up to 1km in length.

SOURCE: ANALOG DEVICES

Connectivity megatrends

According to Fiona Treacy, Strategic Marketing Manager–Industrial Communication for Analog Devices, the digital or smart factory and the evolution of connectivity networks is one of the megatrends driving IIoT markets in 2021.

In combination with the increased deployment of condition-based monitoring technologies across the factory floor, this will enable new data streams to be activated and utilized to increase productivity. The deployment of increased numbers of Industrial Ethernet connected edge nodes across both factory and process facilities will result in operations managers having data at their fingertips to optimize operations and inform decision making.

Also coming on stream is the advent of 5G technology, bringing with it the wireless connectivity needed for AMR's (Autonomous Mobile Robots) which will see them make more strides toward the realization of their full potential. Finally, as more and more devices become connected and interconnected, the security burden is increasing for all, with 2021 likely to bring new solutions and technology's with partners working together to scale solutions.

"The launch of Single Pair Ethernet, 10BASE-T1L physical layer devices will prove a game changer on the road to realizing edge node connectivity. Enabling both power and data to be transmitted over a single twisted pair cable up to 1km in length," Treacy stated. "For the first time we will see devices across process facilities directly become IP addressable. This will change both the control network topology but also the maintenance and deployment burden. It will now be possible for Field devices to be programed or reconfigured from any connected devices without the need to deploy service personnel."

The increase bandwidth of 10Mbps will enable new data streams to be transmitted beyond control data, like auxiliary device variable or other health parameters. This new information will enable the optimization of processes and the increase in asset utilization. 10BASE-T1L connectivity promises to extend the benefits of IIoT to the remote corners of factories and process plants, where sensors and other endpoints were until now out of reach of the enterprise network.

Emergence of TSN

Treacy said that the second key technology coming closer to fruition in 2021 is Time Sensitive Networking. With the hardware portions of the standard mostly completed, we expect to see the first TSN compliant layer 2 switching technologies sampling into automation equipment vendors. Time sensitive networking (TSN), is foundational for meeting the many powerful outcomes of IIoT. With TSN, all data across the factory—from the floor to servers, front office, and everywhere in between—can coexist and communicate.

A third trend that Analog Devices sees is Gbit technology starting to dominate in new designs with vendors seeking to future proof beyond 10/100Mbit speeds.

Challenges for users

Both new technologies will provide control and automation engineers more visibility into their production environment by providing access to enhanced data streams. With TSN being the first step to breaking down existing data silos that hinder seamless connectivity, it can enable ubiquitous access to precious, decision-making data.

TSN will create a common language that will enable equipment from different manufactures coexist on the same Ethernet network. It enables real-time, deterministic data crucial for accuracy and precision in control environments. Finally, it will help to close the divide between Information Technology (IT) and Operating Technology (OT) specialists, by providing a common set of tools, in support of a converged network.

"10BASE-T1L will provide new insights from previously unconnected devices in remote locations and enable automation engineers to transform their commissioning and upgrade work practices," Treacy stated. "In conjunction with new analytics software these new data streams will enable the extraction of actionable information and inform control engineers decision making. It will help drive changes in maintenance routines, scheduled downtime planning and moving toward more active predictive maintenance approaches."

Impact of the IIoT

The benefit of IIoT and the Smart factory are clear for all to see, however the reality of retrofitting existing facilities to avail of the benefits and upgrading connectivity networks takes time and requires an outlay of capital. Undoubtable there are pocket of industries and segments of factories that are making great strides toward the realization of the vision.

Treacy said that having a clear goal around the data and information required and how it will be leveraged to drive output will help business owners grapple with the cost benefit analysis and enable clear ROIs to be realized in the long run. As 2021 unfolds we are likely to see more proven use cases come to attention which will help crystalize the benefits and opportunities gained from those who invested early in lifecycle.

"In 2021, I am excited to see the launch of the first 10BASE-T1L enabled field instruments and field switch devices. These foundational products will be the first step toward a network of 10BASE-T1L connected instruments across process facilities worldwide and will bring the benefits of increase data, power, and IP addressability to life," Treacy said.

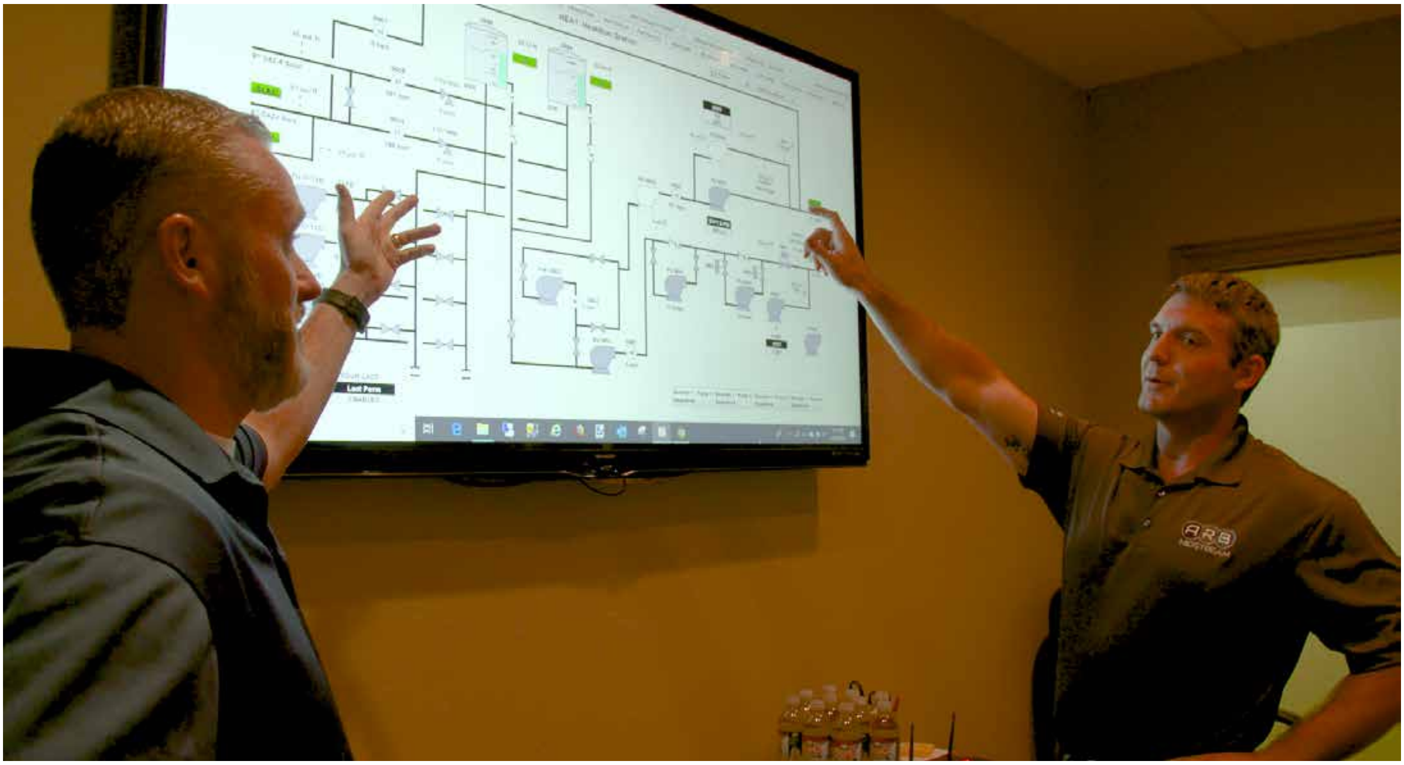
She added that the roll out of some TSN enabled automation equipment prototypes at the controller level will enable the use cases with existing Industrial Ethernet Protocols to be firmly tested.

"Finally, we need to enable the transition from existing legacy analog communications to Ethernet technology. For this reason, we expect to see the roll out of software configurable I/O devices which can be configured as needed to meet the deployment use case in retrofitting projects. This will support a hybrid deployment of both Ethernet and legacy analog and provide flexibility to enterprise to leverage existing investments while upgrade segments of facilities in a phased approach," she added.

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

SCADA pipeline system from edge-to-cloud in record time

ARB Midstream built a complete SCADA system for an oil pipeline with 37 sites in just six months. The resulting system uses cloud computing, a local OPC UA server with the ability to leverage multiple protocols and an architecture that set a new standard for future SCADA projects.



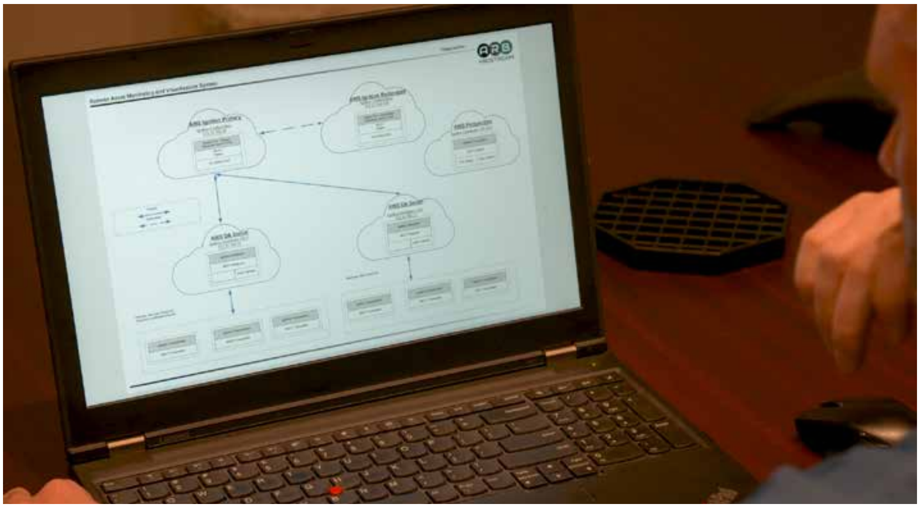
SOURCE: INDUCTIVE AUTOMATION

The overlay network uses the 172 IP address range on top of the SD-WAN's IPv6, creating a large pool of IP addresses that won't conflict with each other.

HOW ABOUT THIS FOR A DAUNTING TASK? In six months, build a complete SCADA system for an oil pipeline with 37 sites—while also doing hardware upgrades, creating a new network, and building a control room from scratch.

It was a big challenge for ARB Midstream, but with help from system integrator Industrial Networking Solutions (INS) and the right blend of technologies, the project was successful despite the tight schedule.

ARB Midstream, based in Denver, is a growth-oriented company that provides midstream and marketing solutions for crude oil, refined products, and liquefied petroleum gas. INS is a system integrator based in Richardson, Texas.



SOURCE: INDUCTIVE AUTOMATION

ARB Midstream and Industrial Networking Solutions collaborated on an ambitious, cutting-edge project.

When ARB purchased a crude oil pipeline system in Texas and Oklahoma, the agreement called for ARB to begin operating the pipeline in six months. The system includes more than 900 miles of active pipeline, and 950,000 barrels of storage.

"We wanted cloud computing," said Jerod Blocker, operational technology manager for ARB Midstream. "We didn't want to build a traditional infrastructure. We chose to spend money on the software and on the edge compute. And we wanted a local OPC UA server with the ability to leverage multiple protocols."

INS believes the architecture for this project sets a standard for future SCADA projects in the industrial space.

The software-defined wide-area network (SD-WAN) connects networks over large geographic distances. INS also delivered a cloud-hosted SCADA solution with management, visibility, control, reporting, edge computing, MQTT, and store-and-forward capabilities.

Best of the Best

"This application uses best-in-class vendors," said Mo Moore, manager of software services for INS. “We have Ignition by Inductive Automation for HMI/SCADA, Cradlepoint for cellular communications and software-defined networking, Moxa industrial computers, Cirrus Link Solutions for MQTT, Ignition Edge, and Amazon Web Services for cloud-hosted services with redundancy."

In addition to the tight timeline, some key hurdles to clear were wetter-than-usual weather, and less-than-thorough documentation provided by the selling company. Work progressed, however, and all sites were being operated by ARB by one day prior to the six-month deadline.

"ARB approached us to look at replacing some older VSAT equipment and maybe even some older cellular equipment at some of their remote locations," said Dave Brewington, services manager for INS. “We also needed a secure, reliable, and scalable network that would allow ARB to grow. Cradlepoint’s NetCloud Perimeter allowed us to create an abstracted overlay network built on cellular technology. That allowed us to have fully secure and encrypted end-to-end communications between remote assets and the cloud.”

The overlay network uses the 172 IP address range on top of the SD-WAN’s IPv6, creating a large pool of IP addresses that won’t conflict with each other. It simplifies network management and eliminates the need to memorize all the local IP addresses. The new network is also carrier-agnostic, enabling it to use a mixture of copper, fiber, cellular, and satellite for connectivity. The system chooses the best connection in each situation.

SOURCE: INDUCTIVE AUTOMATION

ARB chose to follow API standards for SCADA security, HMI displays, and alarm management.

MQTT technology

Both ARB and INS were impressed with the performance of the MQTT technology. “The retirement of the VSAT solutions and going to the MQTT model over cellular was a much better approach,” said Moore. “It really helped ARB implement a secure, robust, cost-effective, and scalable infrastructure.”

MQTT uses little bandwidth, and it reports by exception, which can be a big improvement over traditional polling. “On the first day, we saw a 35-percent difference in data-plane utilization, because we weren’t sending up tags that we didn’t need to send up,” said Moore.

On this project, a weak cellular network meant that even basic communications were having trouble getting through. But the data from MQTT seamlessly made it all the way up, very quickly. “With

Cirrus Link’s MQTT setup, the lightweight protocol to get the data to the cloud, or to your control center, is amazing. It really is a huge, huge benefit,” said Moore.

SOURCE: INDUCTIVE AUTOMATION

The design team created a new network that is carrier-agnostic, enabling it to use a mixture of copper, fiber, cellular, and satellite for connectivity.

Creating the operations control center was another big test for the two companies. But they pulled it off, and ARB is very happy with the result.

“One thing I really love about this system is that we started this control center from scratch—and we built it and had it operational in three and a half months, which is pretty incredible,” said Tom Charboneau, control center manager for ARB.

Fast development

ARB’s screens use high-performance graphics, and Ignition templates were used to speed up development. ARB chose to follow American Petroleum Institute standards for SCADA security, HMI displays, and alarm management. By committing to that early in the process, ARB helped itself and INS to quickly agree on color schema, graphics, and the approach to alarming.

With Ignition’s unlimited licensing, there were no extra costs for increasing the number of tags, users, or devices. That was a big factor in ARB choosing Ignition — along with the many features within it.

ARB now has a secure, robust, and reliable system that will allow the company to acquire more assets in the future and easily integrate those assets into the existing system. And ARB and INS can feel good about beating the huge time crunch. “With all these technologies, we were able to make the deadline,” said Blocker. He also praised the commitment of INS, and the power of Ignition. “It seems to me, the technology capabilities of Ignition are limitless,” he said.

Industrial Networking Solutions distributes products, offers technical support, and provides IT services for wired and wireless machine networking applications.

Application report by ***Inductive Automation.***

View Video

Optimal network solutions for automotive manufacturing

The automotive industry has continually pioneered new manufacturing and assembly processes, driving the adoption of key innovative technologies on the factory floor. To enhance their competitiveness, companies need interconnected and flexible production systems that can decrease cycle times while increasing quality.

INDUSTRIAL COMMUNICATION TECHNOLOGIES play a key role in the successful implementation of complete solutions for data/information integration. The automotive sector is often an early adopter of innovative technologies and as a result it is one of the most automated manufacturing industries in the world. It is the main driver and largest segment of the industrial robotics industry, and for 34% of over 2.7 million robot installations worldwide.

The use of advanced automated systems allows businesses in the sector to maintain low cycle times that support high-volume, fast turnaround production with improved quality. For example, thanks to technology, it takes 13 to 35 hours to turn raw materials into a car that comprises tens of thousands of parts. Key applications that car makers currently automate include welding, injection moulding, painting and surface coating, glue dispensing, assembly and inspection.

Similarly, automotive manufacturers can support large-scale mixed model production programs in their assembly. As a result, businesses can effectively use a single production line to deliver different vehicle models with a high degree of customisation.

Smarter, better, faster

As new, promising digital technologies emerge and develop, they are often adopted by automotive manufacturers to optimise various aspects of production. Currently, one of the most common ambitions among manufacturers is the creation of flexible systems that can autonomously run entire production processes, self-optimise their performance across a broader network and adapt to varying conditions in real or near-real time.

Even following this trend, the automotive sector is ahead of the curve, with 30% of factories in the industry already converted to smart factories and a further 44% expected within the next five years. This results in over 70% of vehicle manufacturers currently involved in this initiative.

At the heart of Connected Industry applications are large volumes of data, which are generated, shared and analysed in order to offer a unique insight into machines, processes and facilities as well as supporting automated closed-loop feedback control. Therefore, the implementation of a highly advanced networking technology to connect multiple parties and share information is paramount to set up intelligent, interconnected plants.

SOURCE: CLPA

The automotive sector is an early adopter of innovative technologies among manufacturing industries.

When implementing automated systems, businesses require a high-performance, secure and reliable networking technology in order to get the necessary data from factory floor devices, which are otherwise disconnected, to set up Industry 4.0 applications.

Key needs of connected industries

The automation specialist needs to select and use automation devices that leverage a state-of-the-art industrial communication technology that can support the real functionalities of data-driven applications.

Key elements that automation specialists should include in their products are interconnectivity and the use of a network solution that features sufficient and well-utilised bandwidth as well as the ability to support the convergence of information technology (IT) and operational technology (OT).

The first aspect enables automation products to communicate and interact with other devices within an enterprise, e.g. supporting effective field-level communications. Optimal level and allocation of network bandwidth, on the other hand, allows automation devices within a network to effectively handle the ever-increasing traffic of data generated by smart machines while minimising latency and jitter during transfer.

Toyota's plant in Wałbrzych, Poland, the company's biggest engine and transmission manufacturing operation in Europe, was able to increase the availability of its production lines and improve the transparency of data by selecting a network technology with these features. In particular, the chosen solution, CC-Link IE open industrial gigabit Ethernet, ensured the necessary level of performance was met thanks to its large bandwidth, and its openness allowed it to seamlessly integrate multiple devices from a range of vendors.

Maximum network performance

The latest evolution of CC-Link IE, CC-Link IE TSN, further enhances the network's capabilities, and allows manufacturers of automation products to address current and future needs. The technology is an open industrial Ethernet technology that combines 1 gigabit/second bandwidth and Time-Sensitive Networking (TSN).

By selecting it for their products, device makers can leverage a widely adopted technology with the highest bandwidth currently available as well as TSN features to support IT/OT convergence.

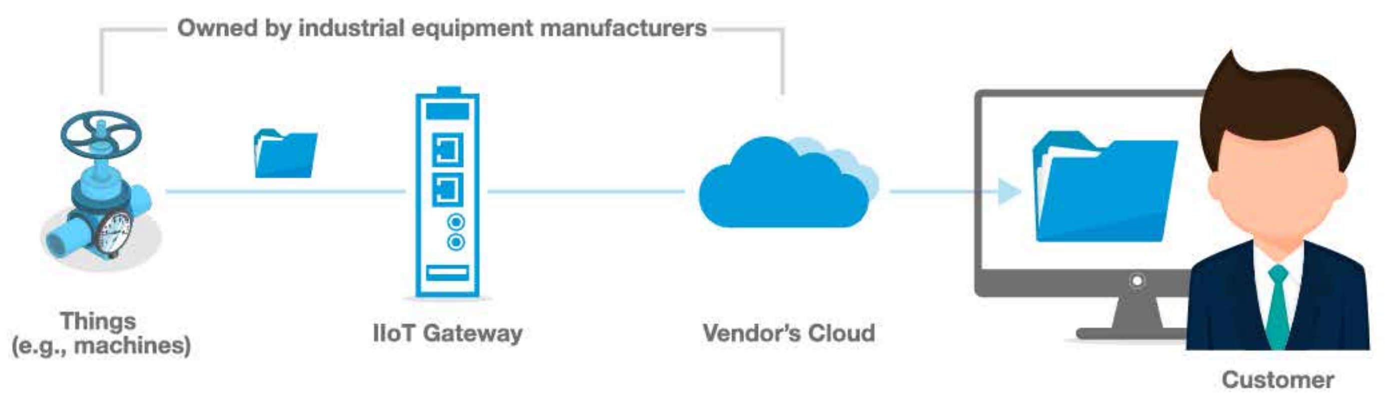
Automotive plants that use CC-Link IE TSN compatible automation devices can therefore fully realise smart, interconnected factories, reaching the next level in productivity and performance. In particular, businesses will be able to further reduce their cycle times and production costs and increase flexibility to deliver vehicles with a high degree of customisation and quality.

John Browett, General Manager at ***CLPA Europe.***

View CC Link TSN Video

Deciding if open or proprietary IIoT solutions are right for you

The IIoT has become a key technology for the success of most businesses. Find out what's the best solution for machine-to-cloud connectivity. One question is "What can I buy?" versus "What do I have to build by myself?" Available solutions for open architectures have expanded rapidly over the last 12 months.



SOURCE: MOXA

A proprietary IIoT connectivity solution.

THE EMERGENCE OF THE INDUSTRIAL INTERNET of Things (IIoT) has changed the way the Operational Technology (OT) world uses data. In the past, data was simply collected for monitoring purposes to ensure production goes according to schedule. Now, data can go beyond a mere stream of information.

Through analysis, data not only can help optimize products and services, but can also significantly improve operational efficiency, increase profits, and create new business models that previously were not possible. The vast business opportunities presented by data have made the IIoT a key technology for the future success of nearly all businesses.

The benefits presented by this shift have triggered a demand for machines that cater to data acquisition and analysis, anywhere and everywhere possible. Previously, companies valued only production data, which monitors the productivity of machines or assets to ensure smooth operations.

Nowadays, along with production data, machine condition data is just as crucial. Enterprises depend heavily on the predictive analysis of real-time operational data to prevent potential failures in order to reduce maintenance cost and the risk of other possible damages. Furthermore, industrial equipment manufacturers can use the historical data of machines to provide customers with more accurate and faster maintenance services to reduce personnel costs. Lastly, this data can be used to optimize a machine's operation based on environmental and business objectives that require dynamic updates and changes as opposed to the historical "set-and-forget-it" mentality.

Despite the considerable benefits of big data, the advancement of the IIoT in the industrial space is still slow. The hindering factors are multiple: the variety of edge protocols, non-standardized data, connectivity to the cloud, cybersecurity, the management of large-scale systems, to name a few.

Two most common IIoT solutions

In the early days of the IIoT (as recent as two or three years ago), industrial equipment manufacturers' answer to this complex and challenging problem was to provide a turnkey IIoT solution. The customer only needed to pay for this service or feature, and the equipment vendor would take care of the rest.

As time went on, customers found themselves stuck with multiple IIoT solutions from different vendors on different platforms, with little to no interoperability. What's more, they were missing the big picture that all of their collected information supposedly was to reveal. Everything was in silos from different vendors.As customers came to grips with this challenge, market demand called for open architectures that offered customers the option to take charge of and maintain their own IIoT strategy, allowing them to talk to any device in any location.

However, the issue remains complex with regard to the investment and capabilities required to pull this off at scale. Most customers, even those with will well-intended and well-funded solutions, face tremendous challenges building such a type of solution.

Let's take a closer look at the two common connectivity methods: proprietary IIoT connectivity solutions that offer an easy and managed approach but with constraints on flexibility, openness, and data ownership, and open IIoT connectivity solutions that focus on the cross-systematic integration of any device and the end customer's ownership of the solution.

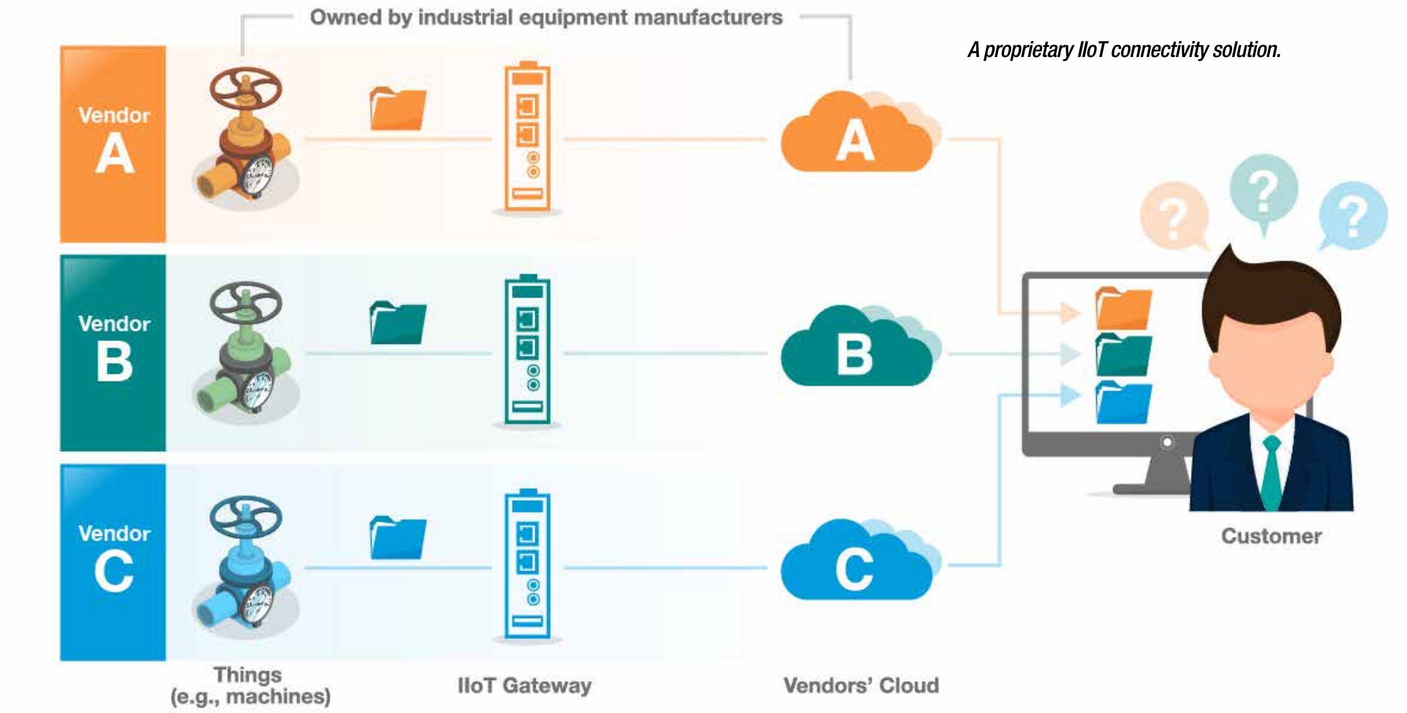
Proprietary IIoT connectivity

A number of industrial equipment manufacturers saw the value that came with data analytics, and began to provide customers with their own IIoT connectivity solution. To leverage the wealth of data, IIoT gateways are installed in front of or embedded in the "thing", and data regarding the status of the "thing" will be transmitted from the machine to the machine vendor's cloud.

This user-friendly turnkey solution allows customers to quickly capture, manage, visualize, and analyze the data collected from these devices on a cloud-based platform. This system is fairly intuitive for users as they only need to log into the machine vendor's cloud to access their data. It further reduces a customer's workload by placing the burden of developing and deploying the system solely on the industrial equipment manufacturer, and lowering overall IT costs for the customer.

A few industrial equipment manufacturers also began to provide data analysis services on top of the data collection offering to help customers better understand their machines' behavior. This offering is favored by customers with specific application needs, such as monitoring the operations of remote equipment.

In the case of the oil and gas industry, punctual operation of remote devices



A proprietary IIoT connectivity solution.

SOURCE: MOXA

(pumps, control valves, compressors, etc.) is top priority. This prompted equipment manufacturers such as Baker Hughes, Emerson, Schlumberger to start using AI to perform real-time analysis of data, such as pump pressure, flow, temperature, etc.

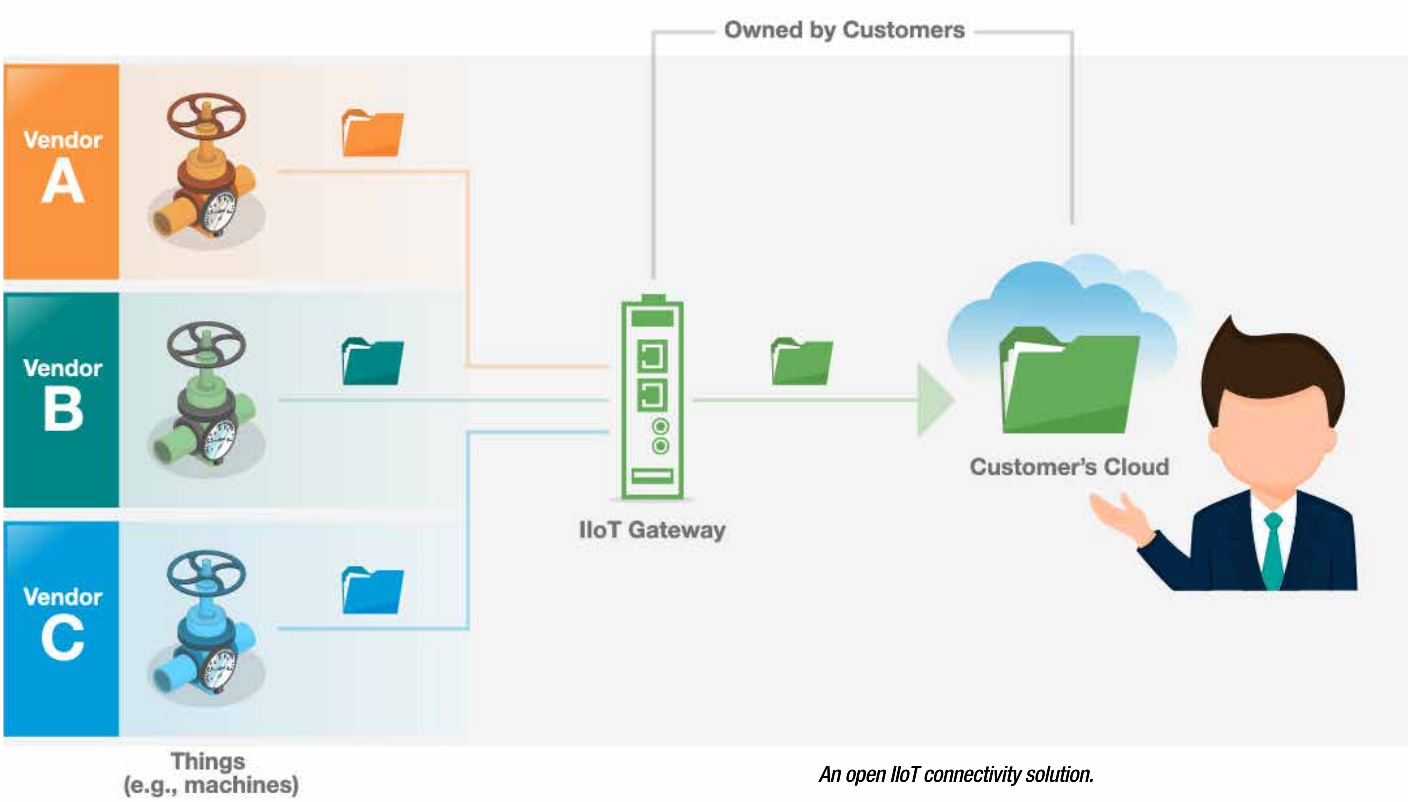
Coupling this data with past benchmarks, they can promptly adjust the equipment parameters to keep them operating normally with minimal human intervention. Thus, proprietary IIoT connectivity solutions' hassle-free deployment and easy-to-use features have made them very popular among customers.

Hassle-free, but at what cost?

This easy-to-deploy solution's homogeneous nature means that its service is limited to the industrial equipment manufacturers' own devices. However, in reality, a medium-sized enterprise usually has equipment and assets from multiple vendors, in multiple locations, spanning many different applications.

This complex, heterogeneous environment often requires the enterprise to use a different solution for each system provided by a different industrial equipment manufacturer. This could quickly result in extra financial investments, not to mention the possible obstacles arising from the isolated information systems that cannot speak to each other.

- *Inflexible Integration:* Within closed IIoT solutions, the data is sent to different platforms, with each using different protocols and different formats, creating a colossal effort at the backend to merge the data.



An open IIoT connectivity solution.

- *Lack of Data Ownership:* Since the customer's machine data is stored on a private platform built by the industrial equipment manufacturer, data ownership becomes an issue. If the data is stored in a system owned by the builder, does it still belong to the customer?

Furthermore, if a customer chooses to switch platforms one day, the risk of incomplete data transportation—if not all together impossible—is huge. This could potentially cause the historical data and past experiences accumulated by the customer to be lost. All of this, coupled with the risk of a data leak, point out a glaring obstacle in the solution.

Is Openness the Answer?

As data starts to play a more significant role in a business' core success, its ownership, availability from all "things" (not just some), and the flexibility of integration are the main considerations when choosing solutions.

In open IIoT architectures, equipment manufacturers open APIs or use open or standard-based protocols to help customers obtain the data by themselves. Contrarily, sometimes customers build their own solutions by connecting individual front-end equipment from different manufacturers to a highly integrated IIoT gateway.

The different data formats from the different manufacturers are unified by the IIoT gateway, thus significantly reducing the integration difficulties when data is subsequently transmitted to the cloud. In addition, the process no longer requires the data to be passed through a third-party's platform, making it more secure.

Take the oil and gas industry as an example. Oil production and real-time oil prices are closely linked, which means transparency in the production line can make or break the profit margin.

In order to gain real-time data from exploration, development, and production to final transportation, oil companies partnered to create an open platform. This called for the industrial equipment manufacturers in the supply chain to work as a team by sharing their equipment, production, or environmental data for the efficient production of an oil field.

Now, the question quickly becomes "What can I buy?" versus "What do I have to build by myself?" The commercial available solutions today for open architectures have expanded rapidly over the last 12 months. Various software components are now available:

- Cloud Edge Software such as AWS IoT Greengrass/Azure IoT Edge to extend cloud infrastructure to the edge
- SCADA Edge Software such as Ignition Edge/AVEVA Edge IoT View to interface a vast variety of industrial edge protocols
- Infrastructure service offerings to extend security, networking, and management to the edge such as ZEDEDA, OpenVPN, and TOSIBOX Lock for Container
- ML/AI edge solutions for edge processing before pushing back to the cloud

Most importantly, don't forget to choose a powerful yet reliable IIoT gateway at the core, which not only can run the above software components, but also has the ability to connect to the cloud (e.g., LTE, Wi-Fi, existing WAN) and edge (e.g., I/O, Ethernet, USB, Serial, other).

Conclusion: proprietary or open?

For companies that want to deploy a quick IIoT solution for a singular vendor's, "thing" to obtain data and reap the benefits of the IIoT, an easy-to-deploy, proprietary IIoT connectivity solution is the more rewarding choice.

For companies that require IIoT data on a larger scale, are interfacing many different "things", and are looking for a more personalized fit with full data ownership, an open IIoT connectivity solution would be able to deliver the necessary optimization.

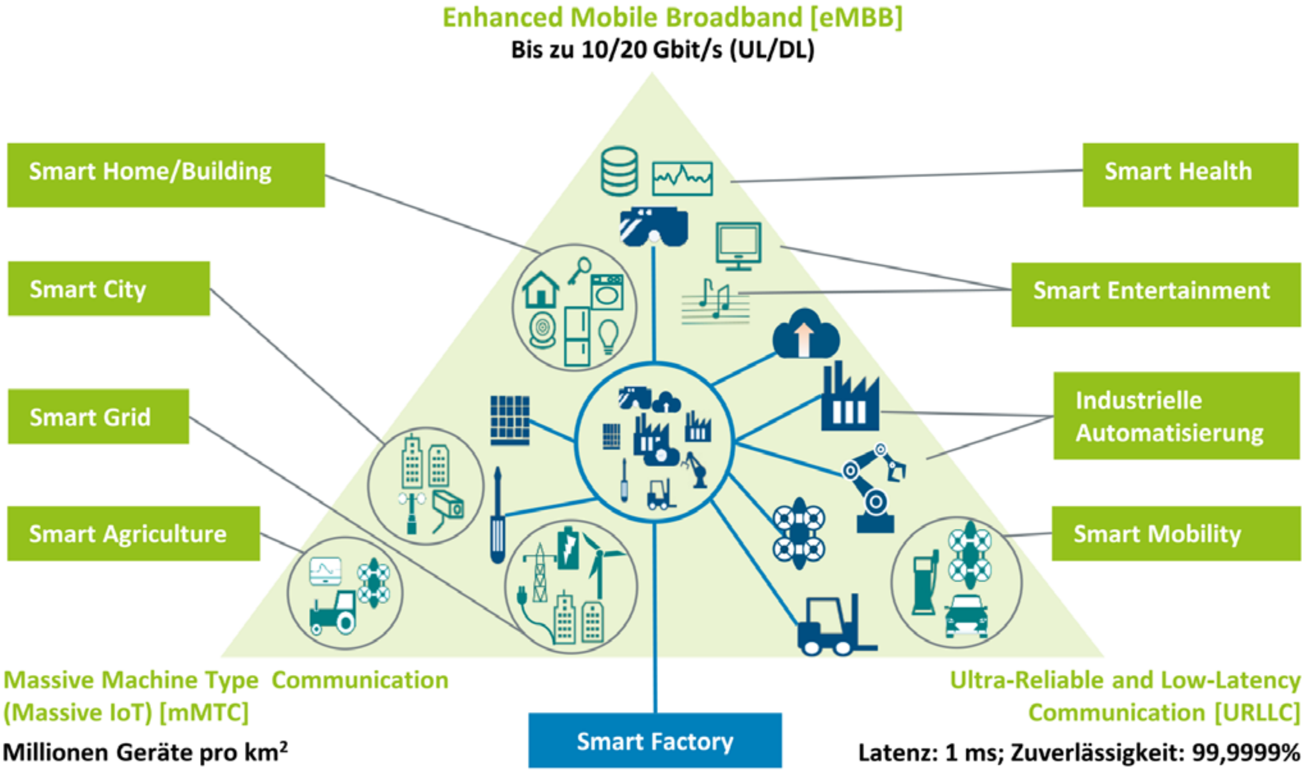
As the IIoT evolves, off-the-shelf software and cloud products, without a doubt, will continue to provide easier and highly scalable products to build open IIoT solutions. Proprietary IIoT solutions are also having to adapt quickly to provide more open API's and cloud-to-cloud integration, as well as solutions for customers to access their data more easily.

Technology report by ***Moxa Corporation.***

Visit Website

5g on test bench for industry: what's possible in the future?

5G and other wireless technologies represent an ideal supplement to wired communication solutions, each with its own specific advantages and disadvantages. 5G will change a lot, but it will not change everything. The mobility of communication subscribers in industrial applications is definitely being advanced.


Enhanced Mobile Broadband [eMBB]
Bis zu 10/20 Gbit/s (UL/DL)
Smart Home/Building
Smart City
Smart Grid
Smart Agriculture
Smart Health
Smart Entertainment
Industrielle Automatisierung
Smart Mobility
Massive Machine Type Communication (Massive IoT) [mMTC]
Millionen Geräte pro km²
Smart Factory
Ultra-Reliable and Low-Latency Communication [URLLC]
Latenz: 1 ms; Zuverlässigkeit: 99,9999%

SOURCE: VDMA

THE GERMAN ENGINEERING INDUSTRY Association (VDMA) recently published its report "5G in mechanical and plant engineering - Guidelines for integrating 5G into products and production". Connection experts from LAPP were heavily involved in two of the applications.

The aim was to provide mechanical and plant engineers with a practical idea of potential applications and the challenges of introducing 5G in production.

You are undoubtedly already familiar with claims that 5G will revolutionise mobile communications, and not only in terms of public mobile networks. To date, the use of such technologies for wireless communication in industry, and particularly in the automation environment, was inconceivable due to a lack of network coverage, real time capability and guaranteed bandwidth. But 5G is different.

Anticipating 5G impact

It could actually turn out to be an interesting technology for industry. There are several reasons for this. Low latency values of up to 1ms promise real time capability, the basis for automated, fast-moving production processes.

Increased reliability and availability of the network, improved localisation functions, connection of up to 1 million terminal devices per km² with peak data rates of up to 10/20 Gbit in the up/down link and, last but not least, centrally controlled allocation of licensed frequencies for industry.

Therefore, protected and secure networks could be set up on company premises with 5G. Users could efficiently connect Industrial Ethernet, TSN and 5G. This would bring the worlds of OT and IT increasingly close together.

Mobile phone operators would suddenly be sitting around the table with machine manufacturers. 5G is currently still at the beginning of its market launch, with the construction of public networks.

Initial developments for industrial devices have also begun. The functions that will be of interest for real time critical industrial applications are still a way away. It can be expected that improvements in latency will extend the range of applications in the coming years.

New options: wireless in industry

Wireless technology has been used in industry for a long time. Wifi and Bluetooth are already used as standard for applications such as hand-held scanners or driverless transport systems (AGVs).

In specific cases, wireless is also used for real time critical applications for transmission of field buses and control data via wireless connections. The objectives that users hope to achieve through the use of wireless systems are varied. In moving applications in machines, where cables are worn by constant movement, wireless data transmission can reduce this wear. Wireless technology is also a problem solver in mobile applications where cables restrict mobility.

In other applications in the production environment, wireless systems have only achieved a limited foothold to date. This is due largely to the fact that the advantages of wireless are not enough to justify its use to meet the requirements of industry, as industrial production processes depend on control data in real time. However, with existing wireless technologies it has only been possible to reliably transmit real time data for PLC control signals for relatively slow running processes. But 5G is now providing mechanisms designed to increase the reliability of connections and raise the prospect of 5G becoming a wireless technology for more industrial applications.

Potential 5G benefits

The 5G function MMIMO (Massive Multiple In Multiple Out) is a good example. MMIMO means that significantly more antennas are used than previously (UMTS/LTE). This technology also allows what is known as beam forming. Subscriber devices can find the strongest out of several signals. This ensures better coverage and thus greater connection stability.

At the same time, more subscribers are possible with lower energy consumption and, if necessary, higher bandwidth. With 5G we are seeing the introduction of TSN (Time Sensitive Network) as a real time protocol. TSN, which has been discussed for a long time for industrial networks, should give 5G real time capability. The final expansion of 5G will thus see possible communication cycles of <1 millisecond. Compared to wireless technologies today, much more dynamic processes would be controllable wirelessly.

Other important criteria for use in production include simplicity and ease of maintenance. Automation specialists are usually not IT specialists, and reliable operation of a Wifi network already poses some enormous challenges for them. As a rule, it needs to be possible for maintenance to remedy machine communication errors without long production downtimes, for example, during night shifts and without in-depth IT knowledge. Wireless technology has to be as easy as the equivalent cable networks. Currently, a defective cable or switch can be replaced quickly and easily without expert electrical knowledge.

Contributing to VDMA 5G guidelines

For some time, LAPP has been devoting a lot of energy to the issue of 5G and is now very confident that there cannot be wireless without cables. LAPP sees 5G as a supplement to its solutions and not as a threat. This is why the company was happy to support the VDMA in creating its practical guidelines.

In the recent publication, the effective benefits are evaluated from a mechanical and plant engineering perspective by looking at a number of different applications. LAPP had a seat at the table alongside users and manufacturers. The partners were supported by the Fraunhofer IIS, which contributed neutral technological knowledge and methodology, collected applications from the panel and ascertained the relevant capabilities of 5G.

LAPP helped design two applications and sat down with competitors to openly discuss the opportunities presented by 5G. The results indicate that while many applications can be implemented with 5G, it is not essential, as demonstrated by existing solutions from LAPP and other manufacturers in the field of Predictive Maintenance. For other applications, the forthcoming 5G releases 16 and 17 will have to show whether 5G really does offer sufficient real time capability.

5G in mechanical engineering

A total of ten different applications from the industrial environment were described in the VDMA 5G guidelines. Lapp was involved in the "real time capable data paths in applications subject to wear" and "M2M / remote IO with field bus" applications. However, it is the "driverless transport systems (AGV)" application that is of particular interest in terms of using 5G.

Driverless AGVs

The guidelines show that driverless transport systems (AGVs) are one of the most suitable applications for 5G. On one hand, necessary latency figures are in a range that is achievable with 5G. On the other hand, 5G is likely to allow a shorter roaming time than today's Wifi. The roaming time is the time required to transfer a subscriber from one access point to the next. If it is too long, the AGV stops. With Wifi connections, this can take 30-50 ms. The use of 5G cuts these times considerably, as there is no need to log in and out.

Another positive effect: With 5G, considerably shorter latency (delay time for transfer of data packets) is possible than with WiFi. This also ensures fault-free operation of an AGV. Another feature is the 5G localisation function, where the target is 20 metres in Release 15 and just 3 metres in Release 16. It can be assumed that subsequent releases will bring further improvement in accuracy, making use for AGVs increasingly interesting.

Industrial Ethernet applications

Another possible application is in transmission of an Ethernet-based fieldbus, such as PROFINET via 5G. Wireless technology could be integrated directly in a decentralised IO system (= remote IO). This would allow connection and transmission of multiple sensors or actuators. In moving applications where fieldbus cables wear in cable chains or robots, signals could be transmitted wirelessly with zero wear. With Release 15, the possible latency of 5ms would be sufficient for this purpose. But not for fast control of servo drives.

Lapp position on 5G

Whether or not the wireless factory is a utopian ideal will become apparent in the coming decades. LAPP is well aware of the effects of 5G on future networking and data communication and is preparing for it.

LAPP is excited not only by changes in data communication in the automation environment, directly in machines and plants, but also by the necessary expansion of infrastructure in individual countries and in factories, what are known as the backbones. More glass fibres, more copper cables and new antenna masts and access points.

The future infrastructure for 5G in cities and communities will need to be wired. The desired freedom of movement in factories thanks to wireless solutions will be made possible by cables, as the access points in the halls continue to depend on them.

LAPP is convinced 5G and all other wireless technologies that exist represent an ideal supplement to wired communication solutions, each with its own specific advantages and disadvantages. 5G will change a lot, but it will not change everything. The mobility of communication subscribers in industrial applications is definitely being advanced.

Industrial wireless solutions

LAPP is working on industrial wireless solutions that tap into the synergy between wired and wireless networks. One example is the IoTKey® system from LAPP, a system that can transfer completely wireless sensor data to the cloud. IoTKey® consists of 3 core components: LoRa transmitter, GSM gateway and IoTKey Cloud Portal. The key here is to combine multiple wireless technologies and to use respective benefits. LoRa is a particularly energy-saving wireless system for transmitting sensor data.

It allows fully autonomous battery operation for up to several years without replacing the battery. The gateway itself transmits the LoRa sensor data to the GSM mobile network. This makes it possible to use the system at any location with a mobile phone signal. Porting the IoTKey system to 5G could expand the range of future applications.

The combination of TSN with 5G is also exciting. In terms of its ETHERLINE ACCESS Industrial Ethernet switch portfolio, LAPP sees TNS as an important future technology. TSN over 5G would lead to consistent real time communication between wired and wireless networks. But development also continues in the field of cable-based transmission.

Single pair Ethernet is in the starting blocks. This new technology will enable Ethernet to be transmitted via just two copper cores instead of 4 or 8 cores as was previously the case. This further improves cost-effectiveness at the lower field level. And this is what 5G ultimately has to measure up to.

LAPP will keep a close eye on the development of 5G and fully investigate its potential for use in other relevant applications.

*Dr. Susanne Krichel, Senior Manager - Business Development IoT and Ralf Moebus, Head of Product Management Automation, **LAPP.***

Visit Website

Secure remote access via public 5G networks

It is only a matter of time until 5G will establish itself in industry. The flexibility of 5G with its different implementation approaches, private and/or public, makes this standard the most versatile mobile communications solution for industry, and solutions previously not feasible are now within reach.

SOURCE: SIEMENS

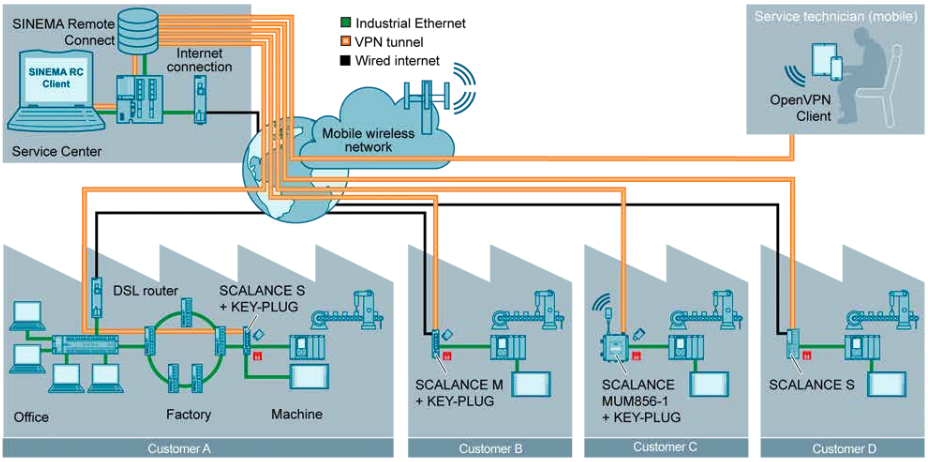
The main benefits of 5G are higher bandwidth, greater reliability, lower latency, and lower power consumption.

SINCE THE 1970s, MOBILE WIRELESS NETWORKS have enjoyed enormous gains in performance with each new generation that has been introduced. The 5th generation of the mobile communications standard (5G) is currently being rolled out. The main benefits of 5G are higher bandwidth, greater reliability, lower latency, and lower power consumption.

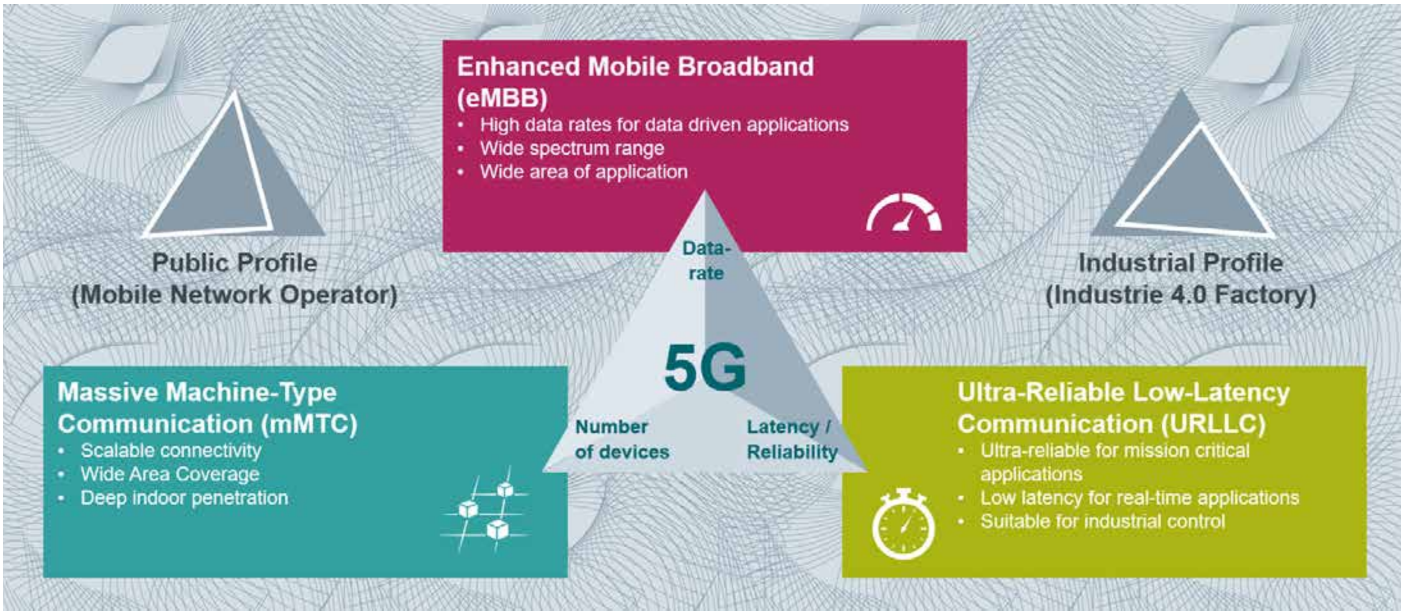
Industrial 5G

This new technology seems predestined for use in industrial applications. Their requirements for wireless networks are different from the ones for public, commercial mobile phone networks. Industrial private 5G networks are the key to success here. But for applications requiring remote access to distant machinery or equipment, a public 5G network is indeed the right answer.

With 5G, a new mobile communications standard was developed for the first time which took into consideration industrial use cases – and it is already being deployed. 5G brings three main scenarios: enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC). These scenarios serve different application areas: eMBB is bandwidth-oriented and URLLC supports the requirements of industrial IoT applications such as low latency with best possible reliability. MMTC is used for applications which require low power consumption and contain a large number



Remote maintenance of standard production machines at different end customers with SINEMA Remote Connect.


Enhanced Mobile Broadband (eMBB)
• High data rates for data driven applications
• Wide spectrum range
• Wide area of application
Public Profile (Mobile Network Operator)
Industrial Profile (Industrie 4.0 Factory)
Data-rate
5G
Number of devices
Latency / Reliability
Massive Machine-Type Communication (mMTC)
• Scalable connectivity
• Wide Area Coverage
• Deep indoor penetration
Ultra-Reliable Low-Latency Communication (URLLC)
• Ultra-reliable for mission critical applications
• Low latency for real-time applications
• Suitable for industrial control

The three main 5G scenarios.

of connected devices. However, the full implementation of these three main scenarios is not possible simultaneously within the same network. A network can only be designed and configured in such a way to fully support one scenario. For example, it can offer either the highest possible data rate or the lowest possible latency. Both at the same time are not possible.

This is where the necessity of different implementation approaches for 5G networks comes into play. A public 5G network is typically set up to provide high bandwidths for video telephony, video streaming, and other data-intensive applications. High bandwidth is a key argument advertised by mobile providers who are already introducing 5G in a number of countries around the world.

However, for the majority of applications in a factory, bandwidth plays a minor role. The emphasis here is mainly on reliability and ultra-short latencies when it comes to communications. Therefore, private networks are an integral part of the 5G standard.

They enable companies to establish their own local 5G networks and adapt them to their mission-critical applications. For this purpose, the German Federal Network Agency (Bundesnetzagentur) has reserved part of the frequency spectrum for use in private, local 5G networks. This spectrum can be obtained for the setup of local campus networks for a reasonable fee.

Wireless connectivity

In addition to requiring local wireless connectivity, the industry is also increasingly demanding remote access to distant machinery and equipment, e.g., for remote maintenance. In those applications, communication usually takes place over great distances.

Public mobile networks enable access to distant participants, even in other countries. Moreover, service technicians can connect to the machinery to be serviced via mobile communications while en route.

Public 5G networks

Public 5G networks are an important pillar for remote access and remote maintenance solutions. The advantage of 5G lies in the flexibility of the technology, which is an integral part of the standard. For example, very high bandwidths can be made available to users in urban areas through small radio cells and high frequencies.

In rural areas, radio cells have to cover a larger area which is why lower frequencies are used and the available bandwidth is divided among more users. Particularly at the edges of radio cells, massive losses in bandwidth and stability of the communication connection can be expected using, e.g., LTE or UMTS. However, it is precisely in these remote locations where a stable broadband transmission is required for remote maintenance or video streams, e.g., of water stations.

With the innovative wireless technologies of 5G, significantly more bandwidth with higher reliability is made available at the edges of the radio cells, and the average data rate for users within a radio cell also increases.

By increasing coverage and bandwidth, 5G networks make it possible to run data-intensive applications even at the edges of radio cells, which would have been difficult to do with previous mobile wireless networks – for example, the reliable and stable transmission of large amounts of data for firmware updates. This saves on-site service calls. To make the connection of the remote stations easier, so-called rendezvous servers are used.

SINEMA Remote Connect

Our management platform for VPN connections, SINEMA Remote Connect, is such a solution. It enables convenient and secure access to remote machinery or equipment – even if they are integrated into other networks. The server application enables an easy management of VPN tunnel connections between control center, service technicians, and remotely installed machinery or equipment.

The rendezvous server solution offers the user a high degree of flexibility and security. The user can choose whether the system is to be hosted locally or on the Internet and which machines or which section of the plant are accessible to service technicians.

In addition, a central user management with optional Active Directory connection, a suite of directory-based identity-related services, facilitates the management of rights. In combination with the high bandwidths, the stability of 5G networks, and the simplicity of rendezvous server solutions, a reliable and stable remote access via mobile communications can be realized even in distant areas.

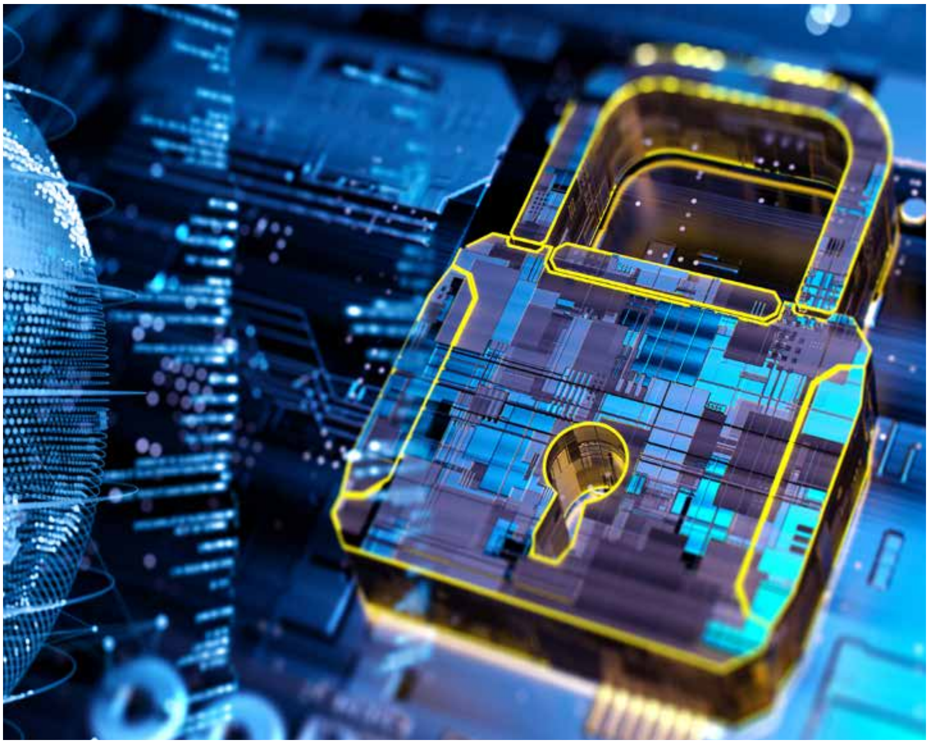
No matter where the journey goes – it is only a matter of time until 5G will establish itself in industry. The flexibility of 5G with its different implementation approaches – private and/or public – makes this standard the most versatile mobile communications solution for the industry. Solutions previously not feasible are now within reach, and applications no one dared to think about may be realized in the near future.

Sander Rotmensen, Head of Industrial Wireless Communication Products, ***Siemens.***

Visit Website

Your factory could be the next target for a cyber attack

The need for edge computing means more connected devices that interact with the real-world based on the data they receive. As computing power becomes pervasive, so does the need for security to address increased cyber risk. Only relying on firewalls is no longer effective with converged IT and OT networks.



As the cyber attack surface continues to shift, there is an increasing need for security solutions at the edge of the network.

YOU ARE HEAD OF A LEADING MANUFACTURER in charge of North American operations working through a normal day when suddenly you get a report from one of your largest factories that shows a list of product defects.

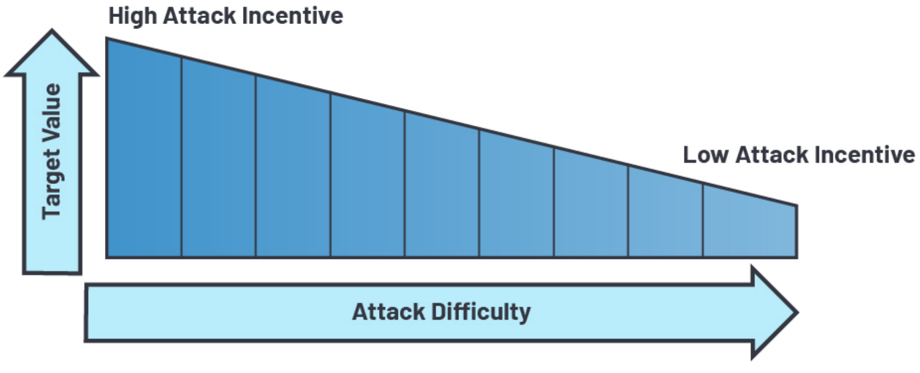
The trend appears to have started some time ago and keeps climbing, but the factory manager can't seem to locate the source of the defect. Everything in the factory seems to be running as intended. Do we take the equipment offline to run more detailed diagnostics, or do we continue and hope the trend ceases and product output reverts to normal?

Finally, you reach a decision, the equipment will come offline for nonroutine maintenance. After hours of diagnostics, there seems to be a breakthrough. Although everything looks normal on the surface, there is a strange anomaly with the PLC software. With further diagnostics, it becomes evident that the factory was hacked! But why was this not discovered earlier?

The hackers must have been very clever and kept the malicious code hidden so that the operators would think everything was normal. After weeks of progressively increasing defects and having to take equipment offline, the factory is back up and running, but were we successful in quarantining all the effected equipment?

Fortunately, we require all factory floor devices, including the drives and servos, to have a hardware root-of-trust so that we can confidently push a software update to all potentially affected machines globally. Maybe this update will save our plant in Japan from having the same issues.

With the cyber attack surface changing, there is increased security risk and a greater need for security solutions at the edge. It is imperative that factories adopt a resilient posture against cyber attacks, meaning the ability to detect and recover when an attack takes place.



SOURCE: ANALOG DEVICES

Cyber economics.

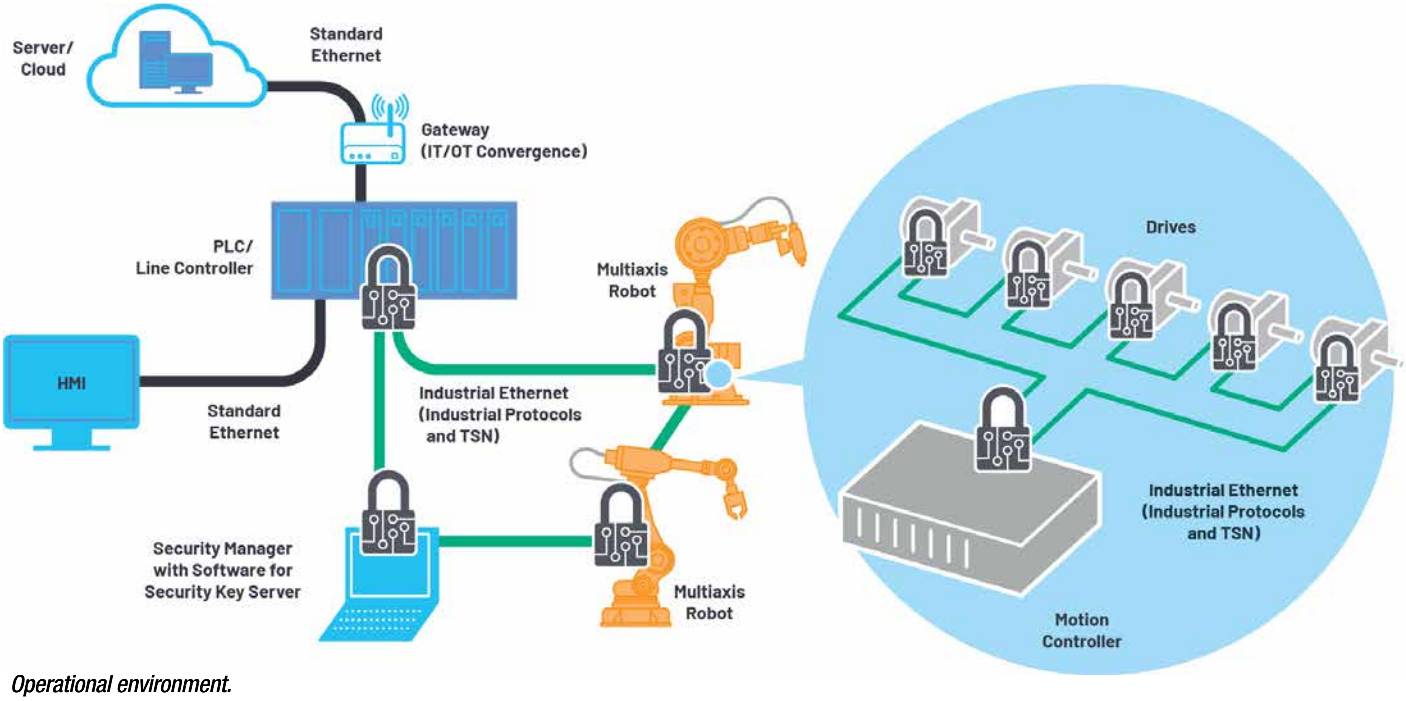
The question is no longer if I will get hacked, but when will I get hacked. Building a connected factory requires smart edge devices to be able to recover from attacks. This requires security to be implemented at the lowest level: the hardware itself.

Being able to trust the lowest levels of a device's boot and issue software updates enables a factory to recover quickly and resume normal operations.

What is changing the security risk?

The need for edge computing means more devices are being connected that interact with the real-world based on the data they receive. These smart devices are critical to enabling the outcomes of today's digital era.

As computing power becomes more pervasive, so does the need for security to address the increased cyber risk. It is only a matter of time before the next smart coffee machine makes the news for being held ransom by a cyber attack. Even though the ransom will be negligible, the incentive to attack a coffee



SOURCE: ANALOG DEVICES

Operational environment.

machine exists because there is a low barrier to facilitate a successful attack, which makes performing the attack worthwhile.

Consider the effort one might put toward holding an entire factory ransom. The potential reward increases significantly, as does the incentive for the attacker. Only relying on firewalls for critical infrastructure is no longer effective with the converged IT and OT networks.

The assumption should be made that someone has already gained access to the factory network. For this reason, device integrity and robust authentication protocols must be in place for all connected devices.

Network connected devices need to be able to authenticate with other devices on the network, establish shared keys, perform signatures on data, and validate data being received. There are standard ways for doing this, but the factory presents constraints that can make adapting security challenging for some use cases.

For instance, the sensitivity to time in motion control applications can create latency tolerances that make traditional means of doing device-to-device authentication prohibitive. Using standard public key infrastructure, devices will challenge each other to establish authenticity and exchange a shared session key using means such as TLS.

This method has already been adopted to many factory applications; however, this method is prohibitive in high speed motion-control applications as many devices need to interoperate together on a specific time scale.

When latency requirements are measured in microseconds, the appropriate message authentication scheme must be selected to achieve the desired level of security and speed. The flow of data from the controller to all devices on the control loop need to be received congruently.

One method to effectively enable this flow of data is to have all devices use the same shared session key. This requires a unique network configuration that allows devices to authenticate with a security manager that will provide the same session key to all devices on a designated security group.

These keys will be exchanged using standard TLS and revert to alternative protocols during time critical operation.

Identity and integrity to the edge

The ADI Chronous^{TM} portfolio of Industrial Ethernet connectivity solutions enables secure communication at the edge of the control loop. Our devices exist at the communication endpoints and are capable of securing network communications at each node point within the system while minimizing trade-offs in power, performance, and latency.

These scalable Ethernet solutions provide the means to extend security in highly time sensitive applications to meet the changing security risks, such as:

- Securing the edge of the factory control network to establish a resilient and trusted architecture.
- Allowing for secure connectivity of robots, drives, and production machines within an integrated OT/IT TSN network.
- Providing means for authentication and encryption (as required) in a highly time critical environment.

Analog Devices' security solutions for ADI Chronous Industrial Ethernet enables the rapid adoption of the connected factory. Leveraging ADI's secure development processes, our Industrial Ethernet solutions ensure the security design enables the system application while allowing for risk to be managed throughout the product lifecycle.

ADI's Industrial Ethernet solutions provide security features such as key generation/management, secure boot, secure update, and secure memory access.

Integrating security in devices at the edge of the industrial control loop will provide trust in data necessary to scale solutions capable of making real-time decisions on the factory floor.

Accelerate the path to Industry 4.0 by assuring:

- Machine/worker safety
- Reliable operation
- Product quality
- Uptime and throughput
- Production efficiency
- Production metrics and insights

With the next cyber attack happening today, how will you address the changing cyber risk? Will the attacker target the device's software or will it be a network attack inserting bad data?

Regardless, your devices will need to provide the ability to communicate securely and recover from the next attack. This requires security to be implemented at the lowest level: the hardware itself.

Being able to trust the lowest levels of a device's boot and issue software updates, enables a factory to recover and resume normal operations.

Erik Halthen, Product Development Manager, ***Analog Devices.***

Visit Website

The path to a product with few vulnerabilities

To develop a product with few vulnerabilities, a process for a secure life cycle (Security Development Lifecycle) should be used. The IEC 62443-4-1 standard describes such a process for automation systems. This article presents that process consisting of eight elements for successful implementation.

THE CERT NETWORK HAS DISCLOSED MORE THAN 10,000 IT security vulnerabilities, each year and every year, in products worldwide in accordance with the concept of "Common Vulnerability Enumeration (CVE).

And there surely are far more unrecognized or unpublished weak points. So, how can we do something about this situation?

At first glance, the CVE concept provides a complete solution. Every notification is assigned to a type of vulnerability (Common Weakness Enumeration), for example, CVE-20: "Improper Input Validation." However, it's hardly possible to strive for an absence of errors in all 1248 entries in the databank [1] as a development goal.

So how can high security quality be achieved? To develop a product with few vulnerabilities, a process for a secure life cycle (Security Development Lifecycle) should be used. The IEC 62443-4-1 standard describes such a process for automation systems. The process consists of eight elements, which will be presented in the following.

IT security requirements

Understanding operating conditions and determining protection requirements

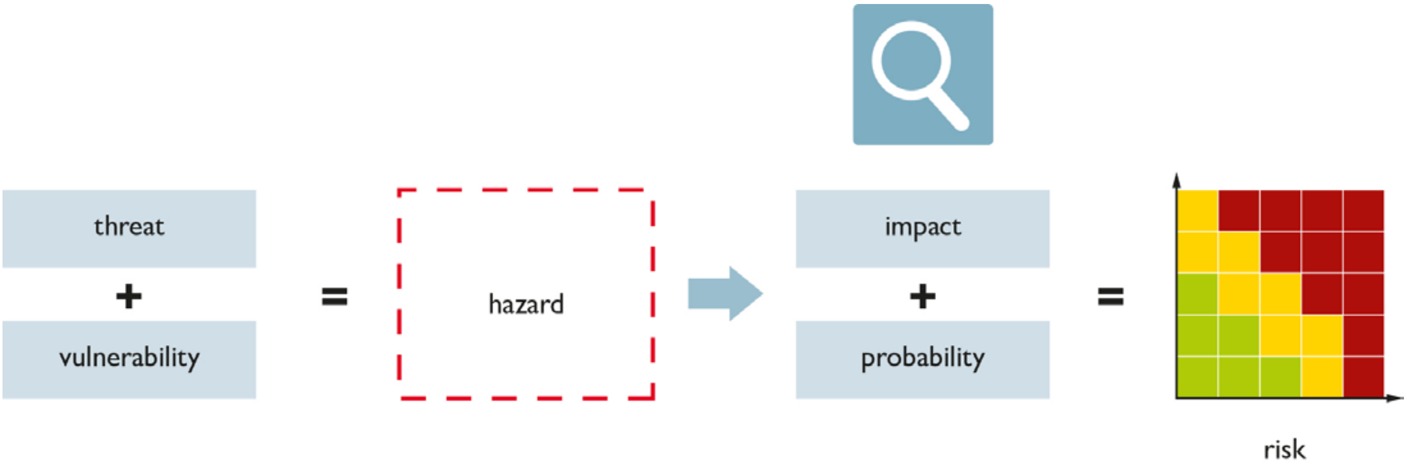
The first step is to understand and describe the relevant terms of use for the product. Is the product operated by trusted personnel in a controlled environment? Or is it as uncontrollable as the card terminals installed in supermarkets?

Which information is processed? Is it just data from the user or is there information from another party - for example, a machine builder or integrator - to be considered? By answering corresponding questions, the need for protection of the product and its functions and data can be determined, and threats can be worked out.

Here, hazards can arise, for example, from the manipulation or readout of data during physical access. If several parties are involved, threats result, among other things, from the disclosure of a machine builder's control program by the user.

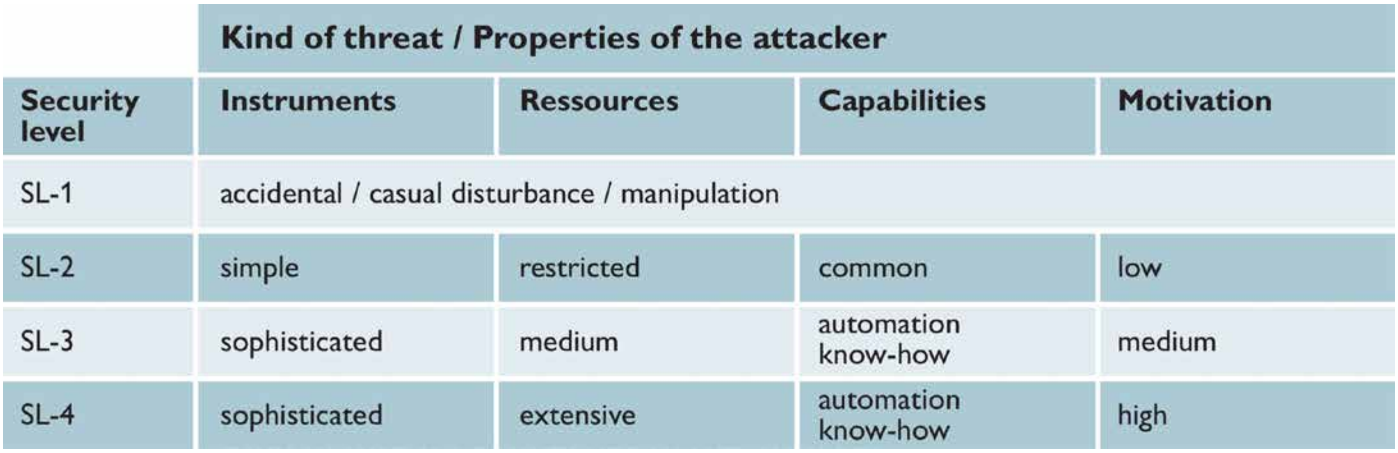
On this basis, the safety requirements that are decisive for further proceedings are formulated. If the product is endangered in its environment, it has to make physical access difficult and such attempts detectable. If information from different parties is to be protected, it proves necessary for the rights management to separate accesses cleanly.

The security objectives also include



SOURCE: PHOENIX CONTACT

Evaluation of threats.



	Kind of threat / Properties of the attacker			
Security level	**Instruments**	**Ressources**	**Capabilities**	**Motivation**
SL-1	accidental / casual disturbance / manipulation			
SL-2	simple	restricted	common	low
SL-3	sophisticated	medium	automation know-how	medium
SL-4	sophisticated	extensive	automation know-how	high

SOURCE: PHOENIX CONTACT

Aspired level of protection.

determining the level of security that is to be achieved and that is based on the attacker's strength. If greater values are to be secured, more attacks will have to be repelled. As a result, the security requirements should be complete when designing and implementing the security concept so that they can be included.

Security by design

Build up a resilient concept

The product is now designed in a way that its structure and functions meet the protection objectives and it is able to repel the threats mentioned above. To this end, proven security concepts such as minimizing execution and access rights, multi-level security mechanisms, and reducing weak points should be considered.

Applying reliable design rules prevents many of the above-mentioned types of vulnerabilities. In doing so, the threat analysis must be continued in accordance with the elaborated draft. Here, the threat arising from potential weak points is assessed to determine the danger. Only when it is considered unlikely enough for all possible damages to occur, the residual risk can be accepted. The security of the design is supported by a four eyes principle.

From encrypted communication connections to special chips for storing electronic keys to processors that execute only digitally signed code, many technical means are available. An appropriate rights and role management can be provided in order to manage the information of multiple parties. This way, we have a resilient concept that cannot be undermined that easily.

Secure implementation

Understanding the craft (of programming)

The neat realization of the design in hardware and software is the second essential element to prevent vulnerabilities. Programming guidelines contain specifications, the observance of which helps to prevent typical errors.

Examples are the rules for the correct handling of the length of character strings or the use of special characters. The correct handling of error messages is also very important. True to the motto "If everything goes according to plan, no errors will occur", these hints are often ignored during development, which leads to security gaps in real use.

Although there are programming guidelines that can be used as examples for almost all programming languages. In addition to the four eyes principle, tools which examine the resulting code for adherence to the specifications or typical error patterns can be used to check the implementation (static code analysis).

If the described way of proceeding is followed, the program is characterized by high quality and fewer errors - also with regard to security.

Security tests

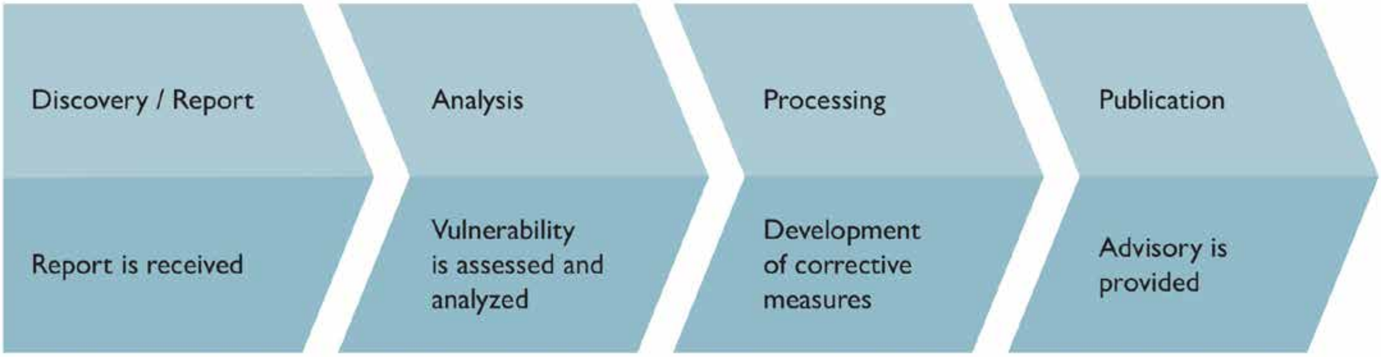
Creating trust

The verification of the security properties has to cover several aspects: For each security requirement established in the specification, the respective evidence must be provided by tests. In addition, evidence is required regarding the effectiveness of all security measures specified in the draft.

Furthermore, a manual or automatic check for known vulnerabilities as well as frequently occurring errors and problems must be carried out in order to uncover typical implementation errors or already published inadequacies in used subcomponents.

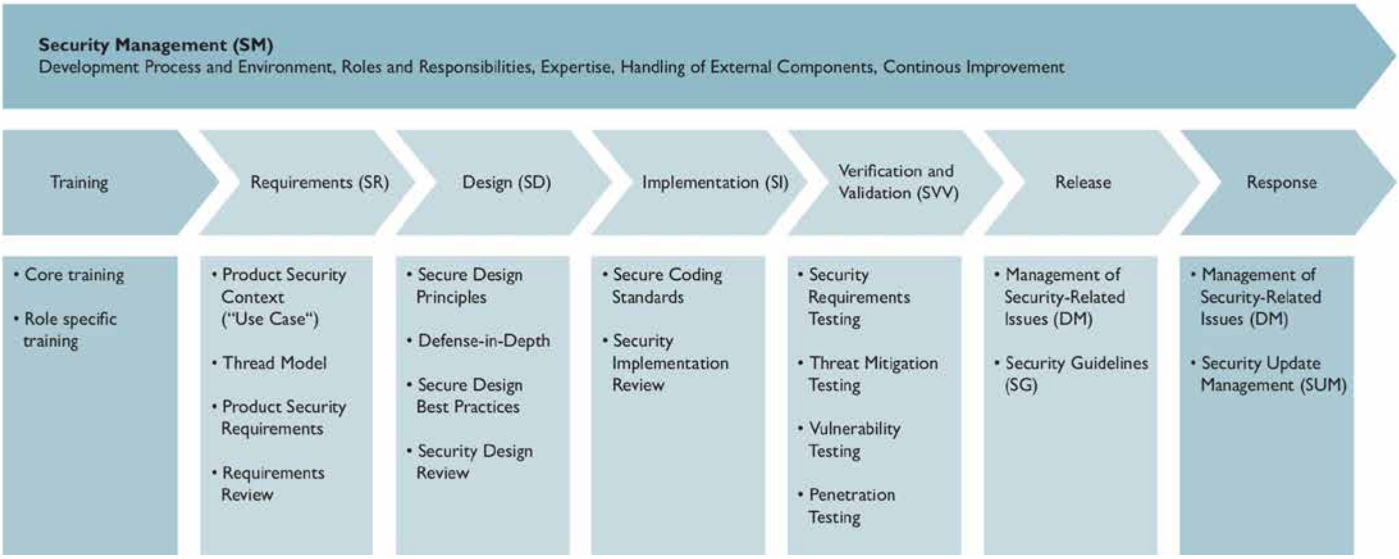
The state of the art also includes fuzz testing: by sending randomly distorted data, the robustness of the product can be checked. Finally, an expert should perform an attack test (penetration test). Independently of the normal team, the specialist tries to circumvent the safety barriers of the product.

As the expert is quite autonomous, organizational blindness should be avoided. The penetration test can be carried out internally or by a specialized service provider.



SOURCE: PHOENIX CONTACT

General course of action for potential vulnerabilities.


Security Management (SM)
Development Process and Environment, Roles and Responsibilities, Expertise, Handling of External Components, Continous Improvement
Training
Requirements (SR)
Design (SD)
Implementation (SI)
Verification and Validation (SVV)
Release
Response
• Core training
• Role specific training
• Product Security Context ("Use Case")
• Thread Model
• Product Security Requirements
• Requirements Review
• Secure Design Principles
• Defense-in-Depth
• Secure Design Best Practices
• Security Design Review
• Secure Coding Standards
• Security Implementation Review
• Security Requirements Testing
• Threat Mitigation Testing
• Vulnerability Testing
• Penetration Testing
• Management of Security-Related Issues (DM)
• Security Guidelines (SG)
• Management of Security-Related Issues (DM)
• Security Update Management (SUM)

SOURCE: PHOENIX CONTACT

General overview of the secure life cycle.

The described way of proceeding results in a high level of confidence in the product's security capability.

Security defect management

Addressing vulnerabilities

Despite the completion of all tests, the following is still true: the absence of evidence (for vulnerabilities) is not evidence of the absence (of vulnerabilities). Products without vulnerabilities do not exist. In this respect, their ongoing monitoring as well as the receipt of safety messages count as an integral part of the product life cycle.

Problems that become public have to be evaluated and may lead to security notes (advisory) and security updates. Therefore, the security quality and resistance of the products must be continuously monitored.

Security updates

Providing patches.

Security vulnerabilities are usually remedied by providing security updates, so-called patches. These have to be tested for side effects and documented in a way that users of the product can decide on their course of action. Updates must of course be made available in such a way that their integrity can be verified. In this way, the security quality and resistance of the products in the field remain stable.

Security documentation

Providing user manuals

For the product to be used securely, users need detailed documentation, for example on the intended conditions of use, the security functions, network connections, and integration into central systems, for example for user management or security monitoring.

The user is also informed about what to consider for the secure use of the product in terms of its setup or operation, i.e. where to find information about possible vulnerabilities and available updates. If such documentation is available, the user can take full advantage of the product's security features and qualities.

Certification: confirming know-how

Phoenix Contact is one of the first companies in the world that has implemented a safe life cycle according to IEC 62443-4-1. This was certified by TÜV Süd.

From a secure development process all the way to continuous vulnerability management by Phoenix Contact PSIRT (Product Security Incident Response Team), security is firmly rooted in the complete life cycle of the products and solutions. Moreover, the company's experience and high degree of vertical integration help the users to reach their security quality benchmarks.

For the secure design of solutions and services, Phoenix Contact - also as one of the first companies worldwide - implemented a secure process according to IEC 62443-2-4 (requirements for the security program) and had it certified.

The Blomberg-based company supports its customers throughout the entire process chain with standardized security. In the inventory and threat analysis of existing or planned systems, tailored service offers form the basis for the implementation of security concepts.

Security management

Settling processes and responsibilities

Finally and, in fact, right from the start, processes and responsibilities need to be clarified, staff qualifications need to be ensured, and all processes need to be organized.

In the end, it must be ensured that no product can be released that has not passed all security tests and for which not all known security problems have been resolved. This allows users to have full confidence in their supplier.

Secure life cycle

Ensuring quality for the long term

Specific security functions, such as encryption or access control, have not been in the focus of attention so far. The international standard IEC 62443-4-2 describes security functions for components that are required with regard to the interaction of security functions according to IEC 62443-3-3.

However, the mere presence of these functions is of little help and creates a false sense of security if the function or the entire product is implemented incorrectly. Therefore, IEC 62443-4-2 requires a secure life cycle according to IEC 62443-4-1.

A product that is developed and maintained in the secure life cycle is always characterized by high security quality that users can trust in. With the certification of the life cycle process, the product manufacturer supports this trust.

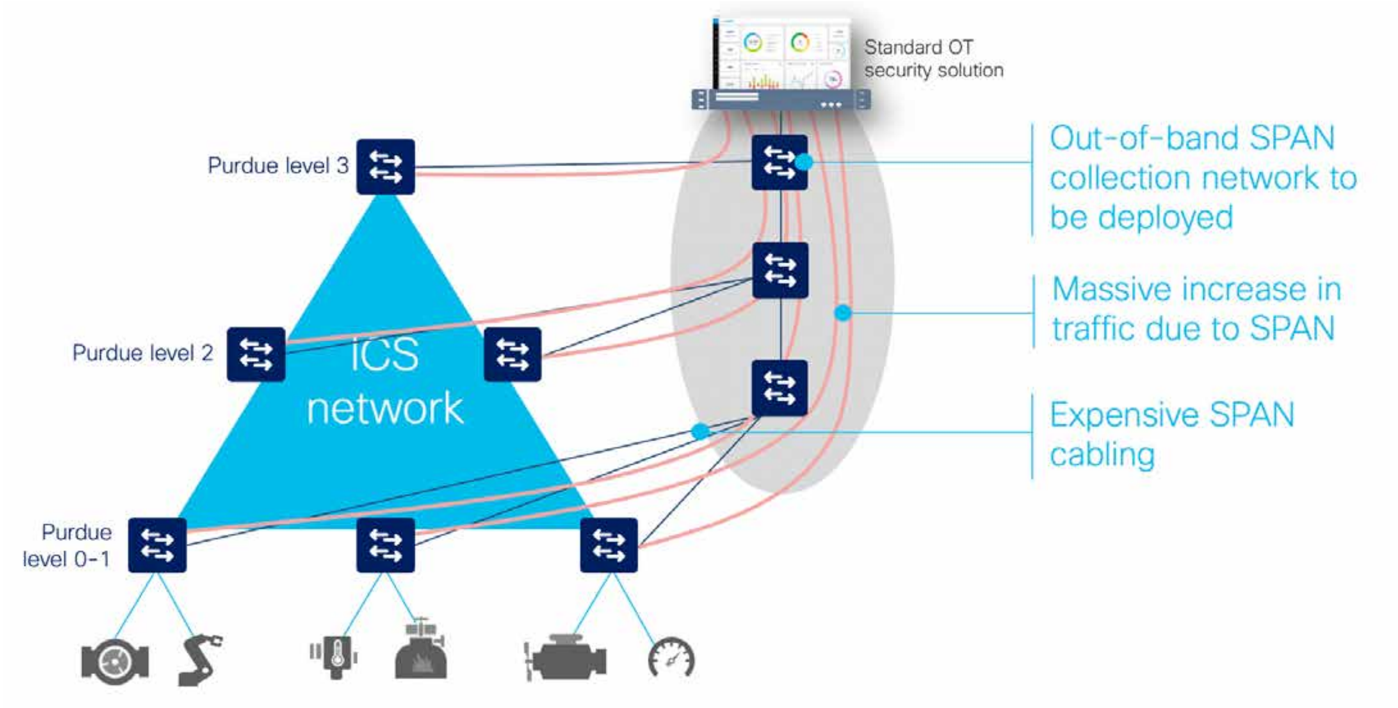
A product certification according to IEC 62443 is based on the secure process and confirms the product properties, but always covers a specific point in time only.

Dr.-Ing. Lutz Jänicke, Corporate Product & Solution Security Officer, ***Phoenix Contact.***

More Information

Securing industrial networks: There must be a better way!

Your industrial network can now help you deploy IoT/OT security at scale in a much easier and cost-effective way. Unique edge computing security architecture capabilities bring the simplicity and cost saving benefits industrial organizations are looking for when deploying OT security at scale.


Standard OT security solution
Purdue level 3
Purdue level 2
ICS network
Purdue level 0-1
Out-of-band SPAN collection network to be deployed
Massive increase in traffic due to SPAN
Expensive SPAN cabling

SOURCE: CISCO SYSTEMS

SPAN based solutions incur huge additional hidden costs.

WITH OPERATIONAL ENVIRONMENTS increasingly digitalizing and connecting to the IT environment, industrial organizations are recognizing the need to protect operational technology (OT) and industrial IoT against cyberattacks.

Deploying firewalls to build a demilitarized zone (DMZ) between industrial networks and the IT domain is the mandatory first step. But as organizations connect more devices, enable more remote access, and build new applications, the airgap erodes and falls short of being sufficient.

Security solutions designed for industrial networks typically monitor network traffic to gain visibility on assets, behaviors, malicious activities, and threats. The process of evaluating and testing these solutions initially tends to go well – after a successful proof of concept, industrial organizations begin to deploy at scale. That's where they begin to run into issues.

Often, it's cost prohibitive for organizations to buy the number of security appliances they need to cover their entire operational environment. Or the networking team doesn't have the resources to deploy, maintain, and manage a fleet of security appliances.

Traffic mirroring that is required to feed these appliances would likely necessitate a separate network, and would also require the resources to deploy, maintain, and manage it. In many deployments the added cabling cost for the separate network itself far outweighs the entire cost of the security solution.

Visibility of operational network

When organizations attempt to secure their IoT/OT network, they encounter two primary issues:

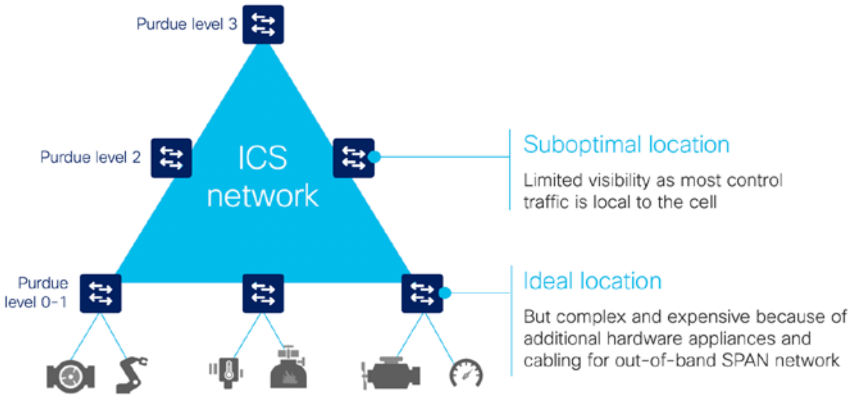
1. *A lack of visibility:* As industrial networks can be quite old, widely dispersed, and involve many contractors, operators often don't have an accurate inventory of what's on the network. Without this, they have limited ability to build a secure communications architecture.
2. *A lack of control:* A lack of visibility also means operators are often unaware of which devices are communicating to each other or even of communications reaching industrial devices from the outside. You cannot control what you don't know.

The first step, then, to securing an IoT/OT network is to obtain visibility. You need to understand what devices are on the network, what they are communicating, and where those communications are going.

The technology to achieve network visibility is available today. Deep packet inspection (DPI) decodes all communication flows and extracts message contents and packet headers, providing the visibility to understand what devices you need to secure, and the policies required to secure them.

DPI allows you to gather device information such as the model, brand, part numbers, serial numbers, firmware and hardware versions, rack slot configurations, and more. It also allows you to understand what is being communicated over the network. For example, you can see if someone is attempting to upload new firmware into a device or trying to change the variables used to run the industrial process.

To achieve complete visibility, all network traffic must be inspected. It's important to note that in an industrial network, most traffic occurs behind a switch at the cell layer where the machine controllers are deployed. Very little traffic goes up to the central network.


Purdue level 3
Purdue level 2
ICS network
Purdue level 0-1
Suboptimal location
Limited visibility as most control traffic is local to the cell
Ideal location
But complex and expensive because of additional hardware appliances and cabling for out-of-band SPAN network

Visibility and detection built into the network infrastructure.

When collecting network packets to perform DPI, security solution providers typically configure SPAN ports on network switches and employ one of three architectures:

1. Mirror all traffic to a central server that performs DPI
2. Deploy dedicated sensor appliances on each network switch
3. Mirror traffic to dedicated sensor appliances deployed here and there on the network

Monitor IoT/OT networks via SPAN

While these approaches deliver network visibility, they also create new challenges. Configuring network switches to send traffic to a central server requires duplicating network flows. A new out-of-band network will generally be needed to transport this extra traffic, which can be complex and costly. Although this can be acceptable for a very small industrial site, this cannot be seriously considered in highly automated industries generating a lot of ICS traffic (such as manufacturing), or when devices are widely spread in locations with no or poor network connectivity (oil and gas pipelines, water or power distribution, etc.).

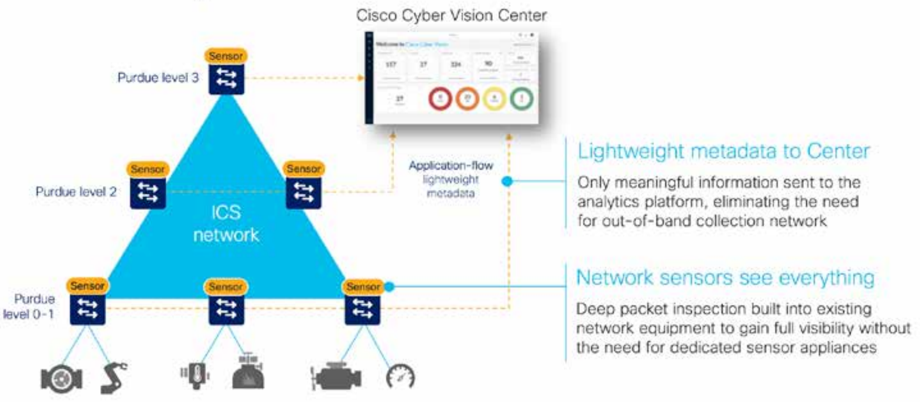
Connecting sensor appliances to network switches addresses the issues associated with duplicating network traffic. The appliance collects and analyzes network traffic locally and only sends data to a server for additional analysis. However, installing, managing, and maintaining dedicated hardware can quickly lead to cost and scalability issues. And because most industrial traffic is local, gaining full visibility requires deploying appliances on each and every switch on the network, raising cost and complexity to intolerable levels.

Some technology providers attempt to address this problem by leveraging remote SPAN (RSPAN). RSPAN allows you to duplicate traffic from a switch that doesn't have a sensor appliance to a switch that has one.

While this approach reduces the number of appliances required to provide full visibility, it still increases the amount of traffic going through the industrial network. Traffic is multiplied because you're duplicating traffic to SPAN it to a remote switch. And the more traffic on the network, the slower it becomes, resulting in jitter — often an unacceptable compromise in industrial networks where processes need to run faster and machines must be timely synchronized.

Alternatives to SPAN

Instead of SPAN, organizations can use network TAP, port aggregators, or virtual switches, but these alternatives come with a few caveats of their own: 1) organizations must still source and deploy dedicated appliances, 2) configuration and management aren't necessarily easy, and 3) sending traffic to the OT security platform requires an out-of-band network to avoid impacting the production network.


Cisco Cyber Vision Center
Sensor
Purdue level 3
Purdue level 2
ICS network
Purdue level 0-1
Application-flow lightweight metadata
Lightweight metadata to Center
Only meaningful information sent to the analytics platform, eliminating the need for out-of-band collection network
Network sensors see everything
Deep packet inspection built into existing network equipment to gain full visibility without the need for dedicated sensor appliances

Visibility and detection built into the network infrastructure.

There is a better way to achieve full network visibility: embed DPI capability into existing network hardware. An industrial-grade switch with native DPI capability eliminates the need to duplicate network flows and deploy additional appliances. Obtaining visibility and security functionality is simply a matter of activating a feature within the network switch, router, or gateway. Cost, traffic, and operational overhead are all minimized.

A DPI-enabled switch analyzes traffic locally to extract meaningful information. It only sends lightweight metadata to a central server, which runs the analytics and anomaly detection. This additional traffic is so lightweight (3-5% of general traffic), it can be transferred over the industrial network without causing congestion or requiring extra bandwidth.

Embedding DPI in network equipment affords both IT and OT unique benefits. IT can leverage the existing network infrastructure to secure industrial operations without having to source, deploy, and manage additional hardware.

Because these network elements see all industrial traffic, embedded sensors can provide analytical insights into every component of the industrial control systems. As a result, OT can obtain visibility into operations that it has never had before.

However, not all network equipment can support the embedded sensor feature. Gaining visibility on these local communications will require hardware sensor appliances. Beware that not all appliances are created equal – to maintain the benefits of not deploying a SPAN architecture, these appliances should 1) be centrally managed (so they are easy to deploy and maintain), 2) have limited analytics features (so they can run on low-cost hardware), and 3) only send metadata to the central console (so they don't need extra network resources).

Gaining the visibility that will enable a truly effective IoT/OT threat detection strategy requires capturing network traffic at the cell layer. Leveraging edge computing to embed deep packet inspection in network equipment enables comprehensive visibility.

With its wide range of industrial switches, routers and gateways running Cyber Vision, Cisco offers unique edge computing security architecture capabilities that bring the simplicity and cost saving benefits industrial organizations are looking for when deploying OT security at scale.

Ruben Lobo, Product Line Manager, ***Cisco Systems.***

Visit Website

System-integrated measurement simplifies power management

A highly efficient power measurement chain provides a range of solutions from the sensor to the cloud. These include capturing the physical value with new SCT current transformers, to the IoT Coupler and finally to cloud-based data analysis. A broad spectrum of power measurement terminals covers requirements.

SOURCE: BECKHOFF AUTOMATION

Improved power transparency simplifies energy management and raises the availability of equipment.

AN END-TO-END POWER MEASUREMENT chain that extends from the sensor to the cloud simplifies energy management, and improves the availability of machines and entire installations.

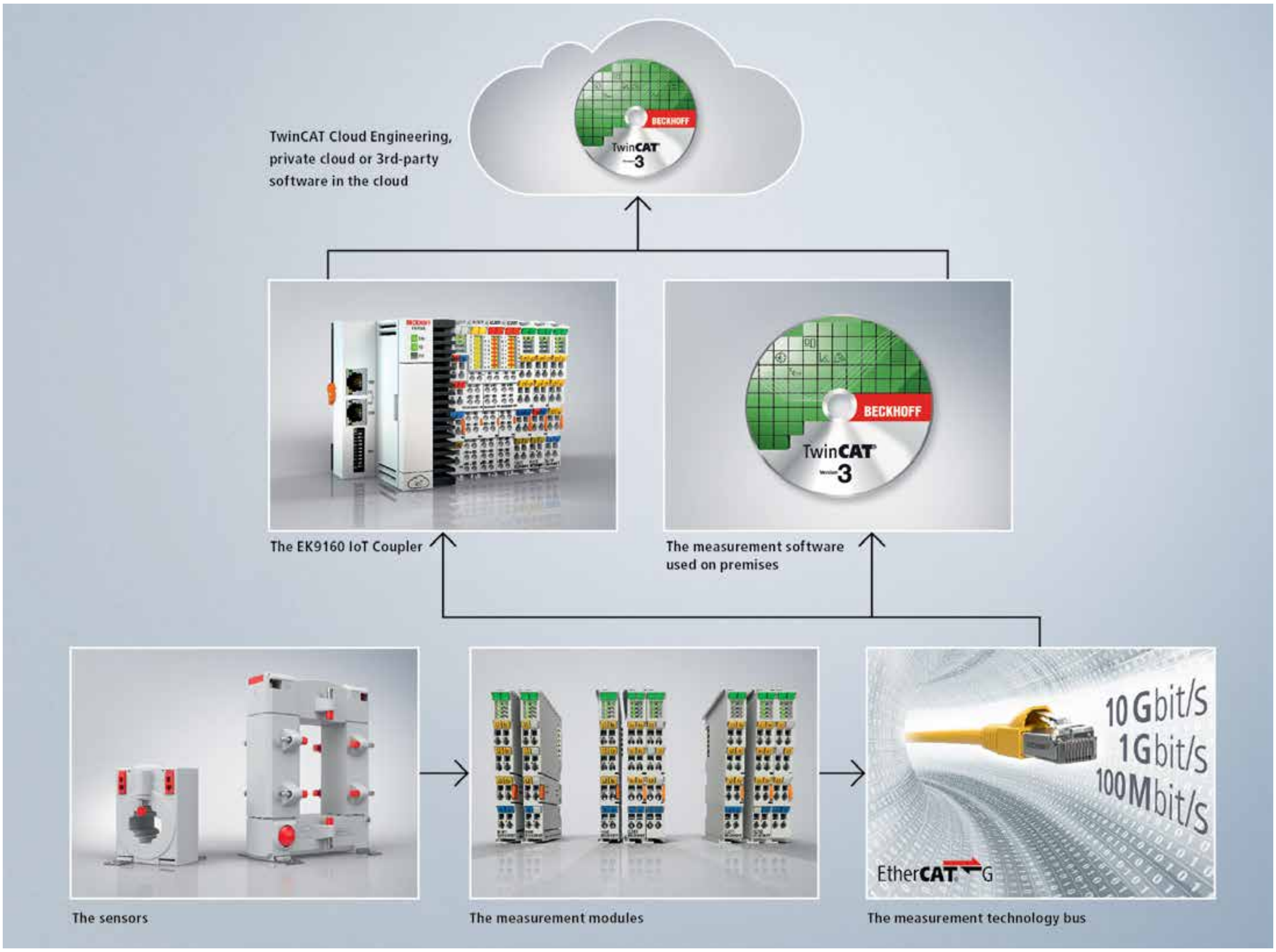
The solutions range from capturing the physical value with new SCT current transformers, to the IoT Coupler and finally to cloud-based data analysis. A broad spectrum of power measurement terminals covers all requirements, from a current input terminal to highly efficient distributed power measurement.

By having access to continuous and integrated power measurement tools, users can perform extensive inline analyses that allow them to detect deviations instantly in order to take quick corrective action and minimize downtime. For example, a steady increase in a machine's power consumption may be an indicator of excessive wear on bearings, while a decrease may be a sign of quality problems.

Up to now, such continuous monitoring was extraordinarily complex because it required external sensors to be installed at great cost and often using special parts. With power measurement terminals from Beckhoff Automation, this can now be accomplished with little effort using standard components, even in retrofits on existing machines and systems. By measuring the power on an existing motor cable, for example, asymmetrical currents can now be detected within milliseconds and not only indirectly via an unusual rise in the motor's temperature. And in case of vibrations, mechanical weak spots can be identified via an increase in harmonic content.

SOURCE: BECKHOFF AUTOMATION

With the EtherCAT power management terminals, tasks with optimal scalability include power monitoring, process control, network control and maintenance.


TwinCAT Cloud Engineering, private cloud or 3rd-party software in the cloud
BECKHOFF
TwinCAT 3
The EK9160 IoT Coupler
The measurement software used on premises
10 Gbit/s
1 Gbit/s
100 Mbit/s
EtherCAT G
The sensors
The measurement modules
The measurement technology bus

SOURCE: BECKHOFF AUTOMATION

The end-to-end power measurement chain within PC-based control can be optimally adapted to requirements on both the software and the hardware sides.

Power transparency boosts efficiency

Machines and plants are dynamic systems that get expanded, modified, converted or otherwise adapted to new production requirements over the years. In order to obtain maximum transparency even for systems that have become unwieldy, it is recommendable to have an all-encompassing measurement system that collects all relevant power data reliably and makes it possible to analyze it quickly in the cloud, if necessary.

To make evaluation of measurement values as easy as possible, Beckhoff has developed the so-called power quality factor (PQF) which allows users to assess power quality for a machine or system based on a single number without having to analyze the frequency, voltage, harmonics or symmetry individually.

If a machine malfunction occurs and the PQF simultaneously drops to zero, users can conclude that the might not lie in the machine itself but in the power supply. Based on this information, the causes and effects of faults can be identified and corrected much more quickly. The PQF can also function as an early-warning system and simplify the clarification of potential questions regarding liability.

Distributed power measurement

The new concept of distributed power measurement offers a particularly efficient and cost-effective way to obtain accurate power data even from more complex systems. Its central element is the 6-channel EL3446 input terminal for measuring up to 1A of AC/DC current. It allows the user to determine precise power values even for physically separated voltage and current measurements.

What makes the EL3446 special is its ability as a current power measurement terminal to determine all relevant electrical data of the supply network, including all actual power measurement values. The voltage values required for the calculation of power data are transmitted to the terminal over EtherCAT by a 3-phase EL3443 power terminal (installed only once per network) and synchronized via the distributed clocks in EtherCAT.

The active power and energy consumption are computed for each of up to six connectable phases in the EL3446. This makes the effective voltage and current values as well as active, apparent and reactive power, frequency, phase shift angle and harmonics available for grid analysis and energy management.

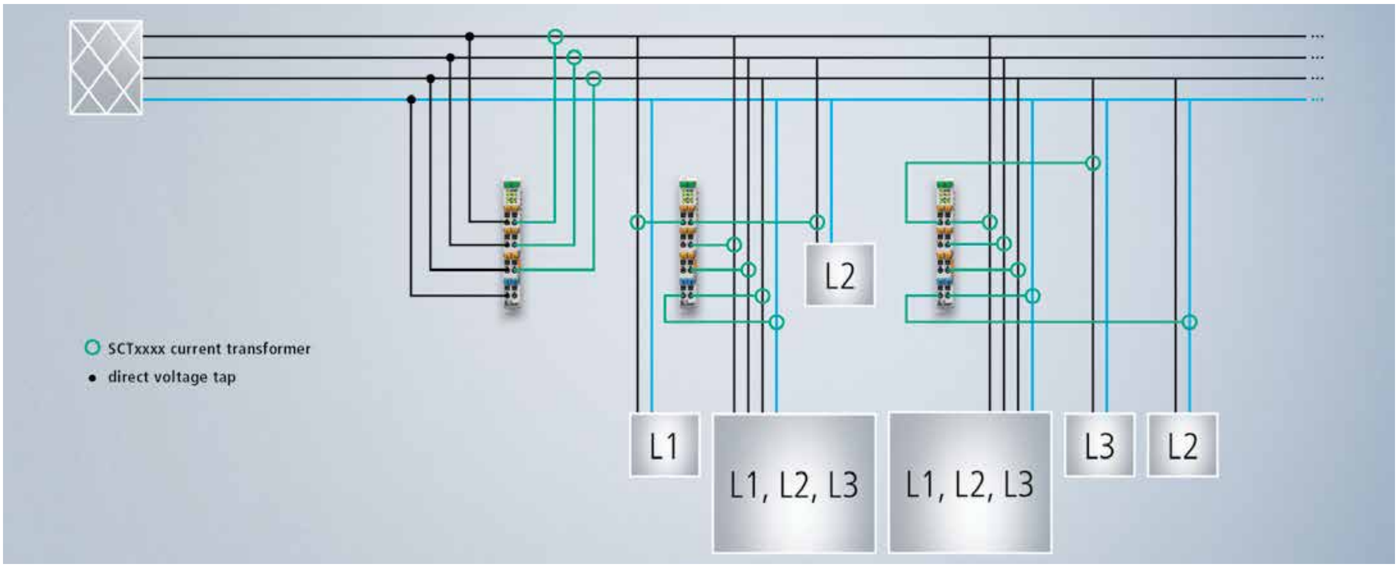
This concept of distributed power measurement – with just one EL3443 and any number of EL3446s – minimizes the hardware and installation effort and eliminates the wiring requirements for the voltage distribution. In addition, the per-channel cost of the power measurement is reduced by almost 50%without having to reduce the scanning speed if the number of measurement points rises.

Another benefit is that only the EL3443 power measurement terminal must be protected with fuses. This eliminates the need for the downstream fuses required with conventional power measurement systems.

Broad spectrum of solutions

The SCT series current transformers serve as the starting point for the seamless power measurement chain within PC-based control. The broad portfolio of models covers all relevant applications from 1 to 5,000 A and from ring-type and split-core transformers to 3-phase transformers.

This allows the user to implement reliable power sensors as a standard component of the PC-based control system directly in the field



SOURCE: BECKHOFF AUTOMATION

With distributed power measurement, a single voltage measurement can be connected digitally to any number of current measurements, making it easy to capture exact power values at each metering point.

with the option to choose between concepts that are highly scalable through a wide range of designs and performance classes.

The SCT portfolio is extremely broad, ranging from low-cost 3-phase transformer sets for building technology to standard industrial transformers for machines to solutions for inspection stations and test benches with extra-high precision requirements.

The choice of the appropriate product category depends on the type of usage, with ring-type transformers being particularly suitable for cost-effective and accurate data collection in new installations. Because of their easy installation, split-core transformers are predestined as an easy retrofit solution.

The EtherCAT power measurement terminals are also finely scalable and can be used for applications ranging from maintenance and closed-loop controlling to power monitoring. In terms of performance categories, they differ by their accuracy and speed in data acquisition with bandwidths ranging from seconds and milliseconds to microseconds for oscilloscope functionality.

For simple measurement tasks such as the monitoring of voltage, frequency and phases, Beckhoff offers the EL3483 as a network monitor and the EL3423 for power measurement.

Terminals in the EL34xx series handle measurements in the lower millisecond range, for example for closed-loop machine control applications.

Power monitoring with the momentary-value capture of current and voltage with microsecond accuracy, for example in test racks, can be implemented with the high-performance terminals in the EL37xx series. Their ability to access instantaneous values of current and voltage in the PLC makes a particularly thorough system integration possible.

Compared to the EL37xx series, the EL34xx series features much easier programming through pre-scaled SI units, statistical analysis directly from within the terminal, and a warning function when predefined upper and lower limit values are violated.

With their many special functions, the EtherCAT power measurement terminals offer other additional benefits. These include features such as min/max/average analysis, power total over preset intervals, user-controlled input signals, and harmonics analysis of current and voltage up to the 63rd harmonic. Also gaining importance is the measurement of fault or differential currents, which the EL3453 includes by default with its integrated 4-current measurement channel, which makes it possible, for example, to find insulation faults before the power supply to a machine is suddenly interrupted.

Cloud communication & data analysis

The power measurement data can be transmitted to the cloud either via the local control PC or the EK9160 IoT Coupler. With the help of TwinCAT automation software, all machine functions ranging from engineering, PLC, motion control, safety management, visualization and measurement technology to communication are governed by the local control PC.

In addition, TwinCAT Power Monitoring provides special network analysis functions. With the IoT Coupler, power data can be transferred safely and easily via communication protocols such as OPC UA PubSub or MQTT to the desired cloud environment enabling functions such as cloud-based engineering, centralized data analysis and easy integration with storage services of various public cloud platforms.

The special feature of the EK9160 IoT Bus Coupler is its ability to connect EtherCAT I/O directly to the IoT with no need for a specific control program. By transferring the E-bus signal representations to various IoT communication protocols, the EK9160 makes it possible to integrate I/O data into cloud-based communication and data services easily and in a standardized manner. It requires neither a controller nor programming, i.e. users can parameterize the I/O data via any browser via a simple configuration dialog with the integrated web server.

The respective cloud service and security functions such as authentication, encryption, a.o., can also be easily configured via a browser. Once the parameters have been set, the bus coupler sends digital or analog I/O values, including the associated timestamps, to the selected cloud service. If the internet connection is interrupted, the I/O data to be transmitted can be buffered locally.

Users can optimize their power management by performing fast, cloud-based analysis of their power data. As the ideal solution for this purpose, TwinCAT Analytics allows for selective or continuous data analysis depending on the user's needs. While the TwinCAT Analytics Service Tool improves and simplifies the commissioning processes for technicians, for example, the Analytics Workbench features enhanced capabilities and supports the automatic generation of program code.

And with 24/7 runtime deployment, the Analytics Workbench makes consistent and seamless data analytics possible. In this way, machine manufacturers can offer their customers individual data analytics solutions and become themselves providers of new predictive maintenance concepts.

Dr. Fabian Assion, Product Manager I/O, ***Beckhoff Automation.***

Visit Website

Blendtech cuts cost of API 2350 compliance

Cost-effective automated reconciliation for petroleum distribution terminals improves safety and accounting. Using an edge controller, Blendtech was able to present their customer with a reliable data aggregation solution that significantly reduced the cost of API 2350 compliance.

THE PATH THAT CRUDE OIL TAKES FROM extraction to conversion to consumption is long and carefully managed. For financial and environmental safety reasons, every step of the distribution process has to be monitored and controlled in a process called custody transfer.

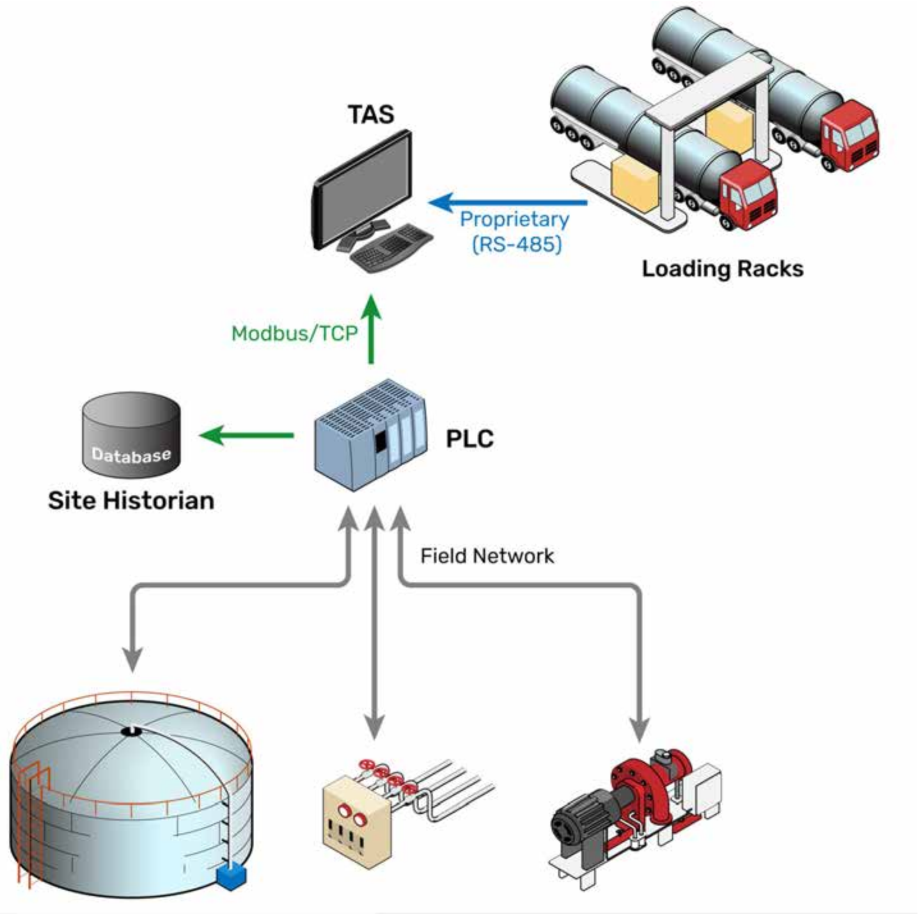
Primary distribution terminals (PDTs) are critical parts of this system, where petroleum products are received— usually from pipelines or ships—and then discharged onto trucks, ships, or rail cars in structures called loading racks.

Many jobs need to be performed to keep these terminals and loading racks running efficiently and in compliance with government regulations and industry standards.

Terminal Automation Systems (TAS) are commonly used to automate these functions. They bridge the SCADA systems used to control and monitor field devices (electronic meter registers, tank level indicators, valves, pumps, etc.) with back-office systems. For example, a TAS might provide point-of-service authorization to permit fuel loading and then direct billing information to the terminal's ERP system.

Recently, however, the American Petroleum Institute (API) introduced updates to API Standard 2350, "Overfill Protection for Storage Tanks in Petroleum Facilities," that significantly changed the way that tank receipts are handled. Critically, it added a requirement to implement a management system with formal processes for reconciling receipts and distributions.

The motivation behind the standard is to increase safety in places like PDTs where petrochemical spills risk vapor cloud explosions and other dangers to personnel and the environment, not to mention lawsuits, fines, and facility closure. But reconciliation is a major undertaking, requiring periodic accounting of incoming and outgoing flow meter registers and tank level gauges to identify potential discrepancies.



SOURCE: OPTO 22

An example control system for a Petroleum Distribution Terminal.

The Challenge

Blendtech is a division of PT Industrial Electric (PTI), suppliers of TAS for oil and gas distribution. The company offers expertise in design, engineering, installation, implementation, commissioning, training, and support of bulk product handling and loading equipment, additive and dye injection, ratio and wild stream blending, and a wide variety of custom process solutions for petrochemical and chemical industries.

One of Blendtech's customers approached them seeking help to comply with API 2350. At the time, this customer was using a labor-intensive verification process every 24 hours, recording information in spreadsheets and reviewing them manually. Thus, in addition to improving compliance, the customer hoped to improve operational efficiency, tank utilization, and accounting accuracy as well.

The fundamental challenge to reconciliation is the quantity of data required, so there are two common approaches to improving compliance:

- Take manual inventory more often
- Bring more field data into the TAS

For smaller terminal operators like Blendtech's customer, neither option is attractive, since either hiring personnel or expanding infrastructure might require a significant investment.

The goal

Blendtech's task was to find a third option, a way of automating this costly process that would be feasible for their customer. Several years ago, Blendtech began working in the space of information technology (IT) and operations technology (OT) convergence, as more of their projects required bringing data from field PLCs into TASs.

Initially, they experimented with Ignition SCADA to bridge these systems, but later used Node-RED on Opto 22's groov Box, because it didn't require deploying and maintaining a PC. Blendtech had used Opto 22 products for over 25 years, integrating SNAP PAC controllers, G4/G1 I/O, and SSRs into their own TAS product.

For this project, they looked to the latest generation of industrial connectivity products, including MOXA gateways and Opto 22's groov EPIC. The goal was to build a transaction history in the customer's site historian using the data reported to the TAS. In particular, they needed data from custody transfer-certified meter registers located at each loading rack and from pipeline manifolds where incoming fluid transfers are measured.

With an accurate transaction history in place, it would be possible to reallocate personnel currently used for reconciliation and have back-office operations staff audit tank usage more frequently. It would also be possible for accounting staff to perform more accurate internal audits, providing a basis for continuous improvement.

The system

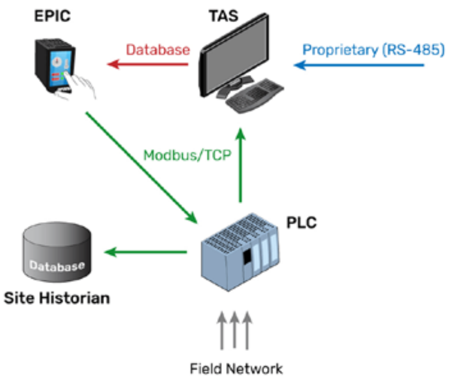
So if meter register data was already reported to the TAS, why didn't the customer already have an accurate transaction history they could use? The short answer is that there simply wasn't a bridge between where the data was available and where it needed to be. There was no connection between the TAS, which resided on a corporate network, and the site historian, which was part of the control network. Further, the data stored in the TAS required normalization, additional processing to format data items consistently, before it could be added to the site historian.

The control network contained an Allen-Bradley PLC that provided some aggregation of field I/O data, but it lacked connections to the loading rack meters and the functionality to read and process data from the TAS database. The flow meters themselves were controlled by their own embedded logic, independent of the field PLC, and reported their values back to the TAS using a proprietary protocol that wasn't accessible to the rest of the control system.

The solution

In order to bridge these separate systems, Blendtech chose to build their solution on Opto 22's groov EPIC. It provided all the functions they needed in a single package—secure connectivity, data processing, and storage—which meant they didn't need a PC or additional hardware to complete the design, and it was backed by excellent user documentation and free customer support.

"It was really the total package—the combination of price, support, look and feel, and overall functionality," said project engineer, Nick Palozzi. With groov EPIC, Blendtech was able to present their customer with a reliable data aggregation solution that significantly reduced the cost of API 2350 compliance.



SOURCE: OPTO 22

Cyber Vision deployment in manufacturing plants.

Step 1: Bridge the networks

Just like the smartphone has in many cases taken the place of dedicated consumer devices (cameras, phones, laptops), the power of edge computing makes it possible to use one device to perform the work of many industrial devices.

At its heart, groov EPIC is an industrial controller capable of high-speed I/O operations; but in this case, Blendtech took advantage of its connectivity and processing power to use it as a secure network gateway.

The groov EPIC processor (GRV-EPIC-PR1) has two completely segregated network interfaces, so that trusted and untrusted networks can be isolated. This segregation solved the basic problem of bridging the corporate and control networks without permitting unregulated traffic between them.

The controller fit comfortably into the existing control cabinet using a zero-I/O chassis (GRV-EPIC-CHS0), a small-footprint housing (5.36" x 3.54") for applications that don't require I/O operations.

Step 2: Retrieve and normalize

While legacy PLCs may be capable of communicating using various industrial protocols, they are usually unable to interface with modern IT systems directly.

With groov EPIC on the network, however, Blendtech could build a custom data processing interface for the TAS directly into the controller using the embedded Node-RED IoT connectivity software. Node-RED boasts a large library of functions for connecting data sources, including drivers for many popular databases.The ultimate goal was to provide time-sequenced data as a series of Modbus registers that the master PLC could read from the groov EPIC processor. That wasn't the native format of the data in the TAS, however, and depending on which loading rack the data originated from, various operations had to be performed to achieve this consistent format.

Blendtech designed event triggers to recognize when data in the TAS had been updated, as well as the source of the data. Then they invoked logic to sequence, format, and scale appropriately for the specific data source. Blendtech used Node-RED to handle all of this, with custom formatting logic in embedded Javascript functions.

Step 3: Transfer

With all this work done, the final step was to move data into the site historian.

"The memory storage of the EPIC was an important factor," noted Palozzi, because with 6 GB available on a fault-tolerant solid-state drive (SSD), the EPIC could also serve as the temporary storage location for everything it retrieved from the TAS, ensuring no additional hardware was necessary to complete their solution.

After retrieval and processing in Node-RED, data was written to the groov EPIC's requests from the master PLC. Once there, the historian could poll the PLC at regular intervals to add this data to the site archives.

An EPIC bonus

Blendtech also took advantage of groov EPIC's built-in touchscreen and embedded groov View server to design a basic HMI for controller and network health monitoring. Since groov View is mobile-ready, the status of the controller can be viewed from any smart device or computer connected to the network, using the built-in user access controls to maintain security.

The future

Ultimately, Blendtech was able to meet their customer's goal, delivering a solution to automate inventory reconciliation at a fraction of the cost of the typical alternatives. With significantly less manpower, they can audit their transaction history every hour instead of every day, improving their accounting granularity and increasing confidence that product is being safely managed.

What's next? With similar installations in Canada and the U.S., Blendtech continues to present their reconciliation solution to more potential customers. The next generation of the product will take advantage of groov EPIC's native support for Ignition by Inductive Automation. By installing the full Ignition Gateway and internal hardware memory map, where it could be accessed via Modbus/TCP SQL-Bridge module on the EPIC, Blendtech plans to design even more robust transactional logic into their TAS database monitoring.

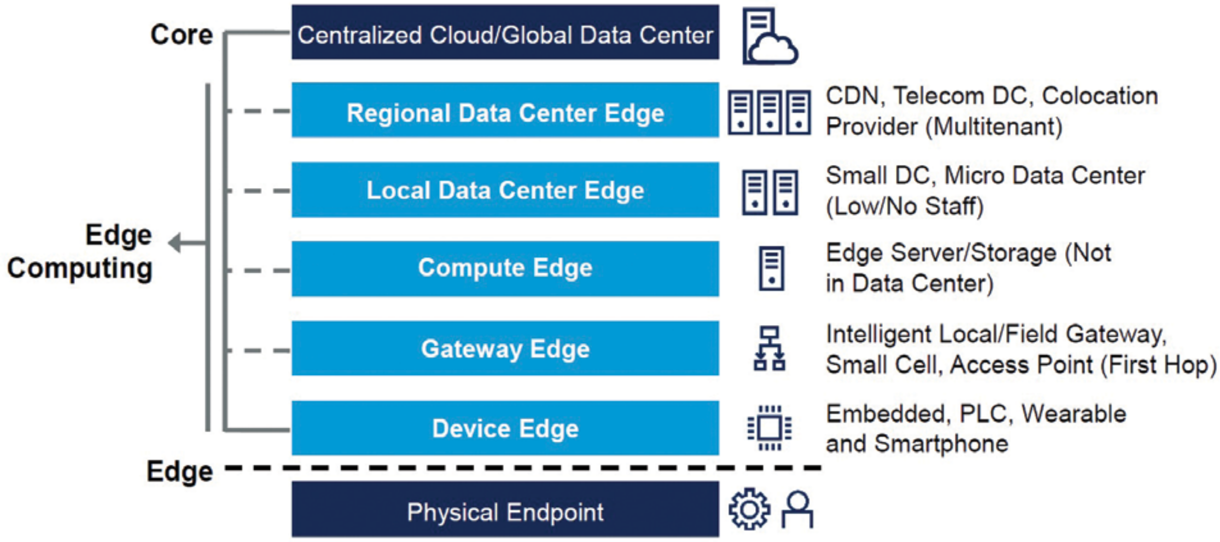
They are also expanding their portfolio of custom IIoT applications and developing a traffic management system for use in distribution terminals. Using the EPIC's I/O control functions, the system will control high-visibility lane and wait-time indicators to optimize the flow of tanker trucks through loading racks.

Applications report by ***Opto 22.***

Visit Website

Edge computing for smart factories and smarter machines

Edge computing platforms offer new revenue and cost reduction opportunities for machine and equipment manufacturers. They also offer OEM machinery builders a technology pathway to developing new generations of smarter equipment that meet changing customer demands and the need for digital transformation.


Core
Centralized Cloud/Global Data Center
Regional Data Center Edge
CDN, Telecom DC, Colocation Provider (Multitenant)
Local Data Center Edge
Small DC, Micro Data Center (Low/No Staff)
Edge Computing
Compute Edge
Edge Server/Storage (Not in Data Center)
Gateway Edge
Intelligent Local/Field Gateway, Small Cell, Access Point (First Hop)
Device Edge
Embedded, PLC, Wearable and Smartphone
Edge
Physical Endpoint

SOURCE: STRATUS

From this topology, it is easy to see that the Device Edge through the Compute Edge are applicable to machine and equipment builders.

DIFFERENT TYPES OF OEM MACHINERY builders face one challenge that is always the same; the market is highly competitive. Each generation of equipment offers price/performance improvements over previous generations.

Design, engineering and product management departments must constantly evaluate the tradeoffs between new technology improvements and associated cost increases as they bring new designs to market.

Automation has been an integral part of equipment design for many years, but new concepts such as digital transformation, Smart Manufacturing, Industry 4.0 and the Industrial Internet of Things (IIoT) are being increasingly applied in the manufacturing world to deliver competitive advantages.

This article focuses on what machine and equipment manufacturers (OEMs) can do to leverage these new concepts and how Edge Computing can meet their unique needs as well as their customers' requirements.

Edge Computing platforms offer OEMs possible, new revenue generating services and improved TCO.

The need for smart machines

In the same way that machine automation, using PLCs and PACs, revolutionized equipment design a generation ago, Smart Factories and Smart Manufacturing are evolving the industrial world again. Applying digital transformation concepts enables companies to operate at peak performance by leveraging the data collected by control systems and sensors. This approach provides real-time analytics to operators, inputs that help improve Overall Equipment Effectiveness (OEE), and data that can be collected and analyzed locally. Data can also be sent to the Cloud for deeper analysis in a variety of applications.

Applications can include optimized maintenance, supply chain agility, and increasing yield across multiple facilities engaged in similar production.

Machines and OEM equipment are fundamental elements of production. Smart Factories and Smart Manufacturing can only be achieved by Smart Machines operating as designed by their OEM or specified by the end user. Embracing digital transformation enables machine and equipment builders to enhance design and supports the development of new services around equipment performance and maintenance.

An important question is what is the best way to develop new generations of smarter equipment, or enable existing designs and deployments to meet the requirements that customers are demanding? Edge Computing is an approach that can solve many of the key design requirements.

What is edge computing?

Edge Computing comes in many forms and can be broadly defined as any computing that takes place outside the data center. With such a broad definition, it is not surprising that there are many confusing definitions that span both the IT industry and the automation and controls industry that we refer to as Operational Technology (OT).

Gartner, a major analyst firm, has published a simple topology that enables everyone to understand what type of Edge computing might be useful to them.

This topology image demonstrates an infrastructure technology stack that shows the types of servers, devices, or platforms that can be characterized as Edge Computing and where they reside from the physical endpoint “at the edge” of the data source.

It alludes to the types of computing power, collection, analysis, and data movement that is available outside the actual data center. Edge provides extremely important benefits for equipment manufacturers and their customers.

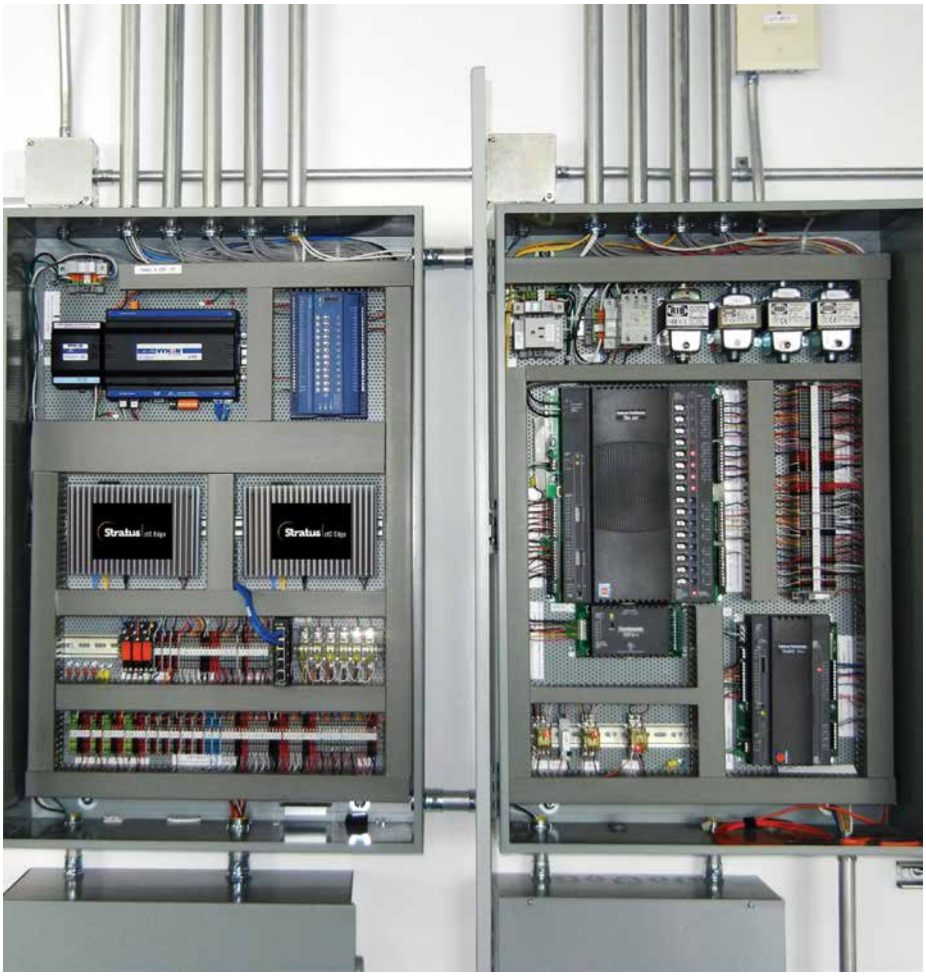
From this topology, it is easy to see that the Device Edge through the Compute Edge are applicable to machine and equipment builders. In practice, all machines and equipment today have aspects of the Device Edge with PLCs, and some have Gateway Edge devices.

In some respects, Industrial and panel PCs used by machines or equipment fall into this Gateway category. They may be the first “point of contact” for a device edge PLC. Yet IPCs have limited computing and analysis power or suffer from common reliability and usability issues that are similar to a typical PC or server that is not manufactured for harsh environments. So, other types of purpose-built Edge compute platforms are required to meet customer needs.

When it comes to the modernization of machine control and automation systems, it is the Compute Edge that should be the focus for equipment builders. Edge Computing delivers all the characteristics and capabilities necessary for machine and equipment manufacturers to enhance their current designs and transition to the delivery of even smarter equipment.

Edge computing technology

Edge Computing is a scalable modular technology that supports the development of standardized, modular software components and applications to increase efficiency.



SOURCE: STRATUS

Ruggedization is important along with eliminating downtime, and offering remote monitoring.

It can help enable equipment manufacturers’ existing applications—such as monitoring and control software—to be consolidated onto a single platform while enabling other critical applications to run on the same platform. This makes it easier to develop smart, Industrial Internet of Things (IIoT)-enabled machines and equipment, and to easily add future applications that support customers’ evolving Industry 4.0 and Smart Manufacturing demands.

When implemented, Edge Computing can facilitate a smooth evolution from the equipment of today to digitalized machines that are integrated into a customer’s operations. This includes multiple capabilities such as on-prem or Cloud connectivity to fully-integrated Smart Machines that embrace Digital Transformation without the need for complex retrofitting and redesign.

Edge computing for OEMs

While the Compute Edge category is quite broad, there are a number of key characteristics that narrow the types of functions that apply specifically to a machine or equipment manufacturer.

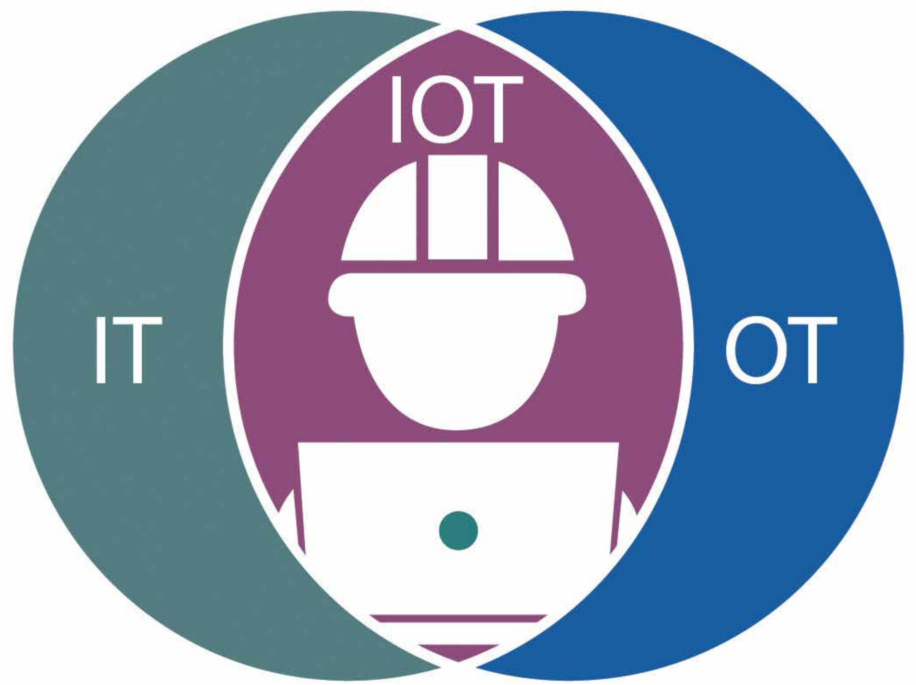
Edge Computing platforms must be capable of running existing control and automation applications in a modular way, without the need for significant re-architecting. Virtualization is a key technology. Essentially, each existing IPC can run as a “virtual IPC” or virtual machine on the Edge Computing platform.

This enables consolidation of all existing IPCs onto a single platform. None of these virtual machines are aware of the other virtual machines so all applications continue to run independently.

Modifying existing controls

With a virtualized Edge Computing platform, it is now possible to add much bigger degrees of flexibility to machine and equipment operation and monitoring. For example, with the traditional IPC/HMI approach, each station on a machine or piece of equipment is limited to what that IPC/HMI can display so only a single operator can monitor complex equipment from a single location.

This is not an ideal model. Using virtualization, equipment manufacturers can achieve increased flexibility for their customers by having multiple people remotely access data and applications at different stations. This autonomous model is preferred and provides customers more options.



Addition of new analytics

With virtualization it can potentially be easier to add new applications simply by creating a new virtual machine on your Edge Computing platform.

This paves the way to for companies to add new applications without impact to existing applications. This can include localized data collection, real-time analytics and data filtering before transport to external locations, such as a customer's data center, or to the Cloud, perhaps your own.This can also depend on such things as data privacy laws and, of course, assumes you have a scalable Edge Computing platform as needs expand.

Support for OT/IT convergence

This is perhaps a topic not often considered by machine and equipment builders, but it is increasingly important in Digital Transformation initiatives.

The control and automation applications that operate the machine are well understood by your design engineers and your customers who operate the machines. They are focused on the Operational Technology (OT).

The expertise to develop sophisticated analytic capabilities, perhaps involving machine learning (ML) and artificial intelligence (AI), plus the capability to securely transfer appropriate data to a data center or to the Cloud is often the domain of Information Technology (IT) experts.

Edge Computing platforms can support both OT and IT requirements. It is important to ensure that a platform that supports multiple types of operations applications is simple to deploy and maintain, and easy to manage by both OT and IT professionals.

New revenue opportunities

Many of the capabilities and new applications that Edge Computing platforms support create the possibility of new revenue generating services, or the optimization of existing service and support capabilities. For example, a trend that is beginning to emerge is the concept of the "machine as a service" or "equipment as a service", whereby the end customer pays based on time or usage instead of a traditional capital purchase. To successfully implement and maintain such a model, the machine or equipment manufacturer must understand the performance and maintenance profile of equipment, and have the ability to accurately collect and analyze the appropriate data.

By 2022, more than 50% of industrial IoT analytics will be performed at the edge, up from less than 10% today.*

- Gartner

Insightful. Real time. Distributed.

* Cool Vendors in Edge Computing, Gartner April 2018

Ruggedization

For a machine and equipment manufacturer, this is perhaps obvious, but Edge Computing platforms are supplied by a variety of vendors – not all of which are aware of the equipment's final operating environment. It is not just about ruggedization, but also about eliminating downtime, making maintenance and support as simple as possible, and offering remote monitoring.

Similarly, Edge Computing platforms in the OT world must be prepared to operate autonomously for long periods of time as often there may be no connectivity to the outside world.

Cost reductions

Ultimately, adopting Edge Computing only becomes viable if it meets the stringent cost constraints of the highly competitive markets in which equipment builders play. When evaluating Edge Computing platforms, it is important to consider capital costs as well as development and ongoing costs. In addition to the savings from things like virtualization, cost is a function of value.

More expensive platforms provide a much higher set of value and benefits than simple devices or gateways with lower computing power. This approach will reduce other costs such as manual monitoring, downtime, staff resources, and application efficiency.

Some of these costs can be less tangible, but as industries move to automation, Digital Transformation and related initiatives, such as Industry 4.0, Smart Manufacturing and IIoT, equipment manufacturers must consider future applications and changes in the customers' environment.

Summary

The machine and equipment manufacturer market is entering an evolutionary period that will bring as much change as the introduction of the PLC a generation ago. Edge Computing is a critical technology that will enable and ease this transition. Edge Computing platforms will play in integral role in expanding the traditional control and automation capabilities of equipment.

They will also provide the bridge for equipment manufacturers to embrace digital transformation initiatives for themselves and to integrate with initiatives of their customers.

Technology article by ***Stratus.***

View White Paper

Improving network availability while decreasing maintenance

A fully connected operation will only reach its full potential if network availability is assured. The use of "smart" network devices as part of a back-up power strategy can improve network availability, as companies move to a network model that harnesses standard, unmodified Ethernet and Internet Protocol (IP).

MANUFACTURERS NEED MITIGATION SYSTEMS, such as industrial uninterruptible power supply (UPS) devices, to help protect against power disruptions on industrial networks and resulting downtime.

The limitless potential of the Internet of Things (IoT) is changing the industrial world as we know it, with the collection of vast amounts of new data, seamless communications across the enterprise and more insight into operations than ever before.

But even the most powerful, connected operations are still dependent on one critical, centuries-old element: power.

Designing, deploying and maintaining a network infrastructure must include how to contend with the inevitable power disruptions that every plant experiences from both natural and man-made causes.

These disruptions can stem from extreme environmental conditions, vandalism, equipment failure and service provider issues. The proactive decisions made to address these risks will ultimately determine if operations continue seamlessly or if everything comes to an abrupt halt.

Several approaches exist, but each should be carefully evaluated in terms of its reliability in an industrial setting, how well it can protect network uptime and how it impacts operations including maintenance programs.

This article will discuss the need for back-up power in the context of today's increasingly connected industrial operations, review the options that are available, and examine the impacts they can have on operations.

SOURCE: PANDUIT

Designing, deploying and maintaining network infrastructure must include inevitable power disruptions.

Protect uptime in connected plants

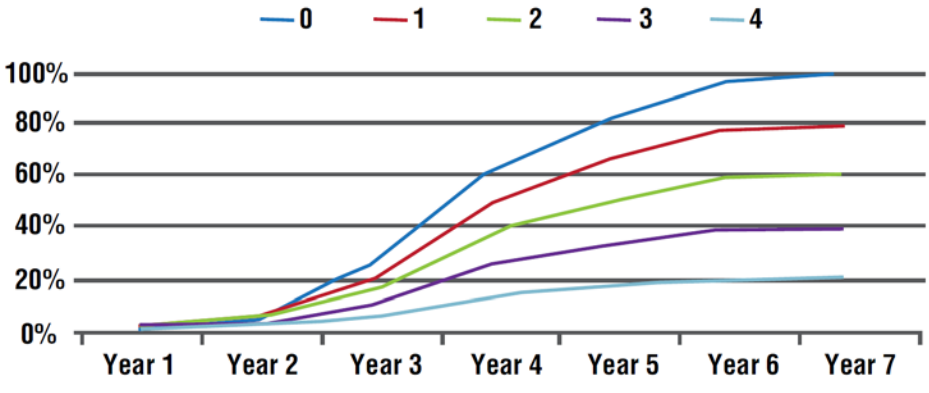
The use of multiple, disparate networks within an industrial enterprise is quickly becoming a primitive practice. Driven by both competitive pressures and opportunities to capture trillions of dollars of value from the IoT, industrial companies are moving toward a network model that harnesses the power of standard, unmodified Ethernet and Internet Protocol (IP).

This movement is driving a new level of connectivity among people, machines, systems, and devices, giving companies the ability to capture, view and report data like never before. It is also enabling greater communication to take place whether between an enterprise and a plant floor or across several plants spread out around the world.

According to I.H.S. Global/IMS Research, this rapid connectivity will continue, as 160,000 new industrial Ethernet nodes are added every day.

For all the benefits that industrial Ethernet offers, it also puts additional demands on manufacturers and industrial operators. Specifically, as a network infrastructure and plant floor operations become more interdependent, network uptime becomes absolutely critical. Whereas machine uptime and productivity went hand-in-hand in the industrial plant of yesterday, the information-enabled industrial plant of the future will be just as dependent on network availability as it is on machine availability.

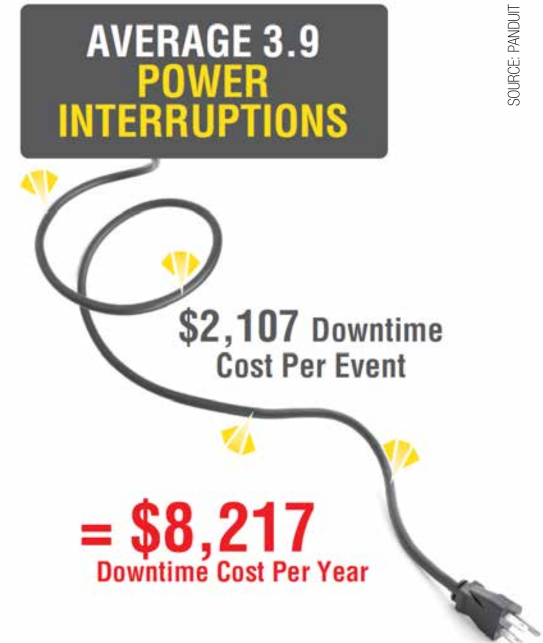
Because of this, a strong commitment to



SOURCE: PANDUIT

Cumulative failure rates by year based on the number of preventative maintenance intervals per year.

network uptime is essential. This includes taking steps such as using redundant devices, building in redundant paths to prevent single device network failures, and implementing a cable management and wiring strategy that ensures maximum data speed throughout the network. However, it also must take into consideration the power availability challenges a plant faces.



SOURCE: PANDUIT

Infographic comparing Uninterruptible Power Supply (UPS) Ultracapacitor vs. Battery.

Availability and power quality

When planning the deployment of network communications across the manufacturing zone and into the area/cell zones, contingencies will need to be in place for the power outages, "blips" and interruptions that will inevitably occur.

Even the briefest power disruptions can trigger the restarting of microprocessor-based devices, such as network switches, programmable logic controllers (PLCs) and human-machine interfaces (HMIs), which can take as long as three minutes to restart. While these devices are restarting, operations are at a standstill.

According to the Electric Power Research Institute (EPRI), the average downtime cost for a three-minute power interruption in the manufacturing sector is $2,107. EPRI also estimates that manufacturers experience an average of 3.9 utility-based power interruptions per year, putting the total annual cost at an average of more than $8,200.

In addition, many manufacturers experience other on-site power interruptions that do not originate with the utility provider and, therefore, are not reported. These local interruptions can be due to on-site transformer or distribution panel issues. Some facilities, especially in rural locations, report experiencing dozens of these on-site power disruption events every year.

While power outages that last several hours will be damaging to any company, the EPRI reports that 70 percent of utility-based outages are relatively brief, lasting less than five minutes. Additionally, more than 98 percent of on-site power disruptions are less than two minutes, according to the companies that report them. However, even with brief power outages, it only takes seconds for the disruption to cut off the energy supply to smart devices, forcing them to begin their lengthy restart process.

The only solution to the threat of power disruptions is to ensure there are continuous-power devices in place that will keep network devices and production operations running.

Consider the network infrastructure

A network architecture for industrial automation may recommend the use of a zoned network topology to create unique zones at every level of the organization, from an enterprise zone and a manufacturing zone, down to individual cell/area zones on the plant floor. Unlike a centralized topology with cabling originating from a central control room, this zoned approach allows for the selection of the network component types that are best suited to each environment or application. Additionally, implementing small virtual local area networks (VLANs) with managed industrial switches for each cell/area zone can segment and isolate low- and high-priority traffic for improved manageability. These cell/area zones require back-up power to ensure the dedicated switches and other network devices will continue running in the event of a power disruption.

Back-Up power options

Network switches and devices can be supported using either a centralized or localized back-up power approach.

A centralized approach could use an on-site generator, which is popular for data centers and increasingly being adopted in new factory construction. The biggest drawback with generators is a lack of continuous power support, meaning there is a need for an additional power solution to bridge the gap from when the outage occurs to when the generator begins providing power.

An alternative to the generator is a centralized uninterruptible power supply (UPS). Unlike a generator, a UPS device provides instantaneous power and does not require a bridge. Retrofitting a centralized UPS into an industrial environment, however, is an arduous task. It can require extensive new wiring and cabling distribution, which can be costly and time consuming.

A localized UPS – placed at each industrial switch, rather than stored in a central location – is a more practical solution for industrial environments. However, battery-based UPS solutions present challenges for use on the plant floor. Just as Ethernet technology must be resilient and adapted for use on the plant floor, a UPS also must be carefully selected to ensure it fits in with overall operations. Key considerations to evaluate before making an investment in a battery-based UPS device include:

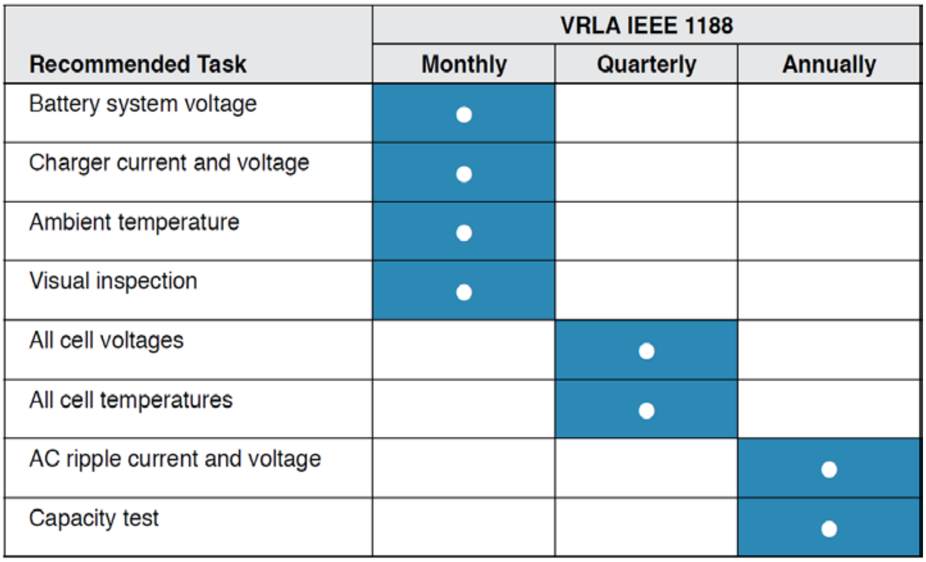
Battery Life: An industrial environment's harsh conditions can significantly reduce the battery life of a UPS. Batteries are prone to losing capacity in colder temperatures, and battery life can weaken significantly in warmer temperatures. Battery life is reduced 50 percent for every 15 degree increase above 77 degrees Fahrenheit. In short, a UPS battery's service life will likely fall short of its design life if a plant experiences hot and/or cold temperatures.

Maintenance Demands: Batteries used in indoor and outdoor manufacturing environments can be a burden on maintenance personnel.

Table 1 shows the multitude of recommended maintenance tasks for batteries. There are also the additional employee demands to order, stock and properly dispose of UPS batteries. Given the challenges operations and maintenance personnel face on a daily basis and the lack of personnel at most plants, battery maintenance is unlikely to get the full attention and support it requires.

SOURCE: PANDUIT

A fully connected operation will only reach its full potential if maximum network availability is assured.



Recommended Task	VRLA IEEE 1188		
	Monthly	Quarterly	Annually
Battery system voltage	●		
Charger current and voltage	●		
Ambient temperature	●		
Visual inspection	●		
All cell voltages		●	
All cell temperatures		●	
AC ripple current and voltage			●
Capacity test			●

SOURCE: PANDUIT

IEEE Standard 1188-2005 - IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications.

Device Management: Battery-based UPS devices typically only provide relay outputs or minimal indicators, such as single-color LED lights to show a battery's input power, charge status or fault condition.

More advanced battery UPS devices can deliver detailed information and control options, but these devices often require the use of proprietary software and a USB or serial port connection to a dedicated computer for continuous monitoring.

This lack of automation or interoperability with a networked operation is enough to discourage most manufacturers or industrial operators from making an investment to address these issues.

These combined challenges can lead to batteries not performing when they are needed most – during a power disruption event. As a result, batteries are blamed as the No. 1 cause of downtime in data centers.

Additionally, lead-acid batteries are categorized as a hazardous waste material with disposal costs. This additional cost contributes to the annual tonnage of hazardous waste materials, a figure that companies include in their annual corporate social responsibility reports.

Batteries pain in the UPS

An ultracapacitor-based UPS is specifically designed for the industrial network and addresses the challenges that have plagued battery-based UPS devices. Ultracapacitor UPS devices are built to endure harsh environmental conditions, have long lifespans, require no maintenance, and provide remote monitoring capabilities – reducing the total cost of ownership by 50 to 70 percent and significantly lowering the risk of downtime by 39% compared to battery-based UPS devices. This allows for the system back-up of network switches with greater confidence.

When comparing battery and ultracapacitor UPS devices, the first concern is whether they both provide power back up. The answer is yes, but not equally. Industrial managed switches are low power devices, drawing 5 to 15 Watts of power (less than 1 Amp). Both UPS options provide the necessary hold time, but batteries are "overkill" – typically delivering hours of backup time. Ultracapacitors are right sized for industrial network switches and also provide a host of other advantages.

For example, ultracapacitors are designed for a broad range of temperatures, including applications exposed to extreme outside temperatures (-40 to 140 degrees Fahrenheit). Ultracapacitors also do not experience a high level of degradation in hotter temperatures. This contributes to an ultracapacitor's long lifespan (10+ years) compared to a battery's one to five year lifespan.

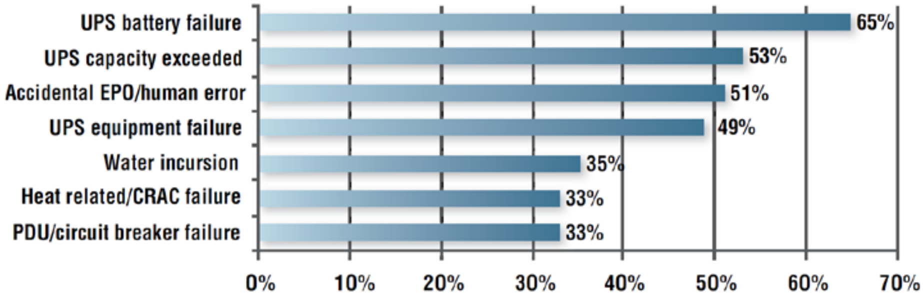
More importantly, ultracapacitors lower the risk of downtime because they eliminate batteries, which have proven to be unpredictable, maintenance-intensive and the leading cause of UPS failure. Manufacturers must conduct numerous preventative maintenance tasks when using batteries or face high failure rates. An ultracapacitor-based UPS, meanwhile, requires no maintenance. These advanced industrial UPS devices also can be remotely managed, minimizing the time and effort needed to monitor them, which reduces operational expenses compared to a battery-based UPS.

Remote device management allows all UPS devices to be monitored from a single location, an office laptop or a mobile device on the plant floor. This is all performed using standard tools instead of proprietary software. Battery-based devices, on the other hand, require an operator or technician to manually walk the floor, open each enclosure and inspect every battery's status. Remote device management can also be taken a step farther using simple network management protocol (SNMP) software agents or network-based devices. This can enable the monitoring of redundant power supply inputs, view the available load to predict the hold time and measure the ambient temperature in the cabinet.

Optimal network reliability

A fully connected operation will only reach its full potential if maximum network availability is assured. Just as the industry is turning to more integrated, data-driven technology to support better decision making in production operations, the use of "smart" network devices as part of a back-up power strategy should be implemented to improve network availability. This is best accomplished using a localized, Ultracapacitor UPS in each area/cell on the plant floor.

Designed to persist in taxing conditions, an Ultracapacitor UPS eliminates batteries, the No. 1 cause of UPS failure, helping reduce overall plant-floor network downtime. 39% decreased risk of failure, reduced maintenance, and a 50–70% lower total cost of ownership compared to battery-based UPS devices illustrate the quantitative benefits of an industrial UPS device, but the confidence in knowing systems are prepared for the next power disruption can prove both immeasurable and invaluable.



SOURCE: EMERSON

Emerson Network Power white paper: "Addressing the Leading Root Causes of Downtime" indicates UPS battery failure is the leading cause of downtime.

Technology article by ***Panduit.***

Visit Website

Root of Trust in EtherNet/IP devices using CIP Security

CIP Security for EtherNet/IP can assist manufacturers in preventing security breaches. The CIP Security standard requires authentication and integrity of EtherNet/IP messages. It also requires both Scanners and Adapters to be authenticated, and implements message encryption to ensure integrity and privacy.

CIP SECURITY PROVIDES CONFIDENTIAL communications between trusted entities, and disallows communication between untrusted entities, on an EtherNet/IP network.

However, no EtherNet/IP device can be secure without a mechanism for establishing trust. Key to any embedded security system, such as CIP Security, is the establishment of a Root of Trust (RoT) and effective protection of the certificates, passwords and keys of the Public Key Infrastructure (PKI).

Failing to provide a RoT in a CIP Security device can compromise the security of an entire manufacturing system. This article examines the various mechanisms for establishing that trust in a secure EtherNet/IP device.

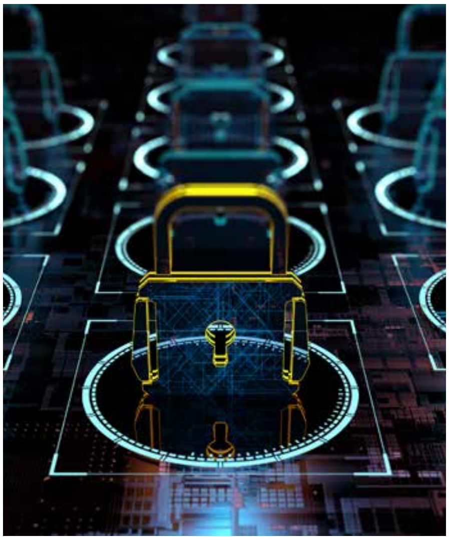
Factory floor device security

The requirement to keep confidential information confidential is hardly new. The spartans of ancient Greece encoded messages vertically on leather wrapped in a helix around a wooden rod. Without the right key, the correct sized rod, the message couldn't be decoded.

While we are now a long way from wrapping wooden rods with strips of leather, the need for confidentially exchanging messages hasn't changed. Today we rely on factory floor Ethernet systems to exchange confidential messages between controllers and end devices. In recent years, more and more of these systems have been extended to link enterprise and cloud applications to the factory floor.

Extending connectivity beyond the factory floor has increased the vulnerability of those systems to attacks. Attackers, sensing an opportunity, have shifted their attention from personal and business computers to the world of factory automation. Because the majority of these attacks are not publicized, no one knows for certain how many plants have had their servers locked, important data stolen, messages altered, and programmable controllers hijacked.

In the early years of Internet connectivity, it wasn't uncommon to have insecure controllers directly connected to the Internet. Over the years, these controllers have been removed, updated or replaced with newer versions that are more cybersecure. Most manufacturing installations have also added Defense in Depth (DiD) strategies that make it much more difficult to get to controllers and I/O networks from the outside.



Failing to provide a Root of Trust (RoT) in a CIP Security device can compromise the security of an entire manufacturing system.

What's often still open and vulnerable, though if you can get to it, is the inside or I/O network side of programmable controllers.

If you can get access to a manufacturing Ethernet network, you can often have free reign to create all kinds of havoc. There's generally nothing stopping you from accessing the controller tags over that network: turning pumps on or off; increasing motor speeds; or opening and closing valves.

In the past, there were a lot of barriers to getting access to these networks. You'd have to get past security gates and through guard houses and locked doors before you could plug into a control network. For those among us prone to mischief, it's now a lot easier with all the cloud connectivity and Internet of Things (IoT) devices (sometimes installed with little planning or forethought). Much of that IoT infrastructure has access to I/O networks, and sometimes isn't as rigorously protected by Defense in Depth strategies. Once an attacker gets in, they can attack the PLC from that soft underbelly, its I/O network communications, as well as play havoc with the I/O devices.

Even when strong cybersecurity protection is in place from the outside, factory floor systems can be compromised from the inside. Most facilities have an army of IoT vendors, automation vendors, technicians, system integrators, and corporate engineers who come onsite and knowingly or unknowingly bring viruses, malware, time bombs and worse into your plant and onto your critical I/O networks.

EtherNet/IP, the Ethernet implementation of CIP (the Common Industrial Protocol), was never designed as a secure communications transport. It is designed for ease of use and flexibility. Anyone can make connections to an EtherNet/IP Adapter and execute any operation, including a reset of the device. This makes EtherNet/IP a very insecure communications protocol.

In light of this relatively new environment, ODVA developed CIP Security for EtherNet/IP. CIP Security is a secure standard for the transportation of EtherNet/IP messages. It allows communication between trusted entities, and disallows communication between untrusted entities, on an EtherNet/IP network.

What is CIP Security?

CIP Security defines the security related requirements and capabilities of CIP devices and specifically for EtherNet/IP. It provides three benefits to a manufacturing system using EtherNet/IP:

1. *Data integrity*: It rejects data that has been modified during transmission.
2. *Authentication*: It rejects messages transmitted by untrusted entities.
3. *Authorization*: It rejects actions that an entity is allowed to perform.

To accomplish these objectives, CIP Security employs two standard IT cryptographic protocols: Transport Layer Security (TLS); and Datagram Transport Layer Security (DTLS). TLS is the standard cryptographic protocol used to secure internet communications and online traffic. CIP Security uses TLS to secure EtherNet/IP acyclic messages (explicit messages). DTLS is a version of TLS designed to secure UDP (User Datagram Protocol) messages. It is used by CIP Security to secure EtherNet/IP cyclic traffic (implicit messages).

But secure TLS and DTLS traffic is only possible if two entities trust one another. CIP Security for EtherNet/IP supports two

Supply Chain Integrity
Secure Boot
Tamper Protection
Root of Trust (RoT)
Access Authorization
Life Cycle Management

SOURCE: RTA

There are many definitions for Root of Trust but it can be thought of as providing confidence that: (1) your operating system is not compromised; (2) your certificates and keys have not been compromised and (3) your device memory hasn't been exploited.

mechanisms for entities to trust another: Pre-Shared Key (PSK) and X.509 certificates.

PRE-SHARED KEY (PSK): Pre-Shared Key is an uncomplicated and simple system that works well in small systems. A private key is known and shared by all the devices in a network. The key is used to encrypt messages. Any device that knows the private key is authenticated and can encrypt and decrypt messages. For added protection, the key is typically changed at some set interval, sometimes as part of a maintenance cycle.

X.509 CERTIFICATES: X.509 certificates are a standard way for two devices to securely communicate. The devices share their certificates. Each certificate identifies the entity authenticating the certificate. That entity can be the device itself (self-signed certificate), the vendor who manufactures the device, or some outside authority that is trusted by all the devices in a network. The public key in a certificate is used to send encrypted messages to the certificates owner who uses his private key to decrypt the message. A private key associated with the certificate should never be disclosed.

A fundamental design tenet of CIP Security is that not all devices on an EtherNet/IP network need the same level of protection. Some devices are less critical and some are more critical to an automation system. CIP Security defines two security profiles to provide that different level of protection:

1) The EtherNet/IP Confidentiality Profile provides secure communications by requiring authentication and data integrity for all EtherNet/IP messages. Devices that are not authenticated are unable to make a secure connection. Messages that fail the integrity check are rejected.

2) The EtherNet/IP Authorization Profile goes one step further than the Confidentiality Profile. It provides User Authorization. With the Authorization profile, an application requesting an action like opening or closing a valve would have to be authorized to take that action.

(It should be noted, however, that the EtherNet/IP Authorization profile is not currently part of CIP Security, and the specification describing how this is to be accomplished isn't available at the time of this writing.)

Devices that do not support CIP Security can coexist with devices that support the Confidentiality or Authorization Profiles.

CIP Security key management

CIP Security and all other key management strategies are completely undermined without an effective key management system.

Attackers can exploit under-secured systems to steal intellectual property, gain access to proprietary information about processes and products, utilize them as platforms to propagate further attacks, and even cause real world physical damage and harm to humans. Proper key management techniques must be practiced to make a CIP Security device difficult to penetrate.

Unfortunately, there is no perfect security system and no flawless mechanism to completely secure the confidential information and security infrastructure in a CIP Security device or in any electronic device.

All that can be done is to raise the bar for what is required by an attacker to penetrate a device and access any protected information and the cryptographic security keys. With upfront planning during product requirements and follow through during implementation, it is possible to raise the bar enough to dissuade most attackers.

Securing a CIP Security device, or any electronic device, begins with following basic security fundamentals. Some of the general techniques (which may or may not be practical for a specific device) include:

- Utilizing a tamper-resistant enclosure. Adding deadman switches or anti-tamper meshes that detect enclosure openings or other intrusions such as drilling. In devices where "high bar" security is required, the device would react to these intrusions with countermeasures, such as erasing cryptographic keys and other critical information.
- Implementing tamper-resistant circuitry to detect circuit board intrusions.
- Implementing a secure boot to authenticate firmware prior to execution.
- Using a microprocessor with a Trusted Execution Environment (TEE).
- Encrypting and storing critical information in secure storage memories.
- Implementing hardware-based random number generators to ensure truly random data encryption keys.
- Offloading cryptographic processing to hardware accelerators which are far more efficient than general-purpose CPUs and enable the generation of longer keys.
- Securing your remote update process to ensure that only factory-authorized code can execute.

All these practices are helpful, but the protection of your private key is paramount. Just as you would never leave home with the front door locked and the key in the lock, you wouldn't create a strong private key and not protect it.

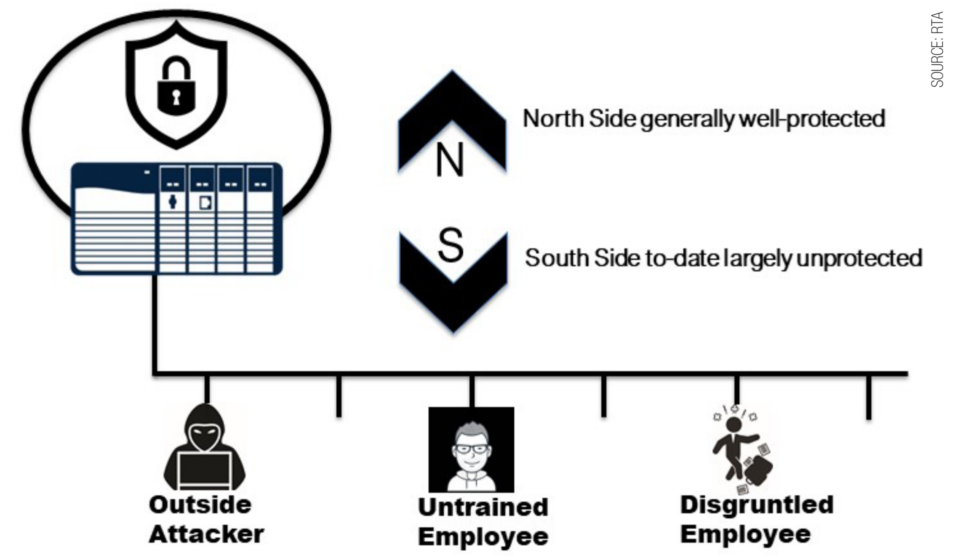
CIP Security depends on the use of strong encryption keys and the protection of those keys. CIP Security uses both symmetric and asymmetric encryption. Both encryption techniques are effective as long as the keys remains private. Encryption keys that are weak, or stored where an attacker can easily discover them, are likely to provide little real protection.

Common poor key management practices:

- Using encryption keys that are too short. An encryption key is simply an input to a mathematical algorithm that generates an encrypted message. It's possible (but not easy) for a hacker with adequate hardware to reverse the algorithm to generate the encryption key. Reversing the algorithmic process is more feasible with shorter keys.
- Using a flawed, non-standard, low entropy, random number generator to create a key.
- Storing an encryption key in application code, file or table.
- Storing an encryption key in file or table.
- Storing an encryption key with poor protection (XOR with weak data, etc.).
- Storing an encryption key with password-based encryption protection.
- Failing to secure debug ports so that an attacker can monitor program execution.
- Failing to provide an audit trail of who accessed what data and when.
- Failing to provide a tamper-proof, secure clock.

These poor practices make your device hackable and, if your device is subject to audit, may result in compliance failure. Devices requiring advanced protection and subject to audits should use an effective key management system that is designed for that purpose and which meets an appropriate NIST standard like FIPS 140-2.

Beyond developing a device that isn't subject to these poor practices, a well-designed CIP Security device must provide a resilient and effective Root of Trust. The RoT is the basis for performing critical


N
North Side generally well-protected
S
South Side to-date largely unprotected
Outside Attacker
Untrained Employee
Disgruntled Employee

SOURCE: RTA

A trusted execution environment (TEE) is secure area of a processor that is protected with respect to confidentiality and integrity. A TEE offers isolated execution, application integrity and confidentiality.

security operations such as generating digital signatures and encrypting and decrypting messages. A Root of Trust can be as simple and inexpensive as a master key stored in the device's non-volatile memory, or as complex and costly as a Hardware Security Module (HSM) whose sole purpose is to protect the Root of Trust from attackers.

Every CIP Security device vendor must decide what Root of Trust is appropriate for their device and how much additional cost in design, development and operating expenses are tolerable for their device.

Security organized around a software RoT is less expensive than a hardware RoT, which adds cost to the bill of materials, consumes precious circuit board real estate and increases complexity in development, testing, support and operations.

Software root of trust

Using a Hardware Security Module (HSM), some type of protected memory or other hardware add-on is sometimes infeasible in manufacturing devices. Adding hardware to a device can be impractical, cost prohibitive or unnecessary. In these cases, cryptographic keys and other critical information can be secured using a software Roof of Trust.

There are any number of approaches an embedded design might use to implement a software Root of Trust. Four common approaches follow.

Method 1: Hide Key in Plain Sight

Description: Store security keys as clear text in standard, non-volatile RAM. This mechanism relies on the inability of most attackers to: 1) penetrate the device internals, 2) access non-volatile RAM, and 3) identify which bytes are the device keys.

Why Use It?: Devices where vendors believe that consequences of an attack are insignificant can rely on this approach. Devices of this sort include simple input only sensors and other input only devices with largely inconsequential data. This approach is generally not appropriate for an actuator where an attacker can affect outputs that might control a process.

Limitations: This approach provides only minimal key protection and should be limited to devices that the vendor is certain will never be used for anything critical.

A determined attacker may be able to run the executable image in a VM, dump the RAM, sniff network traffic, decompile the executables…etc. and easily compromise the device. Access to the pre-shared key means the device has the key for all devices in the CIP Security zone.

This approach should never be used on a CIP Security network using pre-shared keys; a compromized device compromises the entire network!

Attack Surface: Large Cost: Minimal

Method 2: Let OS Worry About It

Description: Shift the burden of key management to the operating system and the OS vendor. Use the key management facility available in your embedded operating system. Many operating systems, including Linux and Windows, now provide secure key management.

Why Use it? Many operating systems now provide key management based on the Advanced Encryption Standard (AES), a specification for the encryption of electronic data created by the U.S. National Institute of Standards and Technology. Vendors are cautioned to thoroughly vet the key protection mechanisms of an operating system. A "name" OS may not offer any additional protection (and sometimes less) than other vendor self-implemented key protection strategies.

Limitations: The security mechanism for well-known open source operating systems are well-known. Attackers know the methodologies, vulnerabilities and weaknesses of these operating systems.

Some of these standard mechanisms require an Initialization Vector (IV) which must be secured. Having to secure an IV to secure secrets is no less of a problem.

Attack Surface: Varies with operating system
Cost: Minimal

Method 3: Multi-level Key Storage

Description: A master key known as a DEK (Data Encryption Key) or a KEK (Key Encryption Key) is used to secure the CIP Security private key or the entire certificate chain.

Why Use it? A DEK or a KEK master key is longer and stronger than the private key it encrypts. An attacker must first find the DEK or KEK and then use it to decrypt the private key. Either just the private key or the entire certificate chain can be secured with the master key.

Limitations: How to secure the DEK or KEK master key is an issue. Some vendors will likely choose to avoid the indirection of a DEK or KEK master key and protection of that additional key. They may instead choose to just focus on protection of the master key.

Attack Surface: Moderate Cost: Minimal

Method 4: No Key Storage

Description: Using Physical Unclonable Function (PUF) technology, security keys and unique identifiers are extracted from the innate characteristics of a semiconductor component. Like biometrics measures, these identifiers cannot be cloned, guessed, stolen or shared. Keys are generated only when required and don't remain stored on the system, hence providing a very high level of protection for the DEK or a KEK master key.

Why Use it? PUF keys are guaranteed to be unique and unclonable since they utilize the inherent randomness of the manufacturing process. No master key is ever stored. Low cost, easy to integrate and ultra-secure key protection. PUF is supported by ARM, Renessas and other silicon manufacturers.

Limitations: PUF technology must be licensed and maintained.

Attack Surface: Small

Cost: Minimal when included with your processor development system

Hardware root of trust

A Root of Trust in hardware often lends itself to a more secure solution for CIP Security devices than a software Root of Trust. A hardware Root of Trust strengthens the attack surface that must be overcome to compromise a device. However, it does that at increased cost and complexity over a software RoT

A hardware Root of Trust can be implemented as simply as performing key management in protected processor memory, using some isolated off-processor memory component for key storage, or implementing a complete HSM using a commercial Trusted Platform Module.

The advantages of HSMs in general include:

- Inaccessibility by systems outside the microprocessor ecosystem.
- Hardware accelerators for processor-intensive cryptographic functions.
- True random number generation.
- Secure clocks for applications where time is critical.
- Protected key management.
- Intrusion protection.

Of these advantages, hardware acceleration and true random number generation provide significant value. With software RoT, the processing of cryptographic algorithms can introduce latency into device communications and validating that a random number generator is producing truly random numbers can be challenging.

Method 1: Non-volatile Memory

Description: Encryption keys are stored alongside other protected information in a special non- volatile memory implemented solely for secrets. Secrets are deemed secure because the device firmware provides no mechanism for unauthorized access.

Why Use it? Implementation simplicity and lower cost development, production and support. It can be implemented with a firmware update and requires no modification to hardware. There is no change to software tool chain and it provides the ability to add security to legacy devices in the field.

Limitations: Requires extremely high-quality source code, open source and third-party libraries, as any flaw may compromise secrets. An attacker with physical access to the device can unsolder the non-volatile memory to discover its secrets.

Attack Surface: Large Cost: Minimal

Method 2: External Hardware Security Module

Description: A dedicated cryptographic module specifically designed for the protection of the embedded device secrets. Located off device, the module can be networked, attached, embedded in a PC server, or attached via USB. These types of modules address a broader scope of security needs but can provide the key storage and data encryption of an embedded system.

Why Use it? Cryptography is managed by an external provider.

Limitations: May be impractical in the embedded environment due to cost and latency issues.

Attack Surface: Small

Cost: Significant, although one module can support many embedded modules.

Method 3 – Onboard Hardware Root of Trust Device

Description: There are various types of hardware RoT devices offered by semiconductor companies marketed as hardware RoT devices. Some vendors offer a class of device known as Trusted Platform Modules (TPMs). Others provide similar devices under various trade and generic names. These modules are typically microcontrollers that securely store secrets and platform measurements to ensure that the platform remains trustworthy. Secrets are confined within a security-hardened, tamper-resistant IC, and thus hard to get at directly, even with an unlimited budget and expertise.

Why Use it? Hardware RoT devices significantly increase the resources and technical expertise necessary to compromise a device. They can simplify aspects of firmware development through a well-documented and well-supported common API.

Limitations: Unit cost and footprint can be problematic for some simple devices. May lead to complacency from over reliance on the device; the "I don't need to worry about it" affect.

Attack Surface: Small

Cost: Varies with the manufacturer

This discussion should not conclude without discussion of bootloader and firmware managers. These devices, such as the STM X-CUBE-SBSFU, provide for secure transfer for microcontroller firmware. The update process is performed in a secure way to prevent unauthorized updates and access to confidential on-device data. Many robust off-the-shelf solutions are available. They validate the integrity of the firmware running the CIP Security device but can be cumbersome and intimidating for field personnel.

Summary and conclusion

The number of well-documented attacks on cities, transportation systems and other public infrastructure systems continues to grow. The level of concern regarding securing manufacturing systems has now reached the C-suite. It is becoming apparent to executives and investors in manufacturing organizations that the growing deployment of Ethernet, cloud communications and IoT applications is increasing their vulnerability to attack.

Unlike with enterprise devices, there aren't a few dominant suppliers that can be relied upon to secure the factory floor. The nature of manufacturing is such that manufacturing devices are designed to accomplish widely disparate tasks and have vastly different computing platforms, operating systems, code complexity and functionality. These devices are now beginning to be equipped with PKI-based security features like CIP Security, but the encryption and authentication underlying all these systems can be completely undermined if proper key management at the device level isn't enforced.

Unfortunately, there is no perfect security system and no perfect mechanism to secure the confidential information and security infrastructure in manufacturing devices, or in any device. All that can be done is to raise the bar for what is required by an attacker to penetrate a device and access protected information and security keys.

Further complicating all this is that embedded devices are mass produced. There may be thousands to millions of identical devices. If a hacker can build a successful attack against one of these devices, the attack can be replicated across devices at many manufacturing sites in different geographies and industries.

The key question is "how high to raise the bar?" The bar can be raised so high that cost and complexity rise to a point where the device becomes essentially unusable. Conversely, the bar can be so low that attackers come to know the weakest link in every manufacturing system.

There are many ways to think about how high to raise the bar for a specific device, but two questions predominate:

- What are the consequences of compromised security? It may be a nuisance if a temperature sensor is compromised but devastating if the device is integral to critical infrastructure in applications like nuclear, medicine or transportation.
- Does the device contain critical and highly valuable data?

When the stakes are high enough, attacks are multi-phased, multi-year efforts carried out by large, well-funded teams of attackers. In these situations, it's not about protecting a device from malformed IP packets and DoS packet floods. Cyberterrorists will invest significant resources in gathering information on the device or devices prior to the attack, and then mount sophisticated and complex attacks.

Unfortunately, most embedded design engineers won't know for certain where and how their products are used, and the level of protection appropriate for a specific application. Devices tend to be incorporated in diverse industries, across geographic boundaries and in unusual applications.

In these circumstances, designers should opt for selecting a Root of Trust model that is affordable yet offering the most comprehensive and highest level of protection appropriate to the typical application of their device.

*John S Rinaldi, President, **Real Time Automation.***

Visit Website

Gateway integrates with PROFIBUS DP

The smartLink HW-DP gateway provides controller-independent access to PROFIBUS DP networks.

Industry 4.0 connectivity is available for new and existing PROFIBUS DP networks. This compact tool can be integrated without affecting the operation of existing installations and therefore enables Industry 4.0 connectivity for a wide variety of PROFIBUS DP installations.

The smartLink HW-DP V1.01 enables access to process, asset, and diagnostic data from PROFIBUS devices and HART devices connected to PROFIBUS remote I/Os. Furthermore, it allows for secure data export to any system inside and outside the company's own network.

Users in the process industry who want to adapt their communication architecture to modern IoT use cases can integrate smartLink into existing plants in a simple and cost-effective manner.

The data which is relevant for optimization processes is made available via open, standardized interfaces such as HART IP and FDT for subsequent applications This means that any HART IP clients, such as Emerson's AMS Device Manager or the Android app DevComDroid, can be used to set parameters for, monitor and evaluate field devices via these open communication standards.

SOURCE: SOFTING

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

Key features include configuration, parameterization and plant asset management using standard industry tools:

- Independent of configuration tools
- Centralized parameterization of PROFIBUS and HART field devices directly from the control room using HART IP and HART over PROFIBUS
- Access to Plant Asset Management applications for field devices configuration based on FDT/DTM and EDDL standards (acyclic master)

Softing Industrial Automation

Visit Website

First type R Profinet robot cable

ETHERLINE ROBOT PN Cat.5e cable complies with new type R standard for PROFINET cables on robots.

Until now, robot application designers have had to decide whether to use a data cable for linear, horizontal travel distances, typical in cable chains, or a data cable that is better suited for torsion. The main reason is that the cable types have a different interior structure.

While relatively short lay lengths are preferred for cables for horizontal travel distances to achieve lower bending radii in the cable chain, long travel lengths are a priority for torsion cables.

A large number of conventional Ethernet cables have not been able to properly cope with this combined challenge. Furthermore, there were no uniform industry standards for robot-compliant Ethernet data cables. The PROFINET user organisation has now drawn up the necessary specifications in close consultation with AIDA (the Automation Initiative for German Motorists).

The new “type R” describes two-pair Cat.5e industrial data cables, which must withstand numerous electrical and mechanical requirements and provide longevity when used in industrial robots. The mechanical requirements are enormous. A type R-compliant cable must endure all of these tests before it is ranked as a robot-compliant cable according to PROFINET: 5 million vertical torsion cycles at ±180° per metre, 5 million cycles in the horizontal cable chain at accelerations of up to 10 m/s² and speeds of 3 m/s over a travel distance of 5 m, an additional 1 million bends in the alternating bending test according to EN 50396 at a bending radius of just 7x outer diameter.

SOURCE: LAPP

Ethernet cables used in industrial robots need to withstand torsion paired with horizontal linear movements.

Lapp

Visit Website

Smart grid gateways with LTE support

Ixxat SG-gateways enable communication between industrial automation devices and energy networks.

SOURCE: IXXAT

Data exchange simplified between energy automation networks and industrial Ethernet systems.

The Ixxat SG-gateway line offers new versions including a 4G/LTE modem for cellular connectivity as well as 4-port Ethernet switching capabilities, giving users energy networking options for substations and power plants.

For energy networking use cases including mini-RTU, gateway and remote access, Ixxat SG-gateways are used in energy automation, e.g. in modern power plants and in large scale energy consumer installations.

The SG-gateways are used for different purposes, and can connect energy control networks with industrial automation devices, enable remote access, act as gateways between different protocols and enable the development of IIoT applications.

With the new, integrated 4G modem and extensive protocol support, the Ixxat SG-gateways are designed for easy digitalization of small, outlying energy distribution stations.

The 4G CAT1 connection offers 10 Mbps downstream and 5 Mbps upstream communication with low latency, high network coverage and a universal data channel– independent of wired Ethernet, DSL or fiber optics. 4G can be used as either the main or backup communication channel.

All supported IP-based protocols, including IEC 61850, IEC 60870-5-104, MQTT and OPC-UA, can be transmitted over the wireless link.

The 4G modem can also be used as an independent communication channel for e.g. device maintenance and alarm messages (SMS or MQTT), enables straightforward implementation of predictive and remote maintenance applications.

Ixxat

Visit Website

AI and machine learning applications

Mouser has expanded its range of products and resources aimed at developers of AI and IoT solutions.

SOURCE: MAXIM

Maxim MAX78000 incorporates two 32-bit microcontroller cores & ultra-low-power accelerator in a single package.

New products include a machine vision development kit from ADLINK suitable for industrial applications, a low-power dual-core processor with neural network accelerator from Maxim Integrated for use in battery-powered IoT devices, and a face recognition development kit from NXP Semiconductors.

The ADLINK Technology Vizi-AI machine vision AI development kit comprises a SMARC computer module based on an Intel Atom processor and an Intel Movidius Myriad X vision processing unit (VPU). Software support includes the Intel OpenVINO software development kit, which includes several ready-to-use, pre-built machine learning models. A collection of ADLINK neural model development tools is also included. With the kit, developers of industrial machine vision applications can rapidly prototype solutions that detect production line problems and deliver actionable insight to improve operational efficiencies.

The Maxim MAX78000 processor incorporates two 32-bit microcontroller cores and an ultra-low-power network accelerator in a single package. The microcontroller cores, one an Arm Cortex-M4 and the other a RISC-V co-processor, provide system control and fast loading of the 442-kByte weight convolutional neural network. The device is highly optimised for battery-powered IoT edge devices and is capable of conducting inference 100 times faster and consuming 1/100th of the power of conventional microcontroller devices. An evaluation kit for the MAX7800 is also available.

Mouser

Visit Website

WiFi 6E tri-band router

The first WiFi 6E router from NETGEAR delivers high-speed WiFi with support for the 6 GHz band.

With the Nighthawk RAXE500, the company has announced its first WiFi 6E router. With speeds of up to 10.8 Gbit/s, the latest addition to the Nighthawk series heralds a new era of fast connections on the new 6GHz band that is free of interference and overload.

Until the introduction of WiFi 6E, wireless routers were limited to the 2.4GHz and 5GHz bands. The new WiFi 6E WiFi standard solves these congestion problems by adding a previously unavailable 6GHz WiFi band that can be used to transmit WiFi signals and connect to a wide variety of devices with faster speed and reliability.

The new third 6GHz band will dramatically increase the capacity of networks to support more devices simultaneously.

"The proliferation of WLAN applications in the last few decades initially claimed the 2.4 GHz band and then finally the 5 GHz band with WiFi 4, 5 and 6," explained Phil Solis, Research Director at IDC. "With the opening of the 6GHz band by regulators around the world, WiFi 6E networks will give devices the leeway they need to use large channels with higher average data rates and lower latency even in dense and congested areas."

SOURCE: NETGEAR

New era of fast connections is available on a 6GHz band that is free of interference and overload.

With this latest technology, the new WiFi 6E router expands the home WLAN many times over for more performance, capacity and experiences in a new world of uninterrupted connectivity.

Simultaneous remote learning, video conferencing and 4K / 8K video streaming are no longer a problem. With the new 6GHz band, the new Nighthawk RAXE500 offers faster speeds, smoother streaming, less interference and improved latency for devices and WiFi -hungry applications.

NETGEAR

Visit Website

TSN Gigabit Ethernet PCIe NIC solution

The combination of TSN with OPC UA provides key technology to realize the IIoT.

ASIX has launched a new TSN product, AXM57104 Quad Port TSN Gigabit Ethernet PCIe NIC Card, which can help converge IT and OT networks for industrial communication applications.

The AXM57104, compliant to PCI Express base spec. v2.1 Gen1, supports enhanced TSN functions included the timing and synchronization compliant to IEEE 802.1 AS-Rev/AS and IEEE 1588V2, the Forwarding and Queuing of Time Sensitive Streams (FQTSS). It specifies Credit-Based Shaper (CBS) compliant to IEEE 802.1Qav, the Time-Aware Shaper (TAS) compliant to IEEE 802.1Qbv, and the Per-Stream Filtering and Policing (PSFP) compliant to IEEE 802.1Qci. AXM57104 also supports 32 synchronous I/O pins, one pulse per second (PPS) output and is field upgradable via In Application Programming.

The AXM57104 is a cost-efficient PCIe to TSN solution for IIoT applications to enable TSN functions on industrial automation platforms, Fieldbus over TSN gateways and converge the non-real-time IT network and real-time OT networks including industrial Ethernet protocols such as EtherCAT, PROFINET, EtherNet IP, etc.

SOURCE: ASIX

Cost-efficient PCIe to TSN solution for IIoT applications to enable TSN functions on industrial automation platforms.

Time Sensitive Networking (TSN) technology is a set of IEEE 802.1 standards under development by the IEEE TSN Task Group and is an OSI model Layer 2: Data Link Layer (DLL) communication technology. TSN provides hard real-time, deterministic, and low latency capabilities on standard Ethernet to meet the real-time data transmission requirements for industrial communication.

ASIX

Visit Website

Modular all-in-one industrial PCs

Industrial PCs offer powerful technology, modular extendibility and integrated Profisafe functionality.

With its all-in-one solutions, Phoenix Contact offers industrial PCs with a completely closed die-cast aluminum housing (IP65), designed for modern operating concepts.

The latest sensor generation makes it possible to operate the screen even when wearing thick gloves. The glass surface increases the robustness of the capacitive technology with regard to aggressive cleaning agents and sharp objects.

Displays with full HD resolution offered in 15.6-inch, 18.5-inch and 21.5-inch versions facilitate the visualization of simple sequences up to complex production processes, while specific details can be displayed via gesture control. The AIO devices contain powerful Intel Core i5 processors so that they are capable of implementing tasks that are very demanding, such as machine control, process visualization, or quality assurance. The AIO devices are space-saving, as their completely closed housings eliminate the need for additional casings. The screw holes on the rear of the housing are dimensioned according to the VESA-100 standard, which makes it possible to mount the device directly to the machine or system. It is also possible to install the device on a support arm or stand using the appropriate rear cover. Upon request, a keyboard module can be used to expand the industrial PCs by up to 11 buttons or switches, which can be used for USB connections, key switches, or other functions. If the user would like to incorporate the operating solution into an existing Profinet network, a gigabit-capable switch with Profinet and Profisafe function is available to forward the data. A signal light can also be easily integrated into the operating concept.

SOURCE: PHOENIX CONTACT

Despite high-performing CPUs, industrial PCs are designed to be fanless, increases their range of applications.

Phoenix Contact

Visit Website

Edge computing package

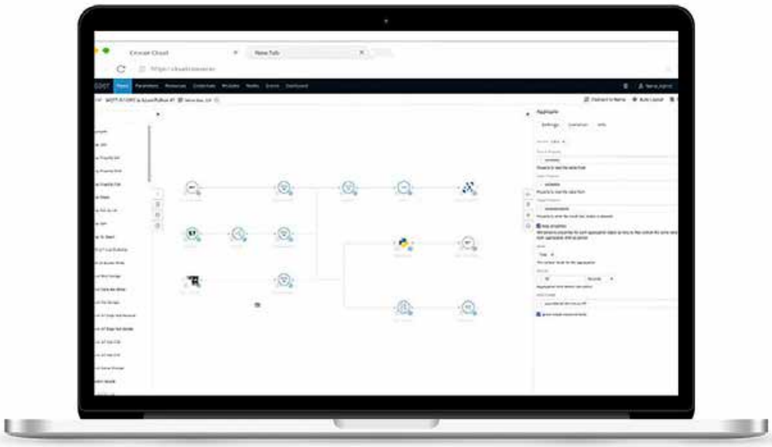
Crosser and TTTech Industrial announced partnership to offer customers a unique edge computing package.

Crosser's edge analytics software is available pre-installed on Nerve Blue, the edge computing platform from TTTech Industrial. This bundle simplifies industrial IoT operations by combining software management and powerful streaming analytics with ease of use.

Industrial customers are increasingly searching for ways to access valuable data from their machines without having to overhaul running systems. The goal for machine builders and plant operators is to use this wealth of data in real-time to make significant improvements in productivity and efficiency on the shop floor. The Nerve and Crosser bundle provides a comprehensive platform for connecting machines, analyzing data and remotely managing software. Crucially, these features are available via intuitive user interfaces that require no specialist knowledge.

Together, Nerve and Crosser enable industrial users to develop and scale by rolling-out new services to machines and plants around the world with the click of a button. Users benefit from the inherent flexibility and openness of the platforms, which can be connected to any data source, any service, and any cloud. Additionally, customers are given the freedom by Nerve and Crosser to be truly independent, with the ability to choose hardware or applications from their preferred vendor.

"We are proud to cooperate with TTTech Industrial and Nerve Blue. Together, we truly simplify the journey for industries that strive for digital smartness," says Crosser's Director, Mikael Samuelsson.



SOURCE: TTTECH

Bundle simplifies industrial IoT operations by combining software management and powerful streaming analytics .

TTTech Industrial and Crosser

Visit Website

Industrial wireless family product line

Industrial wireless family has been expanded with the introduction of new access points.

SOURCE: ANTAIRA

All three wireless products are suitable for a variety of wireless applications including long-distance deployments.

Antaira Technologies' industrial wireless family has been expanded. The ARS-7235-AC series is an industrial IEEE 802.11a/b/g/n/ac wireless LAN access point with added router capabilities. It is designed for enterprise and industrial wireless applications. The device allows a user to position the wireless antennas in a better signal-broadcasting location for improved wireless coverage and signal strength.

The ARX-7235-AC-PD-T is an industrial outdoor IP67 metal housing IEEE 802.11a/b/g/n/ac wireless access point/client/bridge/repeater with router capabilities, and is IEEE 802.3af/at PoE PD compliant. It is designed with an extended operating temperature range of -40°C to 70°C for outdoor applications to withstand extreme weather conditions and temperatures.

Antaira's new ARY-7235-AC-PD is an industrial outdoor IP67 plastic housing IEEE 802.11a/b/g/n/ac wireless access point/client/bridge with router capabilities, and is IEEE 802.3af/at PoE PD compliant. It is designed for industrial and enterprise wireless access applications. This unit has a standard operating temperature range of -40°C to 50°C, which can withstand harsh environmental conditions such as dust and debris.

No matter which industrial wireless product is chosen, all three wireless devices are embedded with Qualcomm IPQ4029 SoC chipset which has dual band 2.4GHz/5GHz concurrent, and supports high-speed data transmission of up to 867Mbps. In addition, all three wireless products are capable of operating in different modes, which makes them suitable for a wide variety of wireless applications including long-distance deployments.

Antaira Technologies

Visit Website

Edge controllers optimize data usage

Combines the advantages of decentralized cloud architectures with those using a local network architecture.

SOURCE: WAGO

Edge devices can take over data mining from controllers that require low latency and a high level of determinism.

In many cases, transferring data from machines and systems directly to a cloud solution is resource-intensive and not feasible due to the low latency often required for industrial applications. Edge computing has established itself because it combines the advantages of decentralized cloud architectures with those using a local network architecture.

Edge devices can take over data mining from controllers that require low latency and a high level of determinism. Collected data can be evaluated directly, displayed graphically and made available to the cloud. WAGO debuts two new edge devices designed for this: the Edge Controller and the Edge Computer.

The new Edge Controller (752-8303/8000-0002) utilizes an ARM Cortex-A9 quad-core processor and offers an selection of interfaces, including two ETHERNET ports, one CANopen port and two USB ports. It also has a serial interface and four digital inputs/ outputs for connecting local devices or sensors. Project design for the Edge Controller can occur in the familiar e!COCKPIT environment, so it fits seamlessly in WAGO's automation ecosystem.

The new Edge Computers (752-9400 and 752-9401) feature a 1.91 GHz quad-core Atom processor and are equipped with standard Debian Linux. An SSD disk can be installed to expand the existing 64 GByte flash memory for very large data volumes. Despite their extended temperature range from –20°C to +60°C, the Edge Computers do without a fan and are very compact, simplifying integration. Standard software, such as Node-Red, can be used on all edge devices.

WAGO

Visit Website

Touch sensing for IoT node HMIs

MCUs offer best-in-class power consumption combined with flexible power modes for lower average power.

SOURCE: RENESAS

Ultra-low power and touch interface MCUs are designed for industrial and HMI IoT applications.

The expansion of Renesas' 32-bit RA2 Series microcontrollers (MCUs) with 20 new RA2L1 Group MCUs increases the RA Family to 66 MCUs.

The general-purpose RA2L1 MCUs use the Arm Cortex-M23 core operating up to 48 MHz. The RA2L1 MCUs are supported by the easy-to-use Flexible Software Package (FSP), which offers software and hardware building block solutions that work out-of-the-box.

The ultra-low power and innovative touch interface of the RA2L1 MCUs are designed for home appliance, industrial and building automation, medical and healthcare, and consumer human-machine-interface (HMI) IoT applications.

The RA2L1 MCUs are designed for ultra-low power consumption, with several integrated features to lower BOM costs, including capacitive touch sensing, embedded flash memory densities up to 256 KB, SRAM at 32 KB, analog, communications, and timing peripherals, and safety and security functions.

In many battery-powered applications, the MCU spends most of the time in a low-power standby mode waiting for an internal or external event to wake-up the CPU and process data, make decisions and communicate with other system components.

When benchmarked for power consumption, the RA2L1 MCU was certified with an EEMBC ULPMark score of 304 at 1.8V, verifying its best-in-class power rating. Users can now minimize power consumption close to the standby levels to extend battery life.

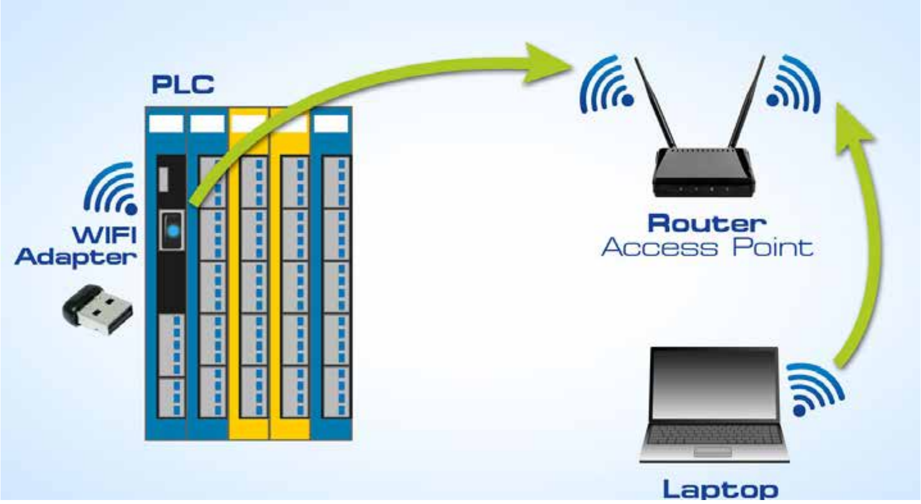
The advanced capacitive touch IP in the RA2L1 MCUs provides enhanced operability for a variety of touch and touchless system implementations.

Renesas Electronics

Visit Website

WLAN wireless communication adapters

WLAN adapters simplify wireless CPU communication, as well as programming a CPU from a wireless device.



SOURCE: SIGMATEK

By connecting to the router with a laptop, all service functions are available.

With the compact WLAN adapters WiFi-C and WiFi-Pro from SIGMATEK, efficient wireless CPU communication is enabled. Using the WiFi adapters, the network cable can be easily replaced. Automation can therefore be economically integrated into the existing in-house IT system – if no wired infrastructure is available.

An additional advantage is a simple, comfortable online connection for servicing. The adapters operate in the 2.4 GHz frequency band and can be used worldwide without limitations. The Plug & Play WiFi-C device, which functions as a client, is already available. WiFi-Pro is planned for further development, whereby the adapter can be configured as a client or access point.

The WiFi-C can be easily connected to any existing infrastructure with a wireless router. By connecting to the router with a laptop, all service functions are available – naturally with the usual transmission security and specific password.

When using the WiFi-Pro, you can set whether it is used as a client, as with WiFi-C, or as an access point. With the latter, no additional network is required to create a connection between the control and the laptop as well as tablet or smartphone.

Both variations support the USB A interface. With the integrated engineering platform LASAL, the control can be comfortably programmed over a virtual connection. Ready-to-use classes and visualization components for selecting access points as well as entering passwords are available.

SIGMATEK

Visit Website

Historian software secure data access

Production workers can now more quickly access data using the FactoryTalk Historian Site Edition software.

New enhancements to the latest version of the FactoryTalk Historian Site Edition (SE) software make it the most reliable and secure release of the software to date.

To help users more quickly access data, the software now uses client-side connection balancing and failback. This balances user connections across multiple servers, instead of connecting them all to a primary server.

In larger systems, where many people are making queries for data that can go back several years, this can reduce server demand to help users access data in seconds instead of minutes.

The FactoryTalk Historian SE software also now offers user-based archive scheduling. This function allows users to schedule historical archiving during down periods or off hours. It reduces the risk that archiving occurs during critical processes, when it can affect server performance and slow access to data.

To better secure production data, all subsystems within the FactoryTalk Historian SE software are now configured to run under least-required privileges. This minimizes the potential damage unauthorized users can do if they penetrate a system.

SOURCE: ROCKWELL

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

The software also now supports the latest operating systems, such as Windows Server 2019. This can extend the life of systems, which can be especially valuable for operators of validated systems in regulated industries.

The new FactoryTalk Historian SE software release is part of PlantPAx 5.0, the modern distributed control system (DCS) from Rockwell Automation, and uses the same FactoryTalk Services as other software included in the DCS. This minimizes the potential for conflict or errors and helps make installation easier.

Rockwell Automation

Visit Website

Radio integrates with 5G RAN software

Integration of radio Unit with Radisys' 5G NR OpenRAN software enables OpenRAN deployments.

Benetel has integrated its Radio Unit (RU) with Radisys' 5G NR OpenRAN software to enable OpenRAN deployments for communication, industrial and private network markets. In addition to the new 5G solution, the two companies executed a licensing agreement for Radisys' LTE software to allow its distribution with Benetel's eNodeB radio platforms.

The pre-integrated Radisys and Benetel 5G NR solution can be deployed in both Non-Standalone (NSA) and Standalone (SA) 5G modes, providing operators with deployment options. The companies have recently demonstrated a successful 5G SA call over the n78 5G band using the integrated solution.

Radisys has designed its 5G NR software suite to support both NSA and SA, providing an easy migration path from LTE/LTE-Advanced deployments to 5G. It is targeted at mmWave and sub-6 GHz frequencies. Radisys' 5G NR software suite is compliant with 3GPP Release 15 and O-RAN standards with a strong roadmap to evolve towards Release 16. Radisys also provides 5G Core Network functions as defined by 3GPP.

SOURCE: BENETEL

The companies have recently demonstrated a 5G SA call over the n78 5G band using the integrated solution.

"Service providers and enterprises want to build their networks with open and disaggregated software and hardware components to reap the benefits of a multi-vendor ecosystem," says Munish Chhabra, Head of Software and Services Business, Radisys. "With Benetel, we are providing a pre-integrated OpenRAN solution that enables operator and enterprise customers to accelerate network deployments to deliver new services and generate new revenues."

Benetel

Visit Website

IoT gateway: process instrumentation

Sitrans CloudConnect 240 provides a second data channel completely independent of the control system.

In the process industry, field instrumentation is a central source of data, when it comes to digitalization. The Sitrans CC240 IOT gateway establishes a second data channel, which makes field level data that was previously hidden available to the user – without adversely affecting the existing control technology.

The system creates a direct connection between the field device and IT or the cloud and reads not only basic process values but also identification, configuration, and diagnostics parameters – for any HART device of Version 5 or later. The system then makes this data available via an OPC UA server or the Siemens MindSphere IoT-as-a-Service solution.

The data is harmonized in line with the Namur Open Architecture information model. This creates a standard perspective on the installed base - regardless of the technology and manufacturer - which means that digital applications can be created for the first time, for both on and off-premise environments. Asset monitoring and management can be implemented, particularly for smaller plants.

Sitrans CC240 supports the connection of up to 64 devices and has an on-board web server with the necessary configuration options and management views so that additional tools are not required.

Connectivity means it can be integrated into existing systems. OPC UA can be used to transfer field device values and data directly to automation or IT systems, for performing calculations or analyses outside the actual control task. The connection to MindSphere supports the distributed use of several Sitrans CC240 systems for monitoring globally distributed assets on a central instance.

SOURCE: SIEMENS

IoT gateway for the process industry can transmit data from any HART-based field devices to the IT world.

Siemens

Visit Website

Time Sensitive Networking package

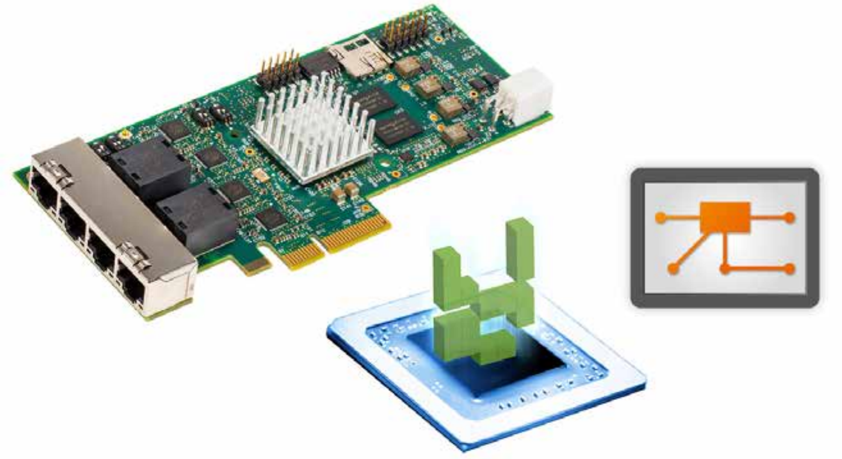
A complete starter package is new available for building, configuring and testing TSN networks.

This starter package combines IP and software, so companies can immediately implement and test TSN with their applications. TSN is an open standard supported by industrial automation vendors. The TSN starter package is offered in three variants, designed to suit every evaluation project. It is available for 6 months evaluation, 12 months evaluation or prototyping. Customers working on prototyping projects can benefit from permanent licenses for the reference design and configuration software, enabling long-term use of the starter package in TSN test networks.

TTTech Industrial's TSN starter package consists of an evaluation board, an IP core and associated software that together provide a stable hardware platform for the integration and evaluation of TSN Ethernet functionality.

The board can be used to implement bespoke configurations on an FPGA and can serve as a 4+1 port switch to build TSN networks configurable using browser-based software. The software plans and configures any TSN standard compliant network/device. It allows the modelling of topologies, addition of streams and deployment of configurations for TSN networks.

Further devices can be added to this network and made available for configuration. TSN starter package components support the core TSN mechanisms of time-synchronization (IEEE 802.1AS) and time aware shaping (IEEE 802.1Qbv), as well as other mechanisms such as frame preemption (IEEE 802.1Qbu), SRP enhancements (IEEE 802.1Qcc) and seamless redundancy (IEEE 802.1CB).



SOURCE: TTTECH INDUSTRIAL

A complete kit enables maximum configuration flexibility while also eliminating much of the technical complexity.

TTTech

Visit Website

EtherNet/IP to BACnet communications

Protocol translator integrates between EtherNet/IP & BACnet IP/MSTP-based building management systems.

Many processes in a factory are depending on proper monitoring and control of the building where the factory equipment is installed. In the same way, lighting in the building can be aligned with working hours to reduce energy waste or to improve the management of emergency situations.

With the new Intesis protocol translator from HMS Networks, system integrators can easily integrate any Ethernet/IP-based PLCs, such as Rockwell Allen-Bradley PLCs models, with any BACnet BMS. The With a capacity of up to 1200 data points, the gateway is a BACnet IP/MSTP server/slave on one side and an EtherNet/IP adapter on the other, featuring independent Ethernet ports. The gateway has been BTL-certified for BACnet and carries the UL mark in order to guarantee the highest communication and quality standards. It is also ODVA pre-certified thanks to its inbuilt Anybus CompactCom module.

A free Intesis MAPS configuration tool for all Intesis protocol translators offers a very intuitive configuration process for system integrators. With MAPS, integrators are helped further in their projects by providing valuable EDE files for the BACnet integration, as well as EDS files and configuration reports for usage in EtherNet/IP PLC configuration tools like Rockwell´s Studio 5000 software.

SOURCE: HMS NETWORKS

New gateway offers bi-directional communication between EtherNet/IP PLCs and BACnet controllers.

Extending the new Intesis Factory-to-Building protocol translator family, the new EtherNet/IP - BACnet gateway is another example of HMS combining technologies. In the gateway, Anybus CompactCom and Intesis communication technologies are used for industrial and building-oriented communication respectively, both proven in millions of installations worldwide.

HMS Networks

Visit Website

Expanded line of industrial RTUs

A rugged, flexible solution for monitoring and control in extreme environments

Red Lion Controls announces the expansion of its SixTRAK line of industrial RTUs with the launch of STIPm-8460 powered by the Red Lion Workbench, which uses an IEC61131-3 compliant editor and runtime engine. Designed for applications that need increased processing and communication speed and storage, the new RTU provides the flexibility and reliability that customers require and expect from Red Lion to monitor and control equipment.

The ability of the ST-IPm-8460 to operate in harsh and hazardous locations is achieved through UL Class I, Div certification, an ABS listing, and an operating temperature range of -40°C to 70°C.

The combination of ST-IPm-8460 and Red Lion Workbench can easily support large, complex projects across multiple devices. The Red Lion Workbench provides customized control, standard language support, powerful debugging/monitoring tools, project automation, and controller redundancy.

Whether an application monitors a few data points or thousands, the ST-IPm-8460 can be easily configured to meet the needs using Red Lion’s EtherTRAK-2 I/O modules.

SOURCE: RED LION

Maxim MAX78000 incorporates two 32-bit microcontroller cores & ultra-low-power accelerator in a single package.

Available for private labeling, the ST-IPm-8460 also offers dual power inputs and support for redundant Ethernet networks for increased uptime, while a multitude of communication ports and supported protocols enable connectivity to a variety of field devices.

The technologies enable customers worldwide to gain real-time data visibility that drives enhanced productivity.

Red Lion Controls

Visit Website