May/June 2021 124
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking & IIoT

Product Showcase

Industrial Connectors & Cabling

Page 23

Single Pair Ethernet technology update 8

The C7015: bringing multi-core in IP 65/67 directly to the machine

www.beckhoff.com/c7015

Up to four cores in IP 65/67: with its extremely robust, fanless C7015 ultra-compact Industrial PC, Beckhoff as a specialist in PC-based control technology offers the possibility to install a high-performance Industrial PC in a highly compact design directly at the machine. Versatile on-board interfaces enable connection to the cloud or to other networks. The integrated Intel Atom® CPU with up to four cores allows simultaneous automation, visualization, and communication in demanding industrial IP 65/67 applications. In addition to classic control tasks, the C7015 is ideally suited for use as a gateway to connect machines and plant sections – and can even handle complex preprocessing of large data volumes thanks to its high processing power.

3 x LAN, 2 x USB, Mini DisplayPort and integrated EtherCAT P port

New Automation Technology **BECKHOFF**

GET CONNECTED…

Visit our new website at: www.iebmedia.com

Comprehensive coverage of SPE

Welcome to the May/June 2021 issue of the Industrial Ethernet Book with comprehensive coverage of Single Pair Ethernet, our first-ever Connectors and Cables Showcase and also a 20-page special report on Industrial Cyber Security.

Single Pair Ethernet is one of the defining technologies as industry moves forward with more potential solutions that address the advanced needs of Industrial Ethernet networks.

Check out our coverage starting on page 8. SPE is an emerging technology that implements data communications using only one pair of copper wires, and is enabling new possibilities by combining Ethernet and TCP/IP communications. In this special report, IEB offers comprehensive coverage of what industry leaders have to say about SPE, and insight into what lies ahead. A broad range of initiatives demonstrates the potential of the technology, and illustrates how SPE together with Industrial Ethernet can enable space- and cost-efficient solutions from the cloud to field-level devices.

According to Bob Voss, Senior Principal Engineer at Panduit, SPE has become the great equalizer. By enabling the entire OT network to be Ethernet and replacing legacy protocols with a universal language, SPE lays the foundation for a higher functioning, more secure network that addresses the looming business continuity risks that get a little closer each day.

Starting on page 21, IEB presents a Product Showcase on Industrial Connectors and Cabling. Learn about the key technology megatrends that are shaping the newest generation of Industrial Ethernet connectors and cables.

Michael Kasper, Director of Accessories Products at Siemens AG told IEB that innovations are being driven by the idea that industrial data communication is not a topic for specialists, but a topic that can be mastered by everyone.

And finally, starting on page 43, we look in-depth into Industrial Cyber Security via a Special Report on how manufacturing companies are leveraging new technology to protect machinery, networks and corporate data.

Recent news of Ransomware attacks underscore the need for industry to strengthen its levels of protection from all types of threats. Technology solutions are providing companies ways to eliminate network vulnerabilities, strengthen security and develop ways to bridge the gap between OT and IT networks. Although the focus is often on external attacks, internal threats can be just as damaging to industrial networks.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **July/August 2021.**
Deadline for editorial: July 15, 2021 **Advertising deadline:** July 25, 2021
View Industrial Ethernet Book website for latest news and products: www.iebmedia.com.

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

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

Industrial network market to grow by 6% in 2021

Annual report from HMS Networks projects continued growth for industrial networks, despite pandemic, and industrial network market shares to grow by 6% in 2021.

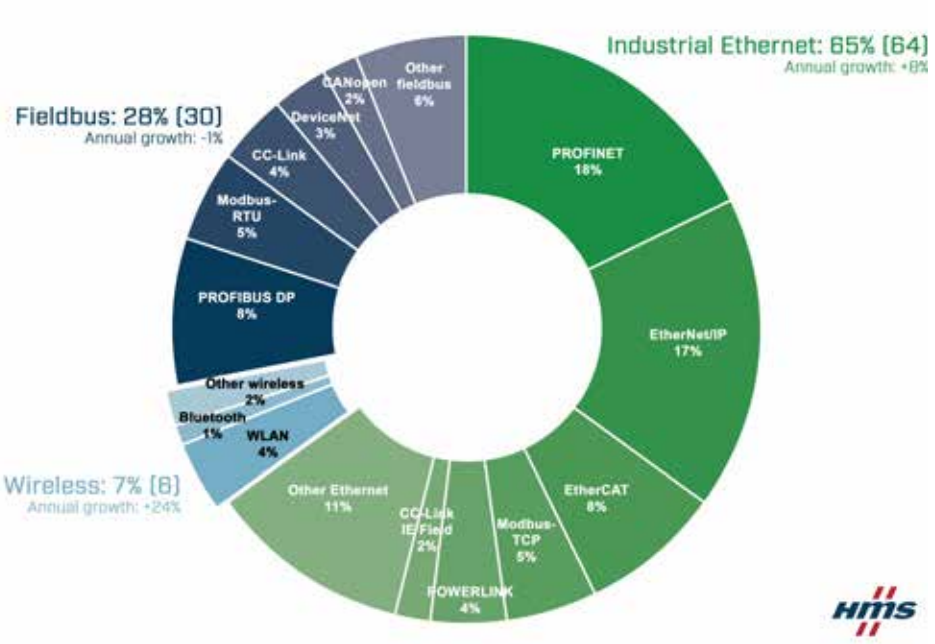
EVERY YEAR, HMS NETWORKS CARRIES OUT a study of the industrial network market to analyze the distribution of new connected nodes in factory automation. This year's study shows that, despite the Corona pandemic, the industrial network market is expected to grow by 6% in 2021.

Industrial Ethernet still shows the highest growth, compared to fieldbuses and wireless, and now has 65% of new installed nodes (64% last year), while fieldbuses are at 28% (30). Wireless networks continue to climb and are now at 7%. PROFINET passes EtherNet/IP at the top of the network rankings with 18% market share compared to 17%.

HMS Networks now presents their annual analysis of the industrial network market, focusing on new installed nodes within factory automation globally.

As an independent supplier of solutions within Industrial ICT (Information and Communication Technology), HMS has a substantial insight into the industrial network market. The 2021 study includes estimated market shares and growth rates for fieldbuses, industrial Ethernet and Wireless technologies.

The study concludes that the industrial network market is showing signs of regained stability and HMS expects the total market to grow by 6% in 2021.



Market shares 2021 according to HMS Networks – fieldbus, industrial Ethernet and wireless.

Industrial Ethernet growing steadily

Growing by 8%, Industrial Ethernet continues to take market share. Industrial Ethernet now makes up for 65% of the global market of new installed nodes in Factory Automation (compared to 64% last year). EtherNet/IP and PROFINET are fighting for first place, but this year PROFINET passes EtherNet/IP at the top of the network rankings with 18% market share compared to 17%.

EtherCAT continues to perform well globally and now matches the leading fieldbus PROFIBUS at 8% market share. Modbus TCP is next at 5% market share and together with fieldbus brother Modbus RTU, these Modbus technologies now account for 10% of the market, confirming their continued importance in factory installations globally.

Fieldbus decline halted

The ongoing fieldbus decline reported by HMS in recent years is almost halted with a fieldbus decrease of only -1% in 2021, as factories tend to stick to existing technologies to a higher degree in uncertain times, such as during the pandemic. Fieldbuses are now at 28% market share of the total amount of new installed nodes (30% last year). PROFIBUS is still the clear fieldbus leader at 8% followed by Modbus-RTU at 5% share and CC-Link at 4%.

Wireless is here to stay

Wireless continues to grow rapidly at a rate of 24%. Wireless now has 7% market share but the market still awaits the full impact of 5G in factories.

With ongoing global activities about wireless cellular technologies as enablers for next level smart manufacturing, HMS expects that market demand will increase for wirelessly connected devices and machines to be included in the less cabled and flexible automation architectures of the future.

Smart manufacturing networks

"Industrial network connectivity for devices and machines is key to obtain smart and sustainable manufacturing, and this is the main driver for the growth we see in the industrial networking market," says Anders Hansson, Chief Marketing Officer at HMS Networks. "Factories are constantly working to optimize productivity, sustainability, quality, flexibility and security. Solid industrial networking is key to achieving these objectives."

Regional network variations

EtherNet/IP and PROFINET are leading in Europe and the Middle East with PROFIBUS and EtherCAT as runners up. Other popular networks are Modbus (RTU/TCP) and Ethernet POWERLINK. The U.S. market is dominated by EtherNet/IP with EtherCAT gaining some market share. PROFINET and EtherNet/IP lead a fragmented Asian market, followed by strong contenders CC-Link/CC-Link IE Field, PROFIBUS, EtherCAT and Modbus (RTU/TCP).

Scope

The study includes HMS' estimation for 2021 based on number of new installed nodes within Factory Automation. A node is defined as a machine or device connected to an industrial field network. The figures represent HMS' consolidated view, considering insights from colleagues in the industry, our own sales statistics and overall perception of the market.

Anders Hansson, Chief Marketing Officer, ***HMS Networks.***

Visit Website

New tools to find, fix and prevent costly OT security threats!

Whilst attacks on Operational Technology systems are becoming more frequent, companies are looking for ways to eliminate network vulnerabilities and bridge the gap between OT and IT. Although the focus is often on external attacks, internal threats can be just as damaging and more likely.

Procentec, the global leader in diagnostic and monitoring solutions, has released four major solutions that will help you to:

1. Control what software is installed on your decentralized network
2. Spot any sudden and potentially critical changes to your devices
3. Facilitate the onboarding, training and reassignment of technicians
4. Create an effective line of defence against internal and external intrusions

CLICK HERE TO DISCOVER HOW THESE SOLUTIONS WILL STRENGHTHEN YOUR NETWORK SECURITY

PROCENTEC
Member of the HMS group.

For more information visit procentec.com or contact
Global Sales Manager Jonathan Machin at jmachin@procentec.com.

CIP Security supports resource-constrained EtherNet/IP devices

ODVA announced CIP Security, the cybersecurity network extension for EtherNet/IP, has added support for resource-constrained EtherNet/IP devices including device authentication and data confidentiality.

CIP SECURITY CAN NOW PROVIDE DEVICE authentication, a broad trust domain, device identity via Pre-Shared Keys (PSKs), device integrity, and data confidentiality for resource-constrained devices such as contactors and push-buttons. Additionally, a narrow trust domain, user authentication, and policy enforcement via a gateway or a proxy are available options.

Despite the progress brought about by Industry 4.0 and the IIoT, a large portion of the installed nodes in automation applications are still not using Ethernet. Limitations including cost, size, and power have historically been a hindrance to EtherNet/IP pushing out to the edge of the network.

The recent integration of single pair Ethernet has opened up the door to overcoming lower-level device constraints and ultimately to expanding the footprint of EtherNet/IP. Adding simpler devices to EtherNet/IP allows for the benefits of additional remote diagnostics, asset information, and parameterization capability. The addition of more nodes to the network within the context of IT/OT convergence makes device level security a fundamental need to ensure that indispensable assets and people are protected from physical harm and monetary loss.

The new CIP Security specification has added a Resource-Constrained CIP Security Profile in addition to the EtherNet/IP Confidentiality and the CIP User Authentication Profiles. The Resource-Constrained CIP Security Profile is similar to the EtherNet/IP Confidentiality Profile, but is streamlined for resource-constrained devices. The same basic security aspects of endpoint authentication, data confidentiality, and data authenticity remain. Access policy information is also included to allow a more capable device, such as a gateway, to be used as a proxy for user authentication and authorization of the resource constrained device.

Visit odva.org to obtain the latest version of The EtherNet/IP Specification including CIP Security.

Implementation of CIP Security for resource-constrained devices requires only DTLS (Datagram Transport Layer Security) support instead of DTLS and TLS (Transport Layer Security), as it is used only with low-overhead UDP communication.

"The continuous updating of CIP Security, including the recent addition of new security features for resource-constrained devices, provides EtherNet/IP devices an enhanced defensive posture to help protect against malicious industrial network intrusion," stated Jack Visoky, EtherNet/IP System Architecture Special Interest Group vice-chair.

The protections offered by CIP Security are now available for EtherNet/IP networks via a resource-constrained version of CIP Security that includes fewer mandatory features. This ensures that devices with the smallest power, size, and cost budgets can be secure and enjoy the communication and control advantages of being connected to an EtherNet/IP network.

EtherNet/IP for in-cabinet resource-constrained devices

The *EtherNet/IP™ Specification* has also been enhanced to allow vendors to bring the network to resource-constrained devices in-cabinet, including push buttons and contactors. Cost, size, and power restrictions have historically limited the usage of EtherNet/IP at the edge, where many nodes are still hardwired.

However, the continued decrease in the cost of semiconductor chips has enabled increased connectivity of simple devices, as evidenced by the rapid expansion of the Industrial Internet of Things (IIoT). The sustained, strong growth of EtherNet/IP combined with accelerating IT/OT convergence has made it possible to deploy EtherNet/IP within cabinets on lower-level automation devices such as contactors and push buttons.

The inclusion of resource-constrained devices within cabinets on an EtherNet/IP network is enabled by recently published enhancements to the specification including the physical layer In-Cabinet Profile for EtherNet/IP along with low overhead UDP-only resource-constrained EtherNet/IP communication. Resource requirements have been reduced via enhancements such as an IT friendly LLDP node topology discovery mechanism, auto-commissioning support, and auto-device replacement support. Additionally, a specification for a new select line circuit facilitates the efficient delivery of system wide sequential commands.

The EtherNet/IP in-cabinet bus solution reduces interface components through use of single pair Ethernet (IEEE Std 802.3cg-2019 10BASE-T1S) and reduces node cost via multidrop cabling that spans a single cabinet with one interface per device and one switch port that supports many devices.

Cost is reduced via cables using composite network and control power to eliminate separate parallel runs. The select line for topology eliminates configuration switches by enabling discovery based on relative position and allows for direct connection with programming tools during assembly for parameterization.

Technology reports by ***ODVA****.*

Visit Website

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADI Chronous™

Industry's Lowest Power **10BASE-T1L** Portfolio

Tailor your system architecture with ADI's PHY and MAC PHY solutions:

- Long reach 10BASE-T1L connected instruments for distances up to 1,700 m
- Ultra-low power consumption enables optimization of system power budgets
- ADIN1100 enables robust connectivity within field switch devices
- ADIN1110 enables flexible processor selection within field instruments

Visit analog.com/ADIN1100 and analog.com/ADIN1110

Single Pair Ethernet update: possibilities and applications

A coalition of industrial companies are working toward a single vision, and backing Single Pair Ethernet with the goal of making SPE technology the infrastructure basis that will make the Industrial Internet of Things (IIoT) and Industry 4.0 possible.

SOURCE: SPE PARTNER NETWORK

Support for the T1 Industrial interface according to IEC 63171-6 as a uniform Media Depended Interface (MDI) as defined by the ISO/IEC JTC 1/SC 25/WG 3 and TIA42 in 2018 is the combination of standards that are driving forward development of Single Pair Ethernet cable and connector solutions.

SINGLE PAIR ETHERNET IS AN EMERGING technology that describes the transmission of Ethernet over only one pair of copper wires. Along with implementing data transmission using Ethernet communications, SPE enables a simultaneous power supply of terminal devices via PoDL (Power over Data Line).

SPE is in the process of developing slim cabling/connection solutions that reduce weight, save on space and make it possible to create an infrastructure for Industrial Internet of Things applications by combining Ethernet and TCP/IP communications.

The miniaturized SPE standard interface for industrial applications, T1 Industrial style according to IEC 63171-6, has a goal of efficiently reaching every sensor and actuator in the field with slim SPE cables. The entire cabling becomes simpler, and can also be installed much faster.

In this report, IEB offers comprehensive coverage and the perspective of industry leaders, along with a picture of how SPE is moving ahead. A broad range of initiatives demonstrates the potential of the technology, and illustrates how SPE together with Industrial Ethernet can enable space-saving and cost-efficient solutions from the cloud to field-level devices.

Developing SPE ecosystem

Tools to drive industrial automation forward

TE Connectivity considers Single Pair Ethernet (SPE) the next generation Ethernet connector because it's different from the current standards in every way. It uses different semiconductors and cables, and the connector itself is different too; it's basically part of an entire ecosystem.

"The standards for SPE are different. For example, the traditional 40 meters shielded Ethernet T1 standard for SPE isn't long enough to meet the distance requirements in industrial networks, and often the transmission rate is lower. But the long distance SPE standard T1L using the shielded twisted pair cable type cover 1-1.5 kilometers, far better than the traditional 4 wire and 8 wire implementations with a range of about 100 meters," Ruud van den Brink, product manager for industrial communications at TE Connectivity, told the Industrial Ethernet Book recently.

He added that the SPE connectors are also different. For example, consider an IP20-based connector. It has two pins, a board connector and a cable connector, and supports the IEC63171-6 standard. Then there's a M8 hybrid connector (an IP67 connector).

The four contacts are what make it a hybrid; two contacts are used for data transmission, and two are used for auxiliary power up to 400-watts. Using power over data line (PoDL) protocols would get you only one-eight of that total.

TE as a founding member of the SPE Partner Network has teamed up with many industry players pushing the IEC63171-6 standards in the SPE eco system.

SOURCE: SPE PARTNER NETWORK

Technical standards and norms relevant to connection technology relating to Single Pair Ethernet (SPE)

		IEEE 802.3						IEC 11801		TIA		
		cg T1S	cg T1L	bw	bp	ch	bu	-3 Am1	-2 Am1	-568.0-D-2 (TR-42.1)	-568.5 (TR-42.7)	-1005-A-3 (TR-42.9)
Status		✓	✓	✓	✓	TBD	✓	TBD	TBD	TBD	TBD	TBD
Data transmission properties		10MBit/s/ 25m	10Mbit/s 1000m	100MBit/s 15m	1,000MBit/s 15 / 40m	<10,000MBit/s 15m	60W max.					
IEC 63171	-1	✓*	✓*	not specified	not specified	not specified	not specified	✓	✓	✓	✓	not specified
	-2	✓	✓									
	-3	✓	✓									
	-4	✓	✓									
	-5	✓	✓									
	-6	✓*	✓*					✓	✓	✓	✓	
Other connectors				✓	✓	✓	✓					✓
Relevance to												
As a general rule: application-specific requirements are being defined by user organizations in particular, not by means of the standards (see the following table)	Industry	✓	✓	–	○	–	✓	–	–	–	–	✓
	Generic cabling	–	–	–	–	–	–	✓	✓	–	–	–
	Buildings	–	✓	–	○	–	✓	–	✓	–	✓	✓
	Process	–	✓	–	–	–	○	○	–	–	–	✓
	Automotive	✓	–	✓	✓	✓	✓	–	–	–	–	–

** In the IEEE 802.3 cg standard, those are referred to as connectors that "may be used"*

✓ relevant ○ partially relevant – not relevant

Unique technology

Current industrial automation systems were built up out of different network structures, each with a different communication standard attached to it. Because the standards are different across networks, gateways are required to help "translate" those communications so machines can seamlessly exchange information. The gateways and various communications standards add delay to the communication and limit transparency.

According to van den Brink, SPE technology is designed so that all machines across the network "talk" in the same language: Ethernet. This is eliminating the need for translation between various communication standards.

SPE connectors and cables are simpler in build-up by reducing complexity and costs,; it offers a scalable (Ethernet) foundation to go beyond previous limited speed and the advantages of interoperability.

"SPE is a new standard making its way into the industrial space with obvious benefits in the industrial automation sector and in the industrial internet of things (IIoT)," he said. "Both require increasingly complex systems yet are built on an outdated legacy of multiple communication standards. At TE Connectivity, we believe SPE is essential to helping IIoT drive industrial automation forward."

Technical benefits

SPE enables cross-network real-time communication without any loss in information so that industrial engineers can build an all Ethernet more streamlined, unified automation ecosystem that's complements the traditional Industrial ethernet solutions.

The benefits of SPE are many, and include:

- Allowing barrier-free communication from the sensor to the cloud
- Providing movement freedom to applications
- Making miniaturization possible with power over data line (PoDL) and hybrid connector solutions (high power single wire)
- Facilitating an open ecosystem
- Allowing real-time, high-speed communication connections up to 1Gb/ second and cable length up to 1,000 meters for 10Mb/second

Impact of SPE technology

"SPE helps accelerate the trend toward transparent communication from machine to machine and machine to human. This allows for real-time, high-speed and secure Ethernet communication," van den Brink stated.

"If you look at the networks topology today, traditional ethernet (4 and 8 wire) is being used and addressed by Mini I/O, by M8, M12 or RJ45. On the factory floor—there's far less Ethernet used, mostly due to implementations with traditional bus and serial communications. With that part of the network implemented with SPE, one transparent Ethernet based network can be built."

Performance & Security

SPE forms a foundation for innovation

According to Bob Voss, Senior Principal Engineer at Panduit, SPE is the great equalizer. By enabling the entire OT network to be Ethernet and replacing legacy protocols with a universal language, SPE lays the foundation for a higher functioning, more secure network that addresses the looming business continuity risks that get a little closer each day.

"It may seem counterintuitive, but one of the biggest drivers for increased adoption of the latest SPE technologies will be the aging workforce. A lot of OT network functionality on the edge of the network is run on legacy protocols, which also poses a few big problems," Voss said.

He added that the knowledge to operate, diagnose, troubleshoot, all the care and feeding stuff, for those aging protocols is locked inside the heads of even older engineers. Their collective retirements are creating a growing skills gap that does not really have a solution. Once this older generation decides they rather be laying on the beach with a piña colada than be on call to fix OT issues ad hoc, you are going to have a serious business continuity issue as well.

"OT networks do two important jobs: they take care of the profit-making assets of the business – machines, process skids, etc. - and occupancy safety and comfort within a building," he concluded. "If these things

SOURCE: SPE PARTNER NETWORK

Seven companies including HARTING, TE Connectivity, HIROSE, Würth Elektronik, LEONI, Murrelektronik and Softing IT Networks formed the founding members of the SPE Industrial Partner Network. Total membership has now grown to 47 companies, as they continue to work collectively on SPE technology.

start malfunctioning and can't be fixed by onsite staff, it can put your entire operation in jeopardy."

Single Pair Ethernet benefits

Voss said there are a number of things that the standards and developments community got right with SPE.

Technical benefits

- Extreme distance: SPE can create Ethernet links up to a kilometer in length – 10 times what I can do with 4-pair Ethernet, plus the option of supplying power
- Provides a significant speed increase – SPE replaces protocols running at 31.2kb/s with 10 Mb/s speeds
- Utilizes a simple, robust media that's easy to field terminate
- Ability to support proven topologies like point to point and multidrop that we use in OT networks today
- Massive increase in network security – replace vulnerable older protocols with IP networking

Operational benefits

- SPE instantly adds value to the enterprise by allowing OT to become an integral part of a single-protocol, seamless network. This is a huge IoT enabler.
- IoT brings more information forward than just what's mission critical, it provides contextual data that can optimize operations. But if all that data is on different networks, it may not be of much help.
- SPE solves this by allowing for enormous, rich data streams to be federated and accessed at the exact moment you need it to make a critical decision.

Security solutions

According to Voss, SPE isn't cyber vulnerable, unlike some of the legacy protocols.

"Sometimes when I speak on this topic people will push back and say something to the effect of 'I don't care if someone breaches the edge of the network and sees something like what our kiln temperature is.' And while that may be true, the fact is that the cyber vulnerability at the edge isn't that third parties can see non-sensitive data, it's that they'll exploit these compromised areas to work their way back up the network." Voss said.

SPE excels in this scenario because Ethernet opens the doors to the full IP security suite - VLAN, segmentation - and all the other cutting edge security that isn't available with legacy protocols.

"I like to say that older protocols rely on 'security through obscurity,' a notion that if no one knows what they are looking at that they won't tamper with it," Voss added. "Unfortunately, cybercrime is a big business these days and taking this type of lax position to security is an enormous risk."

Progress and overall impact

According to Voss, if we were to plot SPE on the diffusion of innovation bell-curve, it'd show that we're still in the early adopter phase. But there is a determination to continue making progress, even if it's one industry at a time.

"For example, we're going to hit a big milestone this year in the processing industry with Ethernet APL - a process industry optimized instantiation of SPE and IEEE 802.3," he said. "Given the combustible nature of petrochemical, oil and gas, and other common industry materials, getting the Ethernet-APL standard right is equal parts important and difficult."

To that point, Ethernet-APL is the result of a collaborative effort among four different standards bodies and a "who's who" of 12 automation manufacturers. When the initiative was announced, the goals and timing were very ambitious, with target dates in June 2021 to

have APL compliant products and performance testing protocols available. The effort put into the development is paying off because, as of now, timetables are still intact, drafts have been submitted, and the standard is being widely embraced across the process industry.

Key next steps

Voss believes that adoption of SPE will gain compounding momentum as more and more use cases and case studies emerge. Automation manufacturers aren't going to adopt new tech for the sake of new tech; they need to see the value first.

SPE provides a wide range of security and deployment benefits while solving the industry skills gap problem that continues to grow as the aging workforce enters retirement.

"Each successful deployment will embolden the next. I think the adoption cycle of BASE-T Ethernet is a great parallel to what we're seeing with SPE," Voss said.

"There are four billion BASE-T ports out there and at the beginning, they were only used for VoIP phones and computers. But adoption ballooned when people figured out that by adding printers to the network, they could serve jobs right from the network by just plugging in an RJ45. No more drivers, no more parallel stuff, no more dedicated computers to support the printer," he added.

SOURCE: HARTING

In connection with the development, standardisation and portfolio structure of the T1 industrial interface in accordance with IEC 63171-6, HARTING also has an eye on the development of the entire single pair Ethernet ecosystem.

For SPE, Ethernet-APL is a great first step because it's an effective solution designed for complex environments with life safety implications. Voss says "kudos to the control industry for embracing it. I suspect other industries will follow up with their own innovation and implementations soon after."

Technological megatrends

New requirements for future connectivity

During this year's 2021 HANNOVER MESSE, HARTING's technology group reaffirmed its focus on answers to the three global societal megatrends of sustainability, demographic

SOURCE: LAPP

Lapp has introduced a wide range of new products for Industrial Communication, mechanical and plant engineering and the rail industry

change and (de-) globalisation. These societal megatrends are closely intertwined with the technological megatrends of autonomy, the digital twin and modularisation.

"These trends are going hand in hand with new, comprehensive requirements for the connectivity of the future," explained Dr.-Ing. Kurt D. Bettenhausen, Director of "New Technologies and Development" at HARTING. "Under the term of Connectivity+, we are grouping forward-looking topics such as DC power supply in industry, electromobility and new industrial ecosystems such as Single Pair Ethernet (SPE). With these and other topics, we will be playing a trend-setting role in shaping a powerful infrastructure for the digitalisation of industry," Bettenhausen said.

Transformation & digitalisation

Today, Ethernet is already the predominant communication medium in industrial automation and will penetrate into the last areas of the automation pyramid in the future. HARTING is creating the appropriate infrastructure for these developments.

"Industrial transformation needs digitalisation", Ralf Klein, Managing Director of HARTING Electronics explained. The aim is to be able to offer customers a reliable, miniaturised and resource-saving infrastructure from the cloud down to every individual sensor.

In this way, HARTING is actively supporting industry's path to the IIoT. However, innovative answers in terms of size, modularity and standardisation of components alone will not be enough, which is why HARTING, since 2017, has been focusing on the development of the entire single pair Ethernet ecosystem in the development, standardisation and portfolio structure of the T1 industrial interface in accordance with IEC 63171-6. Only with all the necessary components and strong partners accompanying the new physical layer SPE will it be possible to realise the technological basis in the form of single-pair copper cabling extending to the field level.

In the meantime, as part of the SPE Industrial Partner Network e.V., HARTING is driving this complete ecosystem forward together with 47 other market leaders. "Setting standards together with partners is an important point for the sustainability and success of a solution. The SPE network is the leading global network," as Ralf Klein emphasized.

Expanding SPE portfolio

Innovations for industrial communication

Single Pair Ethernet (SPE) is a key technology on the way to the SmartFactory and Industry 4.0. It enables more consistent and more economical Industrial Ethernet networks and only requires one pair of wires to transfer data. So far, 2- and 4-pair Ethernet cables have been the standard.

These savings mean that new smart components can be integrated into networks that were previously not networked via Industrial Ethernet. With its ETHERLINE T1 product family, LAPP says it has developed prototypes of single pair Ethernet cables for use in industrial machines and systems at a very early stage.

Its first single pair Ethernet cable is now available from stock. In its spring launch, LAPP presented the new ETHERLINE T1 Y Flex 1x2x22/7 AWG.

"Single Pair Ethernet is an important technology for the future. For broad market penetration, however, we need standardized and uniform connectors," stated Christian Illenseer, Product Manager Industrial Communication at LAPP.

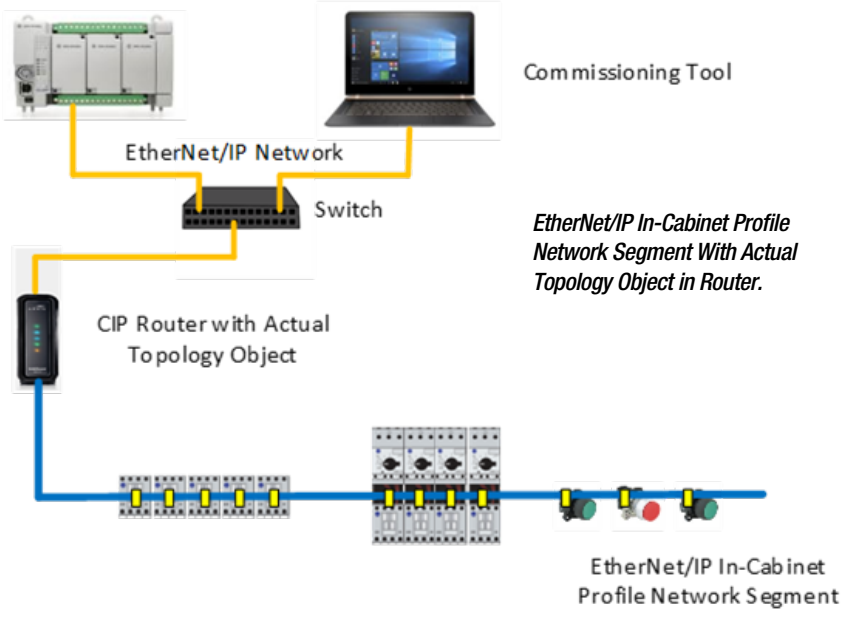
"You only need one standard to ensure the compatibility of the components. We chose the SPE Industrial Partner Network because we are of the opinion that this standard has the greatest chance of success in the market. "

Product innovations

The new ETHERLINE T1 Y Flex 1x2x22 / 7 AWG is a UL-certified, two-wire data line for the fast exchange of information with consistently high data rates and a significantly reduced structure. Thanks to a small bending radii and small outer diameter, it is particularly weight and space-saving, as well as being easy to lay and indispensable for connecting to the field level.

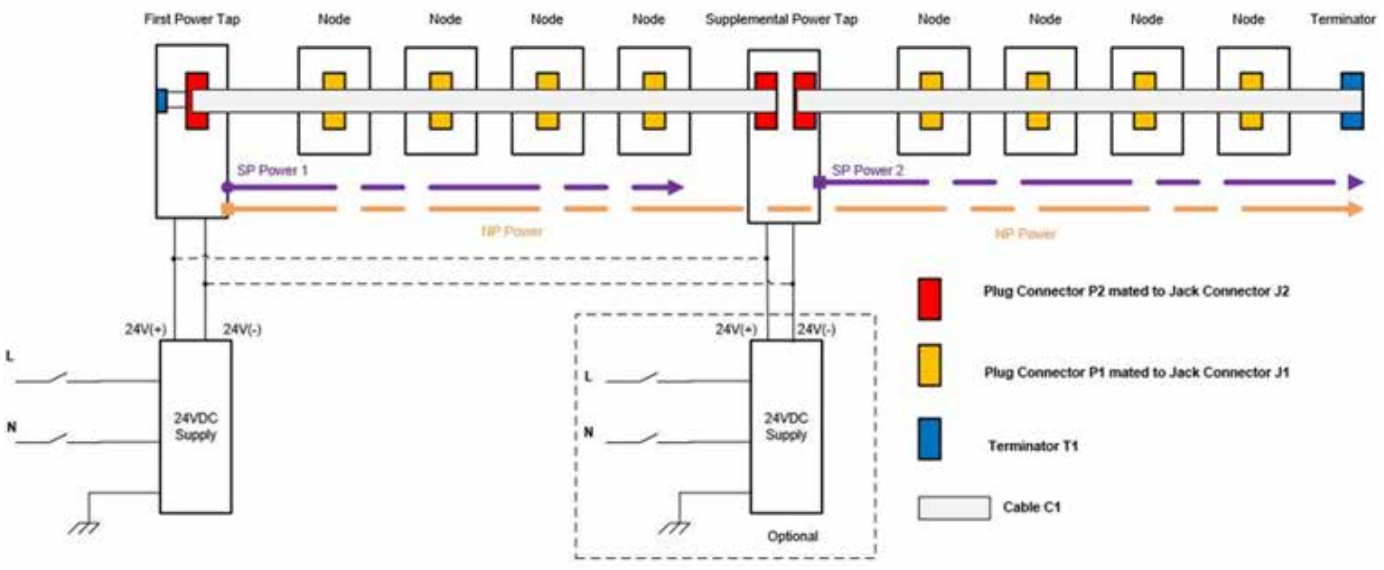
A new Power-over-Data-Line-capable cable, according to IEEE 802.3bu, has been specially designed for the transmission of digital signals in the frequency range up to 600 MHz and up to 40 m away. It enables the simultaneous power and data supply of SPE end devices with low energy requirements (up to 50 W).

The structure of the SPE line guarantees ideal protection against electromagnetic interference: thanks to an aluminum-clad foil and a copper braid shield with a high degree of coverage (SF / UTP), it is double-shielded. In addition, the PVC outer jacket is resistant to acids and alkalis and is conditionally oil-resistant. The UL / CSA certification allows the product to be used in North America. As a UL-listed Power Limited Tray Cable (PLTC), the new Single Pair Ethernet cable can also be laid



SOURCE: ODVA

EtherNet/IP In-Cabinet Profile Network Segment With Actual Topology Object in Router.



SOURCE: ODVA

EtherNet/IP In-Cabinet Resource-Constrained Multidrop Flat Cable Illustration.

openly on cable racks.

The new ETHERLINE T1 Y Flex 1x2x22 / 7 AWG product offers versatile, future-proof application options in automation technology. The world market leader for integrated solutions in the field of cable and connection technology has defined a wide range of applications:

- Flexible use in dry and damp rooms, as well as for medium mechanical stress,
- Structured cabling according to DIN EN 50173 and ISO / IEC 11801,
- Single-pair Ethernet applications 1000Base-T1 according to IEEE 802.3bp and 100Base-T1 (IEEE 802.3bw).

According to Lapp, the IEEE 802.3 bp standard describes a physical layer that allows 1 Gbit / s over single-pair twisted-pair copper cables over a distance of 40 m with shielded lines or 15 m with unshielded lines.

"Possible applications in production automation would be the connection of gigabit communication participants within the control cabinet or sensors with high data rates, such as high-resolution image processing systems.

The IEEE 802.3 bw standard enables the same cable lengths, however, for 100 Mbit/s. This technology should be of interest for connecting devices in the control cabinet, especially because of the reduced distance," the company stated.

In-cabinet & Ethernet-APL

Device and process automation solutions

Two areas of focus for ODVA and its members focus on in-cabinet, resource-constrained device support for devices such as contactors and push buttons, along with the development of SPE solution to enable long reach and hazardous area capable Ethernet within process automation.

In-cabinet device support

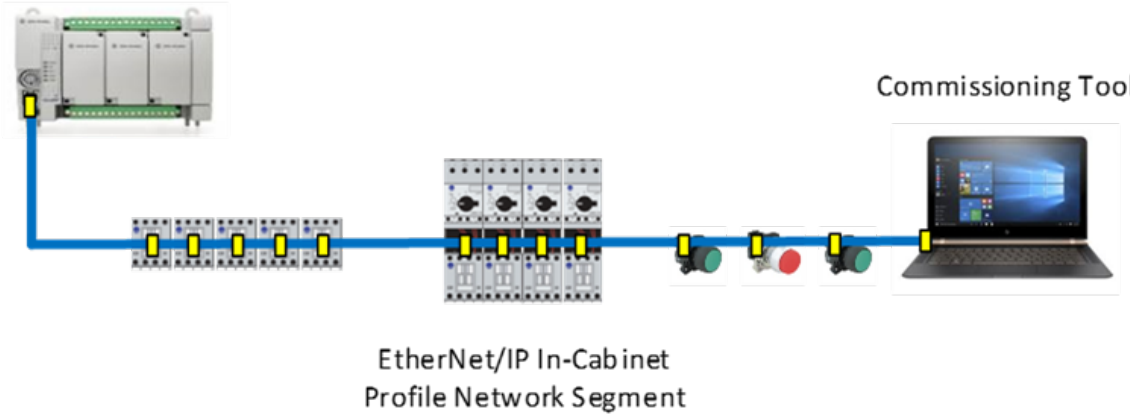
The recently released EtherNet/IP Specification enhancement that enables in-cabinet resource-constrained device support is a significant technological advancement that utilizes Single Pair Ethernet (IEEE Std 802.3cg-2019 10BASE-T1S) to bring Ethernet to low-level in-cabinet devices such as contactors and push buttons.

Limitations including cost, available space, and power consumption have resulted in many edge devices remaining hardwired. However, a lack of network connectivity results in time consuming installation, challenging troubleshooting, and a deficiency of diagnostic information.

The steady decline in the cost and size of semiconductor chips combined with the availability of Single Pair Ethernet has enabled a new EtherNet/IP in cabinet bus solution that uses a multi-drop network and control power cable that spans a single cabinet with one interface per device and one switch port across multiple devices to reduce both commissioning and hardware cost.

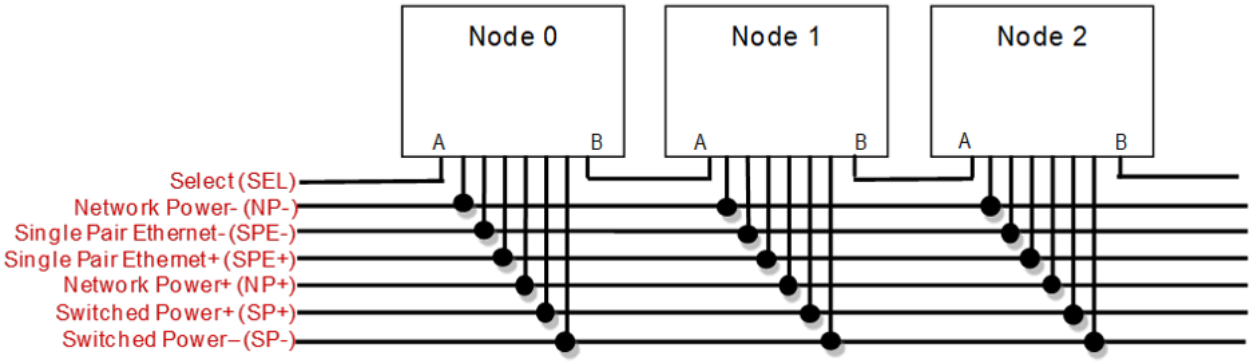
UDP-only communication

The inclusion of resource-constrained devices within cabinets on an EtherNet/IP network is made possible by low overhead UDP-only communication, a LLDP node topology discovery mechanism, auto-commissioning support, and auto-device replacement support. A new select line circuit facilitates the efficient delivery of system wide sequential commands, eliminates configuration switches by enabling topology discovery based on relative position, and allows for direct connection with programming tools during



SOURCE: ODVA

Select Line for EtherNet/IP In-Cabinet Resource-Constrained Bus System.



SOURCE: ODVA

Select Line for EtherNet/IP In-Cabinet Resource-Constrained Bus System.

assembly for parameterization.

According to Dr. Al Beydoun, President and Executive Director of ODVA, "EtherNet/IP for in-cabinet resource-constrained devices will enable the benefits of additional diagnostics, asset information and parameterization capability, automatic node topology discovery, and plug and play device replacement compared to existing hard-wired devices."

"Single Pair Ethernet will enable the use of one seamless CIP network for both constrained and non-constrained devices. UDP-only EtherNet/IP communication and shared in-cabinet external power and communication cabling were designed to help increase installation return on investment," he added.

The EtherNet/IP specification for in-cabinet resource-constrained devices was released in April 2021 by ODVA. Expanding the connectivity of EtherNet/IP to include devices with the smallest physical footprint and most limited hardware resources opens up tremendous opportunity for further digital transformation within automation at the edge. The ability to obtain diagnostic, prognostic, and asset identity information remotely from more devices will drive down incidents of unplanned downtime and improve the efficiency of existing assets. The connection of resource-constrained devices to EtherNet/IP increases the value of existing networks for end users and reduces the need for secondary lower-level networks.

Ethernet-APL

Additionally, the pending Ethernet-APL technology launch that is slated for 2021 will utilize a form of Single Pair Ethernet that has been optimized for the process industries to enable long reach and hazardous area capable Ethernet within process automation.

ODVA is actively engaged with leading standards development organizations and industry members to develop the technology, guidelines, and best practices to promote adoption of and to ensure successful deployment of Ethernet-APL to the field. Ethernet-APL will soon open up process operations to the higher speed and rich data afforded via industrial Ethernet based networks such as EtherNet/IP.

Ethernet-APL is more than just Single Pair Ethernet. Ethernet-APL is made up of Single Pair Ethernet (IEEE 802.3cg-2019, 10BASE-T1L), 2-Wire Intrinsically Safe Ethernet (IEC 60079, 2-WISE), and Type A fieldbus cable (IEC 61158-2, for intrinsic safety). The combination of Single Pair Ethernet, Intrinsic Safety, and Type A fieldbus cable is what allows Ethernet-APL to satisfy the process industry needs for long reach cabling of up to 1,000 meters per trunk length and intrinsic safety protection for all hazardous Zones and Divisions. 2-WISE defines intrinsic safety protection, including simple steps for verification of intrinsic safety without calculations.

Beydoun said that the Ethernet-APL cable specification is important because end users can potentially re-use existing installed Type A fieldbus cable that meets the resistance standards of 100 ohms with +/- 20 ohms tolerance. Type A two-wire cable with shielding is polarity independent to reduce installation errors and only requires a screwdriver to ensure connectivity along with related wire preparation tools to physical connect to the remaining automation installation.

This can potentially result in a much easier migration for existing fieldbus installations that could net significant amounts of time and money savings for large installations and long cable runs.

Impact of new technologies

"Ethernet-APL will use Single Pair Ethernet Technology to help move critical information from the device to the cloud for future applications with modern IIoT and Industry 4.0 solutions," Beydoun said. "Interest in Ethernet-APL from end users has been enthusiastic and will help drive adoption of Ethernet-APL, which will enable companies to gain the benefits of valuable additional data insights that will help drive cost savings."

"EtherNet/IP will be one of the key available industrial Ethernet communication networks that will run on Ethernet-APL as EtherNet/IP was originally designed for the future with a basis in IP technology and has been named as one of the minimum binding requirements for field level to higher system level communication by NAMUR," he added.

Expanding SPE portfolio

Innovations for industrial communication

According to HELUKABEL, the key to Single Pair Ethernet technology is centered on its ability to make it possible to operate Ethernet communication with just one pair.

"This saves space and weight and, especially in times of extremely high raw material costs, this is a resource-saving option for transmitting Ethernet," the company stated in response to a series of questions from IEB. "But also applications that for reasons of cost or analog technology like sensors … is opened up with new possibilities by using SPE."

"Classic Ethernet cables are using 2- or 4 paired cables which are physical bigger than a single-pair-Ethernet cable. Of course, SPE cannot cover all the advantages of classic Ethernet cabling, but there are clear advantages for some areas. SPE offers undeniable advantages wherever there is little space requirement or where you have to pay attention to low weight."

The company noted that SPE is currently only used in automobiles. But in automation technology, and also in process automation, the indisputable advantages of the new technology have been recognized. At the moment there are not all components in series for these areas, but the members of the SPE Industrial Partner Network (www.single-pair-ethernet.com) are working on them.

Currently, there are three cable versions available from HELUKABEL in stock:

- Two drag chain cables for 1 Gbit up to 40m in AWG 26 and AWG 22 and;
- One process automation cable in AWG 18 for fixed installation for 10 Mbit up to 1000m

"Since this technology is still in its infancy, other variants will follow, but this will only emerge over time. For us, one thing is certain: In the future, single pair Ethernet will have its place in industrial and process automation like the 'amen' in church," they concluded.

SPE changing the face of industrial communication

The ambitious goal for Single Pair Ethernet is a new, cross-manufacturer communication standard for digital transformation. Together with other communication technologies such as 5G and TSN, SPE also forms the basis for the intelligent networking that will fuel the evolution of smart manufacturing.

SOURCE: PHOENIX CONTACT

Many in industry believe that Single Pair Ethernet is becoming the connector standard for the network infrastructure of digital transformation.

SINGLE PAIR ETHERNET, OR SPE FOR SHORT, is the trend topic when it comes to industrial communication technology. Usually, the focus is on components. But there is so much more to it than that; it is actually the Ethernet-based communication structure of the future.

There is currently a lot of discussion about components, cables, and connectors, but which PHYs (physical layers) are available? Which cables can be used? How far is the range and what sort of data can be transmitted? And last but not least, has a standard already emerged among connectors? The driving force behind all of these questions is a fundamental paradigm shift in industrial communication – for the entire infrastructure including devices and sensors for numerous application scenarios.

What is already available?

BroadR-Reach technology, an Ethernet physical layer standard for connectivity applications in the automotive industry, can be considered the starting point for the development of SPE. Modern mid-range vehicles have over 100 sensors – a trend that is on the increase. The number of control devices, sensors, actuators, and items of communication equipment keeps growing from one vehicle generation to the next – as does the amount of cabling. Innovative sensor technology with a uniform communication standard is required in the automobile.

Seeking a successor for the CAN bus, it was therefore the automotive industry that identified the TCP/IP-based transmission method and spurred on the first SPE standards. Through the IEEE 802.3 working group, the first SPE standards were published in the relevant task forces as 100BASE-T1 and 1000BASE-T1. Rosenberger Hochfrequenztechnik GmbH & Co. KG is already producing the connectors for these applications on a series scale.

With the cg standard from IEEE 802.3 finally being adopted in 2019, a standard for longer ranges has now been defined for the first time, which will be of interest for many industrial applications. This cleared the way for SPE to enter new fields of application such as factory and building automation. In order to create the first device generations for this purpose,

SOURCE: PHOENIX CONTACT

Universal use: new SPE connectors from Phoenix Contact are based on standards IEC 63171-2 (for IP20) and IEC 63171-5 (for IP65/IP67).

corresponding individual components such as chips, cables, and connectors are required.

Standardization is ongoing

The first PHYs for the cg standard are already available on the market. This standard distinguishes between two variants: the T1L standard for long distances up to 1000 m and data transmission up to 10 Mbps and the T1S standard for shorter distances up to 25 m. This standard also supports multidrop. Therefore, for a bus length of 25 m, at least eight nodes can be connected with 10 cm branch lines. All nodes share the 10 Mbps bandwidth.

The cables for Single Pair Ethernet are described in IEC 61156-11/-12/-13 and -14. These four new standards for SPE cables define both their fixed and flexible installation. To date, the only standard to have been adopted is 61156-11 for fixed installation with transmission characteristics up to 600 MHz and a transmission distance of up to 40 m – suitable for standard IEEE 802.3 bp. The other standards – including those for the cg standard – have not been published yet.

Standardization is also still ongoing for connectors. Connectors for SPE are defined in IEC 63171. With IEC 63171-2, Phoenix Contact – together with partners Reichle & De-Massari and Weidmüller – has developed what is currently the most compact pin connector pattern for this series of standards. It meets two of the requirements for connectors: firstly, miniaturization and cost savings with the introduction of the new technology and, secondly, the industrial-grade latching and automated mounting of device connectors.

The IEC 63171-2 pin connector pattern is also described in IEC 63171-5 – however in that instance it is in industrial IP-protected packaging in an M8 and M12 design. Due to its compact dimensions, this pin connector pattern also fits in a standard M8 connector, and can therefore also be used in standard inductive sensors. Flying leads are also possible for cable-to-cable connection in the field or between field switches. On the device side, the different outlet directions are an advantage: horizontal and vertical to the PCB, a design for THR and SMD soldering processes, and full flexibility when it comes to the mounting direction through front and rear mounting.

SOURCE: PHOENIX CONTACT

From the sensor to the cloud: Single Pair Ethernet is the building block for the consistent use of Ethernet all the way to the field level.

What's next?

In total, the IEC 63171 series of standards contains six different standards for connectors. The user organizations that are currently working intensively on the topic of SPE will have a large say in deciding which standard will apply to which application. Use cases are presented for the various fields of application that consider not only the individual components but the entire ecosystem.

These also demonstrate how and when the popular slogan "From the sensor to the cloud" really takes effect. In order to make SPE technology widely available, it is vitally important that devices, cables, and connectors are compatible with one another.

Device manufacturers still face some challenges when it comes to transferring automotive Ethernet to industrial SPE applications, as the influence of electromagnetic interference is not as predictable as in an automobile and is often far more complex. Industrial Ethernet in its present form was developed over a long period of time. RJ45 connectors have been gradually optimized with regard to shielding concepts, extended temperature ranges, robustness, and integrated transmitters (magnetics) and adapted to the needs of industrial ambient conditions. SPE connectors from Phoenix Contact already offer many of these features. However, the precise requirements of the entire SPE infrastructure will continue to evolve.

SPE as one of many technologies

There are more exciting things ahead. Further IEEE standards for SPE are expected in the years ahead, which are set to cover longer distances exceeding 100 m as well as data transmission up to 100 Mbps.

The portfolio for connectors will also continue to grow over the next few years. As soon as the first innovators develop devices and launch them on the market, connectors for field assembly will also be needed for various cables as will other accessory items for control cabinet and field cabling.

The basic framework for the future of industrial communication technology is currently emerging. SPE is just one element of this, as new communication standards such as the Open Platform Communications Unified Architecture (OPC UA), Time-Sensitive Networking (TSN), and 5G form the basis for integrated networking from the sensor through the machine and higher-level systems to the cloud. As a leading technology company with more than 30 years of experience in industrial communication, Phoenix Contact is therefore actively involved in all of the key standardization committees.

The goal: a new, cross-manufacturer communication standard for digital transformation. Together with other communication technologies such as 5G and TSN, SPE also forms the basis for the intelligent networking of the All Electric Society.

Dipl.-Ing. Verena Neuhaus, Product Marketing Data Connectors, Business Unit Field Device Connectors, ***Phoenix Contact.***

Visit Website

The SPE System Alliance – working together for the IIoT network

The initial technology partnership between Phoenix Contact, Weidmüller, Telegärtner, Reichle & De-Massari (R&M), and Fluke Networks for SPE has progressed to create the SPE System Alliance. Leading technology companies from various industries and fields of application have come together in order to bundle their SPE expertise and ensure the target-oriented exchange of this knowledge. Together, all SPE System Alliance partners are pursuing the goal of driving the development of SPE further forward for the Industrial Internet of Things (IIoT).

The network aims to collaborate on the technological challenges faced when implementing SPE in IIoT applications. The goal of the companies is to accelerate their own development of expertise in SPE technology and to allow it to be implemented faster and more reliably in their products.

Through this orientation toward a cross-industry and cross-application exchange platform, companies from all future SPE ecosystems are coming together. The focus is by no means on individual aspects such as connection technology. Instead, the focus is on taking a much more comprehensive approach to the issues and challenges for SPE faced by many market participants. Rule exchange formats and collaborative project activities provide the freedom for close cooperation.

Getting more power out of Single Pair Ethernet

Innovations in hybrid connectors expand the power transmission capabilities beyond what today's Single Pair Ethernet connectors can achieve using PoDL. Overall, the new innovations in hybrid SPE connections and cables are allowing this technology to expand even further into the IIoT.

THE BEAUTY OF SINGLE PAIR ETHERNET (SPE) is that it eliminates the clunky translation required for different network systems to communicate with each other, unifying machine communication and data transfer among all machines on the network.

SPE allows real-time, high-speed communication connections up to 1Gbps and removes barriers between the sensor and the cloud—all critical when considering the future industrial internet of things (IIoT).

But SPE connectors have faced a limitation: power delivery. For automation applications, the 1.36A current-carrying max in standard SPE connectors using a power over data line (PoDL) is enough. But for applications that require power above that 50-Watt/1.36A threshold, the existing SPE connector design with PoDL can't handle the load.

SOURCE: TE CONNECTIVITY

Single Pair Ethernet connectors have faced an application limitation in one area: power delivery.

Option for high-powered SPE

Enter the SPE hybrid connector and cable. Designed for industrial environments that require higher currents and more power transmission, the hybrid connector uses the form factor of an M8. But this hybrid connector has two pin pairs—one for data transmission up to 1Gbps/600MHz and the other for power transmission up to 8A. To avoid interference with the power and data signals, a metal shield separates the pin pairs inside the connector. Meanwhile, the hybrid cable contains an SPE pair and a power pair, with a shield separating the two like in the connector. The cable's power pair is made of 18AWG wires.

How it works

Separating and shielding the data pair from the power pair significantly reduces the electromagnetic interference "noise" a SPE PHY chip has to withstand as it transmits data. The hybrid connector set-up means that even running at a higher power/current level, there's little to no data lost. That makes the hybrid system attractive for use on networks where the actuators and sensors are mounted directly on machines. Another benefit of this hybrid configuration is flexibility to distribute power across networks vs. the point-to-point connection that PoDL requires. That means it's possible to distribute higher currents to power several cascaded power devices.

SOURCE: TE CONNECTIVITY

Industrial robotics is an application area that benefits from SPE hybrid connectors and cables.

Potential applications

There are situations where you may need to deviate from the PoDL standard, in which case this hybrid SPE connector and cable approach can work well. Potential applications for this technology include:

- If you need higher power levels (up to 8A and greater than 50 Watts), e.g., for the supply of electronic motors.
- If you need more flexibility regarding distributing power over the network to provide power to several cascaded power devices.
- If you need to reduce electromagnetic interference between the data and power lines.

While the hybrid connector has separate signal and power pairs, it still offers one connectivity solution for both data and power—all housed in the small form factor of a standard M8 connector.

Although the hybrid cable is slightly heavier and wider in diameter than the standard ethernet cable, the hybrid cable has a higher power capacity and allows for more flexible network topologies. Overall, the new innovations in hybrid SPE connections and cables are allowing this technology to expand even further into the IIoT.

*Technology report by **TE Connectivity**.*

Visit Website

SPE as universal communicator advances IT/OT convergence

An industry expert provides a retrospective on the evolution of industry, the technology that enables it and how leaders can view their operations through a single pane of glass. As use cases and adoption of Single Pair Ethernet (SPE) continue to grow, so do our capabilities of actually making effective use of convergence.

SOURCE: PANDUIT

"CONVERGENCE", OVER THE PAST FIVE YEARS or so, has become one of our industry's most bastardized buzzwords. This once-novel concept has been relegated to an eye-roll inducing marketing fodder that has all but lost any real world meaning. Or has it?

As we crossed the one year mark of living and working in the COVID era, I couldn't help but reflect on the changes that industry has been through over the past few years. Changes that helped industrial manufacturing adapt during a year of unexpected and unprecedented operational and economic challenges.

Some changes better than others

Like most organizational bodies, the standards community moved to 100 percent virtual settings to conduct business. We were able to maintain effectiveness and accomplish goals, but it became abundantly clear that when it comes to clear communication there's no substitute being in a room with somebody.

Exchanging the option of asking a colleague to discuss the information they presented at a conference over a beer or coffee for the option of learning more by extending a three hour Zoom call isn't something any rational person would prefer.

Reflecting on this one change affirmed something that previously felt equal parts obvious and radical: That clear and direct communication is the key to developing and deploying the innovations that will define the future of manufacturing.

This principle applies to both communication between people and the machines we rely on to build what we sell. For people, improved communication enabled convergence.

Walking down memory lane

Speaking as a representative of the OT community, I can say that we've benefited greatly from our IT brethren. The first spark of effective convergence that I recall goes back about 8 or 10 years when virtualization was new to OT and we were researching use cases and determining how to best productize the practice.

We would have been working from square one if not for an IT colleague who decided to cross the IT/OT barrier by offering to share what he knew about virtualization -- something that had been used in building automation for while at that point -- over a cup of coffee.

Back then an invitation for IT/OT collaboration was rare because ambiguity surrounding which team was responsible for different data moving through our facility created an environment of perpetual territorial tension. We don't do that anymore.

We've evolved as people, professionals, and technologists and through years of improved communication we've learned to speak a lot of the same language. The Manufacturing IT discipline is an example of our evolution. Effective convergence is easier to realize with people who are capable of understanding control and process needs but can also bring the rigor to communicate clearly with the corporate IT folks.

But the human element is only one side of the convergence coin. Unlocking the full potential of convergence requires that our machines also speak the same language and communicate clearly; with us and each other.

Current state of convergence

Convergence is already occurring in the modern industrial space and although each company may apply the practice a bit differently than the next, they all have the same question: What's the next step to take full advantage of it?"

Technology moves quickly and increased adoption of more sophisticated tech like IIoT devices means more bandwidth, more information, and more data...but the same challenges with gateways. This is why companies that embrace the latest network solutions have the best foundations from a convergence standpoint and the best opportunity to take advantage of new data streams.

Utilizing advanced elements of virtualization and automation, like digital twin, enables machine learning algorithms that find opportunities to optimize plant efficiency.

Automating the data analysis gives plant operators a profound advantage. Since they're spending less time manipulating data sets, they can focus on assessing the problem and deploying intelligent solutions. So what's the catch?

What's the most promising network upgrade companies can deploy to realize all of the hypothetical benefits that propelled convergence to buzzword status?

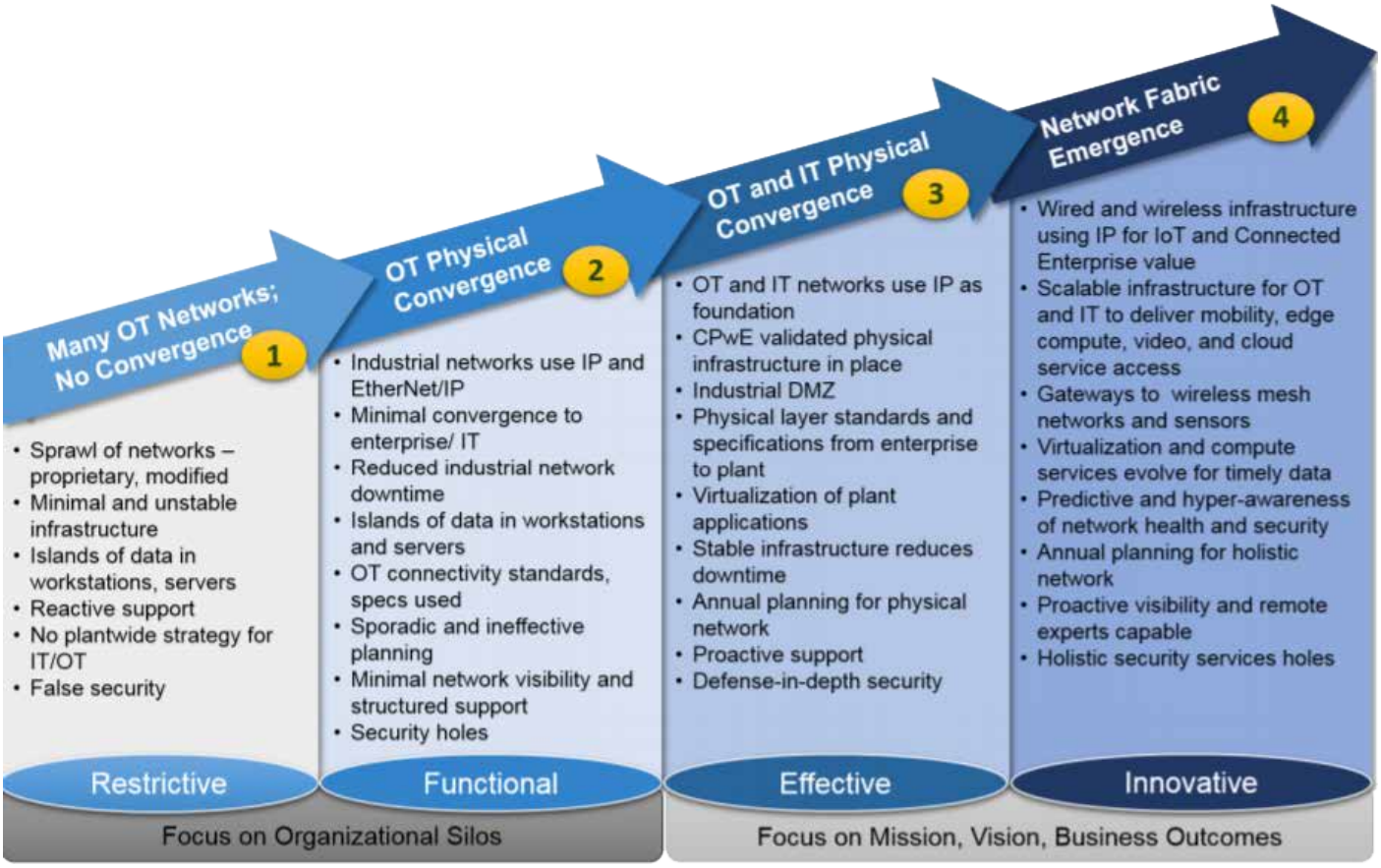
SPE: universal communicator

Convergence can deliver the information needed to optimize efficiency in any scenario. Game changing agility is possible, but not as accessible when the critical information at the edge of the OT network is running on various protocols and needs to be translated.

The sources of the mission critical information that's absolutely needed to transact the manufacturing process, the components that are typically acquired from your favorite automation providers, are engineered to deliver specific data but not to connect any dots that will help increase operational efficiencies.

Operating at peak performance requires more than networking analog and legacy machines by installing sensors throughout the plant floor, uploading data sets to the cloud and looking for trends.

It's possible that valuable insights can be discovered this way but they won't give you access to the most critical element of



SOURCE: PANDUIT

streamlining operations: the context that demonstrates why things are happening.

SPE lays the foundation for a higher functioning, more secure network, instantly adding value to the enterprise by allowing OT to become an integral part of a single-protocol, seamless network, delivering on-demand access to federated data across the entire facility.

Now employees have the context and clarity required to make critical decisions, faster.

Let's say a plant manager needs to increase manufacturing output to meet a spike in customer demand over the holidays. Since both IT/OT networks are Ethernet, the manager converges the data from the all facets of the business to find the right solution:

- *Compute:* Data center resources and network
- *Enable:* Spaces where the people sit
- *Produce:* The network that makes things

SPE enables the manager to take a holistic view of the facility's status. The converged data shows reduced building occupancy because most of the staff are on vacation.

So now instead of just increasing yield, the manager dials down energy consumption across the entire building, except for in the data center which is undergoing server maintenance and needs to remain on the lower end of the temperature threshold.

This company just succeeded in meeting the manufacturing challenge at a better cost because of the visibility and access to controls across the facility - not just production.

Real world example

Three years ago, my team and I at Panduit worked with a partner company that was developing a network infrastructure solution that aimed to change the way companies would think about eSCADA and process control systems. It was a digitally-enabled, unified system that provides integrated substation visibility through the same system that runs the rest of the plant.

Installing the solution on top of the motor controls center responsible for all the reactive power loads in a business -- motors, transformers, compressors, etc. meant the MCC is aware of and communicating with the utilities using IEC 61850 commands and enabling optimal demand response.

Where to start

People and companies who are hoping to better position themselves to take advantage of convergence and guide them to specific areas of the practice can start through education and certifications.

Cisco CCNA

Foundational certification to demonstrate that you know the basics of how to run a network.

Cisco CCENT

Validates the ability to install, operate and troubleshoot a small enterprise branch network, including basic security, WAN technologies, wireless concepts, routing and switching fundamentals, and configuring simple networks.

Experts: Cisco CCIE

ivalidate your end-to-end IT lifecycle skills from planning and design to operating and optimizing. This is Cisco's top certification. Considering that less than one percent of people in the world and only 10,000 in the US have earned a CCIE, it's incredibly valuable but isn't necessary in many cases.

The Industrial Control Systems Cyber Emergency Response Team Trainings

ICS-CERT is part of the U.S. Cybersecurity and Infrastructure Security Agency and educates on how to prevent, track, prevent and resolve network threats.

Conclusion

Going beyond the buzzword, a truly converged business means that decision makers can see and control all aspects of their operation through a single pane of glass. As use cases and adoption of SPE continue to grow, so do our capabilities of actually making effective use of convergence and not just talk about it like it's marketing 101.

Bob Voss, Senior Principal Engineer, ***Panduit Corporate Research and Development.***

Visit Website

OPC UA - from automation pyramid to information network

The OPC UA (IEC 62541) framework with the extensions for field exchange (OPC UA FX) specified by the FLC Initiative, in combination with underlying communication technologies such as APL, TSN and 5G, offers a complete, open, standardized and interoperable solution.

THE FIELD LEVEL COMMUNICATIONS INITIATIVE has reached a major milestone. OPC UA FX extends OPC UA to the field including APL, TSN and 5G technologies

Introduction

A little over two years after its launch, the Field Level Communications (FLC) Initiative of the OPC Foundation has completed the first release candidate (RC1) of the OPC UA FX (Field eXchange) specifications supporting the horizontal communication between shop floor systems, including the exchange of real-time and safety-critical data between controllers (e.g. PLC, DCS) in a vendor-independent way.

This marks an important milestone to further develop OPC UA as a uniform and manufacturer-independent industry interoperability solution that fully scales from field to cloud, including communication and information exchange at the control and field level. For this, OPC UA is taking advantage of enabling communication technologies, such as Ethernet-APL (Advanced Physical Layer) Ethernet TSN (Time-Sensitive Networking, as well as 5G mobile networks.

FLC Initiative: goals/achievements

In November 2018 the FLC initiative was founded under the umbrella of the OPC Foundation. A total of 27 companies, including the largest automation manufacturers in the world, have joined the initiative's Steering Committee and support it financially as well as with man-power and technical know-how.

The common goal is to expand the scope of OPC UA to the field level and to establish OPC UA as a uniform and consistent communication standard in factory and process automation. In the technical working groups, which are open to all members of the OPC Foundation, a total of over 300 experts from more than 60 companies are currently working together in order to develop appropriate concepts and specifications.

Work on the first version of the specification has made good progress - despite Covid-19 and the associated restrictions. The basic concepts for the use case Controller-to-Controller (C2C) have been developed and have been incorporated into a first set of specifications. The first release candidate (so-called RC1) has been completed and is now used to implement prototypes and to execute interoperability testing in order to validate the specifications. At the same time, test specifications are being generated which will later be converted into corresponding test cases for the OPC UA Compliance Test Tool (CTT).

In a second version of the specification, the already developed concepts will be extended for the use cases Controller-to-Device (C2D) and Device-to-Device (D2D), which will then enable that OPC UA can be used as a uniform and consistent communication solution for vertical and horizontal integration, including field, edge and cloud.

This opens up completely new possibilities, especially with regard to the various Industry 4.0 and IIoT use cases and application scenarios which target to make the production more efficient and more flexible.

OPC UA solution for the field level

OPC UA Framework

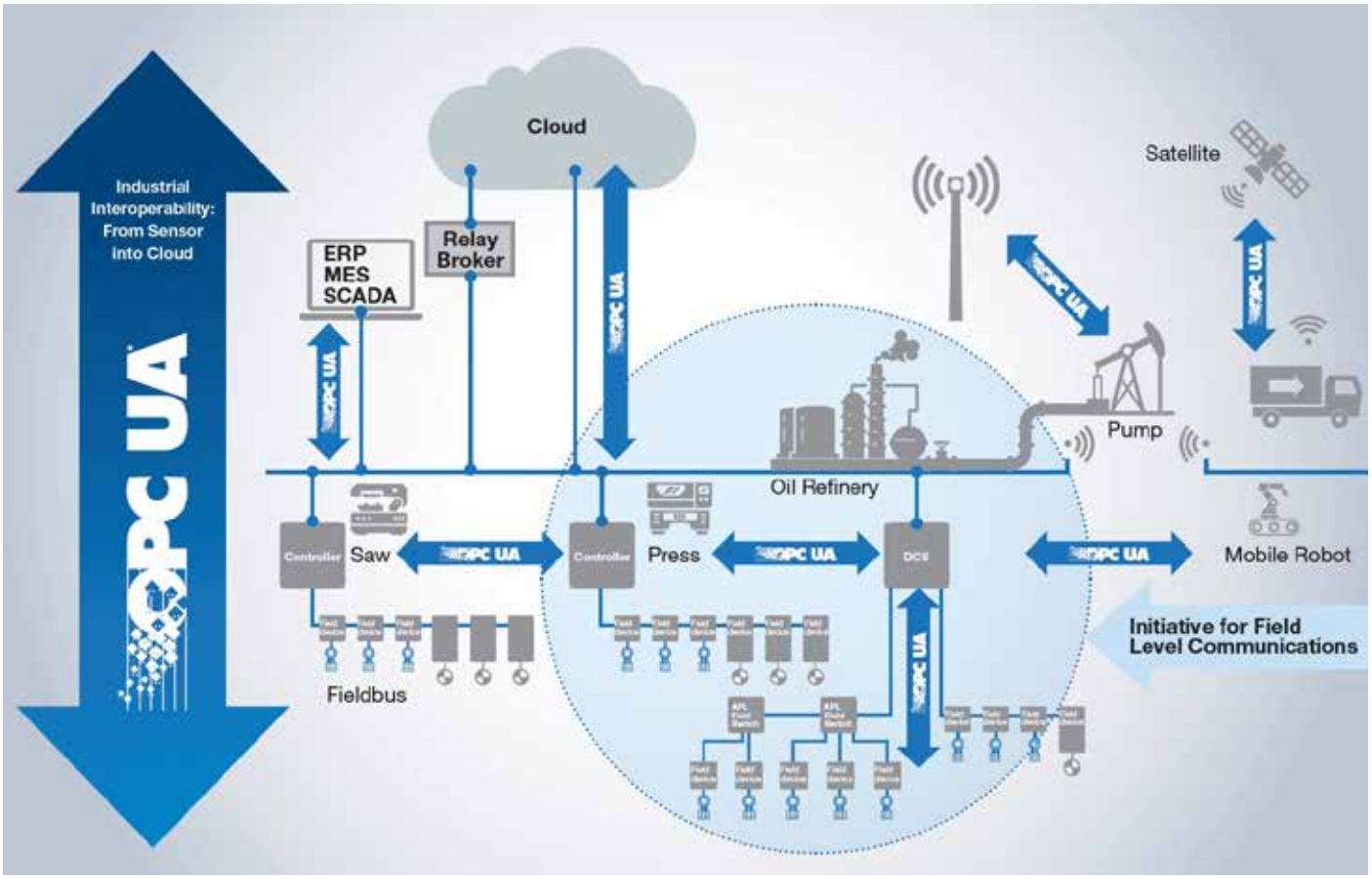
The field extensions specified by the FLC Initiative are based on the OPC UA Framework (IEC 62541), which enables a secure and reliable, manufacturer and platform-independent information exchange.

Controllers and field devices support both, the connection-oriented client/server communication model and the publish/subscribe extensions, which are indispensable for communication at the field level due to the corresponding requirements for flexibility, efficiency and determinism. The security mechanisms specified in OPC UA are also used, which, among other things, support

SOURCE: PANDUIT

The member companies of the Steering Committee of the OPC Foundation's Field Level Communications (FLC) Initiative.

SOURCE: PANDUIT



authentication, signing and encryption of the data to be transported and can be used for both client / server and publish / subscribe communication relationships.

OPC UA FX - Extensions for Field Exchange

The first release candidate of the FLC Initiative consists of four specification parts (OPC UA Parts 80-83) and focuses on C2C communication (Controller-to-Controller) for the exchange of process and configuration data by means of peer-to peer-connections and a basic diagnosis. These parts are labelled with OPC UA FX (Field eXchange):

Part 80 (OPC UA FX 10000-80) includes an introduction and provides an overview of the basic concepts for expanding OPC UA for communication with and at the field level.

Part 81 (OPC UA FX 10000-81) specifies the basic information model for controllers and field devices (automation components) and the communication concepts to meet the various use cases and requirements of factory and process automation.

Part 82 (OPC UA FX 10000-82) describes network services such as topology detection and time synchronization.

Part 83 (OPC UA FX 10000-83) describes the data structures for the exchange of information required for offline engineering using descriptors and descriptor packages.

In addition, a 40-page technical paper was published that explains the overall vision and the technical approach.

OPC UA Safety – fail-safe communication based on Profisafe

Work on the safety solution for OPC UA (OPC UA Safety) is also very advanced. A first OPC UA Safety specification based on client-server mechanisms was developed by a Joint Working Group with Profibus & Profinet International (PI) and was already published in November 2019 (Part 15, OPC 10000-15).

A revision of the OPC UA Safety specification will be available shortly, which describes the extensions for OPC UA Pub/Sub and the parameterization of safety devices including C2D (controller-to-device). OPC UA Safety supports a maximum user data length of 1500 bytes, the creation of any network topology (star, line, grid, ...), hierarchical safety IDs for simplified management of series machines and dynamic connection setup with changing partners, such as modular machines, Autonomous Guided Vehicles (AGVs), Autonomous Moving Robots (AMRs) and tool changers, etc.

OPC UA Motion based on Sercos and CIP Motion

Progress can also be reported with regard to OPC UA Motion. A working group has started in Mid 2020 to develop an OPC UA-based motion solution comprising of motion control functions for various types of motion devices such as controllers, standard drives, frequency converters and servo drives.

The FLC Steering Committee has agreed to base the work on the CIP Motion and Sercos specifications and to adapt them to the OPC UA information modeling and system architecture, taking into account the relevant Industry 4.0 and IIoT use cases. The fact that, as with safety, existing concepts and specifications are being used, the specification work can be significantly accelerated.

OPC UA with APL, TSN and 5G

OPC UA is much more than a protocol. Instead, it is an industrial framework which is fundamentally transport-agnostic and therefore can be easily adapted to different transport layers depending on the application-specific requirements and use cases.

By making use of a universal Quality-of-Service (QoS) modelling concept, which includes real-time communication capabilities with guaranteed bandwidth and low latencies, information and services can be easily mapped to different underlying transport protocols and physical media with their particular QoS mechanisms.

For OPC UA FX two communication profiles are defined. One is mapping the OPC UA protocol (UADP) to UDP/IP. The other one is directly mapping UADP to Layer 2 Ethernet resp. Ethernet TSN. The latter option is being used to reduce the protocol overhead and to increase the protocol efficiency for demanding automation applications, such as Motion Control or High-speed I/Os.

Key technologies for bringing OPC UA to the

field level are Ethernet-APL (Advanced Physical Layer) and Ethernet Time-Sensitive Networking (TSN). But OPC UA applications will not be bound to wired Ethernet technologies only. Wireless communication standards, such as 5G or Wi-Fi 6/7 support similar QoS guarantees and are therefore also supported in the future.

The combination with APL

Ethernet-APL describes a physical layer for Ethernet that was specially developed for the requirements of the process industry. Ethernet-APL enables data transmission at high speeds over long distances, the supply of energy and data via a common, twisted 2-wire cable and protective measures for safe use in hazardous areas.

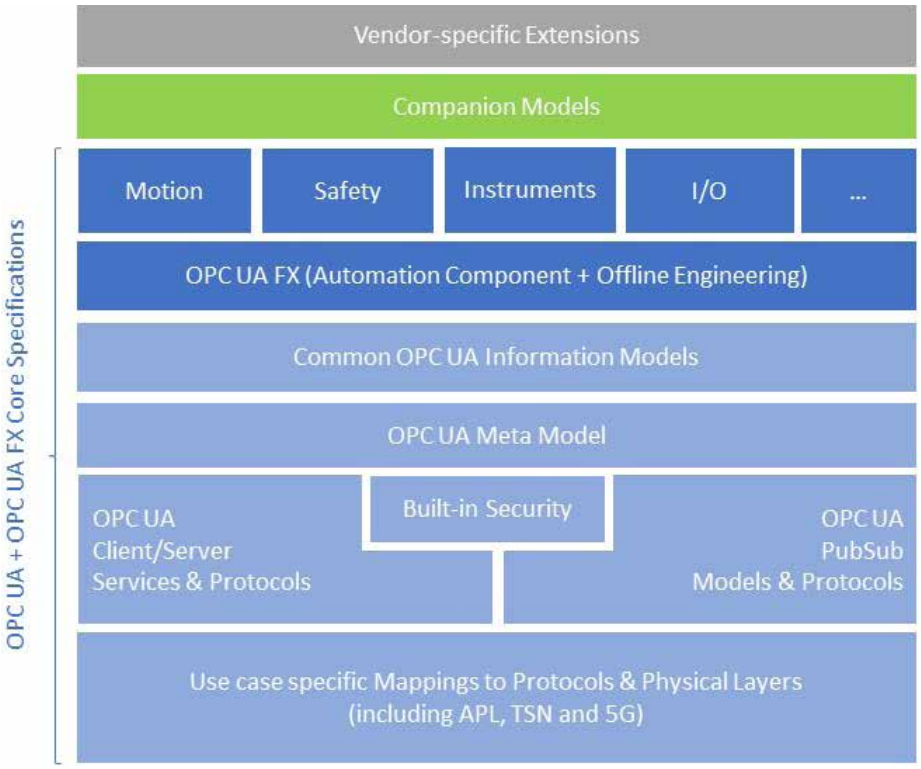
This makes Ethernet-APL the enabling technology for the use of OPC UA and other Ethernet-based protocols in the process industry. Due to the special importance of this technology, the OPC Foundation joined the Advanced Physical Layer (APL) project group in June 2020 to develop and promote APL together with other non-profit organizations and various industrial partners.

The combination with TSN

By using Ethernet TSN, deterministic data transmission via OPC UA is facilitated, which is particularly indispensable for demanding automation applications. In addition, TSN allows different applications and protocols to be operated using a common network infrastructure based on open standards. This enables convergent industrial automation networks to be implemented in which various IT and OT protocols can coexist.

A working group of the FLC Initiative is currently identifying which TSN sub-standards are mandatory for OPC UA-based end devices and infrastructure components in order to meet the specified requirements for performance, flexibility and ease-of-use.

The OPC Foundation has given a clear commitment to the TSN-IA (Industrial Automation) profile, which is being developed by the IEC / IEEE 60802 working group. For this reason, the OPC Foundation has entered into liaisons with the standardization bodies

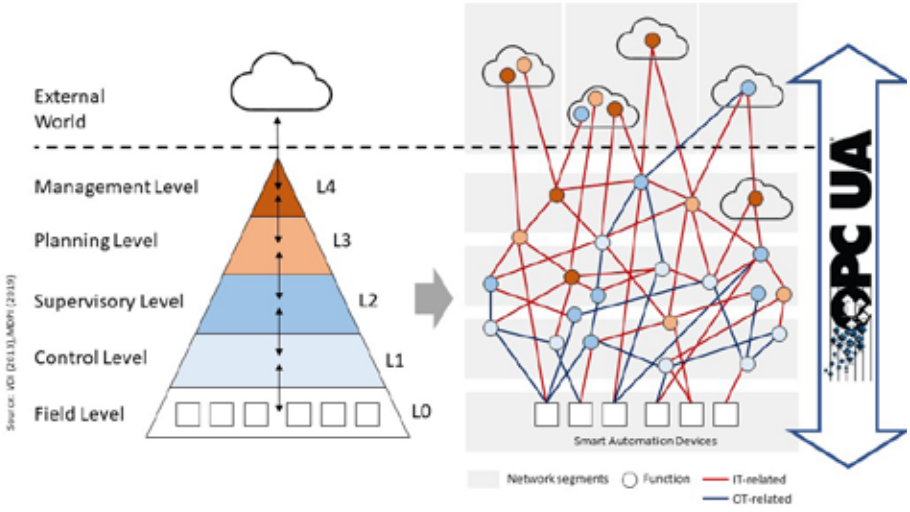


OPC UA Framework with extensions for Field eXchange (FX) .

IEC SC65C and IEEE 802.1.

The combination with 5G

Data exchange via OPC UA is not limited to wired or wireless Ethernet communication. Support for the 5G mobile communications standard is also on the OPC Foundation's roadmap. For this, the OPC Foundation has been working on concepts to include 5G in its Quality of Service (QoS) modelling concept to enable the seamless integration of 5G into the existing OPC UA architecture. Furthermore, a cooperation with the 5G Alliance for Connected Industries and Automation (5G-ACIA) has recently been established, in order to identify and leverage the synergies of combining OPC UA with 5G with the goal to support Industry 4.0 & IIoT applications with a reliable and at the same time flexible communication solution.



Summary and conclusion

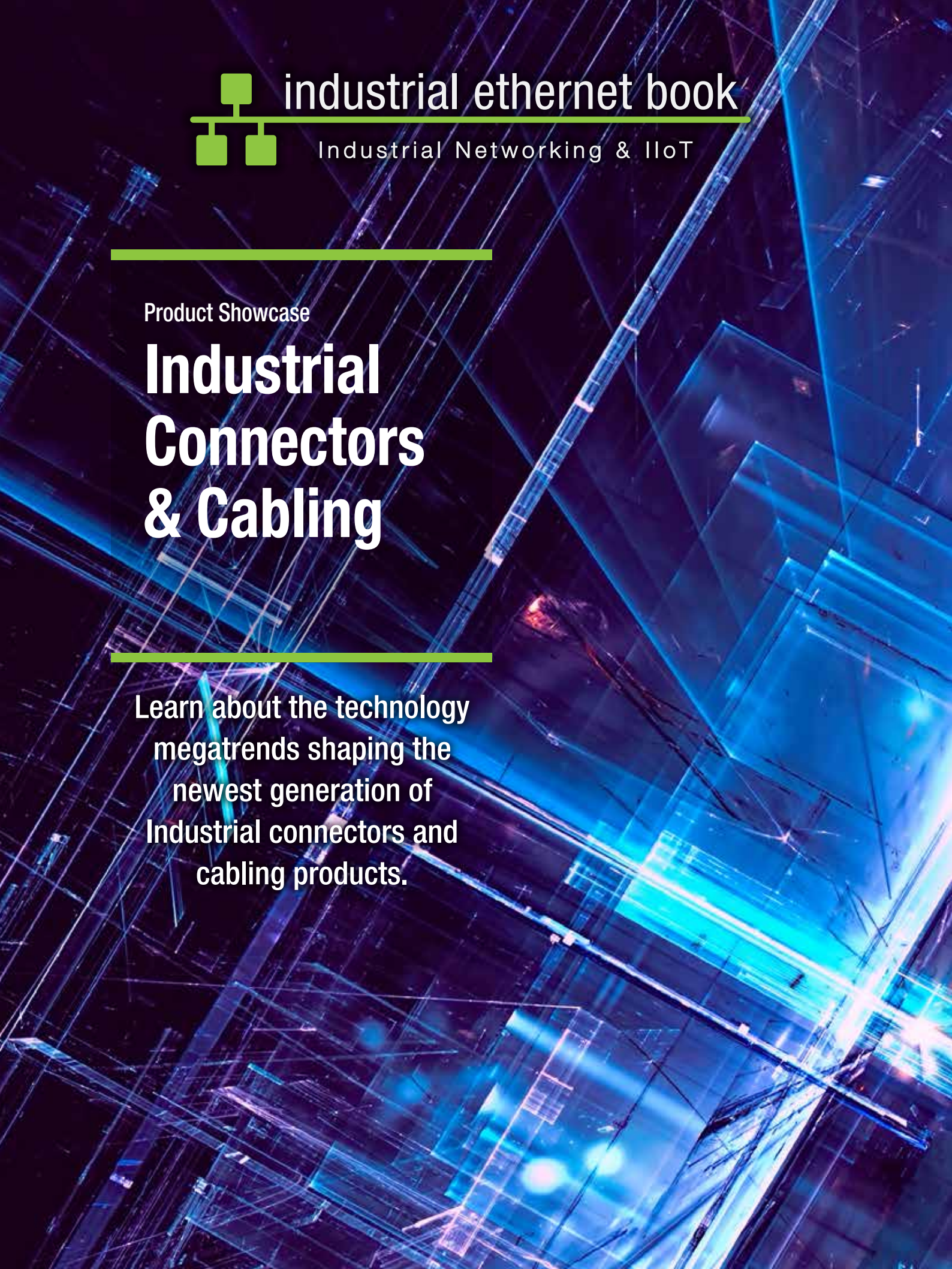
The OPC UA (IEC 62541) framework with the extensions for field exchange (OPC UA FX) specified by the FLC Initiative, in combination with underlying communication technologies such as APL, TSN and 5G, offers a complete, open, standardized and interoperable solution that not only fulfills the requirements of industrial communication, but at the same time enables consistency and semantic interoperability from the field level to the cloud and vice versa.

With this approach - and by adopting additional device companion specifications that are developed by numerous organizations all over the world - information is made available with a standardized semantics directly at the data source, if possible: A flow meter for example offers directly standardized "OPC UA flow measuring data" as soon as the APL cable is plugged in.

And analogously, servo drives directly process standardized "OPC UA drive setpoints" and provide standardized "OPC UA actual drive values" as soon as they are integrated into a machine network with Ethernet TSN.

Peter Lutz, Director FLC, ***OPC Foundation.***

Visit Website



industrial ethernet book

Industrial Networking & IIoT

Product Showcase

Industrial Connectors & Cabling

Learn about the technology megatrends shaping the newest generation of Industrial connectors and cabling products.

SMART TECH SHOW | AI & BIG DATA SHOW | RETAIL TECH SHOW | VISUAL TECH SHOW

SMART TECH KOREA 2021

10th Anniversary

Connect the Future

Date 23 ~ 25 June, 2021

Venue COEX, Seoul, Korea

Smart Tech Korea Secretariat

- T.+82 2 6000 7717
- H. www.smarttechkorea.com
- E. info@smarttechkorea.com

Enjoy the convenience of exploring Smart Tech Korea!

Industrial Ethernet Connectors and Cables Product Showcase

Industrial connectors and cables are in a period of rapid innovation. Along with the emergence of Single Pair Ethernet, this new environment is creating higher demands on products is producing solutions that are offering higher data rates, increased levels of protection and options for miniaturization.

THE LATEST GENERATION OF INDUSTRIAL Ethernet connectors and cabling are being driven by a series of key technical trends and more stringent requirements aining to boost industrial network performance. Compared to IT applications, industrial applications place higher demands on new products.

"It is not only the signaling performance that is constantly being driven upwards by higher data rates, but properties such as increased protection class, miniaturization and expanded mechanical requirements also play a decisive role," Michael Kasper, Director of Accessories Products at Siemens AG told IEB.

"Of course, the convenient handling of the connector must not suffer from these technical requirements. Particularly in the Operational Technology (OT) environment, in which cables often have to be assembled on site, the user demands a simple, error-avoiding design of the connector. In short, Cat6A, small size and assembly in the field must not be mutually exclusive," he added.

Technology innovations

Kasper said that innovations are being driven by the idea that industrial data communication is not a topic for specialists, but a topic that can be mastered by everyone. By using new materials and connection technologies, plugs can be easily installed in the field without additional special tools, even by untrained personnel. Colored markings in the connector help to avoid incorrect contact. In addition, clear installation videos, which can be easily accessed via a QR code on the packaging, help ensure that the installation is suitable for industrial use.

A growing set of application requirements that are also influencing new product development and connector/cabling solutions.

One area is increasing data rates, or applications in which fewer wires, that are to be used for Ethernet communication and require high-performance connectors that must be fault-tolerant and easy to use at the same time.

"The user expects that these products can be installed by anyone without having to check them for correct quality using complex testing procedures before commissioning, as in the laboratory, Kasper said. "The construction of communication networks, also in industry, must be as easy as it is for the commercial target group in home use. No specialist knowledge or special equipment may be required to set up communication networks."

SOURCE: SIEMENS

Industrial connectors and cables are responding to a growing set of application requirements.

Single Solutions

"The big trend/need in industrial networking is the drive toward finding and using a single solution vs. having to rely on multiple components and parts," Ruud van den Brink, product manager for industrial communications at TE Connectivity told IEB.

"The industrial internet of things (IIoT) is about connecting and processing data in real time from machines, factories, enterprises and supply chains around the world. It's a data-driven world where decisions are faster, more rational and more efficient. And it's one where factories are smarter, with machines talking to the entire world, learning and continuously optimizing each other's performance. These smart factories require smart machines," he said.

The unique technical benefits that these innovations provide are focused on ways to make communication networks more effective. Most automation networks today are built up out of different communication protocols from serial or bus communications, to Ethernet. Ideally, the whole network would be built up with Ethernet-based connectivity using Ethernet-based connector types so you don't have any conversions between protocols or limits in information flow.

"In newer networks, Ethernet is taking over at the expense of serial communication and bus communication," van den Brink added. "If we look at all of these trends, there are a couple solutions that we support. The first one—RJ45—is very well known; a connector that comes out of the office space and has made its way into industrial networks. Performance-wise, it's a typical office connector, which causes various problems when used in an industrial environment. Other solutions stand up better to the demands of the industrial environment, including Mini I/O—a very small, ruggedized connector, and the M8 and M12 products, which have addressed the industrial requirements for quite some time."

But for a true glimpse into the future, many industrial companies are considering Single Pair Ethernet (SPE). SPE addresses an application space that's been more or less out of reach for the other three connectivity methods, finally getting Ethernet into the industrial network.

Engineering challenges

At TE Connectivity, IIoT work is all about getting data from the network into a database for further processing to optimize an IIoT-based network. Their goal is to interconnect all of the different sources of data so all available data makes it into the database for further analysis.

"We know engineers are facing a number of challenges in their industrial environments," van den Brink said. "Networks have grown more automated and complex while also becoming decentralized so more local connectivity and connectivity on the factory floor is required. This demands solutions that are not only waterproof and dustproof, but also able to withstand intense vibration, shock and heat. Plus, the connectors are growing smaller and more dense. As a result, reliability is more important than ever. Customers need a product that's rugged, yet easy to install and repair, with fast data transmission speeds (10 – 100 Mb per second)."

These challenges are compounded by the different components, connectors, systems and parts used in many networks today. van den Brink said TE is addressing all of those fields and as such, has a total solution available for every company that plays a role in implementing industrial IIoT networks.

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

RJ Industrial MultiFeature connectors

New Industrial Ethernet connector facilitates access to the IIoT. Faster assembly saves users valuable time.

The RJ Industrial MultiFeature is a significantly improved version of the classic RJ45 in terms of handling. Thanks to a robust metal housing and integrated knives that automatically shorten the strands to the correct length during assembly, handling is greatly simplified. Shorter assembly time saves valuable time in system installation. Consequently, the most frequently deployed data interface has been further optimized for use in industrial environments.

Targeting designers of miniaturized devices, HARTING will be showing all the innovations and portfolio extensions revolving around the space-saving ix Industrial® Ethernet interface. The interface is 70% smaller in size, offering Gbit Ethernet with a more compact footprint while increasing stability at the same time. Standardized in IEC 61076-3-124, ix Industrial® represents the future standard for 8-wire Gbit Ethernet in automation scenarios.

In traditional RJ 45 solutions for industrial networks, the time for confection is 50% for preparation of the cable and 50% for connecting. With the new RJ Industrial® Multifeature, users get a robust and reliable connector with integrated cutting tools for fast and easy assembly. A time saving of about 25% in the assembly is possible.

SOURCE: HARTING

The RJ Industrial® MultiFeature is a significantly enhanced version of the classic RJ45.

This completely dispenses with this time-consuming step and the entire assembly is more than 25% quicker. There is no longer a need to shorten the individual wires 8 times using the wire cutter and the quality of the connection process is also improved. The wires are always safely shortened in the same place in each connector and this also ensures that the HF performance of all assemblies is identical.

HARTING

Visit Website

Industrial Ethernet cable solutions

Helukabel offerings include cables and field harness connectors, and Plug & Play patch cables.

The RJ45 and M12 d- or x-coded overmolded patch cables product range from Helukabel has been enlarged with ix Industrial acc. IEC 61076-3-124 standard.

ix Industrial is key to the miniaturization of devices such as cameras or computers. The secret lies on the socket side which is on the circuit board. Compared to a classic RJ45 socket, a socket with the new mating face offers up to 70% space saving compared to other alternatives.

With this new mating interface, three different codings allow for efficient Ethernet and bus transmission or signal cable interconnection.

A-code for Ethernet/Profinet transmission
B-code for signal or bus transmission
C-code for Ethernet

Thanks to the double locking of the ix Industrial connector, there is an enhanced protection from vibrations compared to conventional RJ45 connectors. Vibration which has until now been a problem can now be a thing of the past.

Furthermore, the 10-pin assignment option means that the connector has a promising future in terms of hybrid cables. For example, 2- or 4-pair Ethernet cables can be expanded with two power supply wires and connected with only one connector.

SOURCE: HELUKABEL

Compared to a classic RJ45 socket, a socket with the new mating face offers up to 70% space savings.

If a customer cannot use pre-assembled cables due to issues with spacing, there is, of course, the option to purchase cables and plugs / sockets from Helukabel as individual parts and to install these in the field to create effective solutions.

Helukabel

Visit Website

Expanded single-pair Ethernet range

New products reflect an expansion of solutions for industrial communications.

With the ETHERLINE T1 product family, LAPP was ahead of the game in presenting prototype single-pair Ethernet cables for use in industrial machinery and systems.

As part of its spring launch, LAPP is introducing the new ETHERLINE T1 Y Flex 1x2x22/7 AWG. This is an UL-certified 2-core data cable for high-speed information exchange that maintains the same high data rates while significantly reducing the setup required. Thanks to its small bending radii and small outer diameter, it is exceptionally lightweight, space-saving and easy to install and is indispensable for connection at the field level.

The new Power-Over-Data-Line compatible cable complies with IEEE 802.3bu and was specially designed for transmitting digital signals in the frequency range up to 600 MHz over distances of up to 40 m. It enables a simultaneous power and data supply to SPE terminals with low energy consumption (up to 50 W).

The design of the SPE cable guarantees ideal protection against electromagnetic interference: Thanks to an aluminum-laminated foil and copper braid shield with a high degree of coverage (SF/UTP), it is double shielded. In addition, the PVC outer sheath is resistant to acids and alkalis and is partially oil-resistant. UL/CSA certification enables the product to be used in North America.

SOURCE: LAPP

The LAPP portfolio already includes single-pair Ethernet cables. The company based the connector on the standardised connector face set out in IEC 63171-6, providing a complete solution for SPE infrastructure in industry.

Another new feature is the ETHERLINE CABINET CAT.6A.for the control cabinet in PROFINET networks. Thanks to their small bending radii, Cat.6A patch cables can prove especially useful in confined spaces.

Lapp

Visit Website

Hybrid connection solutions

HDC HMN shielded Cat 5e modules from TE Connectivity provide solution for robotics & automation systems.

TE Connectivity (TE) has launched HDC HMN shielded Cat 5e modules to expands their HMN range — modules that enable high-speed data transmission.

The HDC HMN system, designed for harsh industrial applications, offers various options for power, signal and data connections. The new addition makes TE's HDC HMN system an option for robotics and automation applications.

New modules are available with two or six contacts in each circular insert, with up to three inserts in a single HMN module.

The HDC HMN modules offer:

- High signal integrity through individual shielding of each Ethernet pair
- Enhanced flexibility with high-density data inserts in standardized module, compatible with entire HMN range
- Ease of assembly

"TE customers using HDC HMN modular connectors will benefit from these additional options to create, customized interfaces," said Ewa Bazior, product manager at TE Connectivity. "The connectors also allow transmission of power, signal and high-speed data with an optimum amount space on the panel and a reduced number of cables needed."

SOURCE: TE CONNECTIVITY

Hybrid connection solution from TE Connectivity offers versatility for industrial applications and robotics.

Possible applications include connections between control cabinets and a robot base, various connections between fixed and moving parts in automated assembly and production lines, and connections in electrical and pneumatic handling equipment.

TE Connectivity

Visit Website

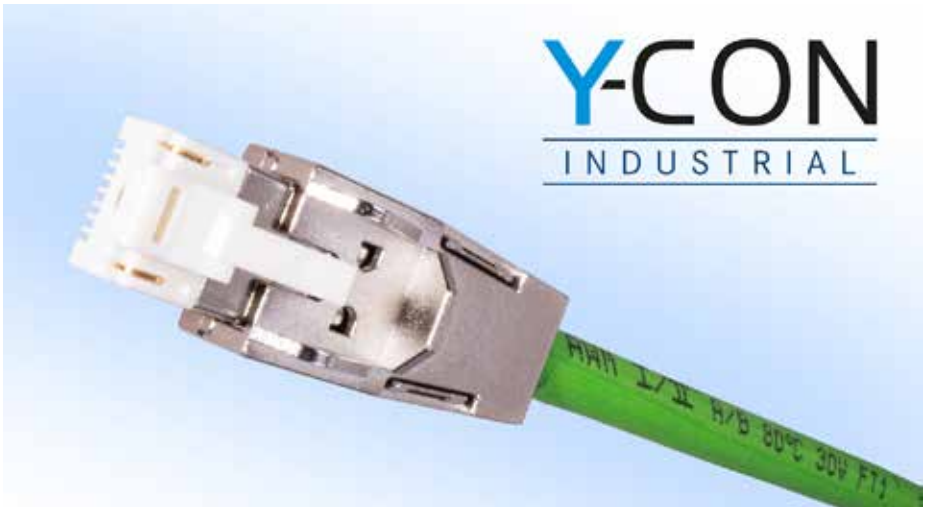
IP20 metal cover

Y-Con Cover 20-TC for RJ45 Y-Con plugs with piercing contacts is available from Yamaichi.

The new Y-Con Cover 20-TC from Yamaichi replaces the current version of Y-Con Cover 20, which has a great acceptance in the market for many years. Like Y-Con Cover 20, the new Y-Con Cover 20-TC is an IP20 full metal version, which protects the plug from all kind of influences in an IP20 industrial area.

Strong mechanical resistance paired with a high protection against EMI disturbance guarantees the optimal signal transmission.

Moreover, the Y-Con Cover 20-TC can be assembled tool free. The new snap hook concept makes screws redundant so that the upper and lower part only need to be pressed together.



SOURCE: YAMAICHI

Snap hook concept makes screws redundant, so that the upper and lower part only needs to be pressed together.

Characteristics

- Robust die cast housing
- Completely metal-covered RJ45 interface
- Tool-free click assembly
- Reusable up to 5 times
- Supporting outer cable dimensions from 5.5 mm up to 7.1 mm

This saves about 30% to 50% assembly time and thus means pure cost reduction. It does not even take into account the possibility of screws falling down or being lost. If necessary, the cover can be reassembled up to 5 times.

Together with our Y-Con Plug connector series, which is available with a different number of contacts, the Y-Con Cover 20-TC can be used for various RJ45 applications. The plug series is also constructed and tested for rough applications as are common in the industrial sector.

In addition, optional integrated power contacts offer the possibility for the power transmission of up to 2.1A.

Yamaichi

Visit Website

M12-Mini X-Code cable connectors

Provertha offers new 10GigE cable connectors for high-speed Ethernet with shock and vibration protection.

The performance of Provertha's M12-Mini X-Code cable connector series has been officially documented on the basis of certifications according to relevant standards. The certification covers all straight and angled (backplane) 10 Gbit Ethernet variants in the reliable, vibration-proof crimp connection technology. The turned crimp contacts have a significantly higher current carrying capacity for use in special applications.

The M12-Mini X-Code in protection class IP67 (screw-locked) is the industry's most compact 10GigE cable connector for space-saving Ethernet or Profinet connection, which can be used in a temperature range from -40°C to +85°C.

All M12-Mini X-Code connectors have successfully passed the tests according to DIN EN 61373 (category 1, class B, and 2). In addition, they feature the 500h corrosion protection, proven by successfully passing the salt spray test according to EN 60512-11-6. Furthermore, the complete test programme according to the M12 connector standard IEC 61076-2-109 including the test group FP for the electrical transmission parameters was successfully passed in a certified test laboratory.

SOURCE: PROVERTHA

The M12-Mini X-Code is a compact 10GigE cable connector for space-saving Ethernet or Profinet connections.

M12-Mini X-Code cable connectors are suited for railway applications, as well as for harsh industrial environments subject to shock and vibration such as automotive presses. Due to corrosion protection and increased shock and vibration resistance, the M12-Mini X-Code connectors are designed for mobile automation applications.

Provertha

Visit Website

Coaxial connector supports 5G

Ultra-small coaxial connector supports 30GHz, designed for 5G millimeter wave devices and CPE.

Hirose Electric has developed the C.FL Series as a 0.92mm mated height, ultra-small coaxial connector supporting 30GHz, designed for 5G millimeter wave devices and CPE (Customer Premises Equipment).

Millimeter wave bands are anticipated to be used for next generation standard 5G communications. Higher frequencies than ever before are expected to be transmitted in the internal connection between the antenna board and the main board of 5G devices and CPE. Demand for connectors that secure band performance is also increasing.

Hirose has developed the small coaxial connector C.FL Series which supports 30GHz in anticipation of greater millimeter wave band usage.

In spite of the ultra-low profile and small size with 0.92mm mated height, frequency characteristics have been dramatically enhanced by reducing the diameter of the male receptacle contact and optimizing the internal design of the plug.

In addition, the assembly's precision has been improved compared to conventional products, contributing to stable transmission in the millimeter wave band. Furthermore, the applicable cable size is a very thin and flexible, making it easy to route inside devices.

SOURCE: HIROSE

Higher frequencies than ever before are expected to be transmitted in the internal connections of 5G devices.

The newly developed C.FL Series meets the demanding performance requirements for millimeter wave devices. As part of the product lineup, we are developing cable assembly products with a 2.4mm connector or 2.92mm connector on the other side for evaluation and measurement of 5G devices. We anticipate these cable assemblies will be used in a variety of upcoming IoT devices supporting 5G.

Hirose

Visit Website

Cat7 Industrial Ethernet cables

LUTZE offers teal jacket for stationary applications and green jacket for continuous motion applications.

LUTZE is offering two Cat7 industrial Ethernet cables; one for stationary applications (A1040300), and the other for continuous motion applications (104404).

Cat7 Ethernet cables support transfer speeds of 10Gbps and frequencies up to 600 Mhz. Cat7 is backwards compatible which means it can service prior Cat5e, Cat6, and Cat6A standards all while “future-proofing” any upcoming network expansions. Cat7 has the strictest specifications for signal integrity, including shielding between individual pairs as well as an overall braided shield. Cat7 Ethernet cables are designed to ensure network reliability in the harshest industrial environments.

Ethernet cable #A1040300 is intended for stationary applications and carries multiple approvals including CMR, CMX Outdoor, PLTC, and AWM 600V. These approvals allow this cable to be installed in a variety of applications. Designed with a rugged oil resistant teal PVC jacket, this cable is suitable for harsh industrial environments.

SUPERFLEX cable #104404 is intended for continuous motion installations and is rated up to 20 million flexing cycles. This cable is UL Listed Type CMX and is compatible with all major drag chain brands. The green PUR jacket is oil resistant, highly abrasion resistant and designed for harsh industrial environments.

SOURCE: LUTZE

Cat7 Ethernet cables support transfer speeds of 10Gbps and frequencies up to 600 Mhz.

With a wide a variety of cables, connectors and connectivity solutions, LUTZE is a complete solutions provider for industrial Ethernet applications. These cables complement LUTZE’s already broad Ethernet cable and connectivity product solutions.

LUTZE

Visit Website

Intelligent connection: data and power over one cable via PoE

Power over Ethernet (PoE) continues to push forward with increased performance, leveraging its ability to combine data and power in a single cable to connect a wide range of industrial end devices. The result is a larger applications portfolio, and an ability to save time and effort while also reducing costs.

WITH EVER INCREASING PERFORMANCE AND A rising number of supported end devices, Power over Ethernet (PoE) – for the simultaneous supply of industrial end devices with data and power – is becoming a versatile all-rounder in the digital factory. With various components feeding and utilizing PoE, Siemens offers a comprehensive portfolio for even more efficient industrial applications. This saves time, effort, and money – from planning to installation and commissioning to maintenance.

In these times of digitalization, the number of applications in the IIoT, the Industrial Internet of Things, is increasing rapidly. The network components used for this not only have to be long-lastingly and reliably supplied with data, but also with power. The easier that is, the more efficient the solutions, the shorter the time-to-market, and the lower the life-cycle costs.

SOURCE: SIEMENS

Siemens is expanding its Industrial Ethernet switches portfolio by new PoE variants, including Scalance XR-100PoE WG and Scalance XR-300PoE WG. Should the power provided by the switch not be sufficient, the Scalance XR-300PoE WG, for example, can be augmented with PoE power supplies such as the Scalance PSR9230PoE to deliver up to 570 watts of power.

Data and power over one cable

Power over Ethernet is getting better and better. The technology comes from the home and office area, where WLAN access points, Internet cameras, or IP telephones have been supplied with data and power over a single cable for years.

The resultant added values for industrial networks are obvious – starting with the reduced planning effort for new or to be expanded production networks. These can also be set up and commissioned more easily, i.e., assembled much faster thanks to fewer cables. Less cabling also speeds up troubleshooting and component replacement as well as adaptation of networks to changing circumstances.

SOURCE: SIEMENS

Focus on quality: network components supplied via PoE, such as Scalance W IWLAN access points or HD cameras, greatly simplify complete tracking and continuous quality control. High-performance uplinks of the higher-level PoE switches with data rates of up to 10 Gbps avoid data bottlenecks.

In the industrial environment, PoE supplies infrastructure end devices such as Industrial Wireless LAN access points for wireless communication, and recently also RTLS (real-time locating system) gateways for real-time locating of objects and/or people. In addition, there are classic end devices, i.e., identification systems for tracking products as well as cameras for quality assurance or for building, area and plant monitoring.

PoE-capable Industrial Ethernet switches function as supply sources (power sourcing equipment, PSE). The specialized switches apply a voltage ranging from 48 to 54 V DC to the wire pairs of the Ethernet cables. End devices thus only need an Ethernet connection. Cabling and communication mechanisms remain practically unaffected, as do established cybersecurity, safety, or redundancy strategies.

The electricity requirements of industrial PoE end devices range from a few watts in the case of simple card readers for access authorization to high double-digit values, for example for heated outdoor cameras. The IEEE 802.3bt standard defines eight power classes and an upper limit of 90 watts per port – practically feasible at the moment are up to 60 watts over distances of up to 100 meters.

SOURCE: SIEMENS

State-of-the-art intralogistics: Simatic RTLS (real-time locating system) gateways and Scalance IWLAN access points in the electronics production at Siemens in Fuerth are efficiently supplied with data and power via Scalance X PoE switches.

The power output is usually "negotiated" automatically among the feeding and using devices (hardware-based) according to IEEE standards. The user does not need to configure anything manually in addition. However, they can do this if necessary, as many devices offer the possibility of precisely specifying power output for each port.

PoE industrial applications portfolio

This also applies to the new Power over Ethernet variants of the Scalance X Industrial Ethernet switches from Siemens. Their power budget can be individually split and optimally utilized which may allow a larger number of end devices to be supplied (than with the automated procedure). With the Scalance XR-300PoE WG (WG: workgroup) rack switches, featuring a large number of ports, up to 26 end devices can be supplied with data and power over each data cable.

All of the new PoE switches support the IEEE 802.3bt standard and provide up to 30 watts of power per port. Via their 10 Gbps copper ports, up to 60 watts are possible. Should the power budget offered by the switch be insufficient, additional external power supplies can be used. The Scalance PSR9230PoE power supply in 19" format was specially developed for the rack switches. With up to two of these devices, the power budget can be expanded to a maximum of 570 watts.

The industrial-grade Scalance XP-200PoE devices are designed for an extended temperature range and, with IP65 protection class, suitable for cabinet-free installation in plant environments. The rack/workgroup devices, on the other hand, are designed for use at temperatures higher than encountered in an office environment, the variant with a large number of ports, for example, as a classic star coupler in a control room.

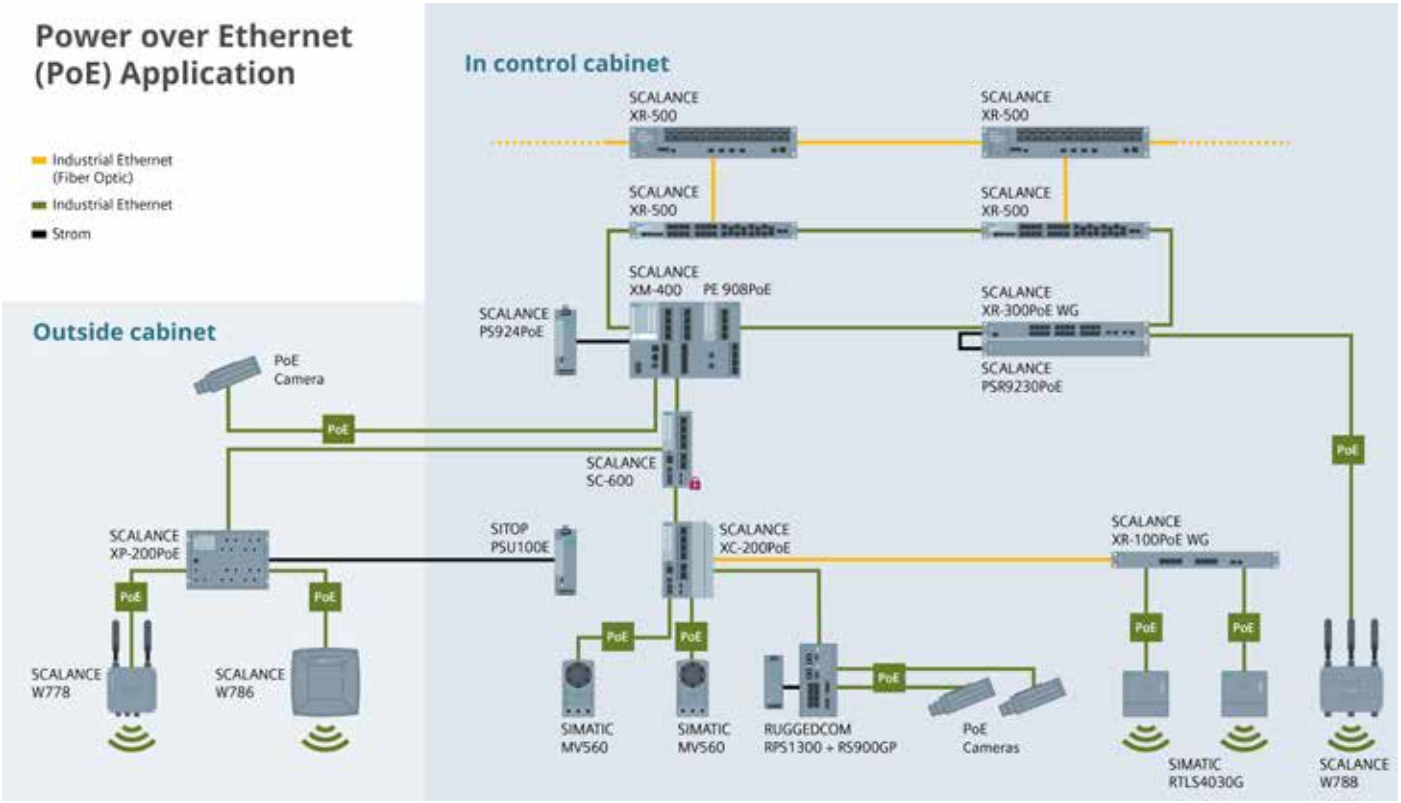
SOURCE: SIEMENS

State-of-the-art intralogistics: gateways and access points in the electronics production at Siemens in Fuerth are efficiently supplied with data and power via Scalance X PoE switches.

PoE variants from the Ruggedcom series, such as the Ruggedcom RST916P or RST2228P, are ideal for the most demanding harsh environments, for example in the transportation, oil and gas, or electric power sectors, as they can supply up to 420 W or 500 W of PoE power reliably at temperatures ranging from -40 to +85 °C. This yields a wide range of potential applications and advantages in industrial environments.

State-of-the-art intralogistics network

A highly complex practical example is the needs-based supply and disposal in the electronics production of the Siemens plant in Fuerth (Germany) using material boxes on Automated Guided Vehicles (AGVs). About 2,000 of these boxes are in circulation on AGVs. The Simatic RTLS real-time locating



SOURCE: SIEMENS

The comprehensive portfolio of PoE-capable network components and end devices from Siemens supports users in the efficient setup of individually structured network solutions which are adapted to the respective industrial requirements.

system provides transparency and, in the future, also collision safety. For position detection, RTLS transponders with a unique identification number are attached to the material boxes.

These transponders are captured by an independent wireless network of RTLS gateways at short time intervals and their positions are determined. The RTLS gateways mounted high up for optimal coverage are connected to the servers via a separate Industrial Ethernet network with Scalance X PoE switches. They are supplied with power over the network cable, as are various IWLAN access points for the wireless communication with the AGVs. This has greatly reduced the installation effort and significantly shortened the commissioning time.

General advantage not only for RTLS projects: the portfolio includes unmanaged and managed PoE switches in Layer 2 or Layer 3 variants. This allows networks to be structured individually and adapted precisely to changing requirements – as has become familiar.

Focus on product & process quality

Unambiguous and complete tracking of components and the monitoring, ideally, of all process steps are essential for a consistently high quality in a highly automated industrial production. Network-capable identification systems such as code readers and RFID (radio frequency identification) readers and cameras, the number of which is constantly growing, play a key role in this. And with it the cabling effort and the amounts of data.

High-performance PoE switches with data rates of up to 10 Gbps provide reserves for the increased use and aggregation of data from increasingly powerful end devices, such as high-resolution HD cameras for quality certification at measuring systems and other locations. With just a single cable, they can be installed and replaced quickly – without specialist thanks to the standardized configuration. Besides the quality, this keeps plant availability and thus productivity high.

The already greatly reduced cabling of industrial PoE components can be simplified even further with the aid of the FastConnect cabling system from Siemens. With it, system-tested solutions from a single source can be conveniently implemented with both RJ45 and M12 connectors.

More effective access protection

In particularly sensitive areas and in the highly automated production with autonomous AGVs or robots, protection against unauthorized access by means of cameras is important. These often widely spread, increasingly higher resolution cameras are also typically supplied via PoE in order to keep the cabling effort low.

Here, the amount of data also quickly exceeds the current, typical transmission rates. The PoE-capable Scalance XC-200 switches support uplink data rates of up to 10 Gbps and resolve any arising bottlenecks. Apart from that, these DIN rail switches can be operated like a classic automation device with 24 V DC, i.e., be powered by a conventional power supply such as Sitop.

The power monitoring in the Industrial Ethernet switch with PoE partially compensates for the lack of management or diagnostics functions in such cameras. And by means of ports which can be switched on/off individually, cameras can be restarted remotely in the event of an error. The use in redundant network structures is also readily possible.

Thanks to increased power, subsections outdoors can also be included via PoE. With up to 60 watts per port, heated cameras can also be supplied – ensuring operation at sub-zero temperatures.

Potential for the future

Power over Ethernet is a cost-effective way of supplying network infrastructure and end devices with data and power using Industrial Ethernet switches. This method is also compatible with upcoming technologies such as time-sensitive networking (TSN) and 5G. With PoE, end devices can be easily integrated into networks and optimally supplied. This makes end-to-end standardized communication solutions also possible for deterministic real-time applications – either wired via TSN or wireless in 5G networks.

Christian Homann, Process Industries, ***Siemens.***

Learn More

Cables create reliable connections in the forge

The VIVA Forging Company relies on LAPP for cables. Its Czech Republic forging operation uses cables in its quality control robots, and for other functions. Bus cables enable high speed PROFINET communication, and screened cables that offer resistance to mechanical damage and oils are used for transmitting sensor data.

HUMANS HAVE BEEN SHAPING HOT METAL for 5,000 years. But over the last hundred years, the hammer and open fire of the forge have been replaced by industrial production, where powerful machines have the power to shape thousands of tons of high-performance steel into components, for example for engines or chassis parts.

One of the leading manufacturers of forged components is the VIVA Forging Company from Zlín in the Czech Republic. On twelve forging presses, 500 employees produce steel parts weighing up to 30 kg for cars, trucks, forklift trucks, hydraulic systems, agricultural technology, mechanical engineering, mining, healthcare and much more, a total of over 20,000 tons a year. VIVA has its headquarters on the grounds of the former ZPS Zlín mechanical engineering company.

Strict requirements for quality

The forged products are delivered to customers like Bosch, Scania, ZF and Linde, and have to meet stringent quality requirements. As a result, VIVA is very selective when it comes to equipment used in its production lines, including the cables and cable systems. In the past the company bought them from wholesalers, but since 2011 they have been ordering directly from LAPP.

"Our customer chose us primarily because we offer a wide range of industrial cables, short lead times, personal advice and technical support" said Bohumir Hales, Product Manager at LAPP Czech Republic.

LAPP cables are used in the systems for high-precision production of rotating and non-rotating components for the automotive industry and mechanical engineering. They connect the processing centre and the robots on two state of the art robot lines, including the communication and safety channels. The robots perform quality testing on the cast parts.

Specifically, the following cables are supplied:

- ETHERLINE FD P FC Cat.5 bus cables for PROFINET for high speed machine network communication
- ETHERLINE ACCESS U08T switches
- EPIC DATA PN AX RJ45 T-connectors for reliable data transmission even in continuous operation

SOURCE: LAPP

LAPP cables are used in systems for high-precision production of rotating and non-rotating components for the automotive industry and mechanical engineering.

- ÖLFLEX CLASSIC 415 C and ÖLFLEX FD 855 CP are screened cables with high resistance to mechanical damage and oils, and are used for transmitting sensor data

In addition, cable types designed for moving supply cables are used, such as the ÖLFLEX FD 855 P, a halogen-free cable designed for power chains in demanding environments. This cable type is used for sensors and control units as well as for supplying power to motors. Another type used in machines is the temperature-resistant ÖLFLEX® HEAT 180 SiHF silicone cable.

SOURCE: LAPP

Cables connect the processing centre and robots on two state-of-the-art robot lines, including the communication and safety channels. The robots perform quality testing on the cast parts.

Short distances

All the materials used have selected to ensure a long service life. Even though working conditions in industry have improved considerably today, forging work still involves a lot of dust, high temperatures and increased risk of fire. The LAPP range includes numerous products suitable for these demanding operating conditions. As a result, 80% of the cables used in VIVA are now LAPP cables, and this figure is rising.

Another reason why VIVA relies on LAPP cables is the short distance to

LAPP Czech Republic s.r.o. in Otrokovice, which is just ten kilometres away. The competence and production centre for ÖLFLEX Connect is located there. Under this brand name, LAPP supplies ready-made products, from simple assembly of cables and connectors to fully assembled cable chains to meet customer requirements, which the customer can use directly in their plant with minimal additional effort.

Application article by ***Lapp.***

Learn More

High data rates for effective vision-based sorting

Optical sorting machines for the seed industry rely on EtherCAT plug-in modules for fast real-time communication technology that optimally supports the high data rates of the vision-based sorters. Compact I/O modules reduce hardware requirements, as well as costs, and cut equipment assembly times in half.

FOR ITS SOLUTIONS FOR AUTOMATIC SEED sorting, VMek relies on EtherCAT from the very beginning. The fast real-time communication technology optimally supports the high data rates of the vision-based sorters. With a switch in the I/O level to EtherCAT plug-in modules, the company succeeded in further reducing costs, device footprint and commissioning times.

In 2012, Kent Lovvorn, general manager of VMek™ Sorting Technology in Midlothian, Virginia, left his previous job with a clear vision: "I wanted to specialize in some segment of high-speed machine vision." The company he founded in 2014 offers numerous software and hardware solutions for optical sorting. The machines, including the Metrix Analytic Lab Color Sorter™ and Element Analytic Production Color Sorter™, leverage new technologies to meet the needs of customers in the agriculture industry, including the top three seed producers in the U.S.

SOURCE: BECKHOFF

The top seed companies in the U.S. divide acceptable seeds from those that do not meet color or size standards using software and hardware solutions from VMek.

The Metrix machine uses two full-color GigE cameras and offers a throughput of 600 seeds per second, while the Element sorter with four such cameras even achieves a throughput of 12,000 seeds per second. Unlike other color sorters, which only separate products into good and bad parts, the VMek systems are able to provide valuable data on every seed in real-time, as Kent Lovvorn explains: "Our software performs composite analysis using the front and back images of each item. The software isolates each part and mates them together to complete a 360-degree full-part analysis."

SOURCE: BECKHOFF

The Metrix Analytic Lab Color Sorter, one of VMek Sorting Technology's top hardware solutions, uses two full-color GigE cameras to separate and gather data on seeds.

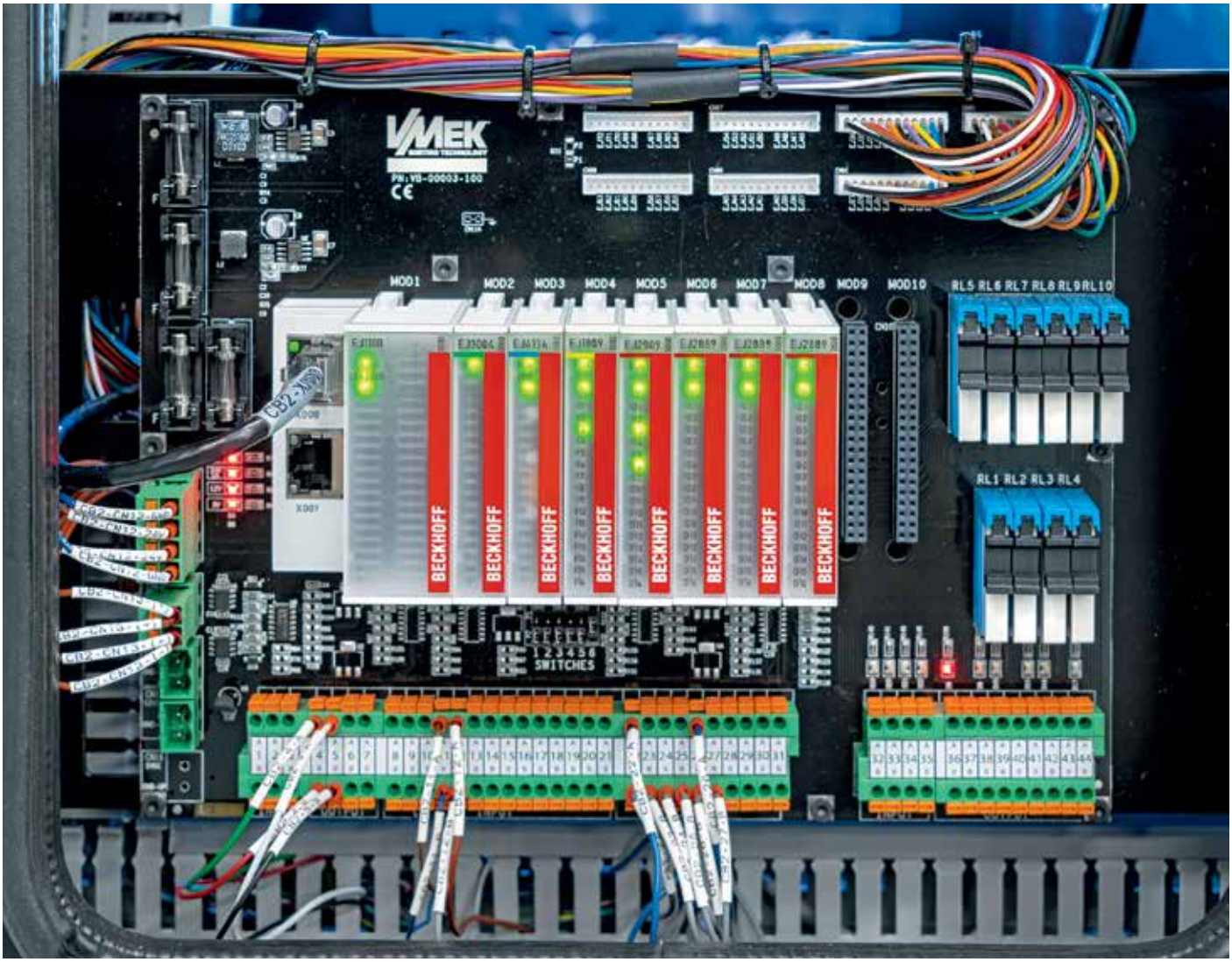
This data allows seed producers to analyze why individual parts were rejected and compare lab results with plant floor realities. They can also use insights to plan for the future, Kent Lovvorn explains: "The seed companies can plan accordingly for the next grow cycle to either enhance or eliminate specific traits."

Improvement in I/O solutions

From the beginning, company founder Kent Lovvorn believed that continuous improvement of these high-tech systems would only be possible by partnering with top-tier vendors: "When I started to lay the foundations for VMek, I searched for hardware and software partners that developed quality components the right way. That's when I found Beckhoff."

During a presentation on the EtherCAT industrial Ethernet protocol, Kent Lovvorn learned about the network's ability to use PCs as real-time machine controllers. He decided

SOURCE: BECKHOFF



The compact EJ boards reduce footprint on VMek hardware solutions. The LED lights of the EtherCAT plug-in modules can be seen through a window on the machines and provide important EtherCAT diagnostic information at first glance.

then that in his opinion EtherCAT was the best technology to use in his high-speed vision machines, and this led to the decision to standardize on EtherCAT I/O terminals from Beckhoff.

During a 2017 redesign of several systems, VMek set out to further reduce costs and space requirements but wanted to continue using EtherCAT hardware. This effort did not need to increase reliability, as the first machine that shipped in 2015 has operated continuously and reliably. The aim was rather to enhance the offerings and decrease time to market by reducing the amount of hardware modules and the requirements for point-to-point wiring.

Footprint, costs and assembly time

Through discussions with Beckhoff Regional Sales Engineer Chuck Padvorac, Lovvorn found a fitting solution: pluggable EJ series EtherCAT modules.

These I/O modules are roughly half the size of standard EtherCAT Terminals, but they provide the same functionality. Together with the JST connectors selected by VMek for this application, they mount directly to custom-designed PCB boards, and the entire signal distribution board connects to the larger PC-based system via prefabricated cables or coded plug connectors. Because the boards come essentially prebuilt, this makes series production more efficient and cost effective compared to traditionally wired terminals.

"The core benefits were logical and came down to the ease of use that enables us to build distribution boards with the exact functionality, size, connectors and labeling we need," explained Lovvorn. "Because the signal distribution board for each machine is customized for our designs and processes, we can build machines prior to buying the EJ components, which delivers benefits in terms of equipment costs and just-in-time assembly."

Sorting technology advances

By implementing EJ series EtherCAT I/O modules with standardized signal distribution boards for each sorting machine, VMek was able to cut time to market significantly. "We estimate that we reduced our equipment assembly time by 50%," Kent Lovvorn said. "We have also minimized service time, if it's ever needed." Small adjustments at the hardware level helped VMek cut costs by roughly 700 U.S. dollars per I/O segment, and the company reinvested these savings in R&D to continue to enhance its optical sorting machines and software.

"As leaders in agribusiness, our customers see our complex sorting algorithms and ability to gather data on every part as indispensable," said Lovvorn.

Therefore, VMek will continue to focus on the continuous development of its solutions in collaboration with partners that work to lead in their fields.

James Figy, Senior Content Specialist, ***Beckhoff USA.***

Visit Website

Blend of networks for production scale in wireless IoT deployments

Nick Sacke, head of IoT and products at Comms365, outlines the key considerations and questions that must be asked ahead of an IoT production rollout. He also describes why there is a necessity to use a blended strategy for network connectivity, rather than to look for a 'one size fits all' connectivity approach.

IOT DEPLOYMENTS ARE UNDERPINNED BY A carefully orchestrated connectivity layer, but there is an ongoing debate about which network types and protocols are better suited for supporting mass sensor deployments. The decision regarding which network is to be used is an early consideration for IoT deployments, but how do you determine availability and which network will give you the best solution and project outcomes?

SOURCE: COMMS365

Sacke says there are two reasons for different IoT networks and protocols: evolution and innovation.

IoT communication technologies

Why are there different IoT networks and protocols? The short answer can be captured in two words, evolution and innovation. Over time, IoT sensor technology has evolved in capability, potential for scale and reduction in cost per module. This has created demand for new wireless network protocols and methods to support new sensor types, many of which rely on battery power and infrequent messaging at long range, and over a wide area.

Doubt, uncertainty and fragmentation in the IoT market, combined with increasing sensor hardware and software innovation, have led to the creation and fielding of several network connectivity options, each with their own attributes. We are very much still in the early adopter stage as multiple standards coexist and compete in a land-grab operation until certain standards take hold.

In recent years we've witnessed the growing expansion and evolution of one dominant IoT Network type, the Low Power Wide Area Network (LPWAN). The early entrants to this market, LoRaWAN and Sigfox, use free-to-air radio spectrum, and have had time to establish themselves across the world.

LoRaWAN in particular has been a runaway success as an IoT Network connectivity option, dominating the market with over 40% market share of new connections, which is projected to continue adding market share through 2025. Both LoRaWAN and Sigfox are now acknowledged as global network and protocol standards for IoT through establishing trust with users who are confident in the usability, scale and reliability of such networks.

SOURCE: COMMS365

LoRaWAN in particular has been a runaway success as an IoT Network connectivity option.

On the cellular side, for new IoT network protocols NB-IoT and LTE-M (evolutions of the 4G spectrum that have now been adopted under the 5G standard), there is still an element of catchup in progress. The GSMA was late in ratifying the standards for these IoT protocols and ultimately their deployment by Tier 1 carriers came sometime after the initial rollouts of the first LPWAN network connectivity protocols.

Despite initial predictions claiming that the cellular IoT Network variants would dominate the IoT connectivity market and squeeze LoRaWAN and Sigfox to the margins, there has been a lack of intensity in UK rollout of the cellular IoT network programmes (at the time of writing, LTE-M has been enabled in the Eastern half of the UK, and NB-IoT has 'holes' in its' coverage, particularly in the Eastern side of the UK).

This means that IoT cellular LPWAN work has been largely limited to testing in the UK, while production rollouts are dominated by Private Council LoRaWAN installations and innovation programmes on public network variants of both LoRaWAN and Sigfox.

Globally, analysts project that there will be a 50:50 split in LPWAN network deployments between the free-to-air (unlicensed spectrum)

and cellular variants (licensed spectrum) – the competition between these network standards will continue for some time to come. In particular, once 5G is fully rolled out and there are radio modules at a workable cost point for IoT, 5G protocols will also have an IoT element for the cellular side that will bring increased scale and efficiency in terms of its capability to connect millions of sensors per square kilometer.

Which protocol to use?

As with most projects, cost of delivery for data is a primary concern that must be addressed. LoRaWAN and Sigfox are now at a level of maturity where the devices are cost-effective. Initially, cellular was a much higher cost, but is now starting to achieve cost-effectiveness. But in terms of usage costs, for NB-IoT and LTE-M, users are still paying for data usage on the network (paying by the byte), whereas LoRaWAN leverages the free-to-air spectrum facility and charges are based on device licensing, and in the case of Sigfox, per message.

Even though there appears to be a clear differential in terms of cost models, the choice of network and protocol isn't straightforward. As IoT rollouts become more commonplace, there are elements within a LoRaWAN environment that create cause for concern. With multiple devices sharing the LoRaWAN spectrum, this can cause potential collisions on the network and lost messages. In order to ensure each message arrives at its destination, the LoRaWAN protocol and software controlling the network has been adapted further to mitigate against this happening by spreading messages across multiple channels, monitoring message counters, and other techniques.

Identifying the parameters of the use case and the nature of the deployment is very important. If a message with telemetry data such as bin fill levels or parking events only needs to be sent when there is a status change, this won't necessarily create network congestion on a LoRaWAN Network, as the messages aren't sent at the same time.

Regular 15 minute monitoring of environmental conditions from multiple sensors in an area may however require additional gateway capacity to ensure spreading the sensor message load. But if your use case requires guaranteed delivery of traffic within a specific time period, or a constant stream of messages cellular protocols such as NB-IoT and LTE-M may need to be used.

Use cases

Another consideration is the protocols certain sectors are already using to gain traction. We're seeing a tremendous uptake and interest in LoRaWAN for local governments that see it as a mechanism they can use to scale multiple use cases at once.

SOURCE: COMMS365

In most projects, cost of delivery for data is a primary concern that must be addressed.

In the utility monitoring sector, NB-IoT appears to be the protocol gaining the advantage. No gateways are required as signal towers are the enablement point and it has deep penetration under the ground with good signal strength to reach its destination.

But when it comes to monitoring elements deep within buildings, LoRaWAN can be more effective compared to what NB-IoT can do from the outside in. Refrigeration and temperature monitoring is one such example with the rollout of the Covid-19 vaccine which must be stored at precise chilled temperatures. LoRaWAN can provide an effective protocol in this instance, measuring the temperature deep inside the building, all the way down to the probe. Intensive monitoring and data collection will become critical.

For a use case such as measuring readings intermittently, on an alert basis or once an hour, you need to conserve battery power so the sensors last a long time and will likely be leading towards the unlicensed spectrum. Whereas within a healthcare monitoring scenario, such as in someone's home or in an ambulance on the move, readings will need to be sent through immediately, so will need to rely on the licensed spectrum, such as LTE-M.

Blended connectivity

At this point in time, there is no one protocol that is optimised for every use case or can cover an entire estate. The solution is, therefore, to deploy a hybrid model, one which blends different connectivity protocols together, from the unlicensed and licenced spectrums, to achieve total estate and use case coverage. A blended approach is inherently flexible, cost-effective and scalable – ideal for those that are looking to reap the benefits of mass-scale IoT but are uncertain as to how and where to proceed.

Futureproof

Longevity is crucial for the success of an IoT deployment. No business wants to rip and replace the technology after ten years. It's clear that LoRaWAN in particular is on a growth trajectory that will provide that longevity. And the eventual maturity of 5G will also become another option for IoT projects, with much more efficiency in terms of capability to connect millions of sensors. 5G may be a way off yet, but it's likely that many estates of devices and networks will eventually have parts of them consumed by 5G.

With a blended model of different protocols covering each estate, to make it efficient and streamlined, it's important for a single platform to be used that can bring it all together and be received, read and analysed in one place. NB-IoT, LoRaWAN, LTE-M, Sigfox are all becoming industry-standard protocols that are each received in a different format. But they can be streamlined into one hub that intercepts the traffic and converts it into a protocol that the receiving application requires.

By working with a partner offering all types of IoT connectivity in a blended solution, projects can be rolled out in the confidence that each protocol has been considered and is supported, to maximise the functionality, practicality and cost-efficiency of an entire IoT project.

Nick Sacke, Head of IoT and Products, ***Comms365.***

Visit Website

TSN technology: basics of Ethernet Frame Preemption

Ethernet Frame Preemption is a new extension to Ethernet. Part of Time-Sensitive Networking (TSN), it guarantees a constant cycle time for industrial applications. Why this extension is necessary, and the way it works is described in two articles. Look for Part 2 in the next issue of the Industrial Ethernet Book.

TO FULFIL THE NEEDS OF A CONTROL APPLICATION IN AN INDUSTRIAL machine, robot, CNC-machine or any other application requiring real-time processing, all components of such a system must work in a predictable manner. This also holds for any network used: messages must be delivered in time (or at least: not too late). But when Ethernet is used, there is no guarantee that this will happen. Traditionally, the "solution" is to keep the load on the network as low as possible; some vendors recommend to not go higher than 3%.

The problem with Ethernet is that it allows any device to send messages at any moment. Sometimes this is just too much for the network to handle. Messages are then queued in a "FIFO" manner: first-in, first-out. A message with high urgency can then be delayed by messages in front it, which just happened to arrive a little bit earlier. You recognize this probably: the same happens on the highway during rush-hours. In some industrial Ethernet protocols, like EtherCAT and Profinet, solutions have been invented to guarantee predictable behavior. But these are always protocol-specific solutions, and not standard available on Ethernet. A more generic solution has been developed as part of the "TSN"(Time Sensitive Networking) extensions, according to the (new) IEEE standards IEEE 802.3br and IEEE 802.1Qbu, popularly known as "Frame Preemption".

Cyclic communication

In industrial networks, it is very often seen that the application software runs in a cycle; the same code is executed again and again. The cycle times are usually in the order of milliseconds, but this can also be in the microsecond range for the applications with the highest demands regarding handling of events, accuracy, or output.

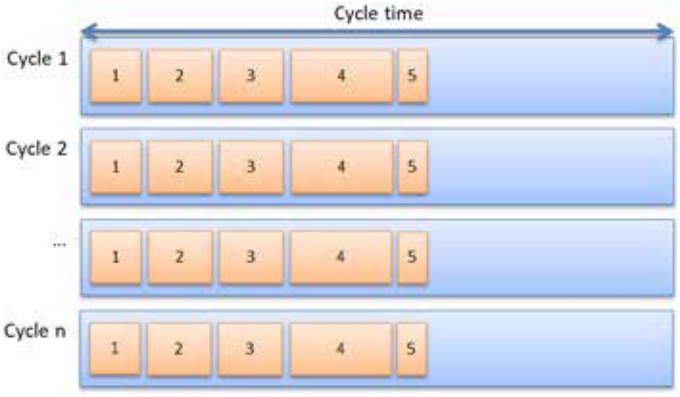
Every cycle the same processing is done: get all current inputs (digital, analogue, encoders, servo's, camera's, etc.), run the application software, set all outputs to their new values (digital, analogue, HMI's, servo's, etc.). This cyclic way of working is typical for PLC's (Programmable Logic Controllers) and DCS's (Distributed Control Systems), but also often seen in real-time applications.

The cycle time is constant. This allows the software to respond in time to any external events: in the same cycle, or perhaps the next. So when the cycle time is exceeded, timely response to external events cannot be guaranteed, and this is often a reason to alert the operator.

Communication is done via the network to the subordinate devices, and they must respond as quickly as possible. What happens on the network is completely predictable: the number of devices is known and the amount of data per device too

Thus, what happens on the network is quite boring: always the same, the whole day: read inputs from device #1, read inputs from device #2, read inputs from device #3, etc. and at the end of the cycle: set outputs on device #1, set outputs on device #2, etc. Given the fixed number of devices and fixed I/O, it can be calculated in advance how much bits are transferred. Give the bitrate, it can also be calculated how long all transmissions are going to take.

So, we can calculate in advance how much time is needed for the network communication. Confusingly, this is also called "cycle time". Ideally, this network cycle time is shorter than the cycle time for the software, so it is not delayed by the network.



Cyclic transfer of 5 messages always takes the same time, every cycle.

In practice, the application software and the network run in parallel: while the software is running with data from network cycle 'n', the network is collecting data for cycle 'n+1'. Even then, the network must be ready before the application software wants to start its next cycle.

Most existing industrial networks, both of the 1st generation (i.e., Profibus, Interbus, CAN, DeviceNet) and of the 2nd generation (Profinet, EtherCAT, etc.) function this way.

Acyclic data

Apart from the cyclic communication done on a network there is often a need for acyclic network messages. These are messages that come at (for the network) unexpected moments, for example due to the operator giving special commands ("Stop!"), because an error occurs somewhere, because diagnostic data is retrieved, because data must be downloaded, a webpage being read from a devices server, or any sort of communication over the network (even network managers starting a backup on a production network). There must be some room for extra messages but not too much, otherwise the network cycle becomes too long and the application software must wait.

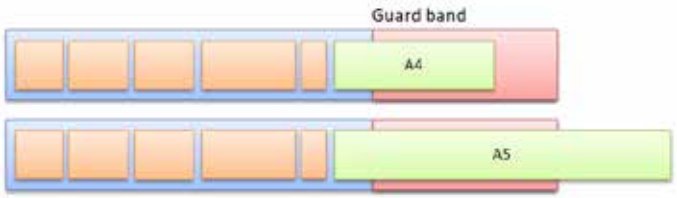
The extra time allotted may also not be too short, otherwise long network messages cannot be completely transmitted within the available time. One solution is to allow for one full-length Ethernet message. Simple as it sounds, it has one drawback: a full-length Ethernet message can contain 1500 bytes of data, which is a huge amount compared to the usually small messages used for cyclic data – and, if there is no acyclic data, the network is doing nothing for the duration of one full-length Ethernet message. Additionally, is it guaranteed that there will be only one acyclic message? Or can there be more? In any case, if there is too much acyclic traffic to fit in a cycle, the next cycle will suffer – its cyclic data is transmitted too late. They must wait for message A3 to be finished (FIFO).

What happens next depends on the application software. Did it miss

Two network cycles, each showing the same number of cyclic messages with the same amount of data. In both cycles one acyclic message (A1, A2) is sent, with different data.

important signals? Is equipment going to be damaged? Is production delayed? Can people get hurt?

Guard band



A too long acyclic message exceeds the time allotted to cycle 1. The cyclic messages in cycle 2 are transmitted too late.

To prevent that too long or too many acyclic messages extend the cycle time, the "guard band" is used. It is a (configurable) period of time at the end of each cycle. Transmission of a network message may only start when it is guaranteed that it finishes in the guard band (= before the end of the cycle). The next cycle can always start at the expected moment. If there are network messages that could not be transmitted in the previous cycle, they can now be transmitted (time allowing).

The figure above (top) shows the transmission of only one acyclic message A4. But there is still time left in the guard band, so more messages may follow (if there are any). If there are none, the time is still wasted. So the network manager will tend to make the guard band as short as possible, but this may give a problem: too long messages (A5) cannot be transmitted anymore, they never fit! (figure bottom). This is especially troublesome in protocols where the application / user has no control over the size of network messages, such as in TCP/IP.

So the guard band solves one problem, but there is still one to go: how to handle very long messages. It is this issue which "frame preemption" is going to solve for us. Its functionality is specified in IEEE 802.3br.

Express messages

Before we continue with the detailed explanation of the inner working of Ethernet frame preemption, we must first agree on the terminology. The real-time messages that are sent first in a cycle are called the "Express" messages. They are never subject to preemption. All other messages (called acyclic above), are called "Normal" messages. If they do not fit in the guard band, they are subject to preemption.

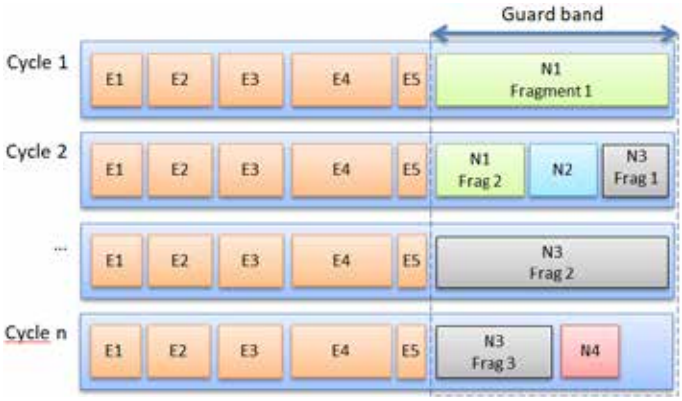
Frame preemption

This (for Ethernet) new technique solves the problem of a too long network message which doesn't fit in a cycle. Simply explained, it does the following:

- D- Stop (preempt) the transmission of too long messages before the end of the guard band.
- Continue the transmission of the remainder of the message in the next cycle, following the express messages.

In Ethernet terminology, the preempted message is sent in multiple (>= 2) fragments. At the receiver, the fragments are assembled again to re-create (a copy of) the original network message.

In the figure above at the right, message N1 is too long to be completely transmitted in the guard band of cycle 1. It is thus preempted. After the transmission of this first fragment is stopped, the next cycle 2 can start at the expected moment. When the express messages have been transmitted, transmission of the second fragment of N1 is done. As there is still time in the guard band available, N2 can be transmitted too. With still time left, the first fragment of N3 can be transmitted. This is such a long message that even in the next cycle it cannot be completely transmitted, so it is preempted again, and the third fragment is sent in cycle 3. With enough time available, N4 can be transmitted. With nothing else to do, the line is silent for the remainder of the guard band.



A too long message N1 is transmitted in fragments over multiple cycles. As long as there is time in the guard band, additional messages may be sent too (N2, N3, N4). If they don't fit they are fragmented too, etc.

For the receiving software, the fragmentation of messages is completely invisible. N1 is passed on to higher protocol levels only when the second fragment is completely received; identically so for message N3 after reception of the third fragment. So, for higher protocol levels it looks like any other Ethernet message. That the total transmission time is a little bit longer is unnoticeable; the message could as well have been sent a little later.

Error handling

What happens when the data in a fragment is corrupted while in-transit? The receiver detects this with a CRC which is appended to each fragment. Corrupted fragments are summarily discarded, just as any normal Ethernet message with corrupted data. But discarding a fragment means that (even when all other fragments are received without errors) the original Ethernet message cannot be re-created, so the message is completely lost. The frame preemption algorithm does not perform any error recovery, unlike TCP/IP which can detect missing fragments in a data stream. But that is at a higher protocol level, which has more intelligence, RAM and CPU power. Adding such a capability to a frame preemption implementation would unnecessarily make it more complex, error-prone and slow.

So the frame preemption algorithm just follows the "I've tried it and it didn't work out; so now it's your problem" way of working, also called "Best Effort" in Ethernet jargon. Or: let higher protocol-levels detect and handle the missing message(s).

Backwards compatibility

Most Ethernet devices will never support frame preemption, as it is very specific for real-time applications. But how does a device with support for frame preemption communicate with a device that doesn't? Simply: without frame preemption being used. The device with frame preemption capabilities asks the other device whether it supports it (via a special negotiation message). Because the other device doesn't support it, it doesn't understand it, so no answer comes back, and so it is decided not to use the frame preemption feature.

If it so happens that the other device does support frame preemption, it will say so, and the new feature can be used. Both devices (at both ends of the cable) must ask the other, so usually both parties will use frame preemption, but it is also possible that only one device does so (however unlikely). This is not a problem for Ethernet, because it is a full-duplex technology. Note that on a switch frame, preemption usage can thus be different for each port.

In the next issue of IEB, we will continue this discussion with a detailed explanation of the implementation of frame preemption.

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

TSN in the railway sector: why, what and how?

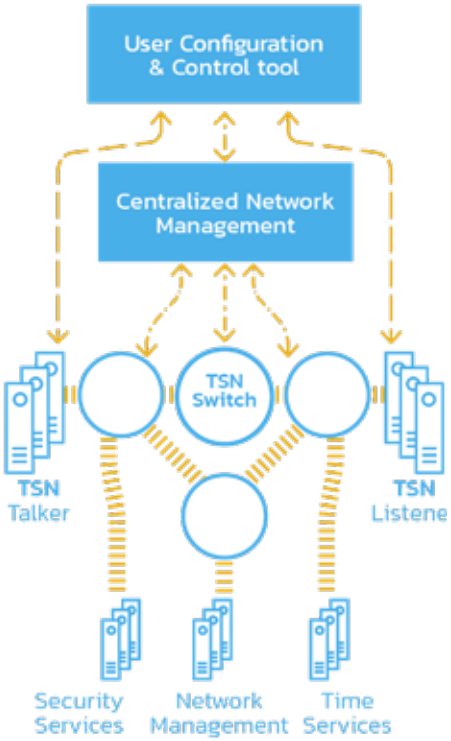
The railway sector has evolved from serial Train Communication Networks to Ethernet based solutions. But the lack of real-time traffic communication and functions isolation capabilities of traditional Ethernet has limited the adoption of standardized Ethernet based solutions.

TSN OVERCOMES IDENTIFIED LIMITATIONS AND it has been identified as the next generation Data Link layer for railway communications by the railway manufactures and operators. This article summarizes why TSN has become the preferred next-generation network protocol for the sector, what is TSN and how it is being introduced within the train networks. Additionally, a proposal for a TSN-capable edge-computing device and an advanced TSN set-up are presented.

TSN in the railway sector

In 1999 a train on-board communication standard was published by the IEC. This standard, the IEC 61375 or TCN (Train Communication Network), allows interchanging data among the different electronic subsystems, supplied by several manufacturers. Also, the standard allows to joint different trains or vehicles. For interoperability among trains of different manufacturers and countries, the Union Internationale des Chemins de Fer (UIC) defines the semantics of the exchanged variables and messages in the UIC-556 leaflet.

Nowadays, the TCN standard allows a safe, reliable, and robust communication, as it is required for a passenger transport system. The information exchanged inside transportation systems has grown so much, that TCN has become obsolete and expensive. As an example of these limitations, Wire Train Bus (WTB) defined in TCN supports a maximum data rate of 1 Mbit/s that limits the usage of the backbone to control and status commands, only. Video surveillance, for example, needs a much higher bandwidth, and passenger comfort functions may demand even more. As a result of these limitations, the evolution of TCN has derived in many cases in solutions based on existing Industrial Ethernet solutions mixed with original TCN standard.



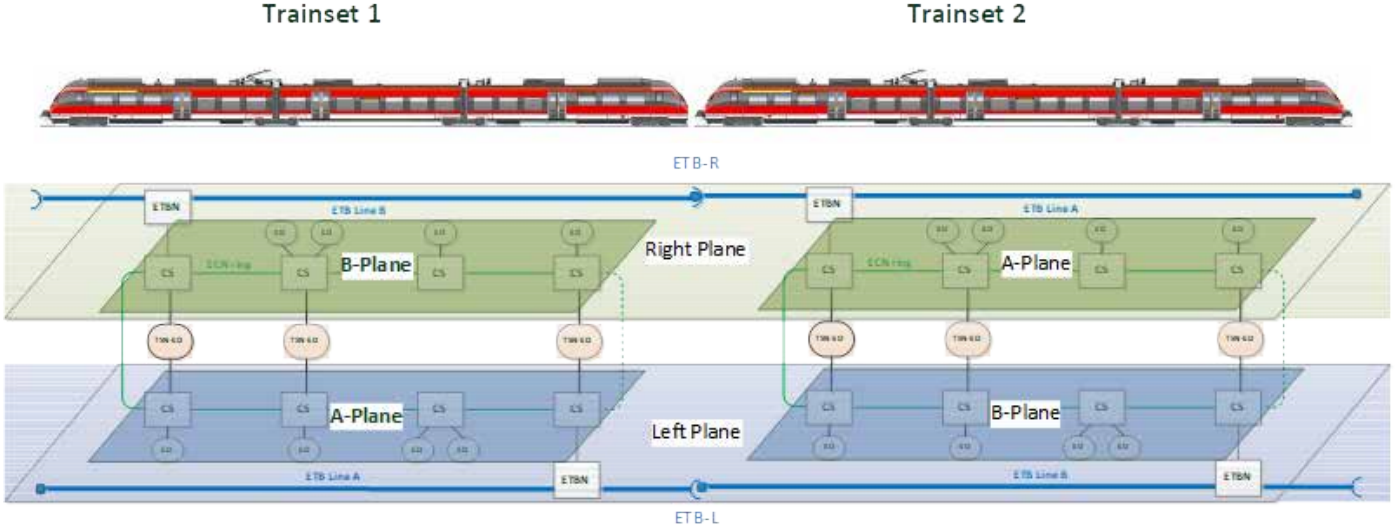
SOURCE: RELYUM

TSN network architecture.

To move forward on an interoperable Ethernet based solution for the Sector, in 2005 the IEC commissioned a new working group to publish a new standard based on Ethernet devices. As a result, Ethernet Train Backbone (ETB) was proposed as the train-wide communication backbone. It replaced WTB in Train Communication Network in the IEC-61375-2-5 standard. IEC-61375-3-4 defined the Ethernet Consist Network (ECN) for the communications inside the car, replacing the Multifunction Vehicle Bus (MVB) specified in the original TCN standard.

Thus, these IEC 61375-family standards define a faster TCN based on standard 100Mbit/s Ethernet in combination with proprietary higher layer protocols like TRDP, IPTCom or CIP. Indeed, current trains use these proprietary protocols, creating a complex ecosystem.

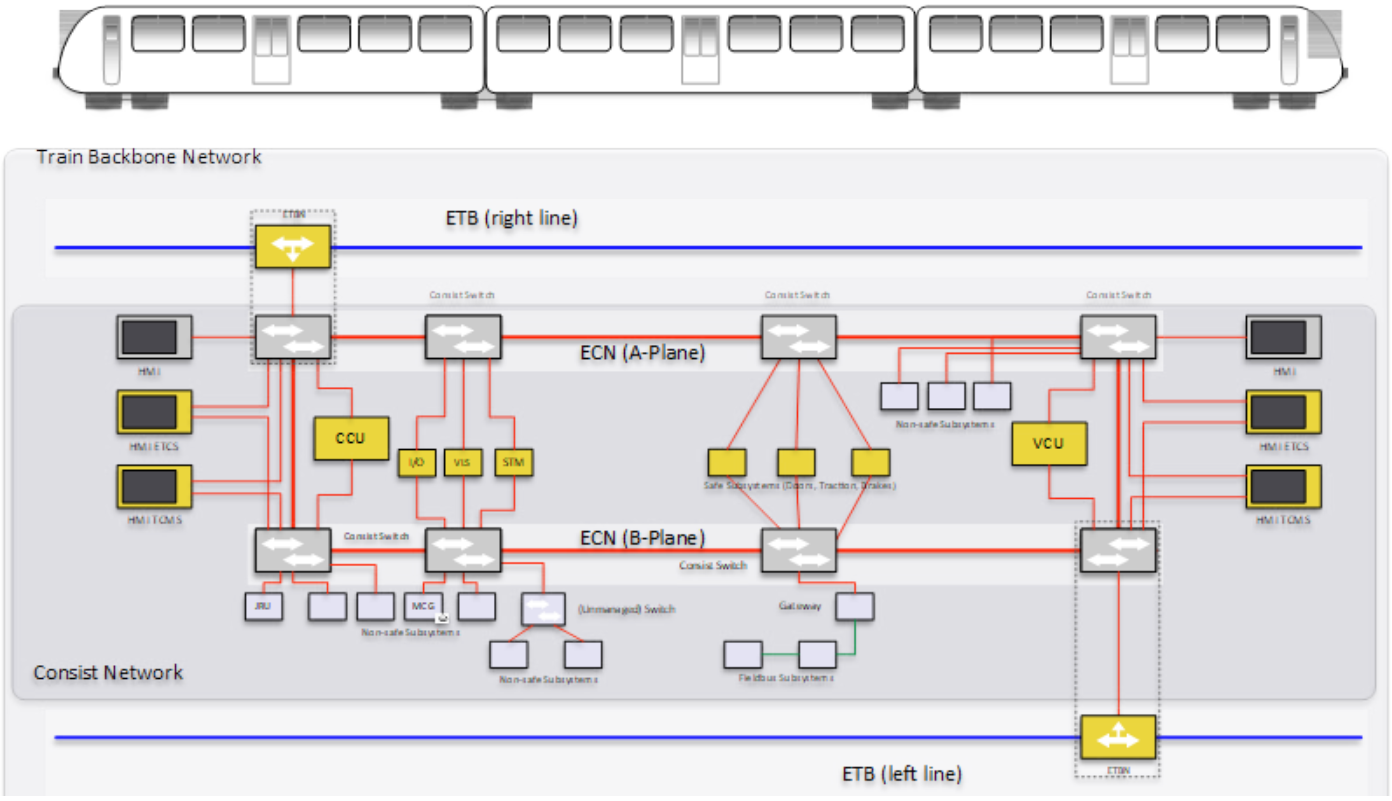
The adoption of Ethernet within this context has revealed some limitations. The standard Ethernet lacks for mechanisms to isolate traffic for different functions and for real time traffic communication. Therefore, it has been used typically for non-critical applications in parallel with specialized networks for the critical ones. Due to this fact, usually multiple



SOURCE: RELYUM

TSN based ETB and ECN networks in NG-TCN. Connecta-Shift2Rail EU Project. CONTRIBUTING TO SHIFT2RAIL'S NEXT GENERATION OF HIGH CAPABLE AND SAFE TCMS AND BRAKES. D3.5 – Drive-by-Data Architecture Specification. https://projects.shift2rail.org. 2018.

SOURCE: RELYUM



OCORAUVCCB integrated in ECN (ng-TCN). Open CCS On-board Reference Architecture (OCORA). UVCC Bus Evaluation. Gamma Release Document. https://github.com/OCORA-Public/Publication. 2020.

buses coexist in the same consist, turning into an increase of Life Cycle Cost (LCC).

Time-Sensitive Networking (TSN), the next generation standard Ethernet, provides strict determinism, redundancy, high-bandwidth, and interoperability. TSN overcomes the limitations identified in the sector. Thus, it can offer simpler network infrastructure and simplifies the whole sub-systems integration. As it will be presented in the next section, the new generation train communications networks proposed by the Train manufactures are based on TSN.

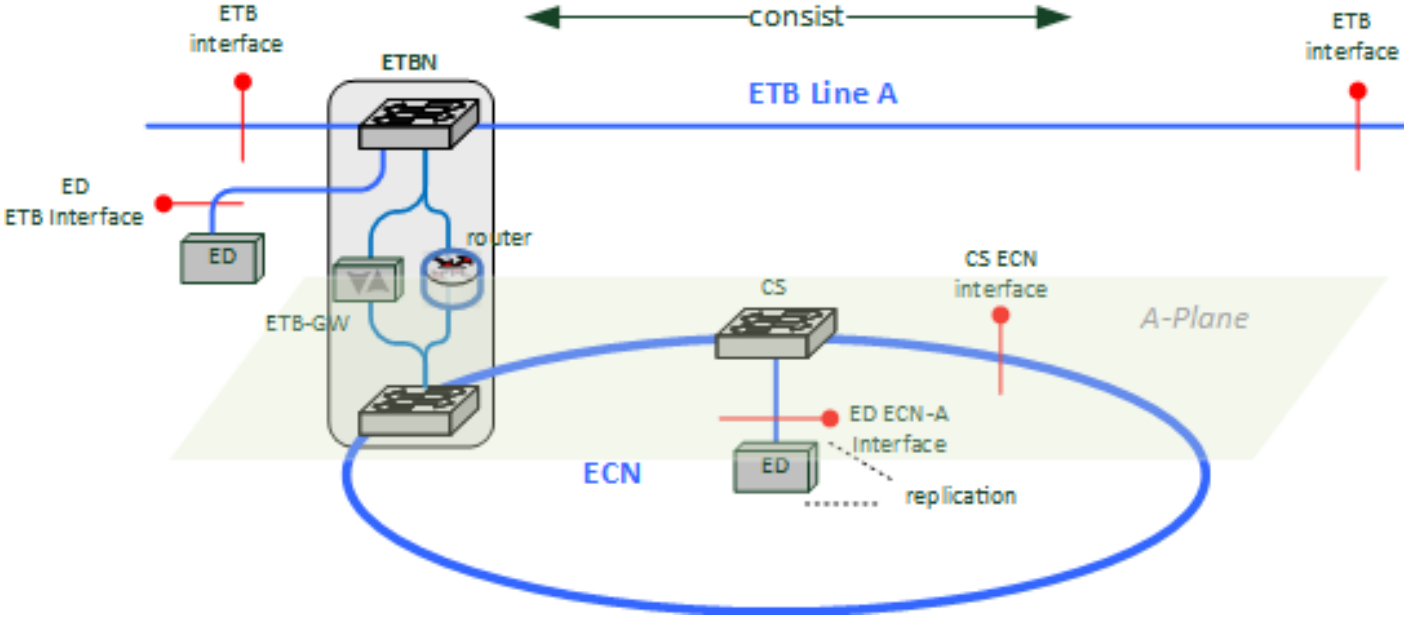
The relevance of TSN in the sector is not only driven by the train manufacturers. Railway operators, like Deutsche Bahn AG or SNCF have pushed the Open CCS On-board Reference Architecture (OCORA) platform for cooperation to the benefit of the European Railway sector to develop an open reference architecture for on-board command-control and signaling systems.

TSN is the proposed Data Link layer for real time traffic in this architecture.

What is TSN?

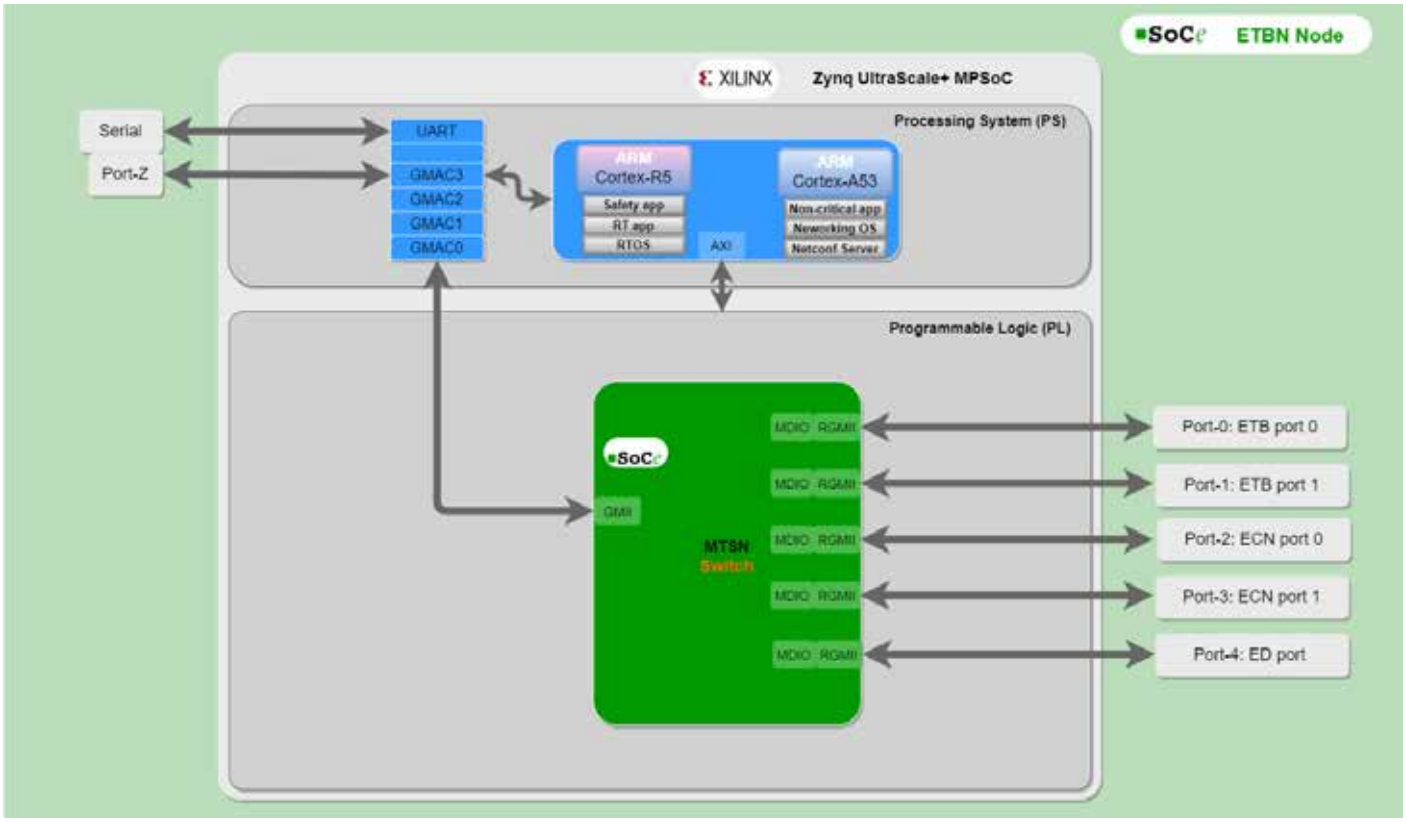
A significant success in merging critical and best effort traffic in a single media was achieved by Audio Video Bridging (AVB) initiative. Indeed, some of their technical solutions were valuable alternatives to other sectors.

As a result, the original AVB working group



SOURCE: RELYUM

5x ports ETBN. Connecta-Shift2Rail EU Project. CONTRIBUTING TO SHIFT2RAIL'S NEXT GENERATION OF HIGH CAPABLE AND SAFE TCMS AND BRAKES. D3.5 – Drive-by-Data Architecture Specification. https://projects.shift2rail.org. 2018.



SOURCE: RELYUM

SoC design for a five port ETBN.

evolved to IEEE Time-Sensitive Networking (TSN) Task Group, which oversees developing the standards related to TSN. These standards propose enhancements for IEEE 802.3 networks to define a unique Ethernet based solution for OT and IT.

The fundamental base in TSN is the Time-Aware Shaper. It is designed to separate the communication on the Ethernet network into fixed length, repeating time cycles. These cycles are divided into timeslots according to the TSN configuration agreed between peers. The different time slots can be configured and can be assigned to one or several of the eight Ethernet priorities. The operation of the Time-Aware Shaper is defined in IEEE 802.1Qbv.

Considering this functionality, three basic traffic types are defined: Scheduled traffic, Best-effort Traffic and Reserved Traffic. Scheduled Traffic type is appropriated for the hard real-time messages, and the Best-effort Traffic is the general Ethernet traffic that is not sensitive to any other Quality of Service metrics.

The Reserved Traffic type is for frames allocated in different timeslots but with a specified bandwidth reservation for each priority type.

The Time Aware Shaper allows defining the number of time slots available in each cycle, their duration and which priorities can be transmitted. Thanks to this mode of operation, the Scheduled Traffic has dedicated time slots to ensure the expected deterministic behavior. The best-effort traffic is accommodated in the remaining timeslots of each cycle of operation. An important improvement for the prioritization and bandwidth usage optimization in TSN is the support of Credit Based Shaper, as defined in IEEE 802.1Qav.

This functionality allows using Reserved Traffic type, upgrading the priority of designed traffic in a state between the Scheduled Traffic and the Best-effort one.

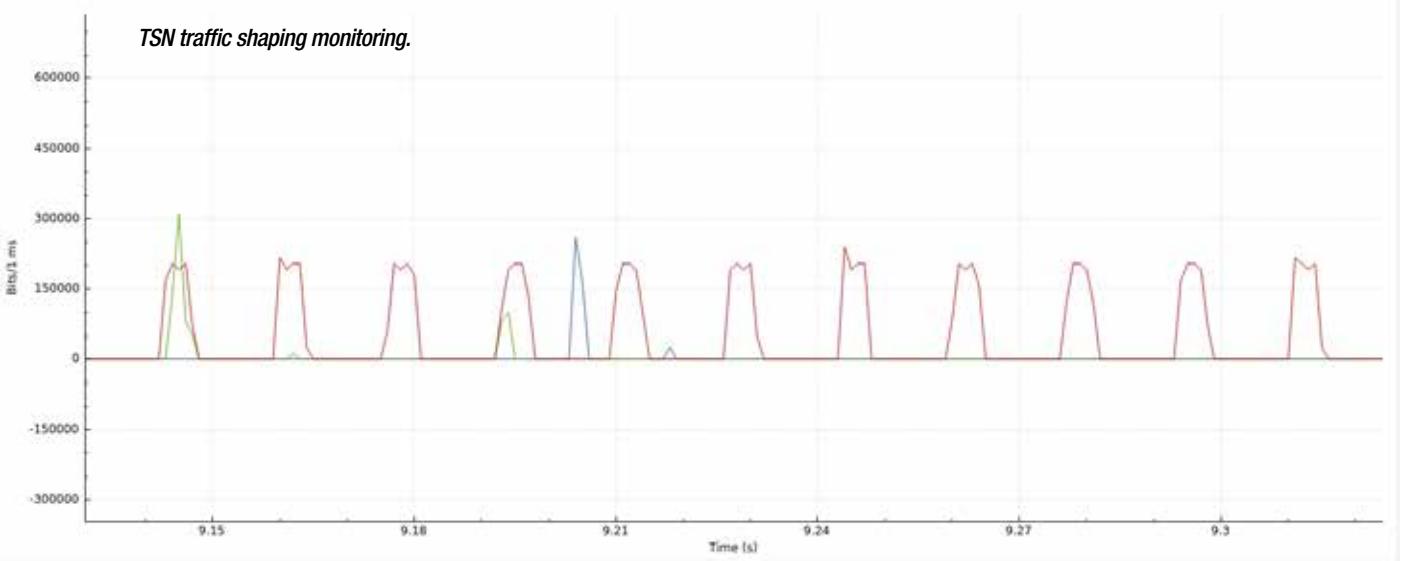
The technical challenge of providing nanosecond range synchronization accuracy among the TSN devices that compose the network is faced using IEEE 1588 timing synchronization protocol. Thanks to the accuracy provided by this technology, it is feasible ensuring controlled network delay and jitter implanting effective time-triggered Ethernet based solution. The specific IEEE 1588 profile for TSN is named IEEE 1588ASrev.

The configuration plane of a TSN Network is one of the most active topics in the standardization groups, industry, and academia.

TSN communications are based on a data streams set between a Talker and a Receiver. Based on the agreed parameters for each Stream, it is necessary to configure all the elements of the TSN network to switch the frames based on the selected parameters. This operation is performed by a Centralized Network Configuration (CNC) node. This CNC shall be able to talk to the equipment of

SOURCE: RELYUM

Credit Based Shaper test using an evaluation kit.



TSN traffic shaping monitoring.

SOURCE: RELYUM

different vendors in a standardized way. The early advances in this field are based on IEEE 802.1Qcc standard.

As it can be depicted from this introduction, TSN is not a single standard. Instead, it is a group of standards that are evolving at a different pace. Furthermore, many of them are still draft versions and probably, its evolution will depend on the real demand of these specific features from the market. The following list summarizes the most relevant standards involved in TSN: 802.1ASrev Timing and synchronization (currently, 802.1AS is used in most TSN implementations); 802.1Qbv Time-aware shaping; 802.1Qcc Stream Reservation Protocol Enhancements and Performance Improvements; 802.1Qci Per-stream filtering and policing; 802.1CB Redundancy; 802.1Qbu Frame pre-emption and 802.1Qch Cyclic queuing and forwarding.

TSN in the railway sector

Train manufacturers and Railway operators are pushing TSN to overcome the technical limitations of standard Ethernet and to ensure interoperability at different levels (on-board equipment, trains, tracking infrastructure, signaling, etc.).

A comprehensive overview of this trend can be seen in the integration of Universal Vital Control and Command Bus (UVCCB) defined in OCORA initiative (pushed by the railway operators) and in the Next-Generation Train Communication Network (NG-TCN) elaborated by the train manufacturers in Shift2Rail projects.

A redundant network structure combines a ´ladder' (Right Plane B and Left Plane A) for the Ethernet Backbone (ETB) with a ring configuration in the Consist Networks (ECN). Non-critical devices are attached to the ECN via a single link while the critical ones connect to Plane B and Plane A.

The Consist Switches (CS) will oversee the networking in the ring and separating the ETB traffic for ETB Line A and ETB Line B to ensure the redundant operation.

One of the key TSN features in this approach is IEEE802.1CB. This substandard defines a procedure of frame replication and elimination at stream level. IEEE802.1CB offers zero-delay recovery time in case of network failure, as PRP or HSR, under any network topology.

OCORA UVCCB can be integrated in NG-TCN network because both are based on TSN technology. The logical separation between different operator services can be done using different virtual local area networks (VLAN) enriched with the traffic shaping capabilities of TSN.

Attending NG-TCN ETB and ECN network topologies, the two type of switch devices are Ethernet Train Backbone Node (ETBN) and Consist Switch (CS).

CS are TSN bridges capable of supporting high-speed TSN networking in the ring. Currently, 1 GbE is the target speed, but 10 GbE is being considered as well. CS shall support Qbv and Qci among other TSN standards for a reliable mix of traffics with different criticality in the ring, and there is a demand for variants with a different number of ports. IEEE802.1CB in combination with MSTP will offer seamless redundancy for designated traffic, even in the ECN rings.

ETBN devices provide the physical connection between ECN and ETB. The minimum configuration for an ETBN is three ports, two for ETB and one for ECN. However, there are many variants that need to be addressed. As an example, a five ports ETBN is suggested in the specification.

Two ports connect ETB line, two additional ports allow direct connection to ECN ring and an additional port offers direct connectivity to non-critical Electronic Devices (ED).

The functionalities defined for ETBNs are wider than TSN bridging operation. As an example, they will oversee the ETB inauguration and control, TND info services management and support IP routing for the best-effort traffic. Therefore, ETBN nodes shall be seen more as a complete edge computing solution with TSN networking capabilities than simple networking devices.

From the hardware and software technology point of view, it is a challenge defining and developing a flexible, robust and long-term embedded platform able to fulfill all these requirements. Solutions based on powerful reconfigurable platforms that combine multiple CPUs and FPGA in the same semiconductor, like Zynq Ultrascale+ MPSoC from Xilinx, are gaining popularity within this high-end equipment for the Industry in general, and for the Railway sector, in particular.

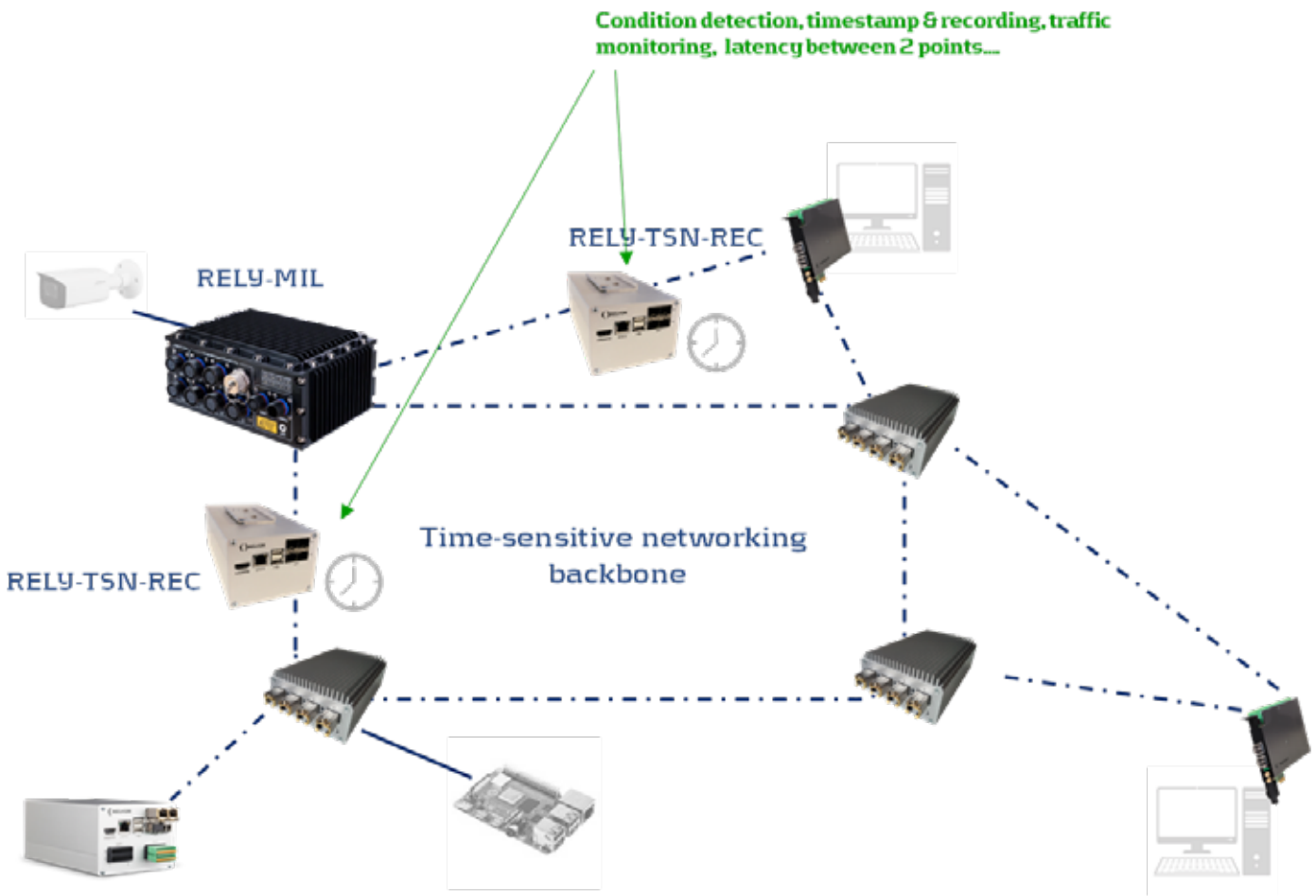
The FPGA vendors ensure long-term supply of their integrated circuits. In addition, the reconfigurability nature of these devices enables hardware upgrades attending the evolution of the standards or potential fixes to cybersecurity vulnerabilities.

This new generation of Railway equipment combines several new and complex technologies. As an example, there are technology companies specialized on TSN that can provide field proven TSN technology or cybersecurity stacks.

These third-party hardware or software IPs can be integrated in reconfigurable platforms in combination with vendor specific services. As a result, the time-to-market and the design risk of these projects might be significantly reduced.

The block diagram on page 43 illustrates how a five port ETBN can be implemented on a Xilinx Zynq Ultrascale+ MPSoC device. The MTSN switch IP implemented on the FPGA bridges TSN traffic. This IP switches and shapes TSN supporting redundancy according IEEE802.1CB, key TSN feature for NG-TCN.

The four ARM-A53 CPUs run a networking-oriented Operating System. Among other services, it provides TSN configuration management, IP routing and cybersecurity. The two ARM-R5 CPU hosts offer safety-critical and real time services, operation isolated from the networking services.



SOURCE: RELYUM

TSN based ETB and ECN networks in NG-TCN.

This TSN IP can be configured at synthesis time to support up to thirty-two ports. The number of ports and the TSN features included in the IP implementation can be selected at HDL code synthesis time by the designer. This flexibility ensures that the generated design is optimum in terms of FPGA resources utilization.

For the design, the IP has been configured to support six TSN ports. Five externals, providing connectivity to ETB, ECN (ring) and to external ED, and one internal connecting the Processing System section to the switch.

The equipment manufactures that are introducing TSN within their products demand solutions to test and verify this new technology. There are several ongoing pilot TSN activities in Aerospace, Industry and Railway sector.

Some of these initiatives are carried out by a group of manufacturers focusing on interoperability test. However, manufactures and research centers are developing their own TSN pilot according to the specific goals of each sector.

In general, the first hands-on with TSN is done running a comprehensive TSN kit. A complete video demonstration is embedded in the set-up to facilitate the exploration of the effects of the synchronization, traffic scheduling and traffic shaping under network saturation. In addition to the functional operation analysis provided by the Videos, the traffic shape can be visualized using the popular Wireshark application on a PC.

The next step is defining a more complete pilot that allows TSN evaluation, testing and verification. The TSN end-node operation is evaluated in host computers using the RELY-PCIe TSN cards and in third-party end-point shields. The bridging operation is carried out by the four and twenty-four port TSN bridges.

In these setups, the customer can analyze how run its own applications, and the whole network configuration and behavior. To perform a deeper analysis, the TSN traffic can be timestamped and recorded using specific equipment..

Conclusion

The railway sector has evolved serial Train Communication Networks to Ethernet based solutions. But the lack of real-time traffic communication and functions isolation capabilities of stand Ethernet has limited the adoption of standardized Ethernet based solutions.

TSN overcomes the identified limitations, and it has been identified as a strong candidate for the next generation Data Link layer for railway communications by the railway manufactures and operators.

The new generation of TSN and capable edge-computing equipment for the railway industry requires the integration and development of a variety of technologies and capabilities.

Reconfigurable platforms (SoCs) with powerful hardware and software capabilities combined with specialized third-party IPs cores, like MTSN IP from SoC-e, are the preferred alternative to reduce design risks and time to market of these emerging products.

The process of evolving to new technology like TSN is not straightforward. It requires hands-on, testing, validation and joint work among the different players. In this sense, Railway sector has put TSN working in real train and the wide ongoing research and development activity in this field show that the future is here.

Dr. Armando Astarloa, Professor at the University of the Basque country and founder-partner, ***System-on-Chip Engineering S.L.***

Visit Website

Connectivity Report

Industrial Cyber Security

How manufacturing companies are leveraging new technology to protect machinery, networks and corporate data.

industrial ethernet book

Industrial Networking & IIoT

Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

Offering the deepest, richest archive of Industrial Ethernet and IIoT content on the web.

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

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

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

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

industrial ethernet book
Industrial Networking & IIoT

Securely managing remote operational technology networks

Multiple obstacles are hampering the use of remote services, with cybersecurity being the biggest concern. Nowadays, cyberattacks are a common occurrence. Without cybersecurity, the door is set wide open for malicious individuals to take advantage of vulnerable networks.

IN FEBRUARY 2021, AN UNIDENTIFIED INTRUDER gained access to the network systems of a U.S. water treatment plant in Oldsmar, FL and briefly altered the chemical levels in the drinking water. Fortunately, an employee noticed the intrusion attempt and blocked it immediately. This incident sparked many discussions on the topic of cybersecurity in operational technology (OT) environments within the media and the industrial sector.

Impact of digital transformation

By adapting to digital transformation, OT network infrastructure starts growing in scale and becomes increasingly complex and interconnected. A single point of failure can bring tremendous harm to the whole networking system. Therefore, ensuring maximum network uptime is critical to keep business going smoothly.

Remote network management is becoming an invaluable tool for handling emergencies quickly and efficiently. Looking back at the Florida water treatment facility case, the FBI assessed that the intruder likely accessed the facility's systems by exploiting cybersecurity weaknesses including poor password security and the lack of firewall protection when logging in to the plant's systems remotely, as well as using unsafe remote access software.

Special attention to OT requirements

Considering the requirements of secure remote network management, everyone is looking for a solution to help simplify daily operations without having to worry about cybersecurity. While there is software available designed for remote access or network management, they often cater to IT networks and are rarely part of larger, consolidated solutions.

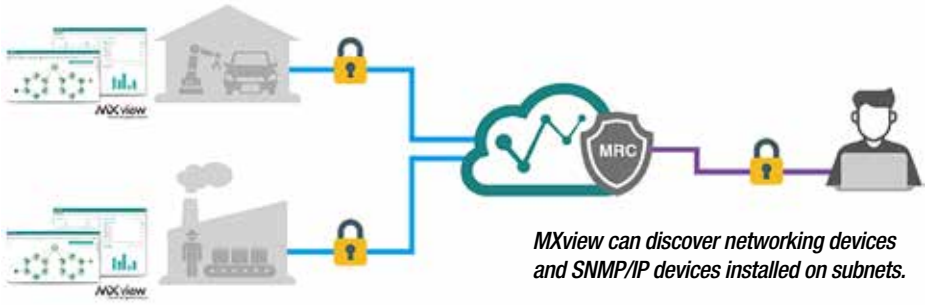
However, OT and IT networks have different characteristics and priorities. While IT prioritizes data confidentiality, OT focuses on network availability and zero tolerance for downtime. This difference makes it difficult for OT networks to adopt IT practices. Another hurdle is that many automation engineers are not familiar with VPNs or know the public IP necessary for setting up remote access.

Secure remote maintenance

For OT engineers, cybersecurity remains the number one concern. A solution with flexible access control could fulfill different OT scenarios and enhance network security. For example, customizable access control lets facility owners decide when and for how long third-party engineers can access their network. Furthermore, access can be restricted to specific network areas.

SOURCE: MOXA

MXview network management software is designed for configuring, monitoring, and diagnosing networking devices in industrial networks.



MXview can discover networking devices and SNMP/IP devices installed on subnets.

These measures can ensure the safety of networks when opening the door for remote maintenance services. Remote services for OT should also be accessible and easy to use. An ideal solution lets OT engineers easily set up remote access when needed, even if they are not familiar with VPNs or know the public IP.

With purpose-built and consolidated solutions, different players in the OT world would be able to enjoy the benefits of remote network management. Let's take a look at how this works in two different customer scenarios:

Facility owners

Manufacturers with facilities scattered across multiple locations require expansive networks to sustain operational effectiveness and efficiency. To manage such large and disperse networks, the network management software installed at the remote sites monitors the local network and sends data back to the HQ control center through an encrypted tunnel. This gives engineers a complete view of the network from a central location for remotely managing operations at each site. If any incident occurs, engineers at the headquarters can remotely access the on-site network device via a secure VPN connection or call in the help of third-party support services if necessary using an on-demand encrypted VPN tunnel.

Service providers/integrators

To help customers manage and maintain their network smoothly, network service providers require a simple solution for responding to service requests from multiple customers and solve issues as quickly as possible. Real-time remote service allows service providers to overcome geographical limitations and streamline their customer service.

An on-demand encrypted VPN tunnel can let support engineers easily access the network management software at the customer's site without jeopardizing the safety of the customer's network.

*Technology report by **Moxa**.*

Visit Website

The first line of defence for industrial networks

Technology solutions are providing companies ways to eliminate network vulnerabilities and strengthen security, bridging the gap between OT and IT and sparking widespread interest in industry. Although the focus is often on external attacks, internal threats can be just as damaging to industrial networks.

SOURCE: PROCENTEC

Whether it's a mistake due to inexperience with a task or protocol, or with the intention to inflict damage, threats can lead to costly downtime.

THE IMPORTANCE OF IT-SECURITY HAS BEEN acknowledged by experts for years, whereas securing Industrial Control Systems seems to have been overlooked. Whilst attacks on Operational Technology (OT) environments are becoming more frequent, companies are looking for ways to eliminate network vulnerabilities and bridge the gap between OT and IT.

The release of four major technology solutions to strengthen industrial network security has sparked a widespread interest in industry.

External and internal threats

Although the focus is often on external attacks, such as malware, phishing and hackers, internal threats can be just as damaging and more likely to occur. Whether it's a mistake due to inexperience with a task or protocol, or with the intention to inflict damage, these threats can lead to costly downtime.

Keeping track of modifications to physical assets is more important than ever. But if an industrial network security doesn't extend much beyond a firewall, devices are vulnerable. A firewall won't protect the network from people who know how to go around it. Even if a network is air gapped, users can't safeguard it against authorised individuals who make an error. The Security License tackles the everyday threat posed by unintentional and bad actors. It permanently monitors any planned or unplanned changes to your devices, giving an industrial network an extra layer of protection.

Some of its key features include 'Quiet Hours' and 'Maintenance Mode'. Quit Hours will notify users if there is any communication on the network when there shouldn't be any (e.g. events, night-time, weekends, holidays etc.). Maintenance Mode allows companies to make changes on their network without getting a security alert.

In addition to this, there are multiple inspections included to tackle the most often overlooked security vulnerabilities. The Port Scan, SNMP Write Access Scan, Device Password Scan and Communication Baseline Scan make sure all the entries to the network are secured.

Accidental or intentional changes

Sudden changes to an Ethernet-based network—like a lost device or the installation of different firmware—can spell disaster if they're unplanned, unauthorized or undiscovered. They could be the result of a malfunction or a sign of an intentional attack.

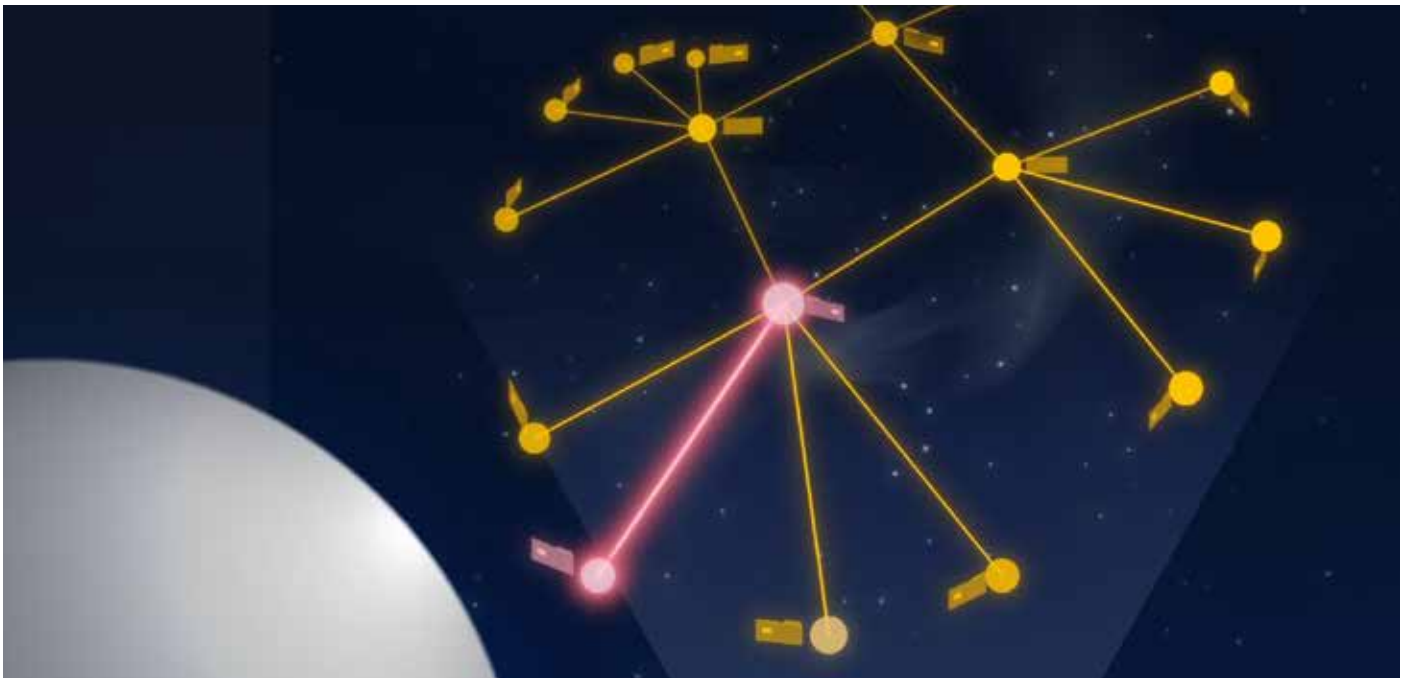
Network Compare is a built-in feature of Osiris, Procentec's monitoring and diagnostics tool. It notifies of sudden changes to the Ethernet-based network. It works by creating a snapshot of the network's status at any given time.

Network Compare sends out a variety of alerts from the notification centre whenever a change occurs, giving users time to act in an appropriate and timely manner. This feature easily Integrates with SCADA and other systems via OPC-UA and MQTT.

Data integrity using blockchain

Updating software in a decentralized OT environment can be a haphazard affair. But not knowing what has been installed can pose serious risks to your network.

According to Honeywell's latest USB Threat



SOURCE: PROCENTEC

Changes to an Ethernet-based network, a lost device or installation of different firmware, can spell disaster if it's unplanned, unauthorized or undiscovered.

Report, the number of USB threats specifically targeting OT-systems has almost doubled from 16% to 28% in 2020.

The risks are way bigger than just spreading malware; a USB-device can even be used to attack systems directly.

LockBox is designed to overcome the persistent problem of unverified and randomly-downloaded software. This blockchain-based platform provides a centrally-controlled catalogue of approved firmware, manual brochures, release notes and datasheets for individual network devices.

It allows sharing of the latest files safely with authorized users and stops the distribution of files via email, shared folders or USB sticks.

Ensuring best engineering practices

Onboarding new field technicians can be challenging, especially when a company has a complex, critical or extensive industrial network. Users can't be looking over their shoulder all the time. On the other hand, you don't want them to struggle on their own, running the risk that they'll accidentally do something that damages the industrial network.

SeeVerify is an interactive tool that guides industrial technicians—step by step—through routine and not-so routine tasks. It enables you to create, edit and publish customized instructions company-wide.

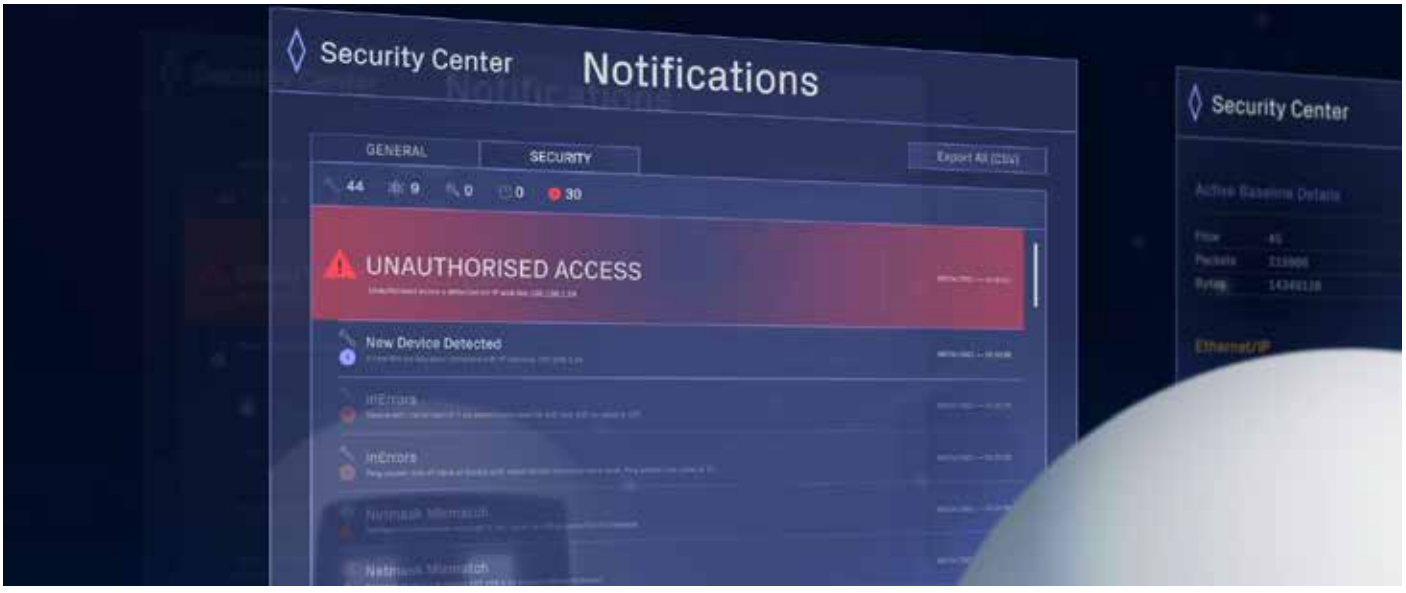
With build in OCR software, multiple templates, decision three algorithms, auto inputs and on-screen guidance, lead engineers have a new easy-to-use solution that facilitates the onboarding, training and reassignment of their technicians.

Network partnerships

Procentec develops and manufactures automation products for PROFIBUS, PROFINET, EtherNet/IP, EtherCAT and other Industrial Ethernet protocols. Some of its products are the most recognised solutions on the market today including ProfiTrace, ProfiHub, ComBricks, Osiris, Atlas and Mercury.

Technology report by ***Procentec.***

Visit Website

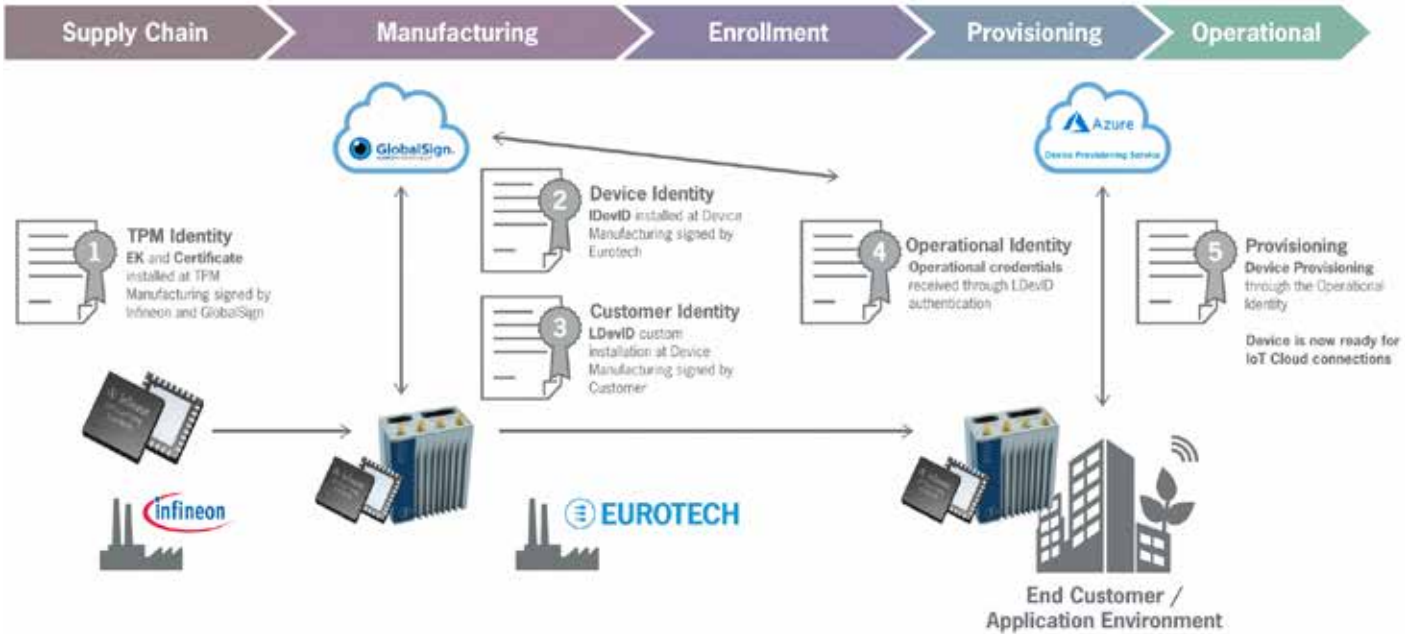


SOURCE: PROCENTEC

According to Honeywell's latest USB Threat Report, USB threats specifically targeting OT-systems has almost doubled from 16% to 28% in 2020.

'Chain of trust' security solutions for IoT device identities

Eurotech is collaborating with Infineon Technologies, Microsoft and GlobalSign to develop a 'chain of trust' security solution for IoT device identities. The companies are working together to deliver zero touch provisioning for IoT applications, and to simplify large scale, secure roll outs of connected devices.



SOURCE: EUROTECH

The device identities life cycle extends from the supply chain, through manufacturing, enrollment, provisioning and operational considerations.

A NEW TECHNOLOGY COLLABORATION HAS A goal to deliver assurance by extending the secured device identity chain from the edge to the cloud. Eurotech is working with Infineon, Microsoft and GlobalSign to simplify large scale, secure roll outs of connected devices.

Building on industry standards, the solution starts the chain-of-trust at Infineon's OPTIGA TPM (Trusted Platform Module) installed in all Eurotech IoT Edge gateways. As platform manufacturer, Eurotech extends this 'trust' to a secure Initial Device Identifier, an IEEE 802.1AR certificate-based identity that is cryptographically bound and uniquely assigned to the device. This identity attests the integrity of the platform supply chain and provides the necessary baseline for zero touch onboarding.

As part of this collaboration, Eurotech has worked with GlobalSign and Microsoft, with its IoT Identity Service security subsystem of the Azure IoT Edge, to extend the chain-of-trust to cloud connectivity. This is achieved through enrollment of additional local certificates confirming device ownership to a customer and using these identities for automatic provisioning of Azure IoT Hub operational identities by the Azure Device Provisioning service.

The solution reduces the complexity of embedding strong certificate identities in cloud connected device architectures. It delivers a blueprint for the management of standard-based digital identities over the life-cycle of the device from manufacturing, provisioning, maintenance and decommissioning.

"We are very proud of partnering with industry leaders Infineon, GlobalSign and Microsoft to lower the barriers of adoption of best practices for hardware-anchored digital device identities," said Marco Carrer, CTO at Eurotech. "This partnership reflects Eurotech's commitment to cybersecurity and supporting its customers to reduce device complexity and management."

"IoT is changing the way businesses think and operate, allowing them to optimize existing processes and opening the door for new business models and revenue streams," said Sam George, corporate vice president, Azure IoT at Microsoft Corp. "Streamlining the process of creating a chain of trust reduces the risk of supply chain tampering and device attacks that stem from compromised device identities. By helping to mitigate these risks, we're enabling organizations to build more durable and resilient IoT solutions—to innovate on a foundation of trust."

"Security remains the key enabler for cloud service adoption. The necessary level of protection can only be achieved by combining software security mechanisms with robust hardware-based security capabilities based on globally accepted industrial and IT security standards. A chain of trust from the node to the cloud using hardware based security anchors allows to securely identify each IoT and Edge device, to protect sensitive data as well as the integrity of the Cloud", said Juergen Rebel, Vice President & General Manager Embedded Security at Infineon.

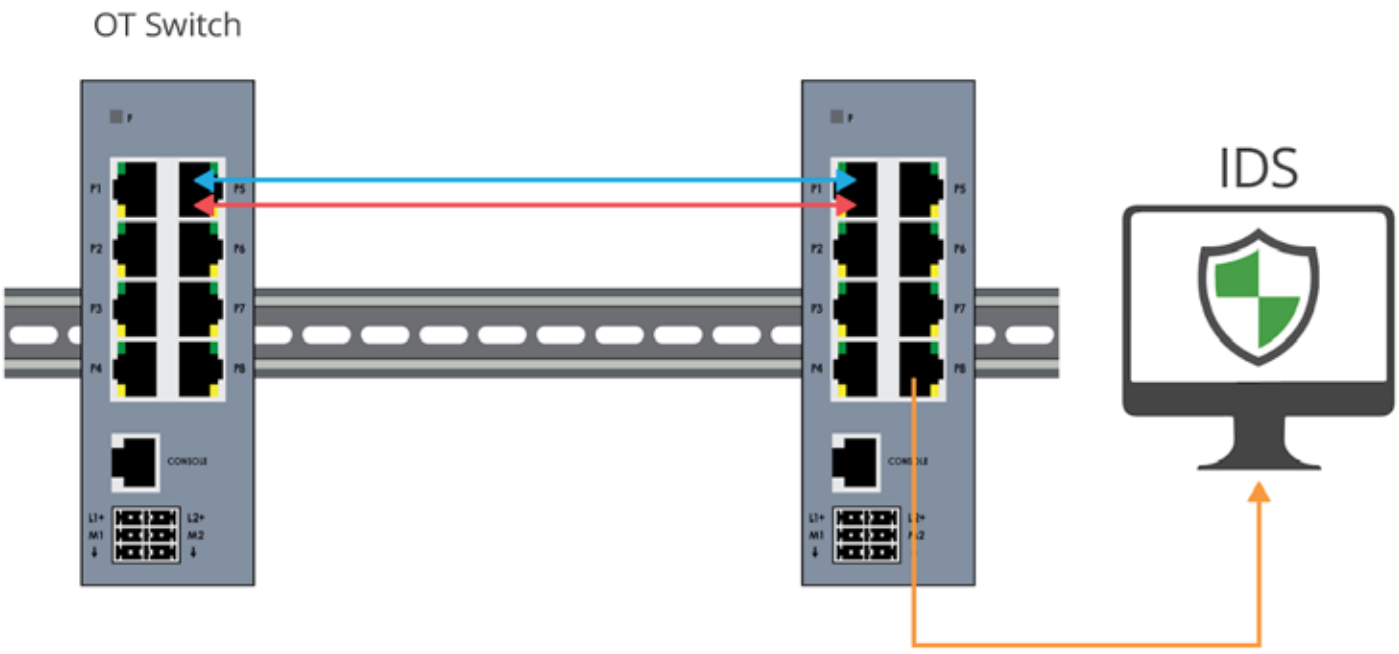
"Secure, zero-touch onboarding of IoT devices to the cloud is an important solution that realizes immediate value through its security and efficiency said Lancen LaChance, VP of IoT with GlobalSign. It's a solid blueprint that benefits the broader IoT industry by providing a proven, best practice solution to a common IoT device identity management challenge. Our collaboration with notable experts Infineon, Eurotech and Microsoft has enabled the entire IoT industry to take one secure leap forward."

News report by ***Eurotech.***

Visit Website

TAP vs SPAN: packet visibility challenges in OT environments

The convergence of Operational Technology (OT) with Information Technology (IT) has exposed challenges for the industrial space, including increased vulnerability to cyber-attacks and network blindspots. Teams are utilizing ICS security solutions designed to efficiently address and manage threats in OT environments.



SOURCE: GARLAND TECHNOLOGY

SPAN (Switched Port Analyzer), is a designated port programmed to mirror network packets seen on specific ports where the packets can be analyzed.

AS INDUSTRIAL COMPANIES WITH CRITICAL infrastructures invest in digital transformation to improve operational efficiency, cyber risks have significantly increased, leading to unscheduled downtime, negative corporate brand perception, as well as data and safety concerns.

Securing and monitoring your network is a core goal for most companies. To accomplish this goal, teams utilize ICS security solutions designed to respond to and manage threats in OT environments efficiently. To properly identify, detect, and respond to security threats and breaches, most ICS security tools focus on threat detection and monitoring, and asset visibility and management.

Implementing these security solutions, OT teams face complex challenges when it comes to architecting connectivity throughout these large and sometimes aging infrastructures. Many weren't initially designed with network security in mind, like having to rely on legacy switch SPAN ports for visibility, that aren't secure, reliable or available.

According to SANS State of OT/ICS Cybersecurity Survey, "visibility is critical for managing OT/ICS systems. According to survey respondents, increased visibility into control system cyber assets and configurations is the top initiative organizations are budgeting for in the next 18 months."

Security and performance strategies start with 100% visibility into network traffic. Security tools need to see every bit, byte and packet or they could miss a threat, and that visibility starts with the packets traversing the network.

A common access point for packet visibility in OT environments has been SPAN ports on a network switch. Many times an engineer will connect a SPAN directly to intrusion detection systems (IDS) or network monitoring tools. But today, in modern ICS networks, network TAPs (test access points) are considered an industry best practice as a more reliable and secure option to access network packets for security and monitoring solutions to properly analyze threats and anomalies.

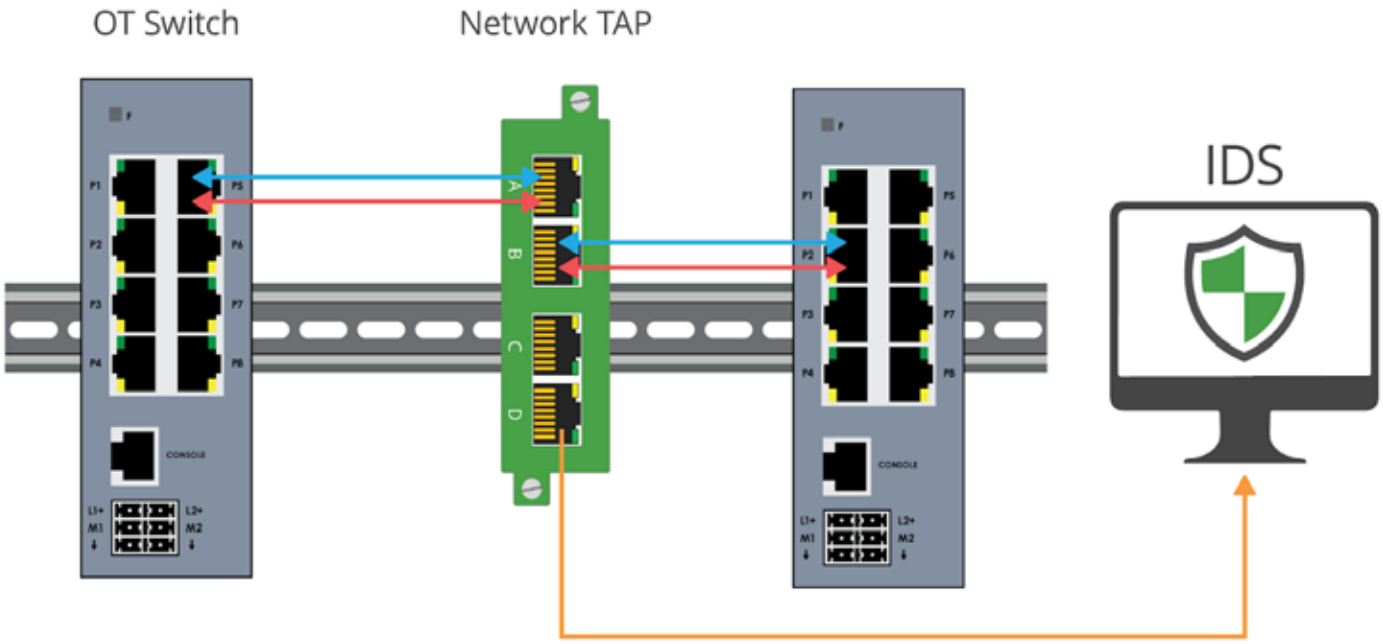
This high level network topology diagram, following the Purdue model, illustrates how an ICS network monitors various segments. From Level 1 control networks of DCS and PLCs, Level 2 process networks of HMI and engineer workstations, and Level 3 DNS operations to Level 4 data center and security control centers. Instead of mirroring traffic directly from the various switches, this diagram showcases how to properly access the packets with network TAPs and unidirectional Data Diode TAPs, providing complete and reliable visibility to ensure the monitoring solutions are seeing every bit, byte, and packet.

TAP vs SPAN in OT environments

Determining when you use SPAN ports or network TAPs comes down to a multitude of issues. And many times a combination of both is a visibility architecture reality. But there are some significant differences which affect the integrity of the traffic that is being analyzed, as well as the performance of the network traffic. Let's review some of the pros and cons of each to help you decide what works best for your network.

Switch SPAN ports

A common visibility use case is to route mirrored traffic from a SPAN port on the switch to a security or monitoring tool. Port mirroring, also known as SPAN (Switched Port Analyzer), is a designated port on a network switch that is programmed to mirror, or send a copy of, network packets seen on specific ports where the packets can be analyzed.



SOURCE: GARLAND TECHNOLOGY

Network TAPs are hardware devices that create an exact full duplex copy of traffic flow, continuously, 24/7 without compromising network integrity.

- SPAN ports provide access to packets for monitoring
- SPAN sessions do not interfere with the normal operation of the switch
- SPAN ports are configurable from any system connected to the switch

The concept is simple enough — the switch is already architected into the environment. Just hook up your security solution. Done. But many times the seemingly simplest path isn't the best path.

High-level SPAN challenges include:

- SPAN takes up high value ports on the switch
- Some legacy switches do not have SPAN ports even available
- SPAN ports can drop packets, an additional risk for security and regulatory solutions

One of the fundamental reasons security teams do not like to use SPAN is because of dropped packets. In IT environments, this usually happens when the port is heavily utilized or oversubscribed. In OT environments, network switches tend to run 10M, 100M, up to 1G so you may think this will never happen. Unfortunately, ICS switches are prone to drop packets at a lower speed, even when network links are not saturated. This can happen for a variety of reasons:

- Packets sometimes can't be stored because of a memory shortage
- 'PAUSE' frame attack - a bad actor can flood the SPAN disguised as a loopback, hiding bad data and forcing dropped packets
- Packets showing a broken cyclic redundancy check (CRC) will be dropped
- Frames smaller than 64 bytes or bigger than the configured maximum transmission unit (MTU) can be dropped because of an ingress rate limit

If dropping the packets isn't an eye opener, SPAN also:

- Will not pass corrupt packets or errors
- Can duplicate packets if multiple VLANs are used
- Can change the timing of the frame interactions, altering response times

The SPAN concept may have sounded easy because it was available, but after weighing packet loss and altered frames, additional SPAN security considerations include:

- Bidirectional traffic opens back flow of traffic into the network, making the switch susceptible to hacking
- Administration/programming costs for SPAN can get progressively more time intensive and costly

Network TAPs

The industry best practice for packet visibility is network TAPs (test access points). Network TAPs are purpose-built hardware devices that create an exact full duplex copy of the traffic flow, continuously, 24/7 without compromising network integrity.

Instead of connecting two network segments, such as routers and switches directly to each other, the network TAP is placed between them to gain complete access to traffic streams. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring or security device in real time, without affecting the traffic between the segments.

- Network TAPs make a 100% full duplex copy of network traffic
- Network TAPs do not alter the data or drop packets
- Network TAPs are scalable and can provide a single copy, multiple copies (regeneration), or consolidate traffic (aggregation) to maximize the production of your monitoring tools

TAP v SPAN, which wins?

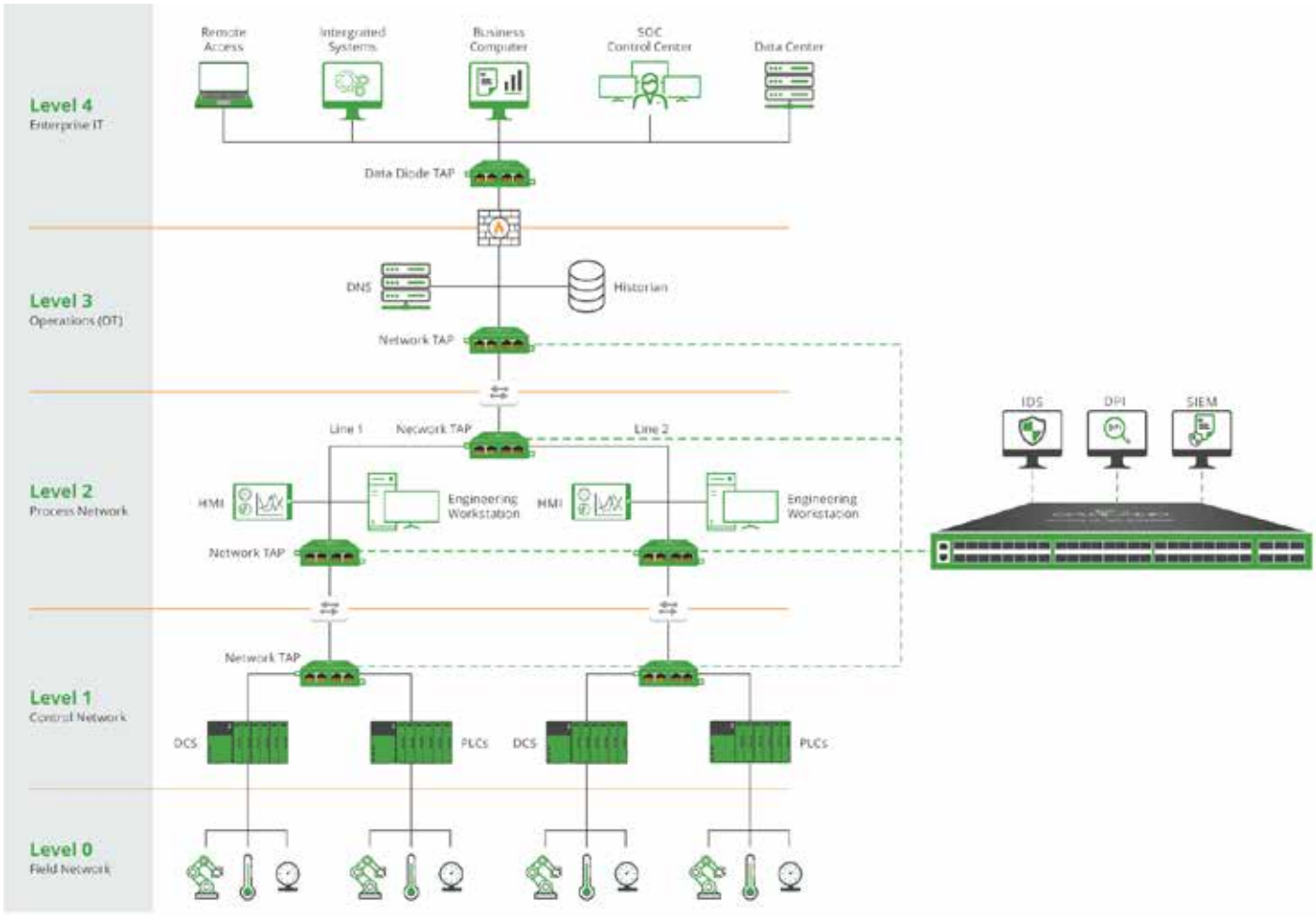
The two methods for network access both provide ICS security tools packets to monitor and protect the network. Understanding the options and challenges allows teams to better architect and secure the network.

Network TAPs

- 100% full duplex copy of network packets
- Enables faster troubleshooting
- Ensures no dropped packets, passing physical errors and supports jumbo frames
- Does not alter the time relationships of frames
- Are passive or failsafe, ensuring no single point of failure (SPOF)
- TAPs are secure, do not have an IP address or MAC address, and cannot be hacked.
- Data Diode TAPs provide unidirectional traffic to protect against back flow of traffic into the network

SPAN

- Provides access to packets for monitoring
- Can take up high value ports on the switch
- SPAN traffic lowest priority on the switch
- Some legacy switches do not have SPAN available
- SPAN ports drop packets, an additional risk for security and regulation solutions



SOURCE: GARLAND TECHNOLOGY

Typical manufacturing system topology

- Will not pass corrupt packets or errors
- Can duplicate packets if multiple VLANs are used
- Can change the timing of the frame interactions, altering response times.
- Bidirectional traffic opens back flow of traffic into the network, making switch susceptible to hacking
- Administration/programming costs for SPAN can get progressively more time intensive and costly

Putting TAP vs SPAN to the test

In a test conducted by a 3rd party (Packet Pioneer), with the goal to see the difference between a data stream captured on a network TAP versus a SPAN port.

The test connected two PCs to a basic Cisco Catalyst Switch at 100Mbps. A throughput test using iPerf was configured and run between the two machines. On one of the PCs, placing a 100Mbps TAP, and a hardware analyzer to capture. Lastly, they configured a SPAN on the switch to forward all traffic to and from this port to another hardware analyzer.

The throughput test finished with a result of 93.1Mbps sustained for 10 seconds between the two PCs.

TAP vs SPAN	Packets Captured	Delta Time at TCP Setup
TAP Capture Results	133,126	243 uSec
SPAN Capture Results	125,221	221 uSec

The SPAN data capture showed almost 8,000 packets missing from the trace. This represents almost 8% of the total packets that were captured by the analyzer from the network TAP. We should also point out that this was on a 100Mbps interface, not a Gigabit interface, and there were no errored frames. The switch bus was not in a near overloaded state.

Also, the difference in the timing between the TCP SYN and SYN ACK in the two traces shows us that the switch is not treating both the SPAN and destination ports the same. In fact, it was forwarding traffic to the SPAN port faster than the true destination. While the difference is only 21 uSec, it shows that the switch is affected when SPAN is enabled. It is not as seamless as it would appear, and this delay was under no load test. With the switch loaded with traffic, the losses and timing will show greater differential and also dropped packets. The results are clear that the network TAP outperformed the SPAN in a head to head packet test, which can mean missing a threat or successfully containing a breach.

Following critical infrastructure's guiding principles — OT teams build their networks to last, to ensure minimal to no network downtime. These concepts rest on the network infrastructure and visibility architecture. Incorporating best practices like network TAPs in the network will help achieve these goals.

Critical infrastructure visibility solutions for OT provide industry the most reliable Network TAP, Data Diode, Network Packet Broker and cloud visibility solutions, and deliver packet visibility while ensuring the secure connectivity needed.

Chris Bihary, CEO and Co-founder, ***Garland Technology.***

Visit Website

Reboot network security to enable digital transformation

Digital transformation in manufacturing can deliver business value by improving operations and using innovative services. The greatest risk lies in the manufacturer's ability to secure the production environment and the end-to-end connectivity between the plant and the cloud-based services and remote users.

SOURCE: CISCO

SECURITY RISKS AND THREATS TO INDUSTRIAL environments have not abated in 2020 and into 2021, but have continued with vigor. The impact includes significant loss of production availability and effort expended to identify and respond to these compromises. These are not new challenges, but the pandemic and its effects certainly have not reduced or remedied the situation.

As operations continue to drive further convergence with IT and OT, and look to improve operational efficiencies and productivity with new market trends and capabilities, such as cloud; they also need to consider a comprehensive multifaceted security approach at the core of the architecture. Security attacks and events are a board-level concern for most, if not all, major industrial operators, given the impact of lost revenue, costs and impact to reputation.

Even before the drastic changes we saw in 2020, manufacturers were under pressure to improve operational efficiency through digital transformation. While investments in digital transformation pay dividends, they also compound long-standing cybersecurity risks. When manufacturing operations are digitized and interconnected, there's more potential exposure and a greater need for forward-looking protection. After all, a single cybersecurity incident can drive downtime and revenue loss, rack up operational expenses and damage a manufacturer's reputation in the market.

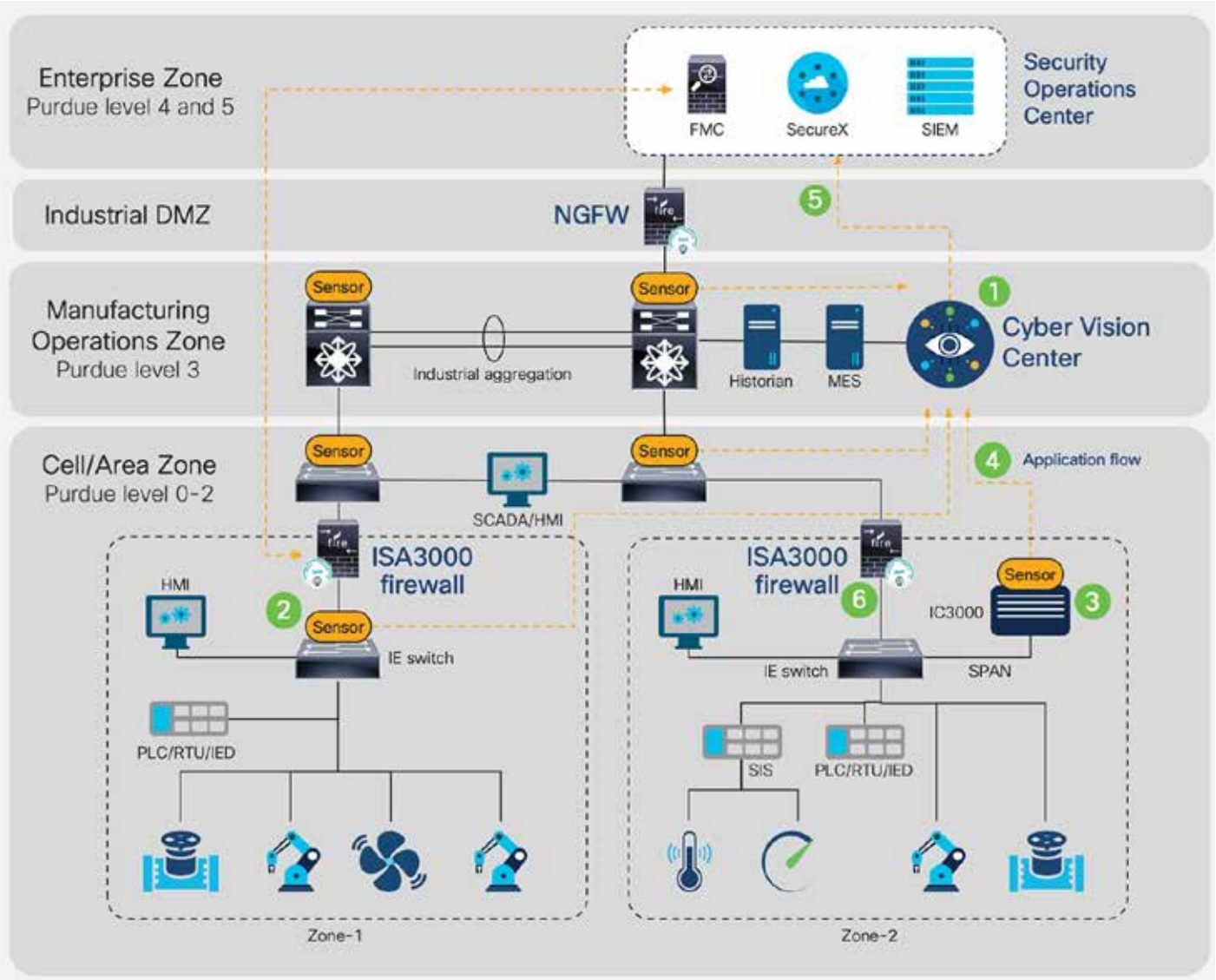
And yet, even as cybersecurity continues to remain a board-level concern, many manufacturers continue to address the risks with patchwork approaches. Security can't be achieved with point solutions. It takes an end-to-end approach starting with the network in production. But it does not end there: as digital transformation requires the integration of production environments with cloud-based applications and resources.

Yes, there are some excellent cybersecurity tools designed especially for operational technology (OT) environments. They promise to identify devices and their communication patterns, thereby surfacing cybersecurity risks. But these tools are only as effective as the network they're monitoring. Legacy networks often make it complex to gain the needed visibility and impossible to automate application and enforcement of security policies. And adding a cloud-perspective requires extending the cybersecurity envelope further.

To enable secure digital transformation, manufacturers need to reboot production network security, embracing a concerted more integrated security strategy and extending those security capabilities beyond the four walls of the operation. This journey starts with the transformation of legacy production networks and introducing hardware and network components that fully enable and efficiently leverage available cybersecurity tools.

Once the planning and design is complete, the next step is to deploy industrial cybersecurity to protect the production network. Digital transformation often introduces remote or cloud-based resources and applications, so the cybersecurity considerations must also include the extended

SOURCE: CISCO



Integrating Industrial Cybersecurity tools at all levels of the network provides not just visibility of the IACS devices, systems and communication but also leverages that knowledge and insight into dynamic and automated policy management and enforcement.

cloud environment, helping ensure end-to-end protection.

Switching for security

For any manufacturer, the production network is the foundation of a secure and reliable production environment. The network should provide security tools with seamless access to production systems and their communications, without interfering with the operation.

With the proper network hardware and software, security tools can serve as security "eyes and ears" – sensing and analyzing industrial automation and control systems (IACS) devices and communications at the edge. What's more, the security tools should be able to perform that work without placing undue burden on the network itself.

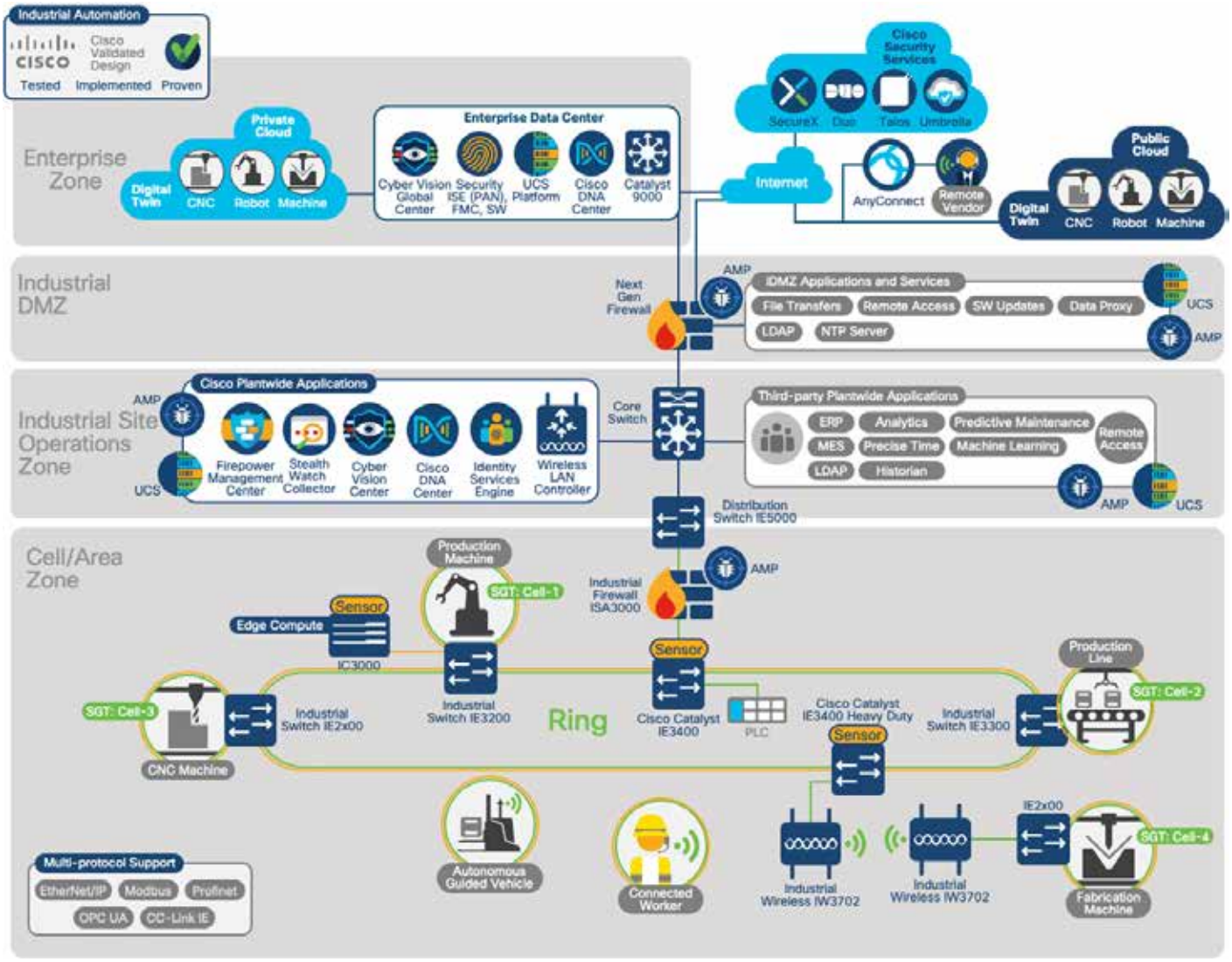
As it does in enterprise networks, a robust security strategy in the production network can also play a critical defensive role. With access to IACS devices and communications, OT security tools can help "profile" device behaviors and communication flows. Manufacturers can use these profiles to develop security policies, which can later be enforced via the network infrastructure.

Using those same profiles, software can apply dynamic network segmentation – making it easy to protect a flat industrial network from anomalous communication flows and malicious traffic.

Of course, transforming an existing network is not a trivial undertaking. Given the 24/7/365 operational tempo of many production environments, there is significant risk if a migration is poorly executed. Before displacing any existing network devices, manufacturers need to perform sufficient planning, testing and preparation to reduce potential downtime (planned and unplanned). This includes the development of a backout strategy, should a migration experience obstacles hindering its timely completion; as well as, establishing the success criteria for a migration with the associated checks and validation.

When planning a transformation, start with a thorough understanding of all requirements for the applications and services the production network supports. Dive deep into all protocols and associated KPIs and metrics required by the deployed endpoints and analyzing industrial automation and control systems (IACS) devices, many of which tend to be sensitive to network latency and loss. Once the requirements are well understood, it's possible to develop role-based templates and network device configurations. These configurations will reflect the protocols and features necessary to support deterministic behavior, application SLAs and current device connectivity.

After the device configurations are developed, the next step is testing and validating the viability of those configurations in the new switches. This can be achieved by executing a limited proof of concept in a controlled "sandbox" or by testing within a limited production environment. In either case, the key is to execute tests and expose the equipment to the rigors and network



SOURCE: CISCO

This diagram depicts a manufacturing architecture that includes security controls and applications throughout all layers of the architecture.

characteristics found in the operational environment while reducing any impact to operations. Using clear pass/fail criteria for each feature, validates requirements are being met and that the network performs as expected. After completing all tests – and resolving any punch-list items – it's time to displace the legacy switches.

Different situations and operations may dictate how the displacement or migration needs to be executed. This, too, requires strict planning and preparation. To properly execute the migration and help ensure successful repeatability for subsequent devices, create a standard operating procedure (SOP) or methods of procedure (MOP) document. This document defines the step-by-step process and correct sequence for performing the necessary tasks. As such, it helps mitigate risk and reduces impact to operations – by defining not only the proper procedures for executing the displacement, but also the backout procedures should something unexpected be encountered.

To further contain costs and impact, default to reusing existing cabling and power, which usually represent the most significant cost and time to deploy a production network. Using existing power and network cable-plant helps reduce the time required to swap network infrastructure hardware.

While manufacturers often possess the staff and experience in performing these tasks, resources may be spread thin. In that case, consider investing in a service contract from a reputable vendor as a force multiplier, mitigating risk and helping drive success. A service team can take responsibility for some or all of the tasks discussed to help achieve the desired outcome, such as reducing operational downtime and/or reducing costs and keeping the project on schedule.

Integrated industrial cyber solutions

Once a legacy network is displaced with a security-capable network infrastructure, manufacturers can move more readily on the journey to secure production environments. With the necessary hardware and software, a manufacturer can accelerate the deployment of cybersecurity solutions that lead to more uptime, secured assets and products, and ultimately decreased operational risk.

Here are five ways to start:

1. Deploy an industrial demilitarized zone (iDMZ) between the operational zone and enterprise applications.

2. Monitor IACS devices and communication and identify risks. Leverage cybersecurity applications such as Cisco Cyber Vision to analyze data collected by the new network equipment to gain ubiquitous visibility.

3. Leverage a tool such as Cisco Cyber Vision to profile industrial devices, group them into production cells and define security policies between those cells.

4. Monitor communications between production cells to confirm that security policies are properly defined and can be enforced without compromising production.

5. Deploy security policies to be enforced by the industrial network and provide ongoing improvements with a network management

solution, such as Cisco DNA Center.

Integrate these steps with other key cybersecurity initiatives that rely on the transformed production networks. These may include policy management, secure remote access, enhanced industrial demilitarized zones, malware protection throughout the environment, and intrusion detection and prevention (IDS/IPS) at key conduits within the production zone.

The current fragmented cybersecurity approach in industrial environments is not keeping pace with the rate and sophistication of threats and attacks. To avoid downtime, revenue loss and reputational impact, manufacturers should consider transforming legacy production networks and migrating to a more capable infrastructure.

As an example, the Cisco Catalyst IE3x00 series together with Cisco Cyber Vision provides deep insights and visibility of IACS devices and communication patterns. This approach also enables segmentation and defense tailored to the existing IACS by leveraging increased visibility to derive tailored cybersecurity profiles. These profiles can later be used to define and instantiate security policies.

With a modern network and more integrated security tools and features, manufacturers can expect to upgrade and deliver a more comprehensive and cohesive cybersecurity posture throughout the lifecycle of the IACS and production networks.

Extending security to the cloud

Digital transformation and leveraging more modern network capabilities to drive efficiency or produce a competitive advantage can be a significant differentiator for a manufacturer. Providing connectivity and access to remote experts, or OEMs pulling telemetry data from critical equipment for predictive maintenance, or even leveraging new services and applications hosted by an ecosystem partner off-prem, all extend the threat landscape, and potentially expose the operation to more risk. Therefore, when embarking on newer initiatives, and extending connectivity beyond the four walls of the operation, such as cloud services, security needs to remain at the core of any solution.

Cloud, and how to leverage the benefits and capabilities it offers, is absolutely a consideration for most industrial operators. Cloud-based services can be achieved via different means. In some instances, cloud connectivity can be achieved via direct connectivity between an operator and a cloud provider. In other cases, communication may rely upon open internet services. With both these options, each presents its own set of unique challenges. However, protecting that communication, resources and application availability are critical to help ensure services remain operational and protected from risks and threats.

It should be noted that services and applications placed in the cloud should be evaluated for their criticality to the continuity of operations. Cloud-based services should be considered a noncritical extension of the operation, and therefore only include applications that are considered unnecessary to ongoing production if connectivity is lost for periods of time.

However, securing the cloud infrastructure is equally as important as securing on-prem networks. Many of the same security strategies and tools leveraged on-prem, may need to be employed in the cloud. Key considerations when considering security for the cloud can include:

- Perimeter security, macro-segmentation and stateful inspection and visibility of applications and flows transitioning to and from the cloud.
- Confidential communication via encryption protects cloud-based and on-prem communication and traffic flows with site-to-site VPN connectivity, or secure individual client connectivity.
- Use of multi-factor authentication technology to verify the user identity before granting access reduces the risk of compromised passwords and help ensure only appropriate users are granted access to the network.
- Adding protection against malware and viruses propagating into production environments from cloud-based and external sources with anti-malware protection built into a production environment's network infrastructure and application servers.
- Ensure systems residing in the cloud are regularly patched and updated and users are accessing the appropriate services with DNS protection.

Consider a scenario where an operator is interested in providing connectivity to a third party OEM or partner, who would like to pull telemetry and usage data from machines and other onsite hardware for the purposes of predictive maintenance. Extracting telemetry into the cloud may be one way of addressing this use case. By leveraging the right combination of security features and applications previously mentioned, this use case can be accomplished without putting the operation at additional risk while providing additional cost savings and operational efficiencies.

As the Industrial Digital Transformation starts to rely on cloud-based services and capabilities, manufacturers could also leverage cloud-based security services to increase visibility, accelerate detection of threats and compromises, as well as speed reactions and responses to those threats. The demarcation point between critical and noncritical assets does not have to exist on-prem. In addition, this model allows for the centralized enforcement of security policies, which promotes consistency, and repeatability, and facilitates the on-boarding of additional sites, as an operator looks to scale out this method of connectivity. This may be important for operators considering driving more onsite automation and managing multiple operations from a regional operations center (ROC). A regional iDMZ between operational zones and the enterprise would enable:

- Cybersecurity workflows and automation of Security Orchestration services to simplify, integrate, automate and scale security operations
- Coordinated visibility and insights across multiple locations from a single security operations center hosting extended detection and response (XDR) tools.
- Enforcing consistent security policies across multiple operational zones.
- Ease of administrative burden and the potential to be delivered as a service by a managed service provider.

Summary

To summarize, the promise of Digital Transformation in manufacturing delivers significant business value through improved operations, better services and products and creating and using innovative services. The greatest risk to achieving those benefits lies in the manufacturer's ability to secure the production environment and the end-to-end connectivity between the plant and the cloud-based services and remote users. Three key steps we outline to overcoming those cybersecurity challenges include:

- Reset the cybersecurity foundation in production environments by accelerating adoption of modern network infrastructure that provides key visibility and security for Industrial Automation and Control systems
- Integrate the deployment of Industrial Cybersecurity tools to provide not just visibility of the IACS devices, systems and communication but also leverage that knowledge and insight into dynamic and automated policy management and enforcement.
- Protect cloud-based and on-prem assets, as well as the communication flows between the production environment and cloud-based applications and services with a holistic security strategy, comprised of a robust set of cybersecurity technologies and tools.

Paul Didier, Kevin Turek and Andrew McPhee, ***Cisco Systems.***

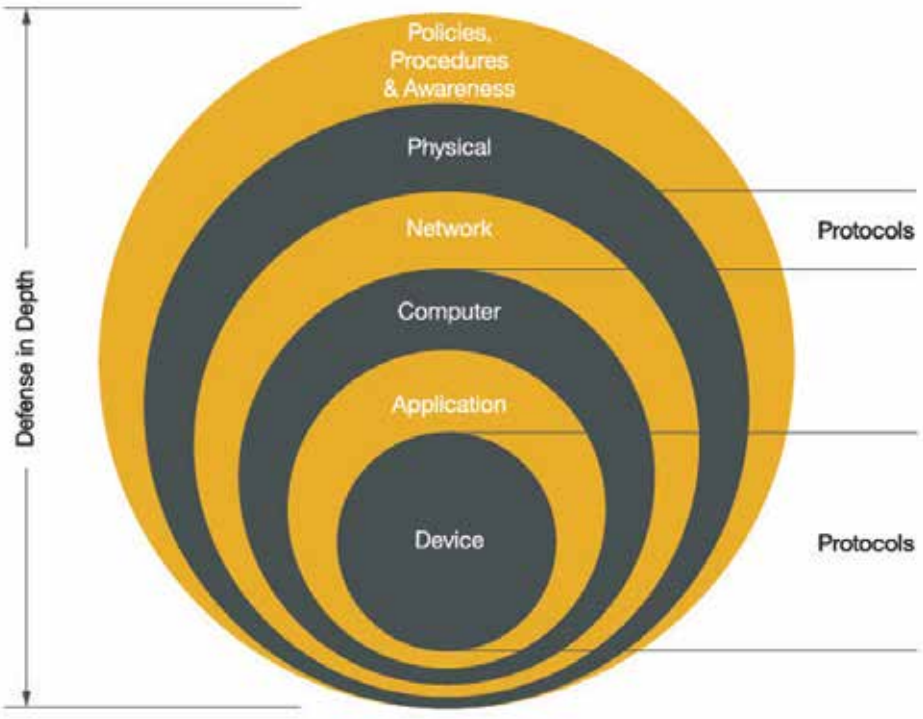
Visit Website

Device level security for critical automation applications

Adding an extra layer of defense, particularly for motion applications, is an inexpensive way to make your facility a more hardened target that will discourage malicious actors in the first place and help to slow them down long enough to enable other defenses to expose and expel them from your network.

A GREAT DEAL OF WELL-DESERVED FOCUS is placed on high level network security in switches and routers with machine learning driven network monitoring, deep packet inspection, abnormal behavior algorithms, and allowed listing among the many valuable defensive measures. What happens if a bad actor makes it past passwords, firewalls, and DMZs in addition to all of the aforementioned important, advanced layers of protection?

Controllers and devices that start and stop the motion of machines are a particularly high value target for threat actors and concern for end users because these devices can be misused to cause great physical and financial harm. Adding an extra layer of defense, particularly for motion applications, is an inexpensive way to make your facility a more hardened target that will discourage malicious actors in the first place and help to slow them down long enough to enable other defenses to expose and expel them from your network. This is why ODVA recommends a complete defense in depth approach, including robust device level security.



SOURCE: ODVA

Defense in Depth Approach.

CIP Security for automation

CIP Security is a cybersecurity network extension for EtherNet/IP™ that provides the last mile of security-related requirements and capabilities for devices. The goal of CIP Security is to enable EtherNet/IP devices to protect themselves from malicious communications. A self-defending CIP Security enabled device is able to reject data that has been altered (integrity), reject messages sent by untrusted people or untrusted devices (authenticity), and to reject messages that request actions that are not allowed (authorization).

CIP Security for EtherNet/IP devices makes use of the IETF-standard Transportation Layer Security (RFC 5246) and Datagram Transport Layer Security (RFC 6347) protocols in order to provide a secure transport for EtherNet/IP traffic. TLS is used for the TCP-based communications such as diagnostics and commissioning, and DTLS for the UDP-based transport communications such as I/O data.

Secure EtherNet/IP transport provides the following security attributes:

Authentication of the endpoints: ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.

Message integrity and authentication: ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS message authentication code (HMAC).

Message encryption: optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS handshake.

The ultimate roadmap for CIP Security development is to enable EtherNet/IP devices to become autonomous, taking responsibility for their own security and effectively securing themselves from attack.

CIP Security flexibility & options

CIP Security provides device authentication, a trust domain, device identity, device integrity, data confidentiality, user authentication, and policy enforcement (authorization). This is accomplished through three separate security profiles that provide flexibility for vendors in adding security features to their device depending on the intended application(s) and use case(s). A security profile is a set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability.

The first security profile is the EtherNet/IP Confidentiality Profile, which provides secure communications between EtherNet/IP endpoints to assure data confidentiality. The second profile is the CIP User Authentication Profile, which provides Authentication at a user level for CIP communications.

This is used as a basis for Authorization and Role Based Access Control. The third profile is the Resource-Constrained CIP Security Profile, which provides a lightweight version of the protections afforded by the first two CIP Security profiles specifically for highly resource-constrained devices.

Security Properties	EtherNet/IP Confidentiality Profile	CIP User Authentication Profile	Resource-Constrained CIP Security Profile
Device Authentication	X		X
Trust Domain	Broad – group of devices	Narrow – Users/Roles	Broad; option to be Narrow via Gateway or Proxy
Device Identity	X	X (Identity of User)	X (via PSK)
Device Integrity	X		X
Data Confidentiality	X		X
User Authentication		X	Via Gateway or Proxy
Change Detection (Audit)			
Policy Enforcement (Authorization)		Fixed	Via Gateway or Proxy

CIP Security Profiles

Resource-constrained devices

Despite the progress brought about by Industry 4.0 and the Industrial Internet of Things (IIoT), a large portion of the installed nodes in automation applications are still not using Ethernet.

Limitations including cost, size, and power have historically been a hindrance to EtherNet/IP pushing out to the edge of the network. The recent integration of Single Pair Ethernet has opened up the door to overcoming lower-level device constraints and ultimately to expanding the footprint of EtherNet/IP.

Adding simpler devices to EtherNet/IP allows for the benefits of additional remote diagnostics, asset information, and parameterization capability. The addition of more nodes to the network within the context of IT/OT convergence makes device level security a fundamental need to ensure that indispensable assets and people are protected from physical harm and monetary loss.

The protections offered by CIP Security are now available for EtherNet/IP networks via a resource-constrained version of CIP Security that includes fewer mandatory features. This ensures that devices with the smallest power, size, and cost budgets can be secure and enjoy the communication and control advantages of being connected to an EtherNet/IP network.

CIP Security can now provide device authentication, a broad trust domain, device identity via Pre-Shared Keys (PSKs), device integrity, and data confidentiality for resource-constrained devices such as contactors and push-buttons.

Additionally, functionality is provided to allow the resource-constrained device to seamlessly integrate with a proxy or gateway device which performs access policy enforcement on behalf of the resource-constrained device

Connectivity end state

As the inevitable march toward seamless device to enterprise connectivity plods forward, driven by Industry 4.0 and Industrial IoT, the reality is that automation devices that control the motion of motors, drives, pneumatic cylinders, etc. will be opened up to both the business benefits as well as the potential for unwanted intrusion as a result of internet connectivity. Today, many machines and skids are already connected via cellular data to allow OEMs to provide end users with remote operations support.

Even the best designed second communication channel for diagnostics can still potentially expose valuable intellectual property and trade secrets. Avoiding all external exposure of automation devices is of course possible, but then the user will not be able to take advantage of the diagnostic and prognostic benefits afforded by increased connectivity.

In the absence of this extreme measure, adding device level security is a low-cost protection that provides a last level of defense for critical motion control devices.

ODVA is committed to providing users with the most secure automation network solutions via CIP Security, which will continue to be enhanced to add new capabilities and protections as technology and threats evolve.

Steve Fales, ***ODVA.***

Visit Website

CIP Security support for user level authentication

User level authentication added to CIP Security provides a narrow trust domain by user and role, and improved device identity including the user, and user authentication.

The CIP Security User Authentication Profile provides user level authentication with a fixed user access policy based on well-defined roles and basic authorization via both local and central user authentication. CIP Security's ability to authenticate via the device or through a central server allows for simplicity in smaller, simple systems and efficiency in large, complicated installations.

CIP Security included robust, proven, and open security technologies including TLS and DTLS; cryptographic protocols used to provide secure transport of EtherNet/IP traffic, hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authentication to EtherNet/IP traffic; and encryption as a means of encoding messages or information in such a way as to prevent reading or viewing of EtherNet/IP data by unauthorized parties.

The profile provides user-level authentication for CIP communication at the application layer. In the future, CIP Security may make use of a CIP authorization profile that will enhance CIP to provide additional security properties such as general, flexible authorization where access policy can be based on any attribute of the user and/or system and potentially extending CIP Security to support other non-EtherNet/IP networks.

The profile uses technologies including OAuth 2.0 and OpenID Connect for cryptographically protected token-based user authentication, JSON Web Tokens as proof of authentication, usernames and passwords, and already existing X.509 certificates to provide cryptographically secure identities to users and devices. It uses a cryptographically secure user authentication session ID, generated by the target on presentation of a valid JWT by the user, to map between an authentication event and messages sent by a user for CIP communications.

The user authentication session ID is transmitted over EtherNet/IP using (D)TLS and a confidentiality-enabled cipher suite per CIP Security's EtherNet/IP confidentiality profile.

Cyber security strategies to secure the real world

Extending cyber security to the connected edge is a key strategy for industry. The devices at the edge need to be more capable, moving the analytics further to the edge and increasing functionality, autonomy, and connectivity. Data links have to adapt to be more capable and provide both increased visibility and control.

SOURCE: ANALOG DEVICES

Recent events highlight how much of a global issue that cyber security has become.

THE DEVELOPMENT OF THE SMARTPHONE started a trend of connected devices that not only perform some form of computing and decision making, but that has changed how we relate with the world around us. These devices are connected through networks and cloud services that provide easy access and sharing of information.

In order to solve for market demand, there is a rapidly multiplying number of connected devices designed to transform and innovate how we seamlessly interface with the world. This trend is changing how we relate to the automobile and factory, but it is also creating cyber security challenges that industry integrators will face. In these markets, there is a much higher demand to operate reliably, which presents unique cyber security challenges when extending the connected edge.

For instance, the automobile is no longer simply a tool used to get us from point A to point B. It is becoming a platform that provides us new means to interact with the world and improve our quality of life. This is being achieved through connectivity and the sharing of data, such as how to optimize battery performance or updating navigation with changing landscapes. The automobile platform is becoming a way to connect and integrate services in a fashion that mimics the development of the smartphone in an environment that demands near absolute safety, integrity, and accessibility.

The industrial market is undergoing significant changes as new technology advances serve as a catalyst for higher productivity. The demand for increased productivity is changing how we interoperate and interact with the factory. The need to interface with the factory in a more intuitive and seamless manner is driving the next industrial revolution. With the wave of advances defining Industry 4.0, there is increased connectivity and requirements for access in the factory.

The devices at the edge need to be more capable, moving the analytics further to the edge and increasing functionality, autonomy, and connectivity. The data links between the devices in the factory and the traditional field connection point have to adapt to be more capable; providing increased visibility and control from the cloud. In an industry known for focusing on stability and availability, there is increasing demand for flexibility.

Solving for the demand to interface with the world around us in a more seamless and intuitive manner drives new capabilities and technologies. However, a major byproduct of these developments is the need for security. Cyber security is a principal factor in market segments that demand high reliability and safety. Those who have malicious intent, commonly called bad actors, can exist within or outside an organizational system and can have many different motivations. The threat to connected devices exists both through the network as well as physical access. Cyber security applied to these edge devices need to adequately address the threat.

Analog Devices provides solutions that connect the physical world to the digital world, where analog-to-digital conversion takes place. ADI is uniquely positioned in the market to push cyber security further to the edge, where data is established. Establishing trust in the data further down the signal

SOURCE: ANALOG DEVICES

Since the Stuxnet incident, industry has experienced a constant flow of cyber security events.

SOURCE: ANALOG DEVICES

	More Mature					Less Mature
	Defense/Gov	Automotive	Industrial	Utilities	Healthcare	Consumer
Pain Points	SWaP Time-to-market	Autonomous vehicles, internally connected ECUs on CAN	Connecting OT networks; cyber confidence	Offsite unattended grid needs security	Personal data protection	High security in low cost devices; data integrity
Potential Consequences if Breached	National security	Shutdown safety features; car theft	Manufacturing shutdown; power outage; safety	Gas, oil, nuclear, electrical catastrophes	Personal data loss resulting in huge fines	IP theft; secure personal data
End Devices	UAV, radios, communication links	Gateways; OBD plug-in	IIoT, ICS, SCADA, circuit breakers	Grid, circuit breakers	Personal healthcare data, IP, scan, imaging	IoT devices

Different industry segments have been faced with a different set of pain points, consequences and potential impact on end devices.

chain provides users with more confidence in the decisions they are making from the data because they have a higher expectation that the data is accurate.

Cyber security is a key element of ADI's strategy not only because it is necessary in our markets, but because it is a catalyst for enabling our customers' systems and increasing the value of the information from our sensors. Ultimately, what our customers care about is trusted data. This means establishing that the measurement is accurate and there is integrity in the data.

Cyber security is hard to understand

Cyber security is not always easy to understand because it is a constantly changing, complex problem and it is a factor at every point in a system or device life cycle. Security is a system solution and the system is only as strong as its weakest link. There is a significant number of cyber-attacks today, with successful attacks increasing as systems become more complex.

System vulnerabilities can be demonstrated though many examples of weak links. In 2016, automotive key fobs were compromised for an entire fleet because only four root keys were used for the past 20 years. In 2011, high assurance identity tokens were exploited through exposure of manufacturing artifacts created and stored on the factory floor. In 2017, a vehicle was accessed through the cellular link, which allowed hackers the ability to update the operating system and rewrite the program remotely.

The Heartbleed Open SSL buffer over-read vulnerability left 200,000 active servers and devices vulnerable and without the means to receive security updates today. To further elaborate on why cyber security can be hard to understand, security is never done. As new vulnerabilities are discovered and new methods of hacking devices are established, devices and systems must constantly be updated to adjust to security changes.

The constantly changing, complex environment of cyber security makes it difficult to understand the problem. The interplay of systems and devices presents a complex security problem that is not solved by any one solution. The solution requires a secure system architecture with an in-depth defense approach. Past methods, such as air gapped systems, do not provide adequate protection in today's connected world and with the availability of physical access to devices on the network.

The problem needs to be addressed as early as possible in the design cycle to allow for a security by design approach, and an architecture and life cycle design that accounts for ever changing and growing threats.

Cyber security at the edge

Cyber security has traditionally been perceived as an IT problem, requiring implementation of good network protocols, operating system and application protocols, firewalls, malware protection, and other solutions designed to guard against network attacks. However, there is not always unilateral agreement on what constitutes the edge.

For network providers, the edge is often considered as the router, gateway, PC, tablet, or other high functioning device. In the industrial automation space, it may be the actuator that controls a pump. In today's changing environment, these edge devices are adapting to include more functionality and higher levels of connectivity.

With these changes, the risk assessment of the system changes. Where cyber security might not have been needed previously, these devices may become the weakest link in a system if proper measures aren't taken to guard against the risks.

Implementing cyber security at the edge gives users more confidence in the data. To reach the highest levels of security, security has to be applied much earlier in the signal chain. Providing confidence that the data has not been manipulated by validating the source provides a higher level of confidence in the decisions being made from that data. ADI is in a unique position to redefine the secure edge by leveraging existing solutions that connect the physical world to the digital world.

When it comes to cyber security, complexity is the enemy. For every 1000 lines of code, there are two to three coding errors, which provide avenues to maliciously exploit a system. Implementing cyber security at the point of lowest complexity provides an environment that gives higher assurance that security has been implemented correctly.

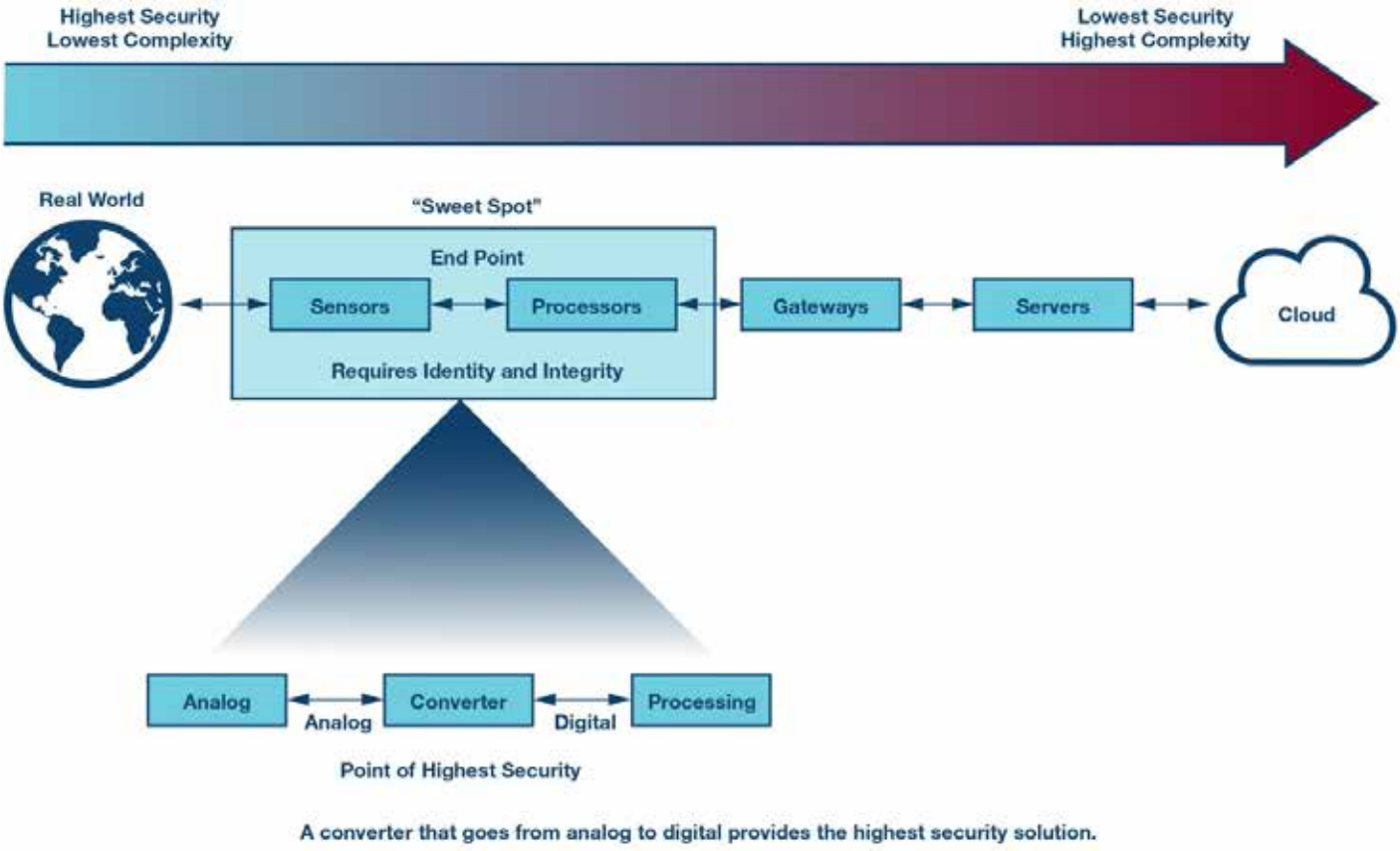
Secure operations can take place within security boundaries implemented within the edge devices, pushing the chain of trust closer to the real world. In highly complex networks, organizations and individuals must continually update applications and configurations to protect against the latest threats. At the device level, one can limit the secure operations to a footprint that becomes much more manageable throughout the life cycle of the product.

Implementing cyber security where the physical world meets the digital world provides the highest level of security by establishing trusted data earlier in the signal chain. As IT and OT converge, cyber security will not simply be an IT network problem. Devices that have not traditionally been security hardened will need to provide a root of trust in the data and security features will need to be applied based on the risk assessment and constraints of the system.

Substantiating identity and integrity at the edge establishes trust in the data earlier, providing more confidence that the data is accurate. ADI is able to provide unique value by redefining the secure edge and applying a hardware root of trust in the data.

Cyber security strategies

Analog Devices is a leader in precision sensing and has a large market share in devices that are relied upon to make real-time



SOURCE: ANALOG DEVICES

Real world systems face a broad range of challenges from the plant floor to the cloud, and varying levels of security complexity.

decisions in high reliability markets. As our customers adapt to the industry's megatrends and seek to meet the demands that change how we interact with the real world, Analog Devices is in an instrumental position to provide the highest level of confidence to our customers. In addition to providing technologies that push capabilities ahead of what is possible, we are making strides to address the problems created as byproducts of these advancements and cyber security is at the forefront of our priorities.

As we evaluate our traditional markets, there are distinct differences in how these markets perceive cyber security and their level of maturity for adopting security solutions. Analog Devices has a strong product portfolio of secure crypto solutions targeted for the defense and government market.

This cyber security expertise has been obtained through the acquisition of Sypris Electronics. By leveraging this strong base in nation state-level cryptographic solutions, we are pivoting into adjacent markets that must operate with high reliability and are driving cyber security solutions further to the edge, where Analog Devices traditionally plays in precision sensing.

Cyber security applies to all markets and Analog Devices' strategy is to effectively assess demands from each market and apply the right cyber security solutions to enable a secure device architecture congruent to the risk assessment within each application. Understandably, cyber security demands are more arduous in markets that must operate with high reliability and subsequently have a more advanced cyber security posture. Our primary focus is to address the industrial market and develop solutions that accelerate the adoption of Industry 4.0.

The industrial sector has similarly seen numerous attacks that range in severity. Some of the most significant have been nation state attacks on key infrastructure targets and targets that could result in loss of life. These attacks have been initiated through malware injected into systems, typically through physical access of a control unit or PLC connected to the factory network. With the emergence of Industry 4.0, the point of attack will continue to expand further to the edge as traditional I/O devices start having more control over operations and are connected through Ethernet to the PLC or directly to a cloud.

With this ever expanding functionality and higher functioning connectivity on a network, the edge devices that at one point had little opportunity to do system damage become a much higher risk to the system. Due to the sophistication of attacks in this market space, the ability to implement cyber security techniques correctly becomes paramount to the overall system vulnerability. This implementation requires an accurate threat assessment to understand potential points of attack and layering on security solutions to adequately protect against these threat vectors. For an edge device, establishing appropriate security boundaries and enabling a hardware root of trust greatly increases the system security posture.

Analog Devices has prioritized our cyber security strategy on the industrial market segment due to its need to operate with high reliability, the impact security has on these environments, and the megatrends that have pushed the problem of cyber security further to the edge where Analog Devices has a significant market share.

The opportunity to enable safer systems in these markets by pushing cyber security further to the edge means that Analog Devices' products will be instrumental in the overall system designs to reduce the threat impact.

Our investment into new technologies is aimed to not only provide security to withstand the threats of today and tomorrow, but make cyber security easier for our customers by solving for product-security lifecycle challenges and making it easier for our customers to incorporate cyber security at the edge.

Erik Halthen, market development manager, ***Analog Devices.***

Visit Website

5G isn't for everyone: how IoT alternate solutions come into play

Complementary IoT solutions are filling the gap here where 5G may be costly, or when deployments simply cannot support its infrastructure. While options for IoT solutions are seemingly endless, it's important to understand the needs of the deployment, and which solution can deliver.

WHILE THE HYPE AROUND 5G HAS BEEN QUITE significant, the reality is that it's a long-term investment and users won't experience the technology's full capabilities for quite some time. To date, 5G deployments have been focused on applications requiring higher capacity, higher data rates and lower latency. But 5G isn't a one size fits all solution, and while the demand for it continues, there's a growing need for complementary IoT solutions where 5G won't necessarily be most effective.

5G solutions require substantial infrastructure support, constant connectivity and immense bandwidth to support the large amount of data flowing from end-user solutions and devices. Many IoT solutions do not need that level of connectivity and in many cases, simply do not need the high end and high energy consumption hardware to support constant broadband connectivity.

With the demand for 5G comes a simultaneous need for complementary solutions that can fill this gap. We're seeing this need grow even higher as we're spending more time at home than ever before, and are relying on connectivity for education, work and employment opportunities, health care and far more.

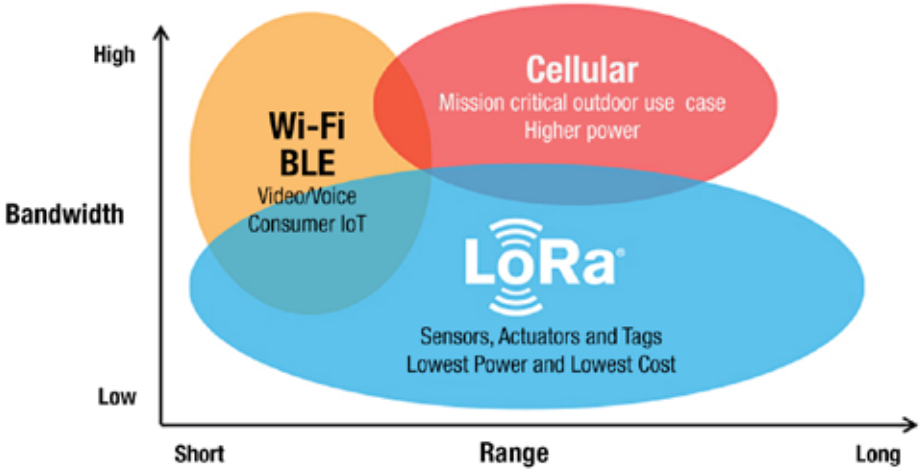
5G may seem like the IoT network that you should deploy given its industry presence, however, every technology brings specific capabilities and benefits to each unique deployment. With that said, it's important for municipalities, organizations and even individuals to understand what their needs are, and which technology can help cater to their demand.

In addition to 5G, here are a few IoT network technologies to consider:

LoRa and LoRaWAN protocol

Pros: A ground-up low power wide area network (LPWAN) design that offers low battery consumption with a lifetime of up to 10 years depending on the deployment. It also spans a long range and can seamlessly be integrated to the Cloud. Furthermore, the technology secure by design and cost efficient to roll out and offers an open business model for public, private and open community use.

Cons: Not ideal of applications requiring high data rates, nor applications requiring lower latency.



SOURCE: TE CONNECTIVITY

Bandwidth, range and cost are important considerations when selecting IoT wireless solutions.

Wi-Fi

Pros: Wi-Fi offers equivalent broadband performance than 5G enabling flexible rollout business models (private, public, and consumer). Wi-Fi enables cost efficient deployment processes while fostering open roaming across domestic markets and globally

Cons: Limited coverage range and requires high energy to properly operate.

BLE

Pros: BLE is low power consumption, cost-efficient, simple to setup and delivers accurate indoor location features.

Cons: The IoT technology offers low bandwidth and short range.

Zigbee

Pros: Zigbee is low power consumption, flexible for users and developers through its backward compatibility, and offers mesh capabilities.

Cons: Has a short range, high maintenance cost and complexity as well as a fragmented ecosystem, deploying not interoperable versions of Zigbee.

NB-IoT

Pros: Can leverage existing 4G coverage, handle large volumes of data and has a download capacity on licensed spectrum.

Cons: Has high battery consumption by design and mobility issues, high cost LTE roll out for massive IoT use cases only, features a complex ecosystem, and multiple releases.

IoT solutions like LoRa devices and the LoRaWAN protocol are driving LPWAN and sensor deployments for the IoT on land, at sea and even in space. Additionally, it not only offers connectivity for traditional IoT applications, but provides incredible benefits for critical infrastructure and solves some of the biggest challenges facing our planet across smart cities, rural areas, supply chain and logistics, and far more.

Recently, we've seen a reinforced need for connectivity due to the COVID-19 pandemic and how desperately the World relies on IoT technology. However, 3.7 billion people across the globe lack connectivity, especially those in more rural locations. By integrating IoT solutions like long range, low power technology, two-way communications to and from satellites in Low Earth Orbit (LEO) is enabled, and those in rural areas who would otherwise be without it, have access to affordable global connectivity. These rural areas may not have the proper broadband coverage or hardware in place to support constant connectivity, therefore 5G isn't the appropriate choice.

Marc Pegulu, vice president of IoT product marketing and strategy, ***Semtech.***

Visit Website

groov models with Ignition 8 onboard

New EPIC and groov RIO models provide more memory and storage to support Ignition 8 software.

Opto 22 has updated its flagship *groov* product line with new models designed to run the latest version of Inductive Automation's Ignition IIoT/SCADA platform. The new *groov* EPIC processor, GRV-EPIC-PR2 (PR2), and *groov* RIO edge I/O module, GRV-R7-MM2001-10 (MM2), both ship with Ignition Edge 8.1 pre-installed and include expanded memory and storage to support future versions.

These releases target the growing market of edge-oriented applications like operational equipment effectiveness (OEE), predictive maintenance (PdM), remote condition-based monitoring (CbM), and digital transformation/ IIoT.

Opto 22 became the first Ignition Onboard partner in 2017 when it introduced Ignition Edge to its groov product line. The *groov* EPIC edge controller uses Ignition to provide embedded OPC UA and MQTT/Sparkplug B communication, as well as optional features like database transaction management and manufacturing execution system (MES) operations. Now, with one Ignition Edge 8 license, Inductive Automation includes all of its OPC UA drivers, allows external client access to the embedded OPC UA server, and introduces mobile HMI and web scripting options.

SOURCE: OPTO 22

The new Cerabar and Deltabar instruments feature proven, reliable, and robust sensor technology.

The *groov* EPIC PR2 processor aims to support this and future releases with more than double the storage capacity of the original PR1 and nearly double the RAM.

PR2 is fully compatible with existing groov EPIC I/O, power supply, and chassis options and provides Ignition 8 developers with an automation environment that integrates PLC, PC, and network gateway functions into a single, secure edge device.

Opto 22

Visit Website

Unmanaged Industrial Ethernet switch

Eight-port unmanaged Industrial Ethernet switch delivers key industrial managed switch features.

Giving users an improved and economical plug-and-play option, the IDEC SX5E series 8-port unmanaged switch supports QoS, IGMP snooping, and broadcast storm protection functionalities. This new device provides many managed switch features to support the rapidly expanding quantity of Ethernet, IoT, and IIoT devices used in critical and challenging commercial and industrial locations. No software configuration is needed, and flexible installation options make this an economical yet high-performance solution.

Industrial networking installations commonly rely on certain advanced functions that are typically only available on managed switches. Managed switches have their place in network designs, but they require extensive configuration expertise, can be more difficult to manage over time, and cost more than other options. To address these and other issues, IDEC has incorporated the most essential managed features into this new switch.

QoS is a networking feature, usually only available on managed switches, for prioritizing specified network traffic so the most critical packets are handled first. The QoS function in the SX5E unmanaged switch automatically guarantees priority for EtherNet/ IP packets which are used extensively for crucial industrial automation tasks. For instance, a programmable logic controller (PLC) communicating with other intelligent automation devices using EtherNet/IP will receive precedence over other general traffic. QoS can be easily turned on/off with a single external DIP switch to give the user flexibility.

SOURCE: IDEC

The new switch supports QoS, IGMP snooping, and broadcast storm protection functionalities.

IDEC

Visit Website

Wi-Fi 6 for industry applications

Siemens expands network portfolio with access points and the first industrial Wi-Fi 6 client module.

With a view to the increasing demands posed by digitalization, Siemens is expanding its offerings for network components for industrial WLAN solutions. The new Scalance WUM766-1 Client Module is the first industrial client module on the market that satisfies the latest Wireless LAN Standard IEEE 802.11ax ("Wi-Fi 6"), enabling reliable and high-performance wireless connectivity.

By combining the Client Module with the new Scalance WAM766-1 Access Points, users can now implement demanding Industry 4.0 applications such as augmented reality or remote-controlled cranes. At gross data transmission rates of 1201 Mbit/s, the Access Points can link a large number of mobile devices in confined spaces, for example shuttle systems in intra-logistics.

Network components can be used outside of control cabinets, in rail applications and in hazardous areas, thanks to industry-specific approvals and their compact and robust design with IP65 degree of protection. Specific mobile devices in networks can also be deactivated using a sleep mode function combined with a digital input/output interface. This helps save energy and extend the service life and maintenance cycles of battery powered mobile devices connected via WLAN.

SOURCE: SIEMENS

Siemens is expanding its offerings for network components by offering new industrial WLAN solutions.

This enables energy-efficient operation of automated guided vehicles (AGV fleets), for example. The new components will also be equipped with an additional function especially for industry called "iPRP" ("industrial Parallel Redundancy Protocol") for redundant data communication via WLAN, providing highly available wireless communication and maximum availability for critical services.

Siemens

Visit Website

GPU-accelerated server targets AI

BoltCOR 32-18 is a rugged, fanless, ventless 2U Server for AI and GPU-acceleration at the edge.

Eurotech's newest GPU-accelerated Server is designed for AI applications at the Edge and on vehicles. The BoltCOR 32-18 is a 2U, ultra-shallow server that combines the extreme ruggedization of a fanless, ventless system with the computational power of a high-end CPU and universal deep learning accelerator. It supports both traditional and GPU-accelerated workloads thanks to an Intel Xeon E- 2276ME, with 6 cores at up to 4.5GHz, a main RAM of up to 64GB DDR4 and one NVIDIA T4 with 320 Turing Tensor Cores, 2560 CUDA cores and 16GB of dedicated GDDR6 RAM.

Designed to enable real server use cases in the harshest operating conditions, the BoltCOR 32-18 comes with high-end feature such as multiple GbE interfaces, optional lOGbE and PoE. Storage capacity is also outstanding thanks to four hot-swappable bays for SATA drives and optional RAID, which complement the internal NVME module.

Wireless connectivity features the latest technologies including up to four dual-SIM 5G/LTE modems in addition to Wi-Fi 6 and Bluetooth 5.1, while a multi-constellation GNSS with Untethered Dead Reckoning delivers geolocation and precise timing.

SOURCE: EUROTECH

New server enables AI and deep learning applications in the harshest operational environments.

The BoltCOR 32-18 features rugged Ml2 connectors and is EN50155 and EN45545; it supports wide power input (24-110VDC, isolated EN50155 Class S2) and EN50155 OTl STO operating temperature range (-25 to +55°C) making it suitable for Rolling Stock and Heavy-Duty applications. It has a 2U, 19" rack mount form factor, and is extremely shallow to fit in most recesses.

Eurotech

Visit Website

Temposonics R-Series V PROFINET

Annoucement highlights new enhancements to the Temposonics R-Series V PROFINET position sensors.

The R-Series V PROFINET is now able to transmit additional sensor status information directly to the controller via the PROFINET protocol. Users can now benefit from directly evaluating the temperature inside the sensor, total operating hours or even the total distance traveled by the magnets to perform predictive maintenance cycles or even machine condition monitoring measures.

The extended R-Series V PROFINET also includes an update of the PROFINET profiles. The encoder profile has been updated to version V4.2. This makes the R-Series V PROFINET the first linear position sensor to be certified for this version. Furthermore, the MTS profile has been updated.

The sensor as well as the corresponding description file have been certified by the PNO. With the MTS profile, it is possible to set desired parameters in a simple way. In addition, with this profile switching points can be set and monitored in parallel to the position and velocity output. The monitoring and output of the status are synchronous to the clock of the controller.

The transducers are available in rod- and profile-style and feature housing that is 37% smaller, enabling more compact construction of applications than with previous generations.

SOURCE: MTS SENSORS

New generation is backward compatible due to proven electrical and mechanical connections and designs.

The sensors are more robust and reliable than ever. Due to improved components, R-Series V supports an extended operating temperature range now reaching from -40° up to +85 °C. Resistance to shock has been increased to 150 g and for vibration to 30 g. In connection with the larger voltage supply range, the sensors are now easier to integrate into harsher and rougher applications and still provide exact measurement data up to 0,5 µm.

MTS Sensors

Learn More

Edge intelligence platform

Platform connects customers with Industrial Internet of Things data to quickly resolve performance issues.

The Cognex Edge Intelligence (EI) platform provides barcode reading performance monitoring and device management to help customers prevent downtime and boost productivity of manufacturing and logistics operations.

"Cognex's machine vision tools and barcode reading systems produce insight-rich data across manufacturing and logistics facilities," said Carl Gerst, Executive Vice President. "With EI's powerful visualization and diagnostics tools, our customers can now use that data to identify performance issues and take corrective action faster."

Within just a few minutes of installation, Cognex's EI software begins securely collecting critical device data and displaying the results in visual dashboards. Customers can use this data to analyze performance trends, monitor configuration changes, and capture no-read and failed validation images for further analysis.

The platform can monitor multiple devices and lines within a single site as well as deploying configurations and firmware updates simultaneously to a large number of connected devices. It also includes audit trail capabilities that track and report any changes to device settings and connectivity features for easy integration with other Industry 4.0 solutions.

SOURCE: COGNEX

Data can analyze trends, monitor configuration changes, and capture no-read and failed validation images.

Cognex EI is designed to help improve overall equipment effectiveness (OEE) and increase throughput across a range of industries including logistics, food and beverage, consumer products, packaging, automotive, medical devices, and electronics.

Cognex

Visit Website

Smart condition monitoring solution

Multisensors form the hardware basis for installation on pumps, gear units, compressors and drive trains.

Sitrans SCM IQ, a new IIoT solution for smart condition monitoring, enables potential incidents to be detected and prevented at an early stage, reducing maintenance costs, downtime and increasing plant performance by up to ten percent.

Wireless, robust Sitrans MS200 multisensors form the hardware basis for installation on machinery such as pumps, gear units, compressors, and drive trains, where they collect vibration and temperature data. Via a Bluetooth connection, this data is sent to the Sitrans CC220 industry gateway where it is encrypted before being transmitted from there to the cloud, in this case the MindSphere industrial IoT-as-a-Service solution. The anomaly detection of the Sitrans SCM IQ system is based on machine learning. It constantly monitors and analyzes all sensor values and detects deviations from the normal operating state in advance.

Anomaly notifications are sent via SMS and/or email, depending on the configuration and defined user group. The app can be used to document the anomalies of machinery behavior and makes them available to a specific circle of users. The Sitrans SCM IQ system comprises multisensors, gateway and app, and can be used in all industrial plants with mechanical or rotating components. It is scheduled to be available from summer 2021.

SOURCE: SIEMENS

The Sitrans CC220 industry gateway ensures secure communication between the multisensor and the cloud.

The Sitrans MS200 multisensors feature a robust and compact industrial design with a high IP68 degree of protection. Bluetooth communication eliminates the need for cabling, which greatly simplifies installation and commissioning. The power supply is provided by replaceable industrial batteries, enabling a long service life.

Siemens

Visit Website

IO-Link master solutions

LioN-X and LioN-Xlight IO-Link masters simplify connectivity for fast and secure data transmission.

Powerful LioN-X IO-Link Masters provide a faster, more reliable and secure approach to collecting, converting and transmitting sensor and actuator data in automated production environments, and is IO-Link specification V1.1.3 ready. Now with increased speed capabilities, the advanced solution enables manufacturers to optimize production processes and improve efficiency through state-of-the-art connectivity.

Available in two new variations, the LioN-X family is built for maximum performance, and the LioN-Xlight is cost-effective. Each product line offers a flexible solution to meet the needs of any manufacturing operation for machine connectivity and data collection.

With the LioN-X family, users benefit from:

- Versatile protocol communication, connecting digital I/O signals and IO-Link devices for fieldbuses, as well as IIoT integration for cloud applications.
- Easy to configure with LioN-Management Suite V2.0, reducing the time to configure LioN-X and IO-Link devices.
- Innovative security functionality, minimizing the risk of unauthorized access to equipment and the network with ACHILLES and vulnerability-tested data transmission.
- Fast data transfer with cycle times around 1ms, ensuring that IO-Link data reaches controllers quickly and reliably.
- Unmatched power and connectivity using M12 Power L-coded connectors.

SOURCE: BELDEN

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

Belden

Visit Website

AWS Quick Start: edgeConnector Siemens

AWS Quick Start for Softing's edgeConnector Siemens docker container application is available.

An AWS Quick Start for Softing's edgeConnector Siemens docker container application is available, in collaboration with Amazon Web Services (AWS).The Quick Start automatically deploys edgeConnector Siemens and AWS IoT SiteWise in the AWS cloud. It demonstrates how to connect Siemens PLCs to the AWS cloud in a secure and scalable way.

Customers are increasingly facing challenges in connecting the cloud to the edge in a secure way. “Many customers that we speak to, are hesitant when it comes to connecting their machines to cloud and using the Internet of Things” says Dr. Christopher Anhalt, VP Product Marketing at Softing Industrial Automation GmbH. Industrial customers lack experience in edge computing and do not have access to reference artifacts and best-practices resources for edge computing and the Internet of Things.

SOURCE: SOFTING

edgeConnector Siemens is Softing’s first commercially available gateway product to support container technology.

The Softing edgeConnector Siemens Quick Start makes it easy for IT as well as for shopfloor personnel to gain first-hand experience with a secure and highly scalable end-to-end solution for Industrial IoT. The Quick Start offers a fast and flexible way to try out edgeConnector Siemens as connectivity solution with AWS. It automates the deployment of Softing’s edgeConnector Siemens, a docker container application with gateway functionality, and AWS IoT SiteWise in the AWS cloud. A simulated Siemens S7-1500 PLC generates IoT sensor data that is sent to AWS via edgeConnector Siemens and visualized using AWS IoT SiteWise. This entire deployment on AWS takes not more than 10 minutes.

Softing

Learn More

Plant-floor asset management software

Manage hundreds or thousands of automation assets using the enhanced FactoryTalk AssetCentre software.

Latest release of FactoryTalk AssetCentre provides firmware and software lifecycle information for all assets in one place. This saves time because workers no longer need to connect to control cabinets and manually record information for each device.

With the software’s enhanced asset inventory functionality, workers can quickly scan a network and see which devices are in a specific lifecycle state. Examples include devices running retired firmware or forecasted to be discontinued in the next six months. This helps identify products in the same lifecycle state and workers can better plan for replacements and upgrades.

This also helps companies comply with the latest cybersecurity standards such as IEC 62443 because the latest versions will address many known security vulnerabilities.

SOURCE: ROCKWELL AUTOMATION

Archive management of change automates process of authorizing who can change files and what they can change.

The FactoryTalk AssetCentre software also has a new security feature called archive management of change, which automates the process of authorizing who can change files and what they can change. It requires workers to explain why files need to be changed and verifies that only necessary files are being checked out. It also locks a file until changes are approved and escalates approval requests when needed.This helps enhance system security, which is particularly useful for some industries such as oil and gas, that require added levels of control over when changes are permitted. For example, one major food company reduced its downtime events from unknown or unauthorized changes by 7% using FactoryTalk AssetCentre software.

Rockwell Automation

Visit Website

TwinCAT Vision with HMI visualization

TwinCAT Vision offers new HMI control package with the option of integrating image processing into HMIs.

TwinCAT Vision combined with TwinCAT HMI Visualization includes an expanded image display control and a color control. The image display control enables directly linking multiple image variables and switching easily between displayed images. It also supports the following:

- Freezing the image to stop it refreshing and allow detailed analysis of the last capture
- Scaling and moving the image within the vision control (by means of touch gestures, mouse input, or direct entry of specific values) for more precise viewing of image details
- Displaying a toolbar with directly usable control elements (e.g. for selecting images, scaling, creating shapes, freezing the image refresh, and downloading the displayed image)
- Displaying an information bar showing current details and values, such as image size, pixel coordinates, color values and shape data
- Drawing shapes (points, lines, rectangles, ellipses and polygons) with modifiable positions and sizes, used to determine size, area and coordinates and to set regions of interest, among other things
- Displaying graphics (a cross, rectangles and circles) or image overlays for the purpose of setting up and positioning cameras and workpieces

SOURCE: BECKHOFF

The color control incorporates various other controls as well as JavaScript programming.

Without the convenience of this control, users would have to go through the time-consuming process of creating and coding these capabilities themselves with the help of other elements.

Beckhoff Automation

Visit Website

Power over Ethernet flowmeters

ABB incorporated power supply through Ethernet connectivity on-board in latest edition of flowmeter.

Power over Ethernet (PoE) offers benefits for process engineers, as it omits the need for a separate DC power infrastructure, providing power and communications via the same cable.

This brings new agility as flowmeters can be installed wherever needed. In addition, ABB 4-wire Ethernet combines classic outputs with future communication protocols. Offering a modular design allows the combination of both worlds and ensures that devices are future-proof, increasing the longevity of the flowmeters.

Furthermore, flowmeters with Ethernet connectivity increase simplicity, flexibility and reliability to operations in process automation, while enhancing real-time visibility of data.

Previously hidden data in field devices, such as measurement values on density, conductivity or concentration of the medium, can be unlocked. This in turn will help customers across all industries identify redundant measurement points in their plants to achieve savings along the way.

An integrated secure webserver based on the ABB Ability Cyber Security framework ensures robust and secure operations that offer instrumentation engineers support during commissioning and troubleshooting.

SOURCE: ABB

Electromagnetic and mass flowmeters open up a new chapter in instrumentation and industrial communication.

It also provides access to configuration, diagnostics and measurement data through a built-in QR code. This allows verification of all parts of the flowmeter and provides insights into its operating condition with automatically generated reports that report performance.

ABB

Visit Website

Pressure instruments offer connectivity

Cerabar and Deltabar pressure instruments provide simplicity by leveraging Bluetooth technology.

Endress+Hauser has announced the release of new Cerabar and Deltabar pressure and differential pressure instruments, with a Bluetooth interface for easier operation and improved efficiency in regulatory control, safety, and other systems.

A high level of safety combined with enhanced productivity follows the Endress+Hauser smart safety approach to increase plant availability. Heartbeat Technology creates the data basis for predictive maintenance and allows the instruments' functionality to be verified without process interruption.

Many industries are struggling with attrition, personnel turnover, and training new hires, and major plant additions are often performed by service providers who may not have a thorough knowledge of the equipment and systems on site. The amount of safety-related equipment continues to grow in many industries, and with it the number of costly required proof tests for maintaining safety integrity level (SIL).

To comply with these and other requirements, Endress+Hauser's new transmitters offer a more user-friendly user interface in its new Cerabar and Deltabar pressure transmitters. Intuitive operation is now provided via the SmartBlue app, which includes guided operating sequences for parameterization and commissioning of the pressure sensor, bridging distances of up to 50 feet. Measuring points that are difficult to reach, or in hazardous areas, are easy to maintain even if they are only integrated into the process via a 4–20mA interface.

SOURCE: ENDRESS+HAUSER

The new Cerabar and Deltabar instruments feature proven, reliable, and robust sensor technology.

The Bluetooth connection has a special protocol that meets increased safety needs.

Endress+Hauser

Visit Website

Certified PROFINET with PROFIdrive

First drive technology manufacturer to integrate certified PROFINET into a servo motor.

Since the end of February 2021, Dunkermotoren's fully integrated PROFINET solution has been officially certified by the PROFIBUS user organization.

Now, another important feature is fully integrated into the motor, which is a milestone in terms of cabling, commissioning and IIoT capability. Dunkermotoren, the world leader in brushless DC motors with integrated electronics from 1 to 4000 watts, claims it is the first drive technology manufacturer to fully integrate its certified PROFINET solution with PROFIdrive into a motor.

The certification assures Dunkermotoren that the high standards of stability, even under extreme bus conditions, are always maintained. Currently the products BG 95 dPro, BG 75 dPro, BG 66 dPro and the BGE 5510 dPro are available with PROFINET interface, covering the output power from 1 to 4000 W.

Dunkermotoren, part of the AMETEK group and drive technology manufacturer from the Black Forest for over 70 years, convinces with innovative, high-quality and flexible drives up to 4000 W output power.

SOURCE: DUNKERMOTOREN

The new product portfolio includes brushless and brushed DC motors, as well as linear systems and AC motors.

The portfolio includes brushless and brushed DC motors, as well as linear systems and AC motors. Since the beginning of 2020, the portfolio has been expanded by the sister company MAE to include stepper motors and blowers.

All components can be expanded in a modular system by gearboxes, encoders, brakes and integrated or external electronics to form the complete drive.

Dunkermotoren

Visit Website