9.2020 Issue **120**

ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking and IoT

www.iebmedia.com/ethernet ■ www.iebmedia.com/wireless

GET CONNECTED...

www.iebmedia.com/ethernet ■ www.iebmedia.com/wireless

Following a legend...

It's never an easy task to follow a legend but Single Pair Ethernet is doing its best to replace the RJ45 connector in a wide range of Ethernet applications with fanfare appropriate to its technological importance. RJ45 has been the enduring and recognizable face of Ethernet for many years now, but SPE is bringing new technology to Ethernet infrastructures that will make it a worthy replacement.

In the last two years, SPE technology has solidified its position and gained industry acceptance that is driving it forward as the infrastructure basis that makes IIoT and Industry 4.0 possible.

A strong partner network has emerged in support of 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 starting in 2018. For the reliable establishment of the entire future SPE ecosystem, standards for transmission protocols, cabling and device components are also jointly supported. The result is that members of the SPE partner program, as well as ISO/IEC JTC 1/SC 25/WG 3, are in close exchange and intensive cooperation with IEEE 802.3 and IEC SC46C for uniform transmission standards and copper data cables.

In this issue of the Industrial Ethernet Book, we offer a line-up of stories highlighting the latest Ethernet Infrastructure technologies.

In "Single Pair Ethernet, RJ45 and clarifying the mating interfaces" starting page six, author Rainer Schmidt of HARTING explains how modern components can now bring fast Ethernet (up to 1 GBit/s) to the smallest application using just one twisted wire pair, and SPE is enabling consistent usage of the TCP/IP protocol for the first time.

On page 18, Manuel Rüter of Phoenix Contact discussed use of SPE technology in industrial applications by offering IP protected solutions. His conclusion is that Single Pair Ethernet work continues with the aim of toughening up this evolutionary new technology for as many application scenarios as possible. But reduced cable weight, miniaturization and simplification of the connection technology will only come into play with achieving continuity with the overall infrastructure.

Only time will show the full impact of this technology but the stage is set for big things. Rüter added to his conlusion, and we agree: "this innovation will influence the network structure in all fields of application from building automation, through factory automation, to process automation. In this context, no one should lose sight of the fact that decisions made today will determine where Ethernet will go in the future."

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **November 2020**
Deadline for editorial: October 9, 2020 **Deadline for artwork:** October 30, 2020

Product & Sources Listing

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

Update your own products

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

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

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

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

The world's first positioning standard for industry: omlox

Uniform positioning standard for industrial products from different vendors is now available. PI (PROFIBUS & PROFINET International) will be handling worldwide coordination and tehnology management.

THE HIGH-TECH COMPANY TRUMPF AND 60 partners have introduced a standard for positioning technologies. Called omlox, this new industry standard provides the means to integrate all existing technologies such as UWB, BLE, RFID, 5G or GPS and deliver positioning data via a uniform interface.

"Despite the current situation, companies should keep their sights fixed firmly on the future and expand their digital applications. A common standard for positioning solutions simplifies logistics enormously and ensures efficiency gains in digital manufacturing," said Thomas Schneider, Managing Director of Development at TRUMPF Werkzeugmaschinen. Omlox may now be used worldwide.

A global language for industry

They have since handed the project over to the PI organization, which is to advance the omlox standard globally. PI has been supporting various industry standards for 30 years now.

"The PI organization has all the processes and a great deal of experience to bring open and easy-to-use standards to the world. As an independent organization, we can continue to make sure that all partners will be able to contribute on an equal footing," said PI Chairman Karsten Schneider.

SOURCE: TRUMPF

Omlox can locate components which enables manufacturers to track products all along the supply chain.

Connecting different vendors

Products may be tracked across the board by incorporating various positioning technologies. Omlox serves to pinpoint the location of forklifts, drones, driverless transport systems or tools from different manufacturers with one and the same infrastructure. It enables position data to be used far more widely across the factory. Users can even locate devices inside buildings with accuracy down to the millimeter range, much like what GPS can serve to do outdoors. The initiators of omlox include the software and IT service providers GFT, T-Systems and AWS, the sensor manufacturers SICK and Pepperl+Fuchs, the research institute CEA Leti, the software vendor Heidelberg Mobil and the tracking solutions provider BeSpoon. Around 60 companies are already supporting the project.

News from ***PROFIBUS & PROFINET International.***

90% of industry to utilize edge computing by 2022

FROST & SULLIVAN'S RECENT ANALYSIS, "5G and Edge Computing—Cloud Workloads Shifting to the Edge, Forecast to 2024", finds that edge computing is a foundational technology for industrial enterprises as it offers shorter latencies, robust security, responsive data collection, and lower costs.

In this hyper-connected industrial environment, edge computing, with its solution-agnostic attribute, can be used across various applications, such as autonomous assets, remote asset monitoring, data extraction from stranded assets, autonomous robotics, autonomous vehicles, and smart factories. Despite being in a nascent stage, the multi-access edge computing (MEC) market—an edge computing commercial offering from operators in wireless networks—is estimated to grow at an astounding compound annual growth rate of 157.4%, garnering a revenue of $7.23 billion by 2024 from $64.1 million in 2019.

"The recent launch of the 5G technology coupled with MEC brings computing power close to customers and also allows the emergence of new applications and experiences for them," said Renato Pasquini, Information & Communication Technologies Research Director at Frost & Sullivan.

Frost & Sullivan predicts that approximately 90% of industrial enterprises will utilize edge computing by 2022, presenting immense growth prospects for MEC market participants, including:

- Telecom operators should work on solutions to meet the requirements for connected and autonomous cars.
- System integrators should provide end-to-end solutions, which would be a significant value addition for enterprises because 5G requires specific skillsets.
- The combination of 5G and the new specialized hardware-based mobile edge compute technologies can meet the market's streaming media needs now and in the future.
- Telecom operators must partner with cloud providers and companies with abilities related to artificial intelligence, machine learning, and computer vision to design solutions for autonomous cars, drone delivery, and others.
- Companies in the MEC space must capitalize on the opportunity for innovation and new developments that utilize 5G and MEC, such as augmented reality (AR) and virtual reality (VR), which can also be applied to games.

News report by ***Frost & Sullivan.***

| PC11-53E |

Maximum performance with minimum footprint

www.beckhoff.com/c6030
www.beckhoff.com/c6032

By integrating Intel® Core™ i processors of the highest performance class up to the ninth generation, Beckhoff offers the possibility with its C6030 ultra-compact IPC to execute highly complex and demanding applications with a reduced space requirement. The devices are ideal for practically any automation and visualization task offering a maximum of processing power through to the Core™ i7 with eight 2.6 GHz cores. Additionally, the C6032 variant offers further interfaces to enable increased flexibility.

Ultra-compact

C6015

C6017

C6025

Ultra-powerful

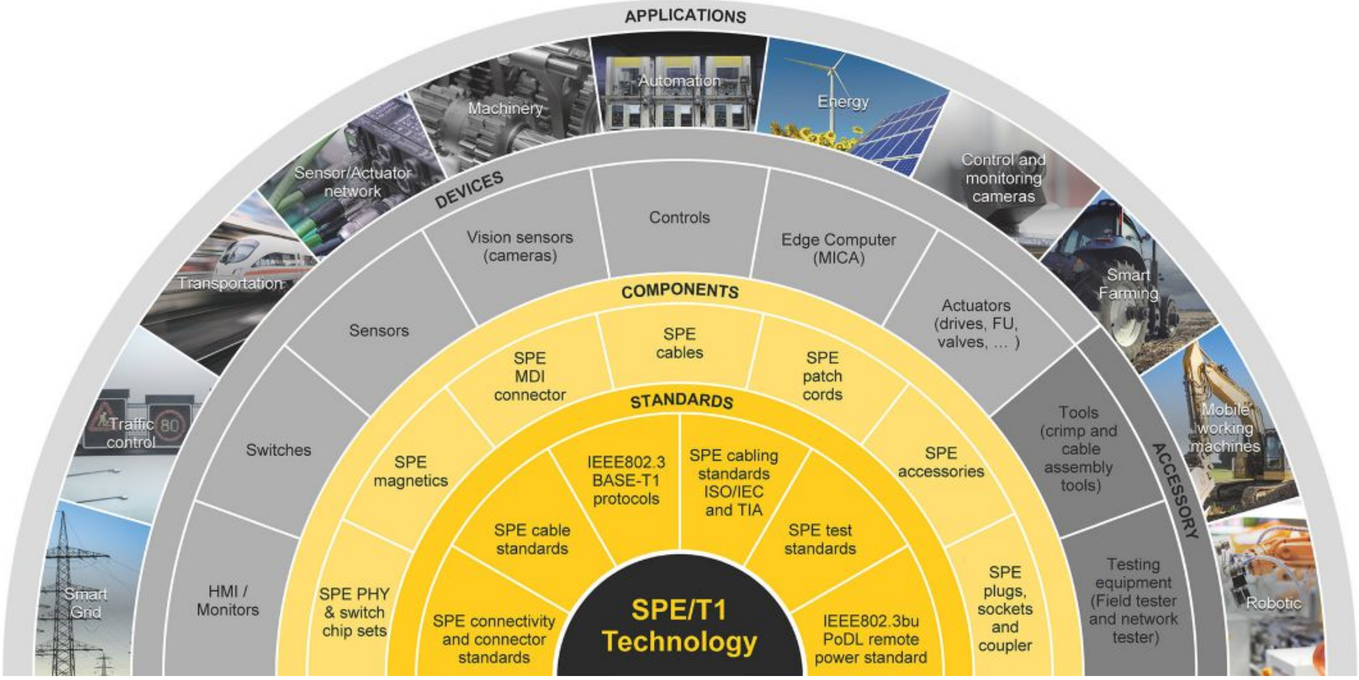
C6030

C6032

New Automation Technology **BECKHOFF**

Single Pair Ethernet, RJ45 and clarifying the mating interfaces

Previously, there has been a classic break in communication systems between Ethernet and fieldbus systems. But now, modern components can now bring fast Ethernet (up to 1 GBit/s) to the smallest application using just one twisted wire pair, and SPE is enabling consistent usage of the TCP/IP protocol for the first time.



SOURCE: HARTING

The Single Pair Ethernet ecosystem demonstrates how technology, standards, infrastructure components, devices and test equipment logically build on and support each other.

SINGLE PAIR ETHERNET (SPE) WAS DEVELOPED for one reason only. It was meant to close the last big gap in a TCP/IP oriented network world – the gap between classic IT and sensor technology which is becoming more and more important.

Thus SPE is not a replacement technology for existing cable-bound Ethernet networks as are found almost everywhere in IT. Therefore it is not a matter of replacing four-pair cabling; instead it is a matter of accessibly docking sensor/actuator networks to our IT networks. For this reason, SPE is also referred to as an “enabler” for IoT and IIoT.

This article intends to shed light on what this means and what this development will look like. At the same time, it will also clear up several entrenched “hypotheses” that only cause confusion but do not contribute anything to the development of SPE and future markets.

SPE technology

Single Pair Ethernet (SPE) is no product of coincidence. It is the simple answer to the question of what future automation solutions have to look like so that they can be implemented successfully on the market. This question stirred up three sectors in particular: the automotive industry, industrial automation, and building automation.

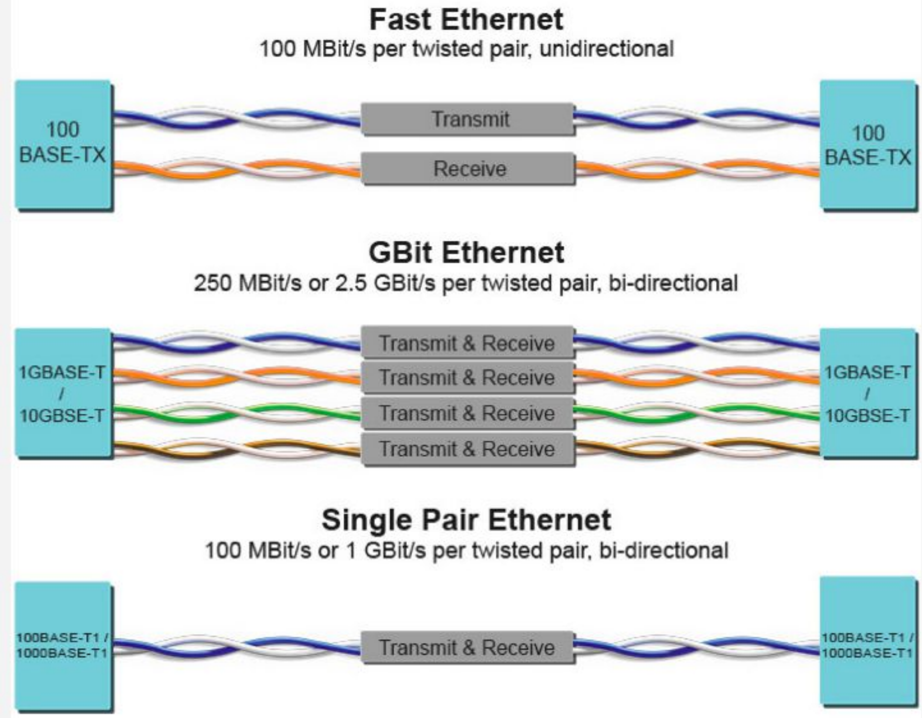
All three areas of application require unimpeded access to sensor/actuator networks for the next step in their respective automation solutions. Only in this way can autonomous driving be implemented in a car, a continuous manufacturing process in industry be implemented in accordance with Industry 4.0, or an intelligent building be achieved in building automation.

These considerations drive the development of SPE – and nothing else. The fact that cabling is becoming simpler and plug-in connectors are getting smaller is an additional positive effect; however it is not the cause for the SPE innovation.

After these initial observations we can move on to the next questions. What will the applications, or more precisely the implementations of SPE, look like in the three largest fields of application and what does it signify for cabling?

In a car, SPE must be implemented in a simple, fast yet stable way, partially under extreme operating conditions. For the car manufacturer this means: simple control of all relevant components via SPE. The cabling for this purpose is generally done unshielded with own developed connection technology. This connection technology is always characterised by simple design, which combines the advantages of plug connectors and terminal blocks, and can be bundled in blocks in a very space-saving way. The first model series are already being delivered with SPE. In 10 years, this technology will become standard and today's CAN bus or comparable solutions will have been completely replaced.

It is basically quite similar in industrial automation as well. Extreme conditions such as large temperature ranges that need to be covered, shock and vibration as well as IPx protection against dust and wetness also play an important role in the design of connection technology. However, shielded cables are primarily used in industry in order to guarantee higher interference immunity in the area of EMC.



SOURCE: HARTING

Multi Pair versus Single Pair Ethernet, technology approach and system diagram.

The design for plug connectors for SPE in industrial automation are thereby oriented on robust, shielded IP20 connectors through to IP65/67 protected versions in the widespread M12 and M8 housing designs.

What does SPE do in building automation? The most exciting story awaits us in this area. This is because building automation systems have solutions such as KNX, LON, EchoNet, TRON and others that must strategically decide how and in what scope they will use SPE in the future. However, they will not be able to bypass SPE technology with the innovative pressure of SPE in sensor technology.

It remains to be seen whether they will also use this technology change in further-reaching changes, such as systems that are completely Ethernet-based. When it comes to cabling, both unshielded and shielded solutions are used that are generally installed indoors and therefore do not need to exhibit the robustness that is, for instance, required in industry. If anything, RJ45 played a role as the service and test interface. Otherwise special terminal blocks with screw or terminal technology is used as the connection technology.

SPE connection technology

In all three areas - car, industry, and building automation - the RJ45 plays no role whatsoever in the introduction of SPE. In all three areas there is also no history (installed RJ45 basis) that had to be taken into account during the introduction of SPE. Thus considerations regarding the backward compatibility of SPE connection technology to RJ45 cabling is of course permissible but not really practical. The applications simply are not there.

Hypothesis number 1

An SPE mating face must be RJ45 backward compatible - is thereby debunked. However, the brief clarification of SPE application areas reveals as well that each one has its own history and above all else, each one has its own special requirement profile.

This also leads to special designs in SPE connection technology (in SPE mating faces). Thus there will not be THE ONE solution that is always in demand from different sides. Or to be quite clear: there will not be one universal SPE-plug. Instead, what is becoming apparent is that there will be three solutions for SPE mating faces:

- One for cars (or multiple ones, depending on the manufacturer)
- One for industry
- And one for building installation

Let us leave out the topic of cars for now and take a closer look at industry and building installation in order to get to the bottom of the question of why “the plug manufacturers” cannot “agree” on a uniform mating face.

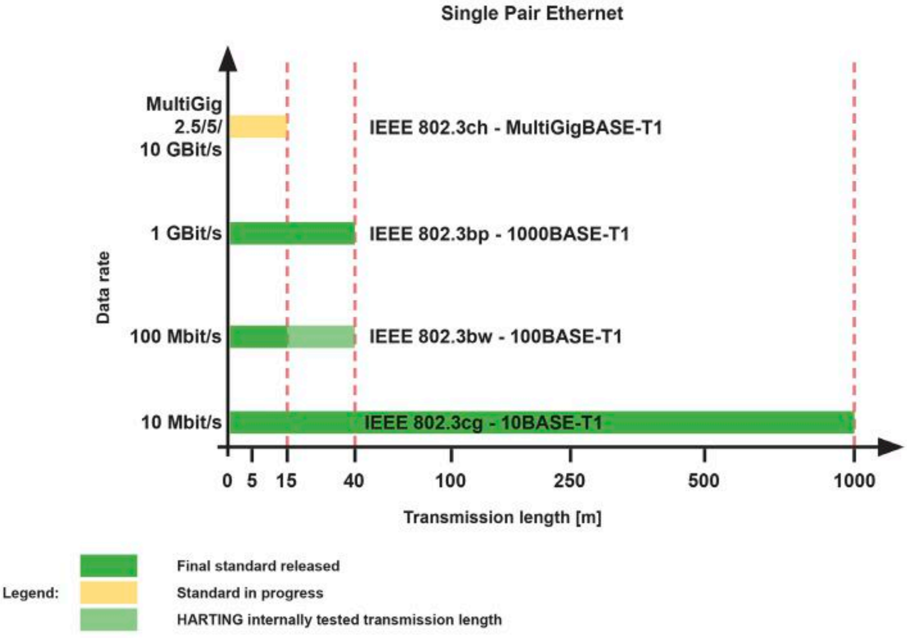
Again for the sake of comprehension: these “plug manufacturers” are not a homogeneous entity, they are competitors on a market that has the final say in deciding which product is enjoyed and used a lot, and which one flops. And this is a good thing, especially for the user, who thereby gets a lot of products to choose from and can decide him or herself which ones he or she prefers. The demand for an “agreement” can also be interpreted in terms of who takes on the technology leadership here.

This question is justified. And this question is also answered. Two technology leaders in industry and building installation have taken initiative in their respective area at the top of SPE.

Both of these fields of application have met - at least with regard to cabling, or more precisely, with regard to the connection of new SPE cabling and structured building cabling - in the ISO/IEC 11801 series of standards.

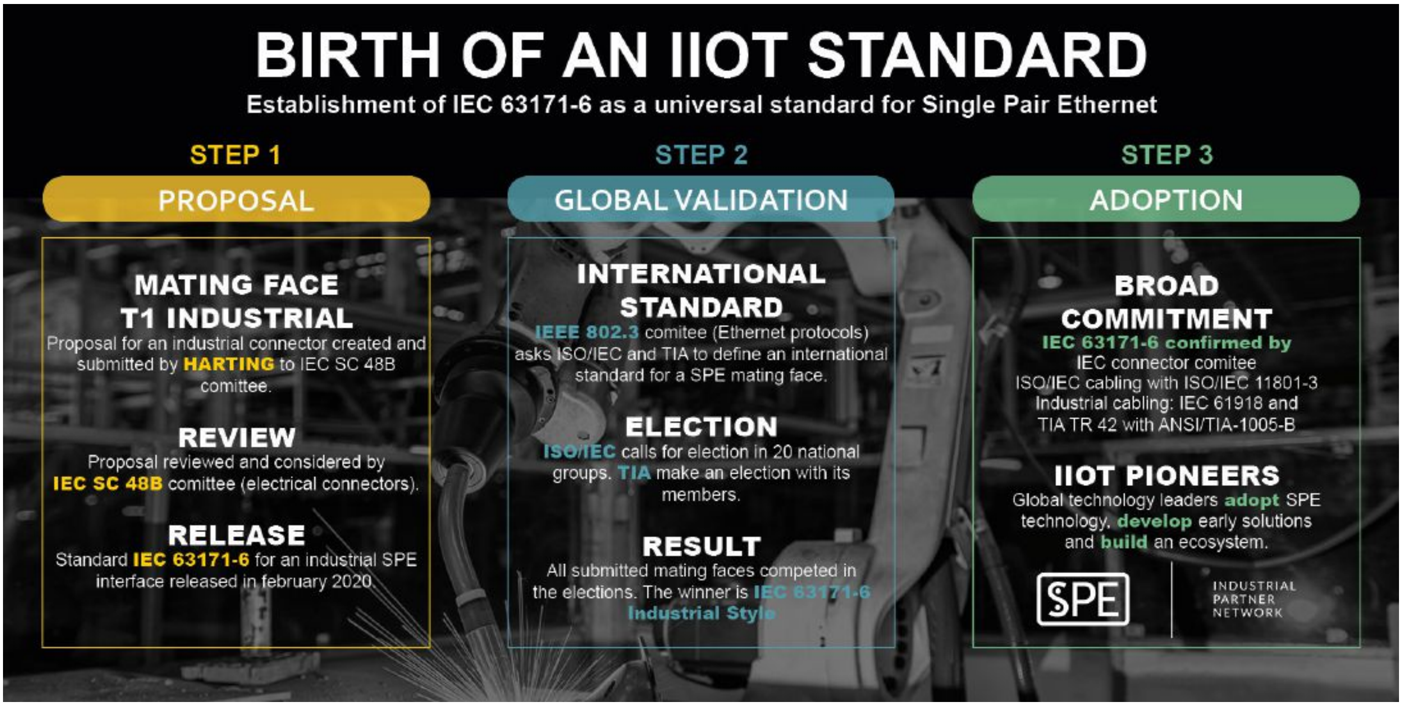
With ISO/IEC 11801-3 there is an industrial part and with ISO/IEC 11801-6 there is a part for building service/building automation.

This fact prompted the IEEE802.3 (Ethernet standardisation) to ask ISO/IEC JTC 1/SC 25/WG 3 (cabling standardisation that also develops the 11801 papers) for a recommendation for an SPE mating face, which led to a selection process within SC 25/WG 3



SOURCE: HARTING

Graphic display of range and transmission speeds for the current IEEE 802.3 SPE standards.



BIRTH OF AN IIOT STANDARD

Establishment of IEC 63171-6 as a universal standard for Single Pair Ethernet

STEP 1

PROPOSAL

MATING FACE T1 INDUSTRIAL

Proposal for an industrial connector created and submitted by **HARTING** to IEC SC 48B comittee.

REVIEW

Proposal reviewed and considered by **IEC SC 48B** comittee (electrical connectors).

RELEASE

Standard **IEC 63171-6** for an industrial SPE interface released in february 2020.

STEP 2

GLOBAL VALIDATION

INTERNATIONAL STANDARD

IEEE 802.3 comitee (Ethernet protocols) asks ISO/IEC and TIA to define an international standard for a SPE mating face.

ELECTION

ISO/IEC calls for election in 20 national groups. **TIA** make an election with its members.

RESULT

All submitted mating faces competed in the elections. The winner is **IEC 63171-6 Industrial Style**

STEP 3

ADOPTION

BROAD COMMITMENT

IEC 63171-6 confirmed by

IEC connector comitee

ISO/IEC cabling with ISO/IEC 11801-3

Industrial cabling: IEC 61918 and

TIA TR 42 with ANSI/TIA-1005-B

IIOT PIONEERS

Global technology leaders **adopt** SPE technology, **develop** early solutions and **build** an ecosystem.

SPE INDUSTRIAL PARTNER NETWORK

Steps in the process of Single Pair Ethernet becoming an international standard.

at the start of 2018.

A requirement profile for SPE mating faces was created by SC 25/WG 3 as a basis for this selection process. Part of this requirement was the assurance of all manufacturers/applicants, that in the event of success a submitted mating face would also apply to standards in order to guarantee plug-in compatibility and freedom from patents.

Various manufacturers participated in this selection process, all of which are active in international standardisation, some of which presented their concepts and added their know-how to the discussion. At the end of this process, all SPE mating face concepts were voted on.

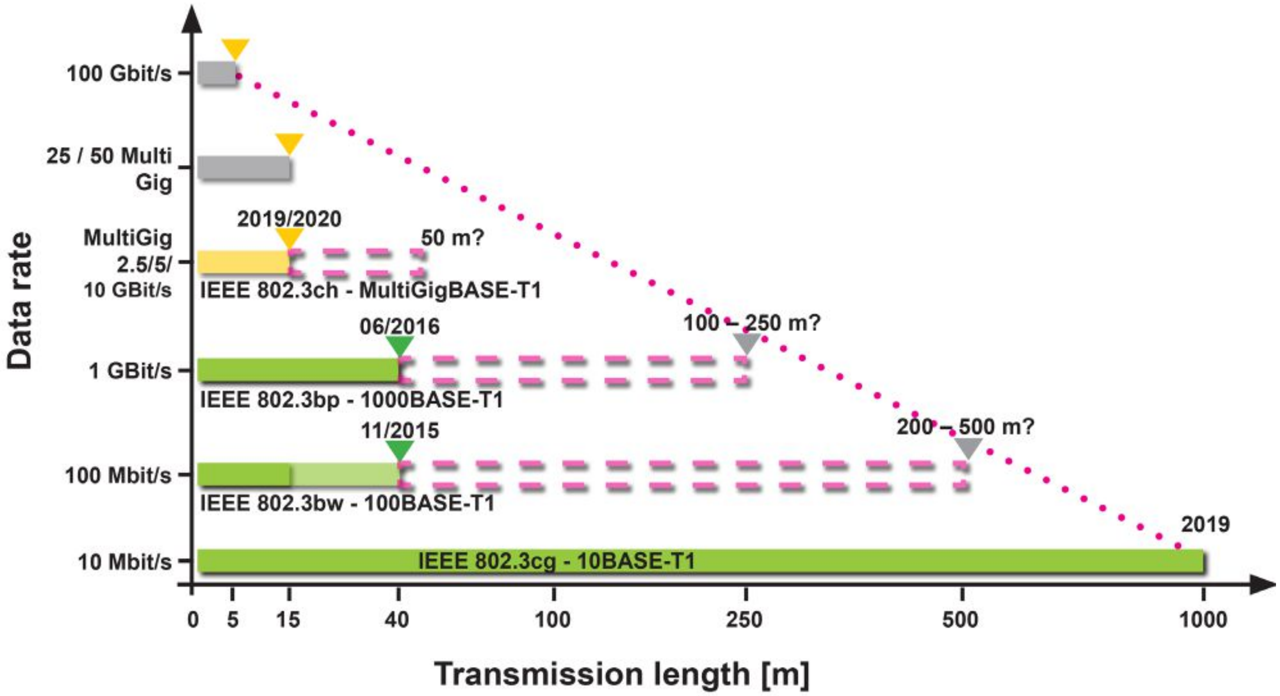
This vote, international ballot, was performed in accordance with the rules of ISO/IEC and 25 countries participated through their NCs - National Committees. Every country only has one vote.

Result in June 2018: There was an absolute majority for the SPE industry mating face as per IEC 63171-6 (HARTING concept), as well as for the mating face as per IEC 63171-1 (CommScope concept) for building installation.

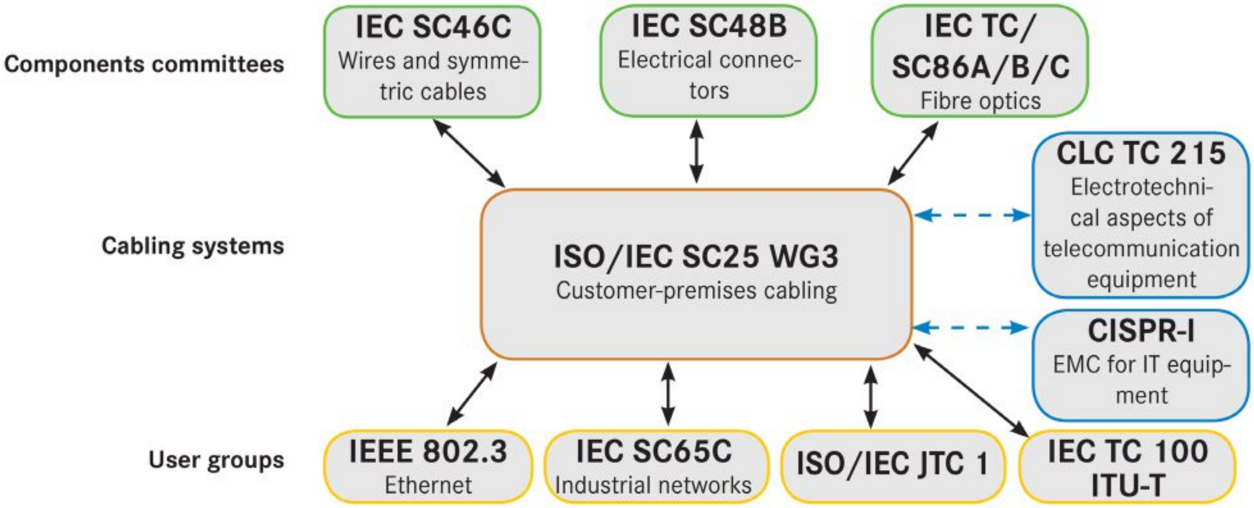
Hypothesis number 2

Plug connector manufacturers cannot agree on an SPE mating face - also is not true. An agreement of this kind already took place mid 2018 through international standardisation of ISO/IEC.

With the ISO/EIC defining ONE SPE mating face for industry (IEC 63171-6) and ONE mating face for building installation (IEC 63171-1) the work on further cabling standards is continuing gradually. Decisions about the SPE mating face are consistently being integrated into the corresponding



Single Pair Ethernet: transmission length and speed.



SOURCE: HARTING

Various standards committees and their work relating to Ethernet communication.

papers of ISO/IEC, TIA and IEEE.

The good news for all users: the standardised SPE mating face for industry as per IEC63171-6 will be adopted into all relevant cabling standards and become a mandatory provision.

In detail this pertains to:

- ISO/IEC 11801-3 AMD-1: Information technology — Generic cabling for customer premises (structured cabling) Part 3: Industry, AMD-1: SPE
- ANSI/TIA-1005-B Telecommunications Infrastructure Standard for Industrial Premises - SPE cabling
- IEC 61918 Ed 4.0 AMD-1: Industrial communication networks - Installation of communication networks in industrial premises, AMD-1 SPE

SPE in process automation

Then there is the discussion about process automation (PA) and the meaning of SPE for pending innovations in this area.

After the first two arguments against SPE and a standardised mating face have missed their target, let's look at the PA argument and that everything is completely different in that area.

It is correct that PA has a somewhat special position within the broad spectrum of industry automation solutions. PA does have a specific requirements profile in its areas of application in the oil and gas industry, the chemical and pharmaceutical industry, as well as in mining, water management, cement and glass production, the food industry etc.

This requirements profile is also characterised by large distances, therefore also the 1000m in IEEE802.3cg. This, on the other hand, has effects on the cross section of copper cable AWG16, AWG 18 and in addition to classic plug connections for SPE also favours connection blocks.

Furthermore, the subject of ex-protection as per IEC/EN 60079-0 and IEC/EN 60079-7 also plays an important role. Thus the connection technology must satisfy the provisions for intrinsic safety in certain application cases, which in turn entails a special design.

Solutions for remote powering are also affected by it. Networking concepts with SPE in PA, for instance, provide for the operation of SPE switches in ex-protected areas. This in turn means higher performance requirements that cannot be satisfied by PoDL, or only partially. This means that providers of PA solutions also fall back on their own remote powering concepts.

Single Pair Ethernet connector variants.

Now the question is what market relevance does process automation have for the development of IIoT and SPE? And here one must bluntly say: the relevance is very low.

In the concert of solutions for industry automation, process automation represents a one-figure percentile. The special case of ex-protection represents a mere fraction. In the end, the hypothesis basically dissolves into thin air - that process automation determines the development of SPE.

Process automation is one and only one application for SPE in industry. Due to the specific requirements of PA the adjustment of SPE components are partially required. Hence PA is not the pacemaker for SPE; it is the other way around. SPE gives PA the opportunity to implement the innovation in the development of TCP/IP networks.

There have been long discussions about it and unfortunately many hypotheses have been proposed that create uncertainty. It is time to clear up these hypotheses.

- SPE and SPE mating faces have nothing to do with RJ45.
- In the standardisation, from the various manufacturer concepts one mating face was selected for SPE in industry - IEC 63171-6.
- Process automation does not determine the development of SPE - it is the other way around.

The end of these hypotheses also means the beginning of a new, real world. SPE is paving the way for IoT/IIoT.

Rainer Schmidt, Business Development Manager, Cable Systems, ***HARTING Electronics.***

Improving industrial security in large brownfield plants

In industrial plants, PLCs run the show. Chemical giant BASF had a large number of PLCs and they wanted to update automatically. But with multiple firewalls to navigate and many third-party devices involved, integrating them on a single network would be a challenge.

AN INDUSTRIAL NETWORK IS A PRODUCTION plant's backbone. As long as it's strong, secure, and reliable, productivity can run at full steam. But should a network error occur, devices may become inaccessible or stop communicating. In a worst case scenario, production may halt altogether.

At its Antwerp site, BASF had 350 devices controlled by Simatic PLCs from Siemens. This included PLCs running compressors, energy meters, charging stations, and other mission critical devices. So keeping all PLCs updated with the latest security updates was vital to protect them from malware, unauthorized access, and other threats. But the PLCs had yet to be connected on a single network. This meant Siemens' on-site automation team had to update every device on foot. With the site spanning 6 km² and updates taking several hours, this was a process that could take a full year to complete.

BASF knew it needed an automation network. But installing one hadn't been feasible for two key reasons. Firstly, the site housed 16 plant clusters with their own firewalls and third-party devices. Secondly, the site's vast size meant installing a new fiber optic network was not financially viable. BASF approached Siemens for new ideas.

SOURCE: BASF

At BASF's Antwerp site, PLCs spread across 6 km² had to be updated manually.

SOURCE: SIEMENS

Sinema Remote Connect and Rack PCs enable a secure and centrally managed VPN connection.

Experts in complexity

With its track record of successfully implementing networks in complex industrial environments all over the world, BASF was confident Siemens could devise an effective solution. And upon receiving BASF's request, Siemens jumped into action, bringing in network specialists to assist its on-site automation team.

This BASF Antwerp team said, "We are familiar with networks, Siemens and PCS 7, but our team was short on technical know-how for developing a concept that could meet the stringent requirements imposed by the IT department. So, we joined forces with product and service specialists from Siemens to create the concept."

In addition to improving security and reliability, BASF wanted a network that would be easy to manage and master. It also wanted to be able to create user groups so every plant cluster could manage their own devices. After assessing all the requirements, the team planned the rollout of a secure, dedicated network with Sinema Remote Connect at its core.

Secure access for remote networks

The first challenge was devising a network that could securely connect technicians and devices across 16 plant clusters. A challenge Sinema Remote Connect easily solved.

Using Sinema Remote Connect, the solution created VPN tunnels connecting every PLC and user through Sinema Remote Connect server. An inventory of the security certificates for every device and user was also created in the server. This meant that whenever a connection was requested the certificates would be checked and verified before the connection was approved.

Sinema Remote Connect further improved

security by encrypting all communications using OpenVPN.

Another advantage of Sinema Remote Connect is that it would provide remote access to Scalance M-800 as well as Scalance S-600 Industrial Security Appliances and dedicated CPs and RTUs. This would allow each device to be configured and integrated automatically, eliminating an otherwise complex and time-consuming task.

Providing technicians with central access to the PLCs in all parts of the BASF plant was realized by Sinema RC Client. Once all groups and rights in the Sinema Remote Connect server were configured, Sinema RC Client's address book function would enable every technician to see the parts of the network they can access.

Transparent network monitoring

To fulfill BASF's requirements for central network monitoring, Sinema Server was implemented.

The engineering team created one user group for each plant cluster so they could access their own devices and monitor their performance in private. In addition, Sinema Server's network monitoring software would provide BASF with around the clock monitoring, and diagnostics, including diagnostics for SNMP, Profinet, and Simatic.

SOURCE: SIEMENS

The automation solution integrates 16 plant clusters with different network infrastructures. One user group for each plant cluster enables access to devices and monitoring performance in private.

SOURCE: SIEMENS

Sinema Remote Connect with Field PG connects every PLC and user.

Putting it to the test

Before rolling out the network, the team ran a proof of concept project in the lab. This project was to verify how devices would respond when added to the network and whether firewall rules needed to be modified.

“We wanted to ensure we developed a network that would meet the stringent requirements for security, seamless implementation, and ease of use,” said BASF Antwerp. “The proof of concept project translated into significant time savings, while for the businesses on site it meant better service.”

Along with saving time and lowering risk, the proof of concept project enabled development of workflows for installing and managing devices. Siemens trained BASF's technicians in these workflows in a workshop, so they could manage the network independently.

“Good preparation is the key to success," said Bert Vanstraelen, Service Engineer at Siemens Customer Services in Belgium. “Giving BASF’s technicians training in the new system will ensure they can perform their own maintenance in future without IT support.”

Rolling out

Following the successful test project, Siemens built out the network in stages. Close cooperation between BASF and Siemens’ team ensured the network’s central elements were completed within one month. The PLCs were then linked to the system step-by-step, allowing the network to grow organically.

With the successful implementation of Sinema Remote Connect, BASF now has the reassurance knowing all PLCs across 16 plant clusters can be monitored and updated around the clock by their central maintenance team using the TIA Portal – the engineering platform for automation from Siemens.

At a ground level, desktop access through Sinema Remote Connect means Siemens’ automation team no longer has to travel around the different plants. This has freed Siemens’ technicians to focus on providing high quality services across BASF’s site.

Future upgrades planned

There are now plans to further improve the network monitoring with Siemens’ Network Management System Sinec NMS. Sinec NMS will further enhance transparency and ease of use by providing BASF’s technicians with desktop access to devices for prompt fault resolution, security monitoring, and device configuration with hardening.

SOURCE: SIEMENS

Scalance S615 Industrial Security Appliances made controllers accessible from central Sinema Remote Connect server.

The project’s success also reinforced to BASF the value of both technology and expertise at overcoming complex challenges. In fact, the project has been such a success. BASF is now planning to upgrade its logistics systems. The new system will be completely integrated to the Sinema Remote Connect architecture, and the team will be there to support them every step of the way.

Summary

BASF’s Antwerp site had PLCs spread across 6 km² that had to be updated manually. The PLCs belonged to 16 plant clusters with different network infrastructure. Sinema Server enabled the creation of user groups for each plant cluster and provided desktop access to devices and diagnostics.

Scalance S615 Industrial Security Appliances made both Siemens and third-party controllers accessible from central Sinema Remote Connect server. Sinema Remote Connect enabled the creation of secure and centrally managed VPN tunnels. A proof of concept project was completed before rolling out the entire system. A task that once took a year can now be completed automatically.

BASF now has a secure, strong central update management for the plant network and can provide a higher quality service across the Antwerp site.

Maximilian Korff, Digital Industries, Process Automation, ***Siemens.***

Industrie 4.0: smart electronics production via PC-based control

Advancing the smart factory with PC-based control technology, electronics companies are developing platforms with unified interfaces as part of a flexible manufacturing strategy. Intelligent networks combine multiple users and machines with a range of advanced services.

SOURCE: CYGIA

CYGIA's smart factory solution for electronics manufacturing utilizes IoT and monitoring technology to facilitate information management, to track the production process, reduce manual intervention on production lines, and to streamline production planning.

TWO COMPANIES IN CHINA, CYG INTELLIGENT Automation Co., Ltd. (CYGIA) and CYGDM, have used PC-based control technology to develop a smart factory platform with unified interfaces and protocols as part of a new and flexible manufacturing strategy for electronics products.

The platform combines sensors, actuators, operator terminals, control systems and communications equipment in an intelligent network that connects multiple users, including humans with machines, and machines with services.

From an Industrie 4.0 perspective, the platform maximizes integration, both at the device level and at the vertical and horizontal production levels.

Formed in 2006, CYGIA is one of China's foremost high-tech companies. Its business is customer-specific automation and test solutions for industries such as consumer electronics, semiconductors, automotive, energy, medical engineering and lighting technology, among others.

CYGDM, founded in 2015, is a software and hardware services vendor specialized in developing and implementing smart factory solutions. Examples of projects include the ALC line control system, the iSPC smart data analytics system, and smart warehouse management and logistics systems.

Open control for smart factory

CYGIA's smart factory solution utilizes IoT and monitoring technology to facilitate information management, to track the production process better, to reduce manual intervention on production lines, and to streamline production planning. Other technologies deployed as part of the solution include simulation, multimedia, and augmented reality.

CYGIA and CYGDM chose powerful CX2030 and CX9020 Embedded PCs from Beckhoff to deliver the requisite computing power.

The CX2030 handles higher-level hub control in the smart factory, while the CX9020 is used as control platform for distributed sub-stations. The open architecture of PC-based control, combined with ultra-fast EtherCAT communication technology, meets all their requirements when it comes to keeping response times as short as possible, while at the same time supporting time-division multiplexing and multitasking, programming in high-level languages, and extensive data storage capacity.

On the software side, the integration of the Beckhoff TwinCAT 3 automation software into Visual Studio is a key benefit for CYGIA's experts. In their view, the standardized bottom-layer control platform, created in TwinCAT 3's object-oriented development environment, combined with the upper-layer control platform developed in .NET, has made it easier to integrate a wide variety of devices and to shorten the time required to develop their smart factory solution.

Plus, being able to develop the software on a modular and distributed basis, they say, results in greater software efficiency while minimizing development and maintenance costs.

In the higher-level control system, they use both ADS.Net components and the Dynamic Link Library (DLL) to implement asynchronous communication between the server and multiple clients.

The entire communication architecture, they claim, not only saves time, it is efficient and compatible, too. In addition, the TwinCAT Automation Interface enables developers to program device interaction using COM technology.

With TwinCAT, CYGIA's engineers can use a unified, object-oriented, modular program framework, Structured Text, object-oriented

SOURCE: CYGIA

Information displayed on the central control platform's HMI.

programming and customer-specific libraries, all of which help streamline the development of this complex system. Joshua Wang, R&D Director at CYGIA, explained: "We've succeeded in improving programming efficiency through modularization and standardization. We only need to modify a few methods when developing new production technologies. The program may be large and complex, but we can reuse the code efficiently, nonetheless. The program has a clear structure, is easy to read, and is highly portable."

It makes the most of TwinCAT 3's built-in capabilities for system configuration, PLC code development, motion control configuration, bus and module configuration, and HMI development, as well as its oscilloscope functionality. And the program structure, process control, data structure, alarm release and security control have all been standardized as well.

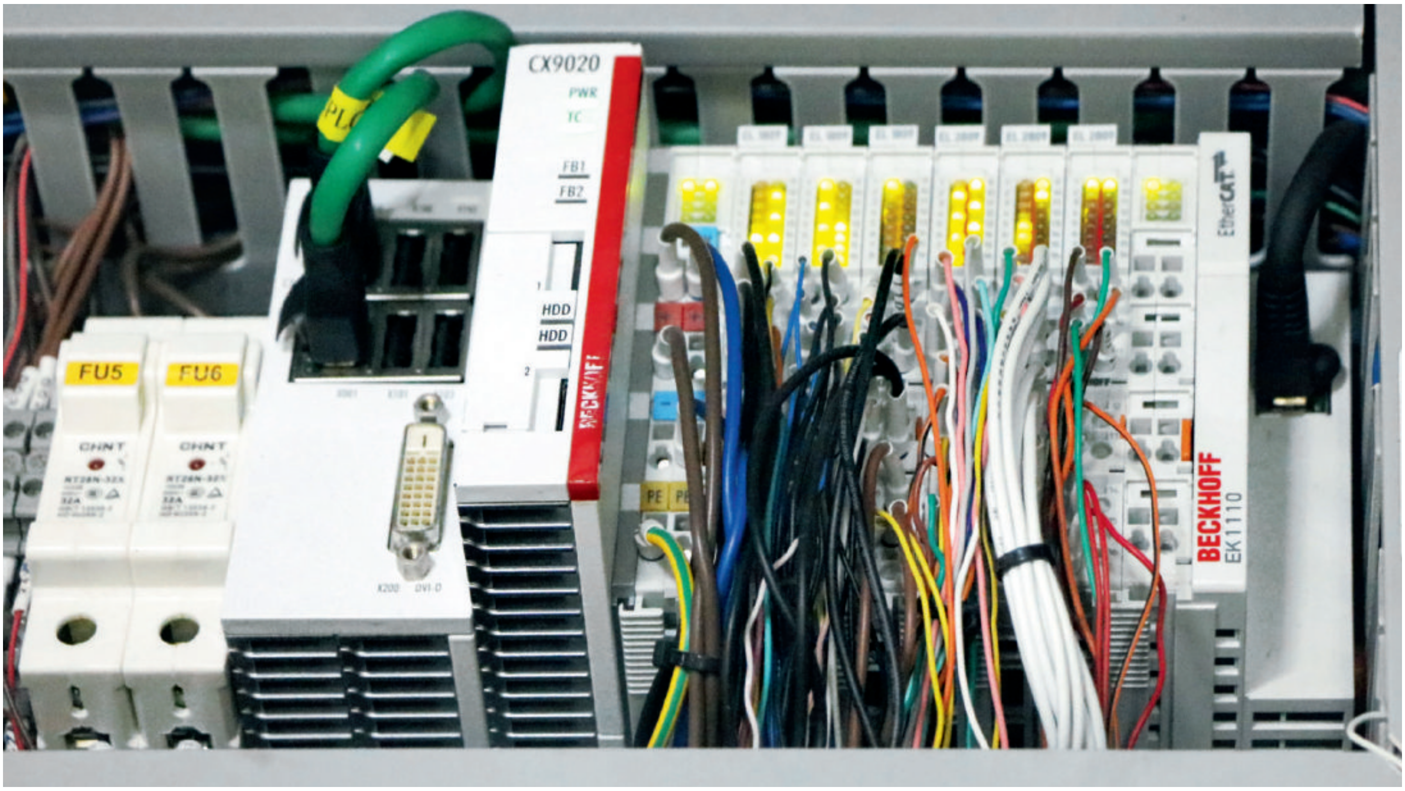
Smart mobile phone production

The software and hardware fulfilled CYGIA's requirements for smart solutions in electronics manufacturing.

Compared to a conventional setup with separate production stations, CYGIA's system can achieve greater manufacturing and supply-chain flexibility and improve capacity utilization. For instance, it enables the ERP, MES and monitoring systems involved in the manufacture of mobile-phone circuit boards to exchange data, resulting in comprehensive process automation that spans everything from order booking and handling, material distribution, product manufacture and inspection to packaging, warehousing, logistics and transportation.

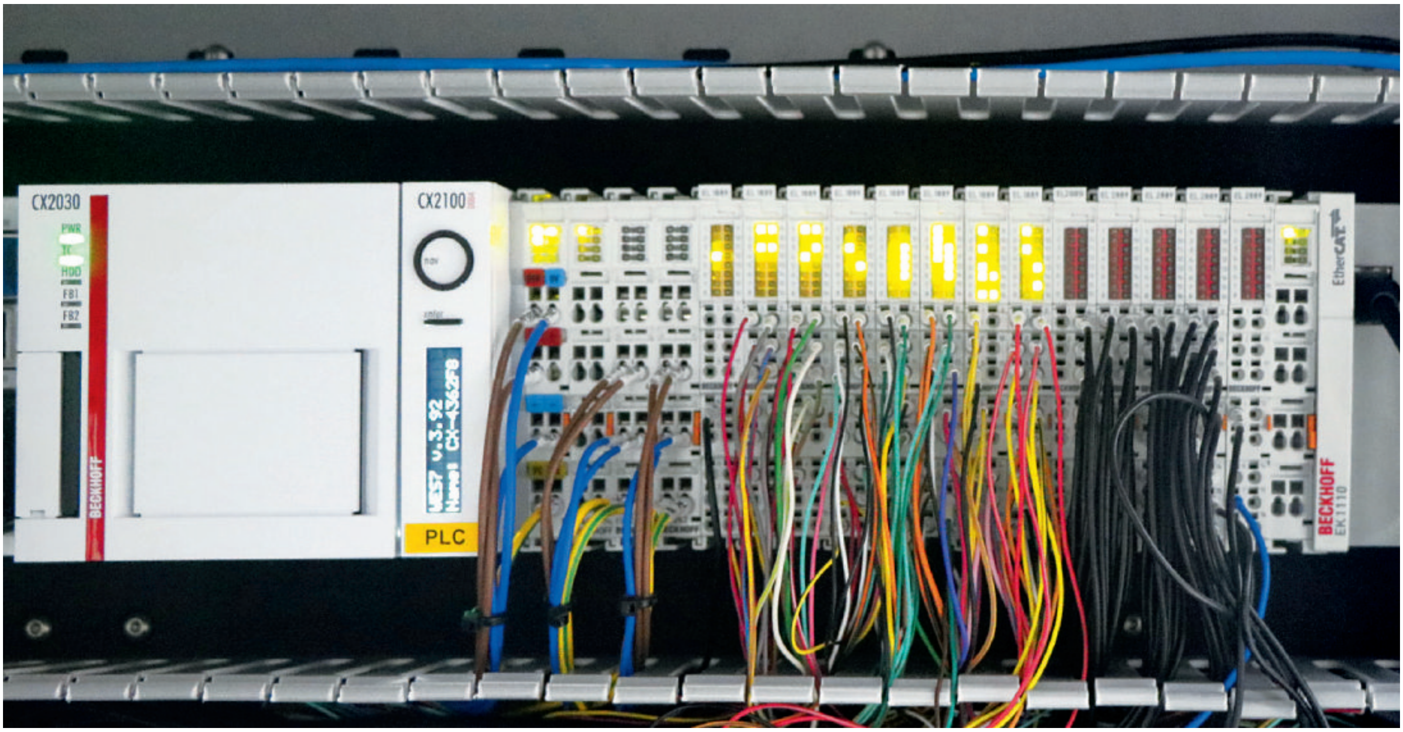
The smart factory's system architecture combines order, asset and quality management functions with a management dashboard, inventory control and product traceability.

The intelligent warehouse assigns codes to all goods and creates unified racks and pallets



SOURCE: CYGIA

The CX9020 Embedded PC that controls the smart warehouse.



SOURCE: CYGIA

The CX2030 Embedded PC (left) that serves as the main controller for the automated production line.

that are carried by forklifts or shuttles into the intended positions. Each storage location is controlled by the warehouse management software. Product locations, inventory levels, open storage locations and storage strategies are all administered through a parameter management system.

The CX9020 Embedded PC is the core element in inventory control, running the PLC program, connecting to the local MES over TCP/IP, and operating as an NC controller for material requirements planning. It also connects with the extended part of the feed and removal mechanism, in a chain topology, via an EK1110 EtherCAT extension.

The main elements in the automated production line include hollow-board printing, surface mounting, reflow welding, dispensing, screw locking, automated optical inspection, integrated and functional circuit testing, and packing and unpacking.

The line has three CX2030 Embedded PCs in total, which communicate at extremely high speed with the higher-level central control system and are essential to ensuring efficient production and precise fabrication of semiconductor components.

The master CX2030 runs both the PLC program and the motion control and HMI software. It also sends data bidirectionally at high speed between the control system and the MES over TwinCAT TCP/IP (TF6310), and controls the printing, surface mounting and reflow welding processes.

Here, TwinCAT PLC/NC PTP 10/NC I (TC1260) provides full motion control functionality that can dynamically position 20 EtherCAT servo axes per machine. The NC I interpolation function serves to achieve smooth, steady, coupled movements on two axes and to control the arc-welding process.

The second CX2030 Embedded PC runs PLCs, motion control and HMI software, handles communication over TCP/IP, and exchanges data with the ALC line control system. It also receives instructions from the MES over TCP/IP to run tests and execute packing and unpacking processes.

It can also flexibly configure ten EtherCAT servo axes through a synchronization device that can switch quickly and efficiently between specific test environments for different products. The third CX2030 handles PLCs, motion control and HMI software, and in addition controls a high-resolution TCP/IP camera for optical inspection.

EtherCAT networking performance

CYGIA chose EtherCAT as a high-speed communication system to ensure fast, precise transmission of sensor signals. The company runs master communication on its automated production line over EtherCAT in a star topology.

Slave devices are easy to connect, which simplifies management, maintenance and expansion. A line topology is used at sub-station level to keep the wiring as simple as possible.

According to Jianming Huang, a senior electrical engineer at CYGIA: “The EL1809 and EL2809 HD EtherCAT terminals are not just highly compact and inexpensive, they operate on multiple channels and can be configured flexibly for different topologies. They also support offline configuration and Hot Connect groups, which makes them much easier to set up. In addition, EtherCAT provides a wide range of useful information, such as diagnostic codes, diagnostic types, text IDs and time stamps. This helps to locate and fix master-slave communication outages potentially caused by EMC disturbance, cable damage or equipment faults. This makes maintenance much more efficient.”

Future development potential

CYGIA’s aim with its smart factory solution is to integrate assembly and manufacturing units for discrete electronic components within a unified production system. Other goals are to connect production plants, to visualize production data, to make production processes transparent, and to create fully automated production sites.

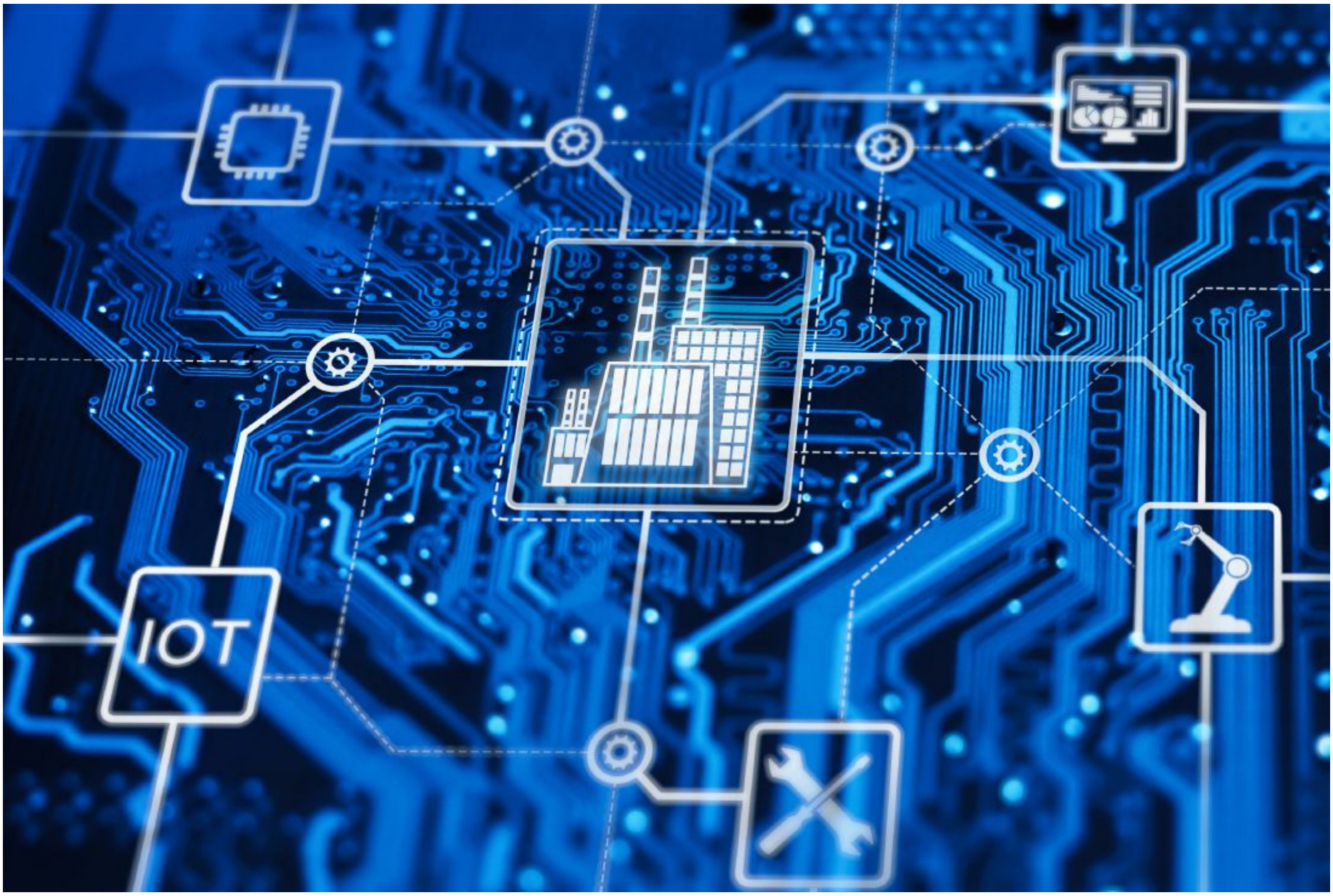
Given the broader trend toward Industrie 4.0, CYGIA also needed smart factory software that would enable access to a wide range of data resources, including cloud computing, big data, and IoT.

With TwinCAT 3, Joshua Wang has found the right solution and is now looking forward to the new production model the company has lined up: “We’ll gradually incorporate TwinCAT 3 functionality to support big data analysis, IoT advancements, and machine vision in future upgrades. Going forward, this will further enhance the setup of this hybrid control system to fully exploit the benefits of cloud data storage and distributed data interaction.”

Kevin Gao, Technical support engineer, ***Beckhoff China.***

TSN in manufacturing recovery and future-proofing of factories

TSN technology is already able to address the demands of Industry 4.0 that are emerging now by maximising the use of the increasingly common gigabit bandwidth. In addition, it holds the promise of being able to evolve accordingly to meet future demands while protecting existing investments.



SOURCE: B4LLS/ISTOCK

By removing the need for physical separation of critical and non-critical networks, TSN is helping to create a convergence between IT and OT systems in factories.

AS SOME GLOBAL MANUFACTURING SECTORS FACE UNPRECEDENTED pressure, there has never been a more opportune time to implement game-changing automation technologies. Those businesses that have been adopting technologies able to provide greater transparency, higher productivity and better process management will be better placed to move forward and adapt to the new manufacturing landscape.

This article looks at how manufacturing companies can invest in key solutions that support current needs while also future-proofing their activities.Current production challenges mean that there is not just demand for factory automation solutions that can ensure continued manufacture and supply of goods, but that provide the transparency and productivity benefits promised by Industry 4.0 too.

Bearing in mind that the lifecycle times for automation hardware are as long as 20 years, there are many plants operating with aged production systems that could benefit from an update. This is where industry-leading open communication technologies can step in to deliver these necessary improvements in process transparency and productivity.

The case for TSN

As automation plant lifecycles typically last many years, it is essential to know what technologies show the most promise of longevity, rapid return on investment (ROI) and clear technical benefits. It is clear to most automation specialists that one of these will be Time-Sensitive Networking (TSN).

This is a set of Ethernet sub-standards for the OSI-Layer 2 defined by IEEE 802.1. These aim to improve determinism and reliability in industrial Ethernet-based communications by creating accurate time synchronisation across a network, in addition to technology for traffic prioritisation.

Therefore, businesses can combine multiple types of traffic on a single network, with no loss of performance for critical control-related tasks. The end result is an industrial Ethernet infrastructure that permits all kinds of traffic to coexist, regardless of whether it is critical safety or motion control-related data, general control information, video frames from inspection systems, periodic shift logs or even emails.

This consequently delivers several technical benefits. Networks are able to fully leverage the benefits of gigabit bandwidth, their infrastructure is simpler and therefore less costly to design, implement and maintain. Ultimately, systems can be rolled out and start their operations in a shorter time.

By removing the need for physical separation of critical and non-critical networks, TSN also creates a convergence between information technology (IT) and industrial operational technology (OT).

This convergence directly addresses the competitive pressure of Industry 4.0 in order to deliver corresponding business benefits. Key results include better transparency and management of processes, product quality improvements, increase in output as well as reduced downtime. In addition, the enterprise can become more responsive to customer demands and better able to support its business.

An evolving solution

While many of the IEEE 802.1 standards are now complete, some are still under development. Moreover, the IEC/IEEE 60802 working group is still standardising TSN profiles for industrial automation. Hence, TSN is still evolving. The counterpoint to this is that projects have to be done now, and TSN's maturity level is such that vendors have already started to market solutions. As with most technologies, TSN will continue to evolve over time.

However, any risk of moving forward now is mitigated by the fact that the organisations involved have a strong track record of ensuring backwards compatibility. So while TSN will continue to evolve, future iterations will be compatible with what is available today. TSN, as it stands today, can deliver all the benefits outlined earlier, and hence this creates a compelling case for using it to maintain a competitive advantage now.

Specific examples of applications that can benefit from TSN include those that would profit from combining several types of control on one network. For example, a converting application such as a printing press could combine high precision motion control for registration with visual inspection of the process, along with systems related to operator safety. TSN allows them all to coexist on a single network, simplifying system design, reducing cost and increasing uptime.

Time to implement TSN

Plant lifecycles are typically measured in decades. With this in mind, current TSN solutions are a safe bet. The technology is already able to address the demands of Industry 4.0 that are emerging now by maximising the use of the increasingly common gigabit bandwidth. In addition, it holds the promise of being able to evolve accordingly to meet future demands while protecting existing investments.

Its base technology, Ethernet, was first conceived in the early 1970s and has already proved its ability to remain relevant over time. Hence, TSN will likely continue to benefit from this ability and offer advantages during the current plant lifecycles and beyond.

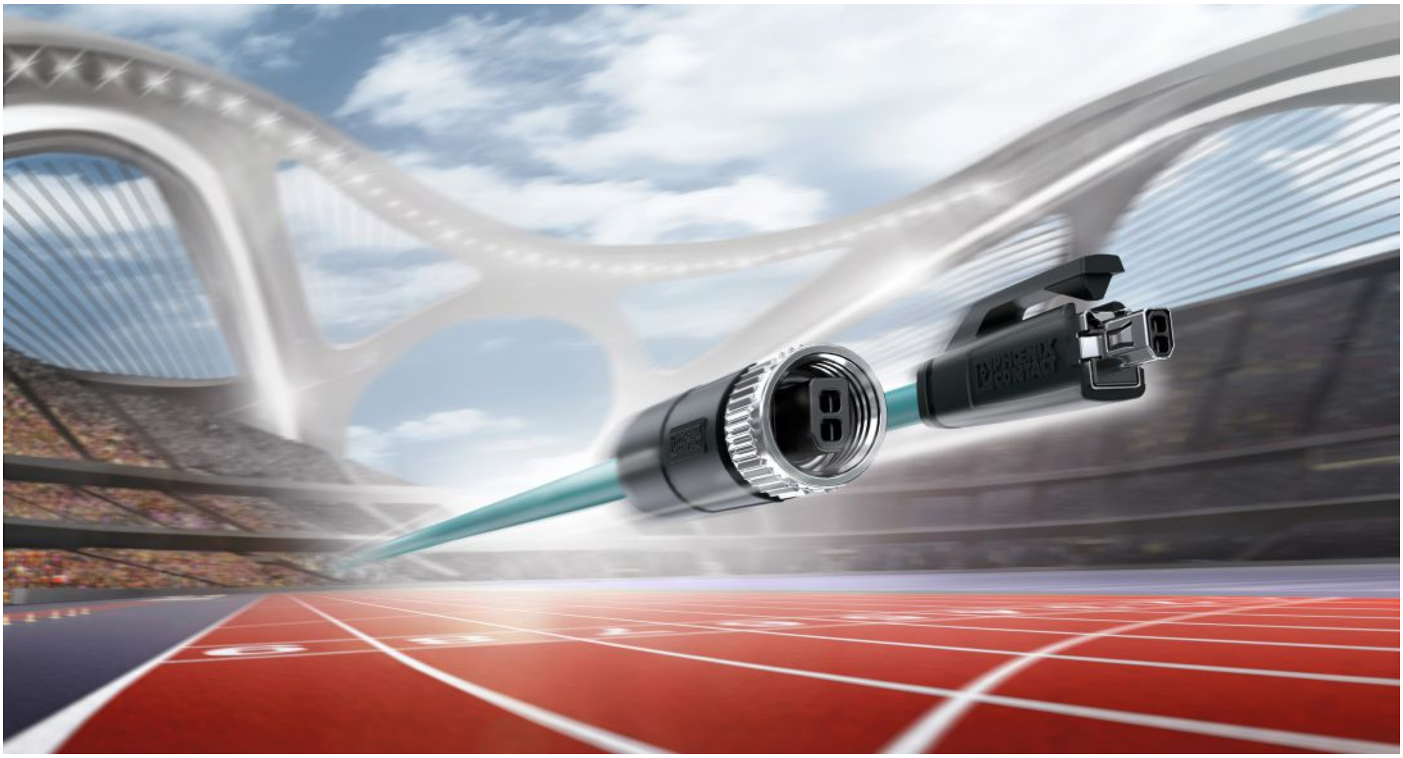
TSN can act as a powerful ally to support businesses to address current manufacturing challenges. The technologies that offer TSN functionalities now are also providing migration capabilities for the future.

To support advanced industrial communications, the CLPA organisation has recently developed CC-Link IE TSN technology, the first open industrial Ethernet to combine 1Gbit bandwidth with TSN functionalities. Thanks to these key features, it offers an effective migration solution that can address current manufacturing needs while acting as a gateway to the future of connected industries. By implementing this technology businesses are enabled to handle the large volume of traffic associated with Industry 4.0 data-driven manufacturing. As a result, they will not only optimise their current operations, but also future-proof them.

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

SPE in industrial applications offers IP-protected solutions

Single Pair Ethernet work continues with the aim of toughening up this evolutionary new technology for as many application scenarios as possible. But reduced cable weight, miniaturization and simplification of the connection technology will only come into play with achieving continuity with the overall infrastructure.



SOURCE: PHOENIX CONTACT

SPE is racing to become the Ethernet communication method of the future. Modularity combined with full connection compatibility represents technological progress.

THERE CAN BE NO DOUBT THAT SINGLE PAIR Ethernet (SPE) is the future of industrial communication. In addition to the safety that a standardized solution offers users, application-specific customer requirements play a significant role.

The prevailing trends and innovations in the age of the IIoT (Industrial Internet of Things) all strive to bring product functions and solution requirements more in line with each other against the backdrop of digital transformations. When examining SPE more closely from this perspective, the following key features are readily mentioned: range of up to 1000 m, high data transmission rates over twisted pair, miniaturization at the device and in the field along with, last but not least, significant cost savings.

All of these aspects present many advantages, providing further support for the extensive and future-proof use of SPE. And behind all these advantages, there are countless customer and application requirements. The true skill of a component provider now lies in their ability to reconcile all of these aspects. If they do not succeed, because specific customer requirements cannot be met, a connector standard gradually develops over time, which the world does not actually want or need. This is why numerous large and small companies are working on the expedient implementation of this technology.

The basic framework for the future of industrial communication technology is emerging in parallel in various committees and projects. 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. The new standards will far outperform existing protocols and interfaces in terms of cost, data throughput, latency, and deterministic aspects. As a technology leader with more than 30 years of experience in industrial communication, Phoenix Contact is therefore actively involved in all of the relevant standardization committees. The goal: nothing less than a new, cross-manufacturer communication standard for industrial automation.

OPC UA is already used as the higher-level communication standard in systems. OPC UA is now being gradually extended with standardized application profiles in the field for I/O, safety or drive applications, for example. Furthermore, standardized device models are being defined for the uniform configuration and diagnostics of devices in the network.

It starts at the sensor...

The overarching goal of consistent Ethernet communication will always be the IP-based integration of all components into a communication system. Many of the sensors that are currently used are not IP-capable. They have to be integrated into the communication system using other systems such as IO-Link. With regard to Industry 4.0 and predictive maintenance, a consistent Ethernet communication system offers significant advantages over existing stand-alone solutions.

M8 and M12 connectors are a widely used connection technology in industrial automation. The Ethernet system codings that are used for circular connectors are proof of this with D- and X-codings used for M12 and D-coding used for M8. In this context, the focus is on easy integration into standard sensor housings together with maximum possible robustness. Due to the significantly cheaper integration of pin contacts and an external thread on the sensor side, it makes sense to equip the SPE field side with socket contacts. Retaining this connection provides sensor manufacturers with an option for easy integration into the sensor.

SOURCE: PHOENIX CONTACT

The little brother of M12: with full IP20 compatibility, M8 connectors are also suitable for fast servicing.

Male and female connectors

Retaining the sensor connection does not just provide advantages for the relevant manufacturer, there are also clear advantages when it comes to cabling in the field. In the context of modern M8 and M12 installations, there is a lot of talk about flying leads or even field coupling. This is why modern sensor/actuator cabling is chiefly designed as a male/female connector version. One end is fitted with pin contacts and the other end with socket contacts. This also means that one end must be equipped with an external thread and the other end with an internal thread. Cables can then be extended without having to use a female/female or male/male adapter, as is typically the case with RJ45. This type of cabling topology provides a high degree of flexibility for users in the field as well as SPE integrators. Full compatibility with SPE connectors with IP20 degree of protection also ensures fast servicing.

Miniaturization – not at any cost

The M8 version of the popular M12 connector has become established as the standard for compact connections: One third smaller than the M12, the M8 is still suitable for industrial use and is easy to handle. The M8 is already widely accepted and is being used successfully in many fields – especially for the connection of compact sensors in machines to obtain process-related information or to supply power to small devices. Although miniaturization is also one of the megatrends in industrial cabling, it must be determined exactly how and where this can be implemented effectively.

SOURCE: PHOENIX CONTACT

For external thread and male contact on the sensor side: female contacts in the field cabling simplify integration into the sensor infrastructure.

While most of the cables used in industrial automation are between AWG (American Wire Gauge) 22 and 26, things are quite different in process automation. Due to the longer distances that have to be covered here, much thicker cables are used that range from AWG 16 to 18. A cable in a process application can therefore quickly reach an outside diameter of 7.5 to 8.5 mm. In this case, the cable easily matches the outside diameter of the connector. There are many reasons why it would not make sense to connect a miniaturized connector to such a cable.

This not only applies to protected connectors, but also connectors in IP20 applications. Considering the aforementioned conditions, it likewise does not make sense to implement the smallest possible footprint on the printed circuit board or significantly increase the port density compared to RJ45. This is why the product launch is initially focusing on pre-assembled cables in the AWG 22 range.

IP20 versions as well as IP65/IP67 versions are available for device integration. The continuous development of the product range ensures consistent use in all fields of application. The aim of the Single Pair Ethernet System Alliance is to combine continuity with practical implementation.

Size M8 – in the shadow of M12?

When it comes to connectors for sensor/actuator cabling or data transmission, talk usually turns to popular M12 connectors. As the technological shift to SPE continues, along with the demand for miniaturization, the M8 size will achieve further significant growth rates in the market. This growth will be further boosted by male/female connector versions for the field and device side. The advantages of M8 with regard to SPE:

- Cabling structure remains unchanged
- Full connection compatibility with the IP20 pin connector pattern for fast servicing
- Wide range of applications due to the modular layout of the pin connector pattern in various housing forms

Summary

Work continues steadfastly on SPE with the aim of toughening up this evolutionary new technology for as many application scenarios as possible. The advantages namely the reduced cable weight, miniaturization, and simplification of the connection technology only come into play with the continuity of the overall infrastructure. This innovation will influence the network structure in all fields of application from building automation through factory automation to process automation. In this context, no one should lose sight of the fact that decisions made today will determine where Ethernet will go in the future.

Manuel Rüter, Product Manager for Industrial Field Connectivity, ***Phoenix Contact.***

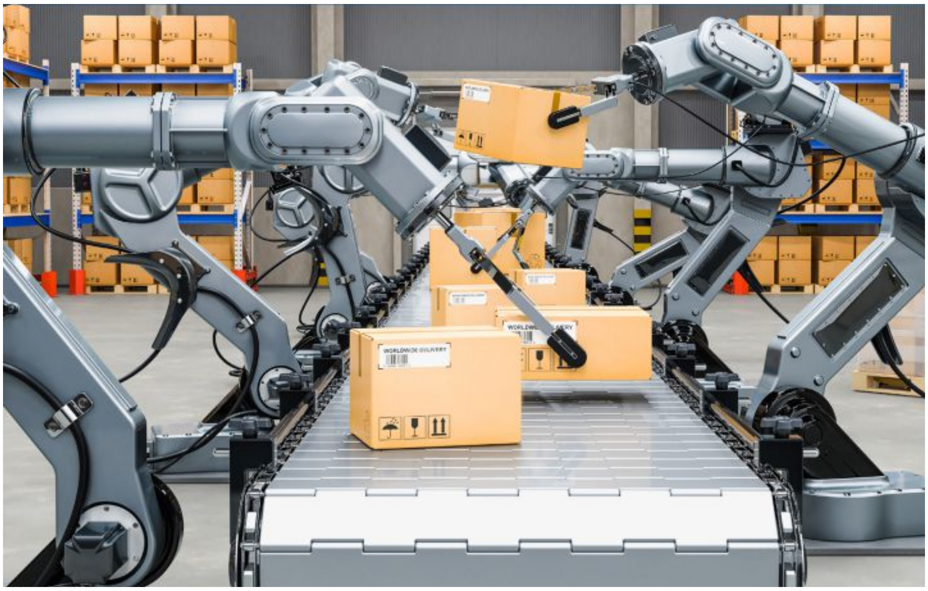
Ethernet trends in the Industrial IoT environment

Learn how machine builders and machine users are improving productivity and more. The emergence and continually increasing utility of Ethernet connectivity is opening up new opportunities for creating more productive and more reliable workflows in industrial environments of all kinds.

SLOWLY BUT SURELY, ETHERNET HAS BECOME the communications protocol of choice for machine, robot and other factory automation applications in the industrial/ operational technology (OT) environment. Use of Ethernet is escalating as users identify and implement new ways to capitalize upon the protocol's advantages over traditional fieldbuses.

This article will discuss several ways in which industrial operators of all kinds are making use of Ethernet technology to increase productivity, improve process reliability and secure other valuable gains on the plant floor. It will also consider these trends from the perspective of the robot and machine builders. OEMs benefit directly from some of these trends as industrial manufacturers themselves.

In addition, they also have the opportunity to differentiate their products and services and gain competitive edge by being well-versed on these trends from their customers' perspectives, and by working to ensure that their offerings help customers most readily capitalize on them.


SOURCE: BELDEN

Use of Ethernet technology continues to change how machine builders and machine users gather data.

Shifting from serial technology

Industrial Ethernet has been in effective use in plant environments for more than two decades—in fact, Belden introduced its first industrial Ethernet switch in the mid 1990's. Over much of that time, traditional fieldbuses such as DeviceNet, PROFIBUS and Modbus were the more commonly used protocols in industrial/operational technology (OT) environments, providing reliable and secure service for most users.

Capitalizing on Ethernet-enabled capabilities and more, OT environments of all kinds are integrating machines, robots and other key pieces of automation equipment in new ways, identifying and benefiting from new processes that can lead to even greater productivity and yields, more reliable uptime performance, higher product quality and greater overall profitability.

A specific subset of OT operators, the OEMs who manufacture the original machines and robots, might additionally benefit from some of these insights. Many whether they manufacture several small presses a day on an assembly line or require months to construct a single highly sophisticated machine on a dedicated build floor can benefit from these trends in their own OT environment; they can also benefit from understanding how they might impact the needs of their customers.

When applied properly, Ethernet ports, sensors, devices and other supporting components can help OEMs satisfy identified end-user goals and differentiate themselves in the marketplace.

M2M communication

Ethernet's ability to communicate instructions at high speeds, accurately to within milliseconds, repeatedly and consistently, opens the door to taking significant human intervention out of the manufacturing equation. It decreases the need for central control as well. Indeed, more and more devices are being developed that control their own logic and behavior and pass instructions directly to the next machine in the line.

For example, an uplink might be created between a robot that precisely places and holds a connector and its partner machine that inserts that connector into a panel. Similar, direct connections can be established between a machine that places an object and the picker that will move it to the next step in the process. Or, a vision system with integrated circuitry and Ethernet ports that performs its own QA can be used to allow passed items to proceed quickly and decisively down the line.

This distributed remote operation can add speed and certainty to the process as well as maintain uptime in aspects of the operation in the event of a central controller issue. Self-contained, stand-alone manufacturing "sub processes" can be strategically developed.

Operators in manufacturing environments in the process of planning a new workflow should consider investigating which small machines might currently be available with onboard controllers installed— there may likely be new products on the market since their last purchase.

And they should discuss the possibilities with their OEMs to see if/how such devices can be incorporated in a line using the appropriate switches and Ethernet infrastructure. OEMs can also consider the reduction in complexity in PLCs and other devices that can be driven by significant distributed control, and the impact that it can have on machine design simplification and cost.

Increasing data capture

The speed and bandwidth of Ethernet is enabling the collection of large volumes of real-time data in ways never before possible. The myriad benefits that this information can enable are still being identified. For example, organizations are using real-time data to perform predictive maintenance by placing a sensor near a wear item and trending changes in temperature or velocity to get the maximum amount of useful life out of a component.

Some are collecting reams of production data secured from smart devices and feeding it through sophisticated analytics packages, allowing them to identify tweaks to a recipe that can optimize yields or lower operating costs substantially in the aggregate. Others are collecting and archiving quality data that can assist with regulatory compliance or liability protection efforts.

Some organizations are well along the way in capturing these benefits; others have barely scratched the surface. Many organizations have likely not gone nearly as far as they can in utilizing the data that lies unrecovered and unexamined in their processes, and there are likely many opportunities for operations of all kinds to reduce their downtime and optimize their productivity by strategically capturing operating data.

End users should analyze their workflow for opportunities as new techniques, software packages and other tools are made available. In addition, they should include machine and robot builders in the discussion about planned communication infrastructure, sensors and other components in their equipment that can help enable valuable new data capture processes. OEMs should be ready to participate in and lead such discussions for optimum win-win partnerships.

OEM-End user partnerships

The emergence of Industrial Ethernet opens opportunities for machine builders and machine users to work more closely in the design and planning stages of an industrial network. Thus, this technology enables a win-win environment for long-term partnership and success. That is, opportunities are emerging that keep them profitably connected and in daily communication even years or decades after the initial sale—quite a different scenario than the way the relationship might have been structured in the past.

Ethernet makes this possible by enabling fast access to detailed real- time status and diagnostic information remotely from anywhere in the world. Theoretically, end users can get instant access to the best machine diagnosticians on the planet—the team that actually built the machine— without the downtime and expense of waiting for an emergency in-person call.

Redundancy mechanisms

In the early days of Ethernet OT networks, redundancy technologies fast enough to ensure that data would not be lost in the case of a connectivity failure in the factory were hard to come by.

Many OT environments went without this vital protection completely or installed what was readily available. One such example was spanning tree, a network protocol developed for and successful in the significantly less demanding office IT environment but not fully effective in meeting the needs of the factory environment. Over the years, faster versions based on the spanning tree framework, including rapid spanning tree, were developed and standardized, but still often left users with lost data in the event of failure.

SOURCE: BELDEN

The key to a successful Ethernet installation is building in redundancy that seamlessly shifts transmissions to keep operations running safely.

Meanwhile, however, several more robust and sophisticated redundancy technologies—offering recovery in intervals of 10 milliseconds or less and adequate even for mission-critical applications— have been developed. Some are even standards-based.

However, based on our experience in thousands of industrial environments, many operations that could benefit from these faster mechanisms have not as yet adopted them, risking the ability for full recovery in the event of a failure. Those operations that have not recently analyzed their needs in terms of the marketplace should consider investigating protocols such as Device Level Ring (DLR), Media Redundant Protocol (MRP), Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). The latter two promise zero packet loss redundancy, wherein no data can be lost because packets are actually duplicated as back up.

A key to adapting these types of protocols is the use of managed switches as opposed to traditional unmanaged switches. End users should inquire in the interview planning process as to the machine builder's capabilities around installing managed switches and other hardware that can provide "built-in" robust redundancy.

Savvy machine builders will proactively ask the redundancy question, offering their expertise and explaining the possibilities to less sophisticated end users—helping deliver maximum uptime for a truly value-added partnership.

Time-Sensitive Networking (TSN)

One of the key benefits of Ethernet over serial networks is the protocol's ability to control high speed manufacturing processes, such as the desired hand-off actions between machines in an assembly line, down to milliseconds, on a constant and repeatable basis.

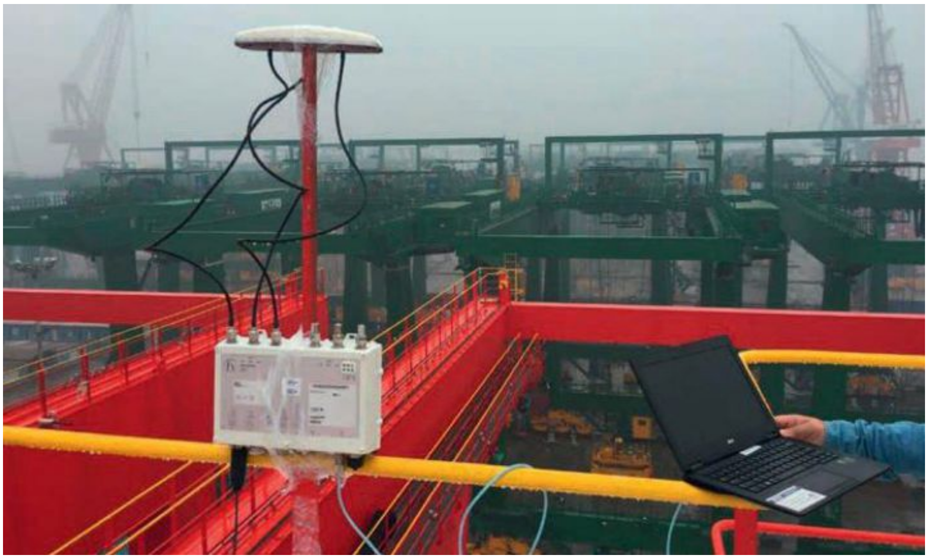
Currently, an "upgrade" to Ethernet, called Time-Sensitive Networking, is emerging that promises to allow manufacturers to control processes significantly more accurately still—down to the microsecond and possibly even into nanoseconds.

As this technology continues to emerge, manufacturers of all kinds will have the opportunity to re-imagine their workflow and consider where opportunities for more precise and more controllable processes might be advantageous, perhaps allowing fine-tuning that boosts productivity and yields and improves safety even further in their facilities. And, ultimately, many savvy machine builders will offer "TSN-ready" capabilities built into their equipment as an option to end users looking to gain a competitive edge.

Cyber security, staffing and more

Unfortunately, these beneficial Ethernet trends can also bring with them a number of vexing challenges for end users and machine builders.

First and most serious among them relates to the fact that the same increased connectivity that drives many of Ethernet's productivity and reliability benefits also opens the OT network



SOURCE: BELDEN

In industrial environments, Ethernet components must be built to withstand harsh operating conditions.

up to outside influences, and therefore viruses, worms, ransomware, malicious targeted hacks and other dangers that can bring the line to a screeching and costly halt.

Some operators think of cyber incidents as an issue only impacting IT networks archiving credit cards or other readily "monetized" data. However, in the OT world, intellectual property can be misappropriated, production can be sabotaged, safety can be compromised and more, both for gain and for sheer maliciousness, as many organizations have discovered the hard way. In addition, even accidental cyber events, inadvertently put in motion by a careless colleague, are taking their toll on operations of all kinds.

No matter how they are initiated, even a single event can cause significant negative impact on productivity, schedules, reputation, quality and more—often to the tunes of millions of dollars per incident. Of special note, while cyber attacks often originate through unprotected networks, OEMs and their customers should be aware that sometimes, networkable devices such as PLCs, HMIs, drives and I/O blocks can become "pre-loaded" with malware or spyware by hackers before they even reach the build floor, much less the end user location.

OT network professionals should be aware of the increasing threats, and be sure to work to build up their cyber security posture in lock step with building their connectivity and reaping the productivity and reliability benefits thereof.

Machine builders and end users can work together to make equipment as "cyber security ready" as possible, with the appropriate firewalls, switches or even more sophisticated devices pre-installed, as opportunities and machine purpose dictate. Care should also be taken to ensure that all devices installed contain the latest, fully patched versions of all software and firmware.

If the expertise to coordinate these processes is not available in house, the increasing demand for cyber security guidance is ensuring a healthy availability in the marketplace, with Belden subsidiary Tripwire perhaps among the most proven and experienced. Such experts can often help with optimal machine design as well as optimum network design. Fortunately, maintaining high levels of cyber security is not insurmountable— the expertise and technology is readily available. Often it is more lack of awareness, lack of action and lack of allocated resources that open organizations up to cyber security issues.

The increasing need for personnel well versed in both Ethernet networking and OT automation is leading to the creation of a new breed of professionals. While earlier on, many Control Engineers "borrowed" networking expertise on an ad hoc basis from their IT colleagues, the need to learn automation in depth often necessitates a desire for more permanent assistance. While that does mean greater head counts, perhaps, the benefits of in-house expertise in this fast-moving environment, with the stakes so high and the opportunities so vast ensures that most find it well worth the addition of key individuals or even departments.

Professionals for hire adept in both sides of the house, while still rare, are becoming less so as demand increases. What is emerging is an Automation and Data Exchange Engineer, or ADX Engineer, who understands the needs of both IT and OT. This new position facilitates and manages the requirements of IT and OT so that both of their needs are met.

Also extremely helpful is the emergence of value-adding partners such as network equipment suppliers who are offering automation engineers free or low cost vendor-agnostic training in networking topics with a focus on the unique characteristics and requirements of industrial networks, using familiar OT examples, as opposed to traditional IT examples. Much has been said about the differing mindsets of IT-trained and OT-trained professionals and how they each lack understanding of the other. However, in reality, our experience shows that a truly skilled person entering a new department will learn the needs of the new environment and adapt their skills accordingly.

Finally, industrial professionals should understand that, when specifying Ethernet equipment, whether for their own networks or to be incorporated into a larger machine, IT Ethernet equipment and OT Ethernet equipment are not always interchangeable if one wants to achieve optimum performance. That is, although they operate similarly in purpose, the environments in which they will be placed can differ substantially and such exposures should be taken into account.

In many cases, electronic devices and cables were designed years ago and their housings were made to be used in a fairly climate-controlled office-type environment, with little thought to the factory environments that may have growing need for them. For example, devices and cabling in an OT environment may be exposed to extremes of heat or cold, excessive vibration, dirt and dust, cutting and crushing, continuous motion, moisture or signal-degrading industrial noise— any of which can cause an interruption to network operation and unplanned downtime.

Fortunately, this type of equipment and cabling are readily available in more robust "industrial strength" versions, so be sure to seek these out—or offer to incorporate them into a larger machine—if the end user environment could benefit from more durable and resilient options.

Conclusion

The emergence and continually increasing utility of Ethernet connectivity is opening up new opportunities for creating more productive and more reliable workflows in industrial environments of all kinds. Knowledge of emerging and continuing trends can give savvy operators the opportunity to grab competitive advantage by developing creative ways to incorporate new technologies into work processes, increasing yields and reducing downtime.

Machine builders can not only take advantage of these trends for their own operations, but they can also use their knowledge of trends to more effectively interact with end user customers, develop even more useful products, and create even stronger long-term, mutually beneficial ongoing partnerships.

Aaron Hammer, Field Application Engineer, ***Belden.***

industrial ethernet book

Reader Service Card

IEB issue 120 - October 2020

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

Return by mail to:

IEB Media
Bahnhofstr. 12
86938 Schondorf
Germany

Or use our online reader service at:

www.iebmedia.com/service

Please enter your contact details below:

Name: ______________________________

Position: ______________________________

Company: ______________________________

Address: ______________________________

____

City: ______________________________

State: ______________________________

Zip Code: ______________________________

Country: ______________________________

Phone: ______________________________

Email: ______________________________

I want to:

□ **Start** a new subscription

□ **Update** my subscription

  □ **Digital** edition or □ **Print** edition

□ **Change** my address

□ **I do not want** to receive promotional emails from Industrial Ethernet Book

□ I want to be **removed** from the subscription list

Signature: ______________________________

Date: ______________________________

Company Activity (select one)

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

Job Activity (select one)

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

IEB Media reserves the right to refuse an application for a free copy of Industrial Ethernet Book or the provision of information on any of the advertisers or articles

Industrial network infrastructure helps optimize performance

Industrial network infrastructure is a valuable business asset. Investments in legacy networks require a clear migration path to optimize return on assets while not missing out on performance enhancements. A robust, well-executed physical layer is foundational to assuring this asset continues to deliver value.

NETWORK INFRASTRUCTURE IS A VITAL YET undervalued business asset. Lose the network and you lose phones, email, Internet, access to business systems or control/visibility of the manufacturing process. Many businesses strive to provide optimum versions of the devices connected to the network, such as computers, phones, machines, etc., yet attempt to economize on the network infrastructure that supports these devices.

This article discusses essential knowledge and tactics in current, near future, and distant future time domains that guide your network plans. It also suggests resources and strategies to assist you in the design, implement, operation, and maintain phases.

SOURCE: PANDUIT

A robust, well-executed physical layer is foundational to factory networks continuing to deliver value.

Current industrial networks

Today industrial networks are a composite of Ethernet protocols and what industry experts term “legacy protocols.” Legacy protocols are a telling term because like other legacies, we must live with them for a while. Legacy protocols age and become more difficult to support over time.

This issue is further exacerbated by the aging workforce megatrend. A large portion of the support staff for legacy protocols has reached retirement age. Forward-thinking organizations instituted plans to retain this outbound knowledge. Other companies meet the need by engaging professional services organizations backed by major automation manufacturers.

Industrial protocol distribution

Legacy industrial protocols (Fieldbus) account for almost half (48%) of the industrial network nodes sold. Ethernet variants account for 46% of nodes while wireless nodes have 6% share. The telling aspect of this story is that Ethernet and wireless are growing double digits while Fieldbus is growing at a shrinking single digital rate.

Network refresh rates

Industrial networks have added expectation versus their enterprise counterparts. Not only does the business require them to operate at peak levels, industrial networks have the longest refresh rate of any business network. Where data centers are refreshed every three to five years, industrial networks are refreshed every 12 to 15 years. Further, the supporting physical infrastructure is often in place for 20 plus years. A major capital expenditure is required to install and commission a new network. ROCE expectations are extremely high for all businesses.

Industrial network refresh rates are accelerating over time as companies work to balance investment performance and network performance. However, we must still anticipate longer than desirable refresh rates to make planning effective.

Network planning and management

Like other business assets, a rigorous process governing the network ensures efficacy and availability as time goes by. There is not a particular methodology that is superior to others. Realistically, the best run business networks result from a collection of elements intertwined with the governing process. Justification for creating the process is simple.

- Lowers total cost of network ownership
- Improves business agility
- Helps the business respond quickly and effectively
- Increases availability

PPDIOO Process is a design and management methodology that spans the entire network lifecycle.

Prepare: Business agility is a result of good preparation. This phase is used to consider the broad vision, requirements and technologies you can employ to make your business more competitive.

Plan: Successful technology deployment must have an accurate assessment of the current state network, its security posture, and the business readiness to support the chosen solution.

Design: A detailed design reduces risk, avoids delays, and controls the total cost of network deployments.

Implement: Here the business works to integrate devices and new capabilities in accordance with the design phase without compromising network availability or performance.

Operate: Business proactively monitors the network to improve service quality, reduce disruptions and mitigate outages while maintaining high availability, reliability, and security.

Optimize: Best-in-class businesses never stop looking for a competitive edge. So, continuous improvement is a mainstay of any network lifecycle.

Effective network management

A range of additional areas need to be addressed to achieve effective management.

Documentation: Does comprehensive, up-to-date documentation exist for your network? Most companies do not have the required documentation, but all of them should consider it an absolute necessity. Accurate documentation and identification substantially shortens the time to recover from a network issue. Many methods to generate this documentation exist, ranging from a summer intern project to engaging a professional services organization to assess and document the network.

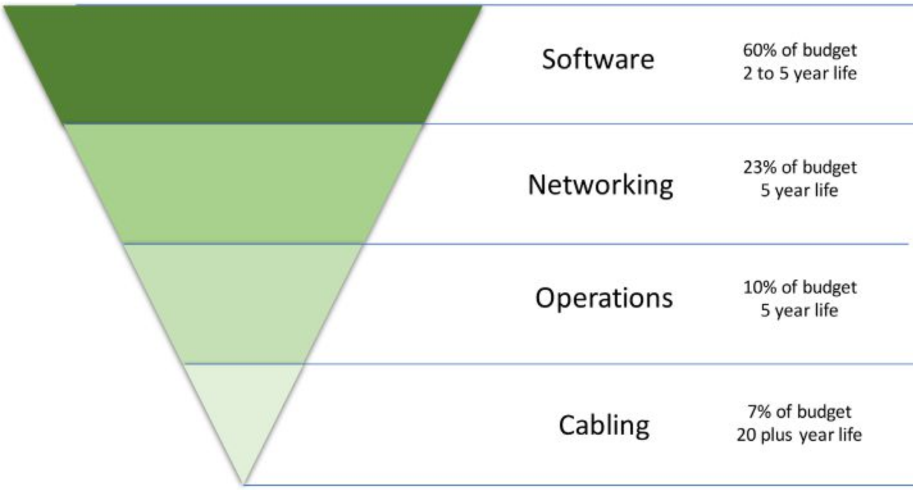
Network Assessment: Professional services organizations, backed by a major automation manufacturer, perform cabling and network infrastructure assessments. Many use software that "crawls" unobtrusively through the network, discovering and visualizing the network footprint.

Legacy Protocols: During the assessment process, pay attention to legacy protocols, i.e., Fieldbus. If legacy protocols are present, plans to migrate them to a modern technology must be at the forefront. Legacy protocols migrate out of the network as it ages because they become difficult and expensive to support, even if their performance is adequate. Their replacement is infrequently a "rip and replace" proposition.

Network Longevity: Consider the age of the existing network and physical infrastructure. Are any of the active components, network switches, servers, programmable controllers, drivers, or other end devices, approaching "end of sale" or "end of support" from the manufacturer?

Aged active components have support costs that grow exponentially after a certain age, so they need to retire before your business is frantically searching for good used replacements to get manufacturing up and running.

Evaluate the age of transmission media and its condition. Consider wire speed as well. Category 5e is adequate for 10Mb/s and 100Mb/s traffic but is insufficient long term. Pay attention to connections and the cable. Jacket materials are commonly thermoplastic which ages over time, particularly in environmental conditions like UV exposure, temperature extremes, and chemical exposure.



Infrastructure investment versus longevity.

SOURCE: PANDUIT

The same exposures age the metallic portion of connectors. Along cable routes, look for sharp bends and areas where cables appear to have been struck or deformed. With multi-pair copper Ethernet media, these physical deformations displace pairs in the cable, damaging its performance. With fiber optic media, there can be microfractures from physical deformation that attenuate or, in severe cases, interrupt signal flow.

Cabled infrastructure

As the network grows the cabled infrastructure must evolve. There are two cabling topologies used for industrial networks, point-to-point and structured cabling. Older industrial networks employ a point-to-point structured cabling topology where each connected asset has a home run cable to the control room or data center.

Engineers chose this solution in the belief that connection points were vulnerable and would cause reliability issues. More connections meant more risk. In the very early days of Ethernet connectors there may have been some credence to that conclusion. Connector and media design as well as manufacturing processes are significantly more robust today. So, in modern networks, this argument is no longer valid. Also, the flexibility and network resiliency gained from a structured cabling topology far outweighs the point-to-point reliability argument.

Enterprise networks were once point-to-point cabling. They quickly evolved to structured cabling for several reasons, notably:

- Structured cabling provides the needed flexibility to accommodate Moves, Adds, and Changes (MACs)
- Structured cabling can adapt network topology and configuration to business needs without pulling new cabling and resultant disruption of business activities
- Structured cabling topologies enhance network reliability and recovery speed from outages

Industrial networks are on this evolutionary path because the value proposition for structured cabling networks is so strong.

Elimination of downtime is the strongest argument for structured cabling topologies in industrial networks. Industrial network downtime is easily monetized in lost production dollars. As such, a business can readily justify adoption of this topology.

Structured cabling enables patching or otherwise re-directing network traffic to rapidly address infrastructure-related outages. It allows outages due to fault in the horizontal cabling to be immediately addressed by patching to a different horizontal link.

After the outage is resolved, the patching infrastructure permits technicians to quickly attach diagnostic instruments to the failed link. The link can be returned to normal service with minimal disruption in network operation.

Installing structured cabling

When installing structured cabling, it's good to have a few guidelines in mind to ensure maximum viability from the new installation.

- Require the cable installer to connect a network analyzer to each link installed, including spares
- Measured link performance becomes one of the job completion deliverables; Doing so establishes that the link delivers expected transmission performance, not just electrical continuity
- Further, if there are problems with a link in the future, baseline performance data exists in your files
- Premium cable manufacturers extend a generous warranty in exchange for fidelity to their offering using a certified installer; It is a worthwhile investigation when selecting materials and installers

Network management software

Another important topic for the current day network discussion is a 3-letter acronym, NMS.

SOURCE: PANDUIT

A key operational goal is to monitor the network to improve service quality, while maintaining high availability, reliability, and security.

NMS stands for Network Management Software. It is an emergent category of software for industrial networks. Just as the name implies, it is purpose-built software used to manage networks.

There are Enterprise NMS solutions and have been for a while. Due to the unique properties of industrial networks, these tools are not suited for the job. When selecting this category of software, make certain the NMS solution you consider is purpose built for industrial networks.

The clarion call for this type of software rises from the increasing sophistication and complexity of business networks. The ability to quickly ascertain what's connected, the health and workload on the network, misconfiguration of devices and of course, failing devices or connections, is key to effective operations with minimum downtime. Industrial networks have two main NMS use cases.

A consultant or system integrator working with the business uses NMS software located on their computer to discover and visualize the network; This application is to assess and document the current state network in anticipation of service activities.

An NMS solution is installed permanently in the network, typically on a server in the DMZ so the entire industrial network is visible and monitored; This application acknowledges the dynamic nature of the network and acts as a watchdog sniffing out problems; visualizes the network so a common understanding of status is provided for varying worker experience levels and dependent on the NMS solution; and provides a portal for secure remote access when needed.

The first use case focuses on the needs of network maintenance. An expert uses the NMS tool to discover and visualize the network. This step generates a baseline documentation package for the network. Typically, businesses retain this expert to perform maintenance, usually to upgrade or expand to the network. Up-to-date documentation for the network is a welcome latent outcome of the exercise.

While the expert's NMS package is connected to the network, performance and health metrics can be seen, helping the expert spot deficiencies that must be corrected. However, these values are a "snapshot" in that the NMS solution does not remain connected to the network long term.

The second use case addresses a greater portion of the network lifecycle. In this use case, the NMS solution resides in the network, typically on a server in the DMZ or the Manufacturing Zone.

Residence in the network allows the NMS software to act as a dashboard, allowing network users to see network health and performance. Further, more members of the workforce interact with the network now than in the past, all with varying levels of network knowledge.

These workers need information out of the network to ascertain if there is a network-related problem slowing down production. A production planner can use that information to make better decisions but may not have the needed skills to access the information.

Living in the network, NMS software tracks traffic and bandwidth, suggesting future improvements to the network. And of course, it is generating and maintaining an up-to-date view of the devices and connections in the network, solving the accurate documentation dilemma discussed earlier.

Finally, best-in-class NMS packages facilitate secure remote access to the network so you can enlist the help of experts without the time and cost involved with travel. In addition, the resident NMS software approach lessens the reliance on outside experts for diagnostics and network management assistance.

Reference architectures

Reference architectures are a considerable asset to the present and future states of business networks. Reference architectures streamline the deployment of standardized networking technologies and convergence of manufacturing and business networks into a cohesive whole. In short, reference architectures provide confidence and the necessary background to design, deploy, and operate a robust, reliable network.

Reference architectures provide valuable common ground to enhance the collaboration of OT (control engineers, manufacturing IT, etc.) and corporate IT staff. This common ground removes obstacles and speeds the combined team toward achieving business goals. Historically there has been some discord between IT and OT realms due to the proprietary and obscure nature of industrial networks, especially legacy protocols.

In the realm of reference architectures for industrial networks, the zenith is the Converged Plantwide Ethernet (CPwE), reference architecture. CPwE is a collection of industrial reference architectures that are use case driven and supported by rigorous testing and validation. The use cases selected represent important business needs and are garnered by exhaustive voice of the customer research.

The reference architectures are presented in a published document titled, "Converged Plant wide Ethernet Design and Implementation Guide." The document content is dynamic; new architectures are proposed for inclusion based on VoC research. All networks are assembled, commissioned, and tested prior to publication. Validation and performance data is published for each architecture, along with a hardware bill of materials, firmware versions used, and any software included in the test setup. CPwE remains ever green; as new devices become available and older devices go end of sale/end of support, the core reference architectures, (e.g., resiliency) are refreshed with new testing/validation and published performance data. Some businesses use CPwE architectures as a springboard to create architectures that suit very specific needs. However, because of their CPwE basis, the architectures are built on a solid foundation.

Network building blocks

Another practice that has risen to prominence are pre-populated and pre-configured network enclosures. The solution allows companies to rapidly deploy or expand without bearing the time penalty and expense of a bespoke enclosure. These solution elements follow the functions of the 3-tier architecture of Converged Plant wide Ethernet – Access Layer, Distribution Layer and Core Layer – with appropriate solutions for each network layer.

Enclosure designs are validated electrically and thermally to eliminate risk during installation and commissioning. Active component placement within the enclosure is optimized for function, thermal performance, and maintainability.

Since the network building blocks are built to a validated design, companies gain enhanced supportability through their use, avoiding the "snowflake" scenario where each bespoke enclosure is "just a bit different." This factor is important in a local deployment but becomes vital when multiple locations across a global footprint are considered.

Network Planning ≤ Two Years

Networks continue to evolve over time. Plotting the evolutionary path for the business network requires insight into future trends and possibilities. This section offers insight via identification and discussion of important technologies. The time domain for these technologies is within the next two years.

Power over Ethernet

Power over Ethernet (PoE) is an Ethernet-compatible technology created to enable Voice over IP (VoiP) telephony. DC power, at a nominal voltage of 48 VDC, is carried on one or more pairs in the Ethernet cable along with the transmitted signal. PoE-powered devices (PD) negotiate with the power source (e.g., PSE, typically a network switch) to ensure appropriate power is delivered. Businesses soon realized the potential of network supplied power. PoE now powers IP cameras, wireless access points, badge readers and access gateways, and office lighting.

Today, PoE in industrial networks performs identical tasks to those it performs in enterprise networks today. These tasks include powering shop floor phones, wireless access points, and IP cameras. PoE holds a bright future as the standards community expands its capabilities.

PoE is a key technology for the future of industrial networks because, with the advent of IEEE 802.3bt that was published in 2018, conspicuous amounts of power can be delivered along the Ethernet connection to a device. With 71 W available at the end of an Ethernet cable, device manufacturers can be very creative. This "one wire ideal" allows device power and communications in a single connection, simplifying all phases of the device life cycle. In doing so, PoE alters the DC power infrastructure of control systems.

Legacy protocols offer serial communications to the device at a very modest data rate. No device power is delivered by the connection. Therefore, local DC power supplies are required near the device to meet its power requirements. Behind the DC power supply are many AC components (e.g., transformer, connection wires, circuit protection, etc.) to convert machine mains power to a usable input to the DC power supply. When this supporting infrastructure can be eliminated, control system DC power infrastructure is simplified and costs become lower.

PoE negotiates with the device at start-up to determine the appropriate power level to deliver. There is no need for pre-configuration of each circuit in a standards-compliant installation. Additionally, since device power is controlled by PoE-enabled ports in the switch above it, toggling device power can be done via network switch commands, simplifying service procedures.

PoE should figure prominently in new network installation to simplify powering needed by devices like cameras and wireless access ports. The transformative effect on the DC power infrastructure, while quite feasible, is going to take longer to become a reality.

Single Pair Ethernet

Work is underway in IEEE 802.3 to create standards for Single Pair Ethernet (SPE). Many variants are proposed from short reach (15 to 40m at 1 Gb/s transmission speed) to extreme lengths (up to a kilometer at 10 Mb/s transmission speed), all over a shielded twisted pair cable. For industrial network applications, the variant to watch is IEEE 802.3cg, the 1km at 10 Mb/s variant. All variants of SPE are considering a methodology for power delivery like PoE called Power over Data Line (PoDL), IEEE P802.3bu.

Single Pair Ethernet drives "Ethernet-to-the-edge" and is a vital portion of legacy protocol migration plans. For 802.3cg, its 10 Mb/s transmission speed provides more than enough bandwidth for end device and sensor data rates. For industrial networks:

- The reach objective of up to 1km is ideal for plants with large footprint, (e.g., oil and gas, petrochemical, etc.)
- Power delivery via the Ethernet connection achieves the aforementioned "one wire ideal" where device power and communications are enabled by a single connection. Given the power delivery aspect, it is conceivable that end device power infrastructure is greatly simplified by SPE.
- SPE, being standard, unmodified Ethernet, supports purpose-built Ethernet forms like EtherNet/IP and Profinet without issue.
- SPE can have a cost advantage versus 4-pair media in edge device applications. This is due in part to simpler cable construction. The silicon and magnetics used for SPE in switches and end devices are much simpler than 4-pair Ethernet.
- Conductor wire gauge for SPE will need to be at least 18 AWG to achieve the 1km reach objective; A latent benefit of this cable construction is the ability to drive higher current levels than 4-pair cable, making LED lighting installations more effective.
- SPE media should be easily field terminable; This aspect can reduce pre-terminated cordset inventories and address slack management issues.

The "front runner" SPE standard is IEEE P802.3cg, and Single Pair Ethernet is gaining prominence by taking Ethernet to the edge of industrial networks. Device manufacturers and network switch manufacturers are closely monitoring and contributing to the creation of IEEE standards that enable this future concept.

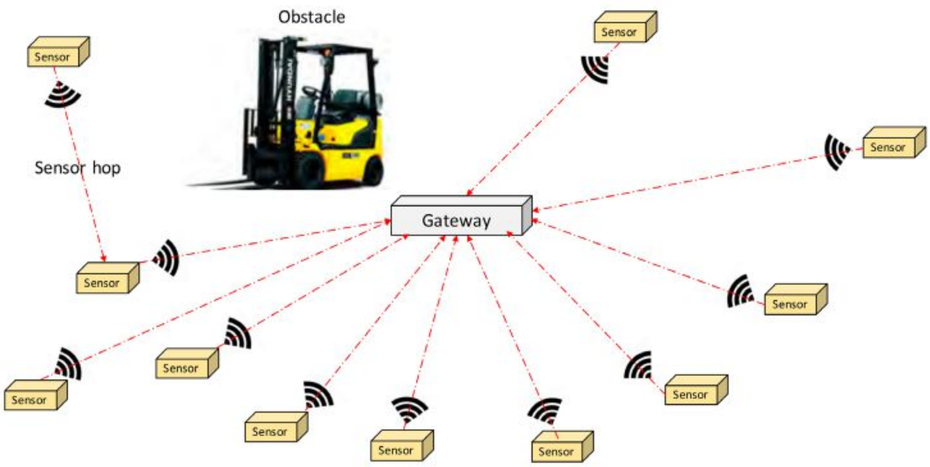
Power over Data Line

Power over Data Line (PoDL) is governed by IEEE standard 802.3bu. The PoDL acronym is frequently pronounced "poodle" in conversation. It represents a necessary adaptation of PoE. A reasonable question is "why can't we just use PoE on SPE?" The reason is PoE requires at least two pairs to work. This is because there is an electrical connection between pair center taps. Since SPE has only one pair, the PoE circuit does not work. However, a simpler circuit implementing a lowpass/highpass bandsplitting filter network that works with SPE.

Using PoDL Class 8 and Class 9, PD power can be 30 W or 50 W respectively at 100m. New classes are required to accommodate the expected higher loop resistance of 1000m links seen in 802.3cg. PoDL and SPE go hand in hand as technologies to watch and include in legacy protocol migration plans.

Wireless Sensor Networks

Wireless sensor networks are gaining popularity as businesses seek solutions that improve decision speed and quality. Wireless networks can be implemented quickly, speeding the availability of additional knowledge to achieve these goals.



Wireless mesh network example.

SOURCE: PANDUIT

Speed and reliability do not yet perform like wired connections. Critical control connections will remain wired for the foreseeable future. However, wireless connections provide a fast and cost effective means to collect additional data to propel analytics efforts, study new facets of an existing process, etc.

There are many wireless sensor networks worthy of consideration but two stand out for industrial applications. These are Wireless Mesh and LPWAN.

Most wireless mesh networks used for wireless sensor applications are based on IEEE 802.15.4. This is the technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). Wireless mesh networks have a unique feature that makes them a provocative choice for industrial data collection; they are self-healing. If a wireless sensing node is blocked from communicating directly with the sensor gateway, it will “hop” to an adjacent node to get back to the gateway. This feature is superb for industrial applications given the dynamic environment with material handling equipment and other large metallic structures often in motion. For example, the chances of a forklift mast blocking transmission at some point in the day is easily an “even odds” bet.

Low Power Wide Area Network (LPWAN) is another technology worthy of note for industrial applications. LPWAN protocols are well-suited for use in industrial settings. These networks are nominally 900 MHz, a frequency range that performs well in highly metallic environments.

LoRaWAN is intended for wireless battery-operated nodes in a regional, national, or global network. It targets key requirements needed for the Internet of Things (IoT) like low data rate, low cost and long battery life while delivering vital features such as secure bidirectional communication, location, and mobility services. In Europe, LoRaWAN operates in the 868 MHz band. North American LoRaWAN installations use the 915 MHz band.

End devices using LoRaWAN can choose from three device classes, allowing different device behavior depending upon optimization needs:

- Class A – battery powered node. Class A operation optimizes communications to conserve battery power at the node
- Class B – low latency needed. Class B devices open extra receive windows at scheduled times to optimize communications but with shorter battery lifespan
- Class C – no latency. Class C devices have nearly continuously open receive windows reducing latency to its practical minimum

LoRaWAN presents performance advantages for wireless sensing networks in industrial environments and is already gaining popularity for many IoT applications. This is a wireless network to watch and include in your future network planning.

Network Planning > Two Years

Industrial network evolution includes a strong influence of better IT/OT collaboration. As these two very capable groups act in concert to improve business outcomes, some advanced IT practices will find their way into industrial networks. These are Time Sensitive Networking (TSN) and Software Defined Networks (SDN).

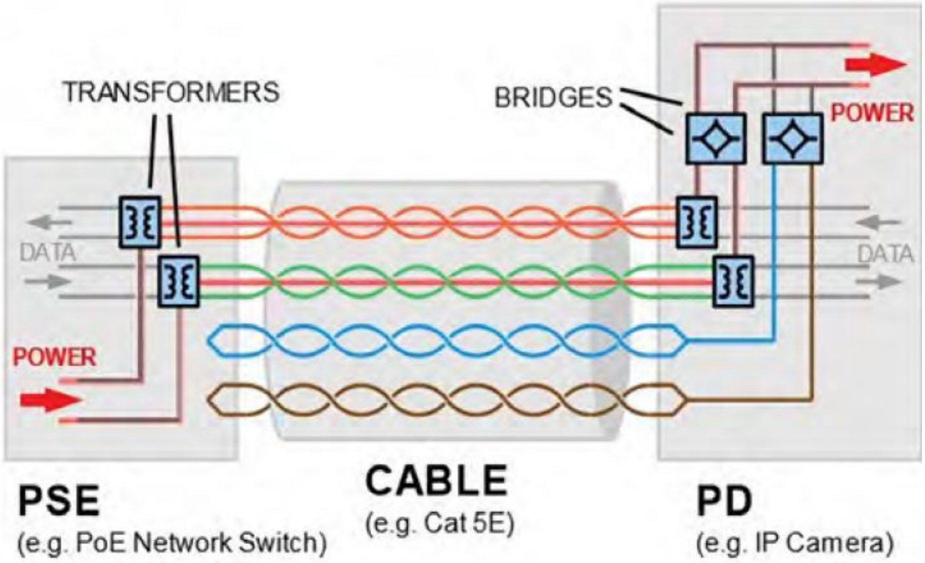
Time Sensitive Networking

TSN gets a lot of attention from automation experts due in part to the increased interest in the Industrial Internet of Things (IIoT). Some of the data collected by IIoT sensor networks is not inherently time sensitive. However, some data is mission critical and time sensitive and must be shared with strict latency and reliability requirements. Further, all data is enriched by adding accurate time context as it allows correlation and analytics to excel. Therefore, TSN is an important technology both within the control loop and outside the loop in IIoT applications.

There are four key benefits that TSN applied to industrial networking provides:

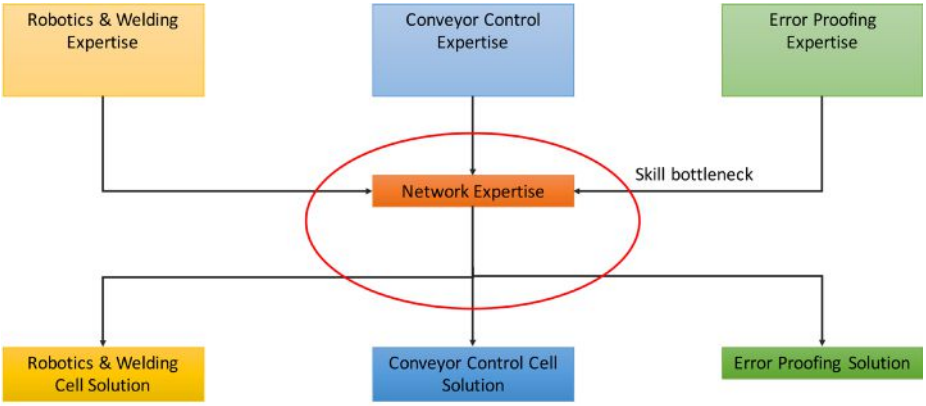
Bandwidth: Machine vision, 3D scanning and power analysis applications running on an industrial network create large data sets which can strain available bandwidth; Propriety Ethernet derivatives industrial networks that are used in industrial control today are limited to 100 Mb of bandwidth and half-duplex communication; TSN supports standard Ethernet in full duplex with higher bandwidth options such as 1 Gb, 10 Gb and even the projected 400 Gb version in 802.3.

Security: TSN embraces top-tier Ethernet security provisions; Segmentation, performance protection, and temporal composability add multiple levels of defense to the security framework Interoperability: TSN integrates existing brownfield applications and standard IT traffic by using standard Ethernet components; TSN inherits many existing Ethernet features like HTTP interfaces and web services; These features enable remote diagnostics, remote visualization, and repair



SOURCE: PANDUIT

PoE general layout. Power transmission using data lines of Cat5 cable.


Robotics & Welding Expertise
Conveyor Control Expertise
Error Proofing Expertise
Network Expertise
Skill bottleneck
Robotics & Welding Cell Solution
Conveyor Control Cell Solution
Error Proofing Solution

SOURCE: PANDUIT

Traditional process/network design flow.

capabilities common to IIoT systems.

Latency and Synchronization: TSN prioritizes low-latency communications to provide fast response and closed loop control applications. It can achieve deterministic transfer times on the order of tens of microseconds and time synchronization between nodes down to tens of nanoseconds. TSN provides automated configurations for high reliability data paths where packets are duplicated and merged to provide lossless path redundancy, ensuring reliable delivery of time sensitive traffic.

TSN provides network designers with tools to ensure that critical traffic is received in a timely and reliable manner. It also frees up congestion to allow non-critical traffic to be converged onto the network and move as "best effort" traffic. This is an essential distinction in that almost all traffic is best effort. Wire speed and limiting traffic to only critical message streams is used to make the network function correctly.

Software Defined Networks

Software Defined Networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality.

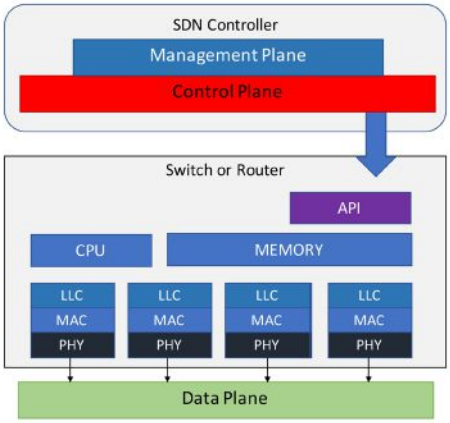
Along the bottom of the diagram are the solutions required by the manufacturing area, a robotics/welding cell solution, a conveyor solution and an error proofing solution. These solutions require automation to function and connections to the industrial network. Along the top of diagram are the domain expertise groups that design and specify the functional needs for each solution. The control engineers (OT staff) must translate the design and functional needs into an automation system and industrial network solution. These staffs are often quite modest so companies engage 3rd party experts to attempt to perform in a timely fashion.

Once in place, the network and automation must be operated, managed, and maintained. A chilling statement from a Gartner blog post crystallizes the gravity of those functions. "... 80% of unplanned outages impacting mission-critical services will be caused by people and process issues and more than 50% of those outages will be caused by change/configuration/release integration and hand off issues."

Traditional network design and maintenance practices tend to reinforce the problem. Significant time and planning are expended. Specialized domain expertise is required for each solution, both from a process and a networking standpoint. Unique manual configurations must be made for each network node. And due to pressing schedules and business priorities, change management and record keeping are often lacking.

While not literally a local laptop connection in all cases, traditionally engineers address and configure one device at a time until the whole network is configured. This is a laborious and potentially error prone method in addition to being very time intensive.

With a simplified view of device management using SDN, network switches and other compatible network devices abstract their control plane. The control plane functionality is transferred to a device called an SDN controller which provides control plane instruction sets to the subordinate devices. The SDN controller also contains management plane functionality. Therefore, a centralized controller handles monitoring, remediation, device behavior, and characteristics all from a central location. This architecture allows companies to create reusable configurations that can be replicated throughout multiple nodes using tested applications. Further extending the concept, it provides access to programmatically modify network nodes from the SDN controller. This functional change creates enormous benefits across the network.



SOURCE: PANDUIT

Device management using SDN.

SDN simplifies the configuration and implementation of network architectures by creating reusable configurations and designs that improve system performance.

The simplified SDN also improves corporate margins because plants do not need to rely on network specialists on the factory floor, thus lowering personnel costs, improving implementation time, and reducing troubleshooting and repair costs.

Machine design is another area that must be addressed differently. When machine builders construct a solution, the individual components used for the machine are not often questioned. However, connecting the machine to the existing programmable automation controller (PAC) can be a challenge when Ethernet is not used and standards are not followed. Some machine builders leverage technology that is so disruptive that redesigns are required to some of those systems. To address this situation, it is critical for manufacturers to specify that wireless and Ethernet components communicate seamlessly with other systems.

A SDN for industrial network applications needs time to gestate and develop, hence its placement in the "> 2 years" time horizon.

One of the critical items for this concept is the retention of network switch features that are optimized for industrial applications. To explain, one artifact of SDN in the data center application space is that companies sought to deploy "white label" switches in the architecture. The "white label" network switches are minimally viable products with very modest feature sets. These are completely appropriate choices for the data center implementation of SDN. However, it could be a stumbling block for industrial networks.

Conclusion

The industrial network infrastructure is a valuable business asset. Investments in legacy industrial networks require a clear migration path to optimize return on assets while not missing out on performance enhancements from new technologies.

A robust, well-executed physical layer is foundational to this asset continuing to deliver value. Rapidly emerging technology advances such as the Internet of Things, Wireless Sensor Networks, Power over Ethernet, and Time Sensitive Networking can further leverage your network with a little education and planning.

Technology update by ***Panduit.***

Automated water management for fracking and water transfer

Automation reduces costs, improves safety for unconventional natural gas production in the Permian Basin. Increasingly, oil and gas companies are looking to automate, especially for water pumping and treatment, but automation for assets located over a broad area isn't easy.

IN THE OIL AND GAS INDUSTRY, TECHNOLOGY advances like hydraulic fracturing (fracking) and horizontal drilling have caused a boom in exploration and drilling. The initial "gold rush" approach to oil and gas development focused on people resources, with most work done manually.

Technicians and operators in the field checked all equipment and processes and manually adjusted and controlled whatever needed control. Even data required for environmental compliance was generally acquired by hand. But today, with greater labor uncertainty and higher but volatile prices, investing in automation is starting to make more sense. Increasingly, companies are looking to add automation in the field, especially for water pumping and treatment, key ingredients in successful unconventional oil and natural gas production. But automation for assets located over a broad area isn't easy.

"Most automation companies don't understand the network piece," notes Dan Arbeau, CEO of netDNA in British Columbia, Canada. With his background in automation, wireless, IT support, and networks, however, Arbeau was ready for the challenge. He started netDNA in January 2018 and has since added partners for additional capital and resources.

The company's focus is automating natural gas exploration and production, especially drilling. In 2014 Arbeau had automated a large pump for evacuating water from dams, a previously manual system that transferred water for fracking. The customer called again for help with a major project in the Permian Basin in Southern Texas, managing water at hundreds of drilling sites.

SOURCE: OPTO 22

Trailer-mounted pumping units are automated with a groov EPIC processor and I/O modules.

Water, water, everywhere

Water is essential for successful natural gas production by fracking. The process typically involves water at every step:

- Pumping water to the drilling site
- Blending the water with proppant (sand or other particles that can't be compressed) and chemicals
- Injecting this fluid into the wellbore and rock formation at high pressure to create fractures
- Handling the fluid flowback that's returned to the surface and storing it in open tanks or pits
- Treating and reclaiming the water, which in addition to chemicals may also include hydrocarbons, salts, metals, and radioactive nuclides

Arbeau notes, "Ninety-nine percent of jobs in the Permian Basin have water pits." Water sources are often not close to the drilling site, so water must be brought in. Pits are used to store water, blend water, handle flowback, and treat the used water. Until recently, all flow and level monitoring, pump control, and the like were typically done manually. Technology is sparse and mostly ad-hoc rather than planned, for example a technician monitoring a level and texting an operator to adjust a pump. Automated pumps, flowmeters, and level sensors are needed everywhere. That's where netDNA comes in.

Mobile trailer-mounted pumping

One netDNA customer, New Wave Energy Services, provides a range of fracking products and services in the U.S. and Canada, including water transport, modular tanks, and buffer tanks. In an industry with remote, widely separated, and changeable operations, mobility is essential. So New Wave designed large trailer-mounted units for water transfer, typically with four 500-800 HP pumps with 12-inch diameter inputs and turned to netDNA to automate them.

Arbeau had used Opto 22 SNAP PACs (programmable automation controllers) on previous jobs. He appreciated their reliability and use of open standards, such as Modbus/TCP, for easier communication with other systems and equipment.

Arbeau had also heard about Opto 22's new groov EPIC (edge programmable industrial controller), which provides additional communication, visualization, and security features for automation and industrial internet of things (IIoT) projects. For the remote communications and mobile nature of New Wave Energy's trailer-mounted units, groov EPIC sounded ideal.

Each New Wave Energy trailer-mounted pumping unit includes a diesel generator and pumps, controlled by a genset controller that talks Modbus/TCP. Arbeau added a groov EPIC processor and I/O modules on each trailer for additional automation:

- Analog inputs monitor discharge levels and suction
- Mechanical relay outputs open and close pumps via the genset controller
- Digital inputs monitor flowmeters

In addition, the EPIC pulls data from the genset controller, including RPMs and associated telemetry, and publishes it to a central broker/server using its built-in open-source tool Node-RED and the publish-

SOURCE: OPTO 22

Solar-powered trailers provide mobility for remote operations.

subscribe protocol MQTT. As of June 2019, six trailer-mounted units were in operation, with several more in the works.

Pits and tanks

In addition to the trailer-mounted units, netDNA also automates monitoring and control for pits and tanks using water.

Automating tanks improves safety as well as providing data faster, more easily, and more reliably. Tanks are monitored for levels, and pumps are controlled to make sure there are no spills. Tanks and pits are also monitored for air quality and hydrogen sulfide (H2S) levels. H2S is flammable and potentially deadly if inhaled, about as toxic as carbon monoxide. Instrumentation and automation help keep employees safe and improve environmental conditions.

At the pits and tanks, netDNA uses a SignalFire self-contained gateway for wireless sensors. The SignalFire talks Modbus/TCP to a local groov EPIC processor. Each EPIC publishes a variety of data tags from its pumps, again using Node-RED and MQTT: 15 telemetry data points; 10 stop, E-stop, and other commands; and more. Production data is also tracked and historized. If a spill or issue occurs, producers need to know exactly what the pumps were doing at any given time.

New Wave and their customers are pleased with the results, and Arbeau is pleased with the capabilities of the groov EPIC system.

"Some engine and pump companies are hungry for automation. Some have systems, but they don't communicate with each other,"says Arbeau. "EPIC makes them talk."

Mobile HMI

In addition to automated monitoring, control, and data acquisition, the groov EPICs serve a custom web-based operator interface (human-machine interface, or HMI) for authorized technicians. netDNA developed the HMI using groov View, a tool included with the EPIC. The tool's browser-based drag-drop-tag interface makes it simple to develop a custom HMI for PCs and mobile devices.

Each trailer unit is equipped with a radio IP (internet protocol) device that provides routing, 300 feet of wireless coverage, and power for a cell modem, which connects to the cellular WAN (wide area network). With the groov View HMI, authorized technicians in the field can use a tablet to connect to this network and run all 20 pumps in a system of pits, monitoring or changing RPMs, for example, from a single screen.

Programming & data communications

The EPIC processor offers programming options, including flowchart-based PAC Control with optional scripting, any IEC 61131-3 compliant language (like Function Block Diagram and Ladder Diagram), or C/C++, Java, and Python via Secure Shell access (SSH) to its Linux operating system. netDNA chose to use PAC Control with its free Modbus Integration Kit, which simplifies communications with the genset controllers and SignalFire sensor gateways.

For data communications, netDNA takes advantage of the EPIC's ability to use MQTT with Node-RED. MQTT is a publish-subscribe (pub-sub) method of communication originally developed for the oil and gas industry, and it has huge advantages for remote or wireless networks. If a network is low-bandwidth, unreliable, or expensive, or if distance makes a direct connection impossible, a pub-sub method is ideal.

SOURCE: OPTO 22

Pump and smart pump controller (side view)

Each client initiates communication to a central broker/server and then publishes data, subscribes to data, or both. The broker/server does not store data, but simply accepts and forwards data packets as required. Network traffic is reduced overall, because data is communicated on a report-by-exception (RBE) basis—that is, only when the data changes—rather than at regular intervals.

netDNA is also interested in looking into using Sparkplug messaging with MQTT, available in the groov EPIC with Ignition Edge from Inductive Automation. Sparkplug encodes the data payload and compresses it. It also tracks the state of clients to make sure all clients can deliver and receive data.

The EPICs on each trailer, tank, or pit publish data to the MQTT broker, and other EPICs subscribe to the data. For their broker, netDNA uses their own hosted secure MQTT server.

Each EPIC contains its own device firewall for data security. The data the EPIC publishes is device-originated behind its firewall, so no inbound port modifications to the firewall need to be made. Once the EPIC makes the connection with the broker, any return data the EPIC subscribes to is received securely over the same connection.

The system works remarkably well for remote, wireless control. Multiple pumps respond to sent commands within a second. To save bandwidth, netDNA sends data in tables instead of individual data points whenever possible.

Looking ahead

With groov EPIC and modern IIoT tools at his disposal, Arbeau spent only three weeks from initial hardware design to having a full system ready for pump control. And thanks to netDNA, New Wave Energy Services can now offer their customers monitoring and control that's faster and less expensive than their competitors.

"It's not that hard to outshine the competition," says Arbeau. "EPIC is helping me be successful."

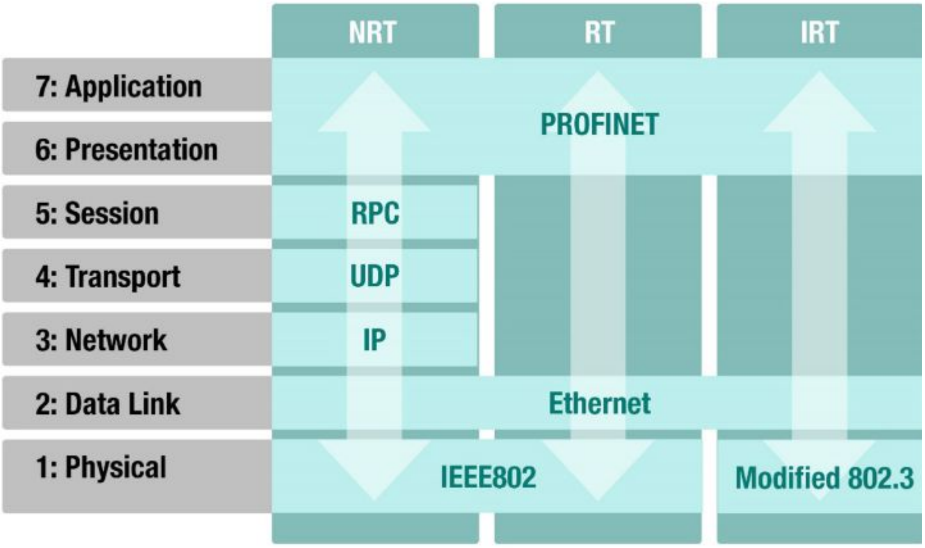
For the future, Arbeau's dream is a multi-use automation black box: an open-chassis skid with EPIC "in the middle" and SignalFire connecting to wireless sensors.

Arbeau envisions the skid used for projects not only in oil & gas, but also in agriculture, mining, and other industries with far-flung assets that need automation and data communications.

Application report by ***Opto 22 Corporation.***

PROFINET Over Industrial WLAN Infrastructure

Two key challenges need to be addressed when building a stable PROFINET application over a WLAN infrastructure. The selected WLAN solution must support L2 forwarding in different configurations, and wireless latency and jitter need to be minimized to meet the requirements of the PROFINET application.



SOURCE: MOXA

The PROFINET protocol stack

WITH THE EMERGING AIOT AND IIOT TRENDS, an increasing number of connected devices are being introduced into industrial operations at a faster pace than ever before. At the same time, wireless connectivity has opened up new doors for many mobile applications and has gained traction in recent years within the industrial sector.

More and more industrial control and automation planners are embracing the benefits of wireless communication and are integrating wireless infrastructure into their system design. This article aims to communicate the protocol requirements, deployment considerations, challenges, and solutions to support one of the most popular industrial communication protocols, PROFINET, in wireless networks.

The goal is to provide an overview of the basic PROFINET requirements and configuration variables needed to obtain an acceptable performance margin in a wireless environment. It provides example scenarios of industrial wireless applications using WLAN solutions to serve as a frame of reference for planning a wireless PROFINET deployment.

PROFINET Overview

PROFINET is the PROFIBUS International (PI) industrial Ethernet standard designed for automation control communication over Ethernet-based infrastructure.

PROFINET devices may require different communication speeds depending on the type of automation process. The PROFINET protocol supports three communication classes, each with a different degree of time sensitivity. These are Non-real-time (NRT), Real-time (RT), and Isochronous Real-time (IRT) communication.

- NRT, sometimes referred to as TCP/IP communication, is acyclic traffic such as sensory, diagnostic, or maintenance data transferred at best-effort speed.
- RT communication is cyclic traffic consisting of high-performance process data transmitted over standard networking infrastructure. This article mainly focuses on the key aspects of RT communication applications.
- IRT communication is the highest performing type of deterministic traffic within the PROFINET standard. However, this requires hardware-based bandwidth reservation and network-wide clock synchronization to function.

The PROFINET RT and IRT communication classes involve a cyclic data exchange over standard Ethernet and take place directly on Layer 2 without any TCP/IP overhead to minimize latency. This means that in an RT/IRT PROFINET environment, data frames are forwarded based on the devices' MAC address. Therefore, it is essential that any underlying network infrastructure deployed to support RT or IRT PROFINET applications is fully Layer 2 transparent to all connected PROFINET devices.

The performance of PROFINET-based communication is limited to the performance ceiling of the underlying network infrastructure. To provide the flexibility to operate reliably over the different network infrastructure components, the cyclic data exchange rate for PROFINET RT communication can be customized to accommodate any infrastructure limitations or to suit the automation context.

In the example using the Siemens TIA Portal, the IO cycle > Update time parameter defines the communication update interval between the PROFINET IO controller and the IO devices. The IO cycle > Watchdog time parameter specifies the number of consecutive response failures before reporting a link failure which, depending on the process design, typically triggers the error handling or safe mode, halting the automation process.

WLAN infrastructure considerations

PROFINET (PN) communication can also be realized over a standard IEEE 802.11 wireless connection. While some PROFINET IO (PNIO) devices have built-in wireless client capabilities, the majority of PNIOs only support Ethernet interfaces. In those cases, system integrators will need to connect the PNIO to a wireless client device that acts as a wireless adapter to communicate with the PN controller.

Even though wireless technology has improved over time with every new iteration of the IEEE 802.11 standard, it is important to note that designing a wireless network is inherently more complex compared to fully wired infrastructure.

In order to design and deploy the right wireless solutions to support PROFINET communication, several key aspects of wireless networking need to be taken into consideration. These include L2 transparency limitations, higher latency, and radio frequency (RF) management to configure the wireless environment for optimal performance.

The following section describes the considerations and challenges integrators need to take into account when designing

IEEE 802.11 industrial wireless networks for PROFINET-based applications. Typical wireless integration scenarios observed in industrial automation and control systems today rely on external wireless devices to serve as the PROFINET IO's wireless adapter.

It is important to evaluate these areas systematically when designing wireless networks, in particular when used for critical PROFINET-based control and automation processes. The following sections of this document will outline several typical wireless deployment scenarios, how each of the wireless design considerations relate to different scenarios, and Moxa's solution to address the challenges presented by each scenario.

WLAN infrastructure overview

Before evaluating potential WLAN solutions, it is recommended to thoroughly review and map out the requirements of the application first. Since different PROFINET applications require different types of architecture, some variables to consider are:

- The number of PNIO devices to integrate.
- The scale of the wireless network (the number of wireless devices to deploy).
- Device mobility requirements.
- The need to connect standalone Wi-Fi clients such as personnel smart phones, tablets, and laptops.

Different types of wireless deployments such as Point-to-point (P2P) and Point-to-multipoint (P2MP) topologies commonly adopted in the industrial sector fit into one of two main configurations: AP/Client or Bridge configurations.

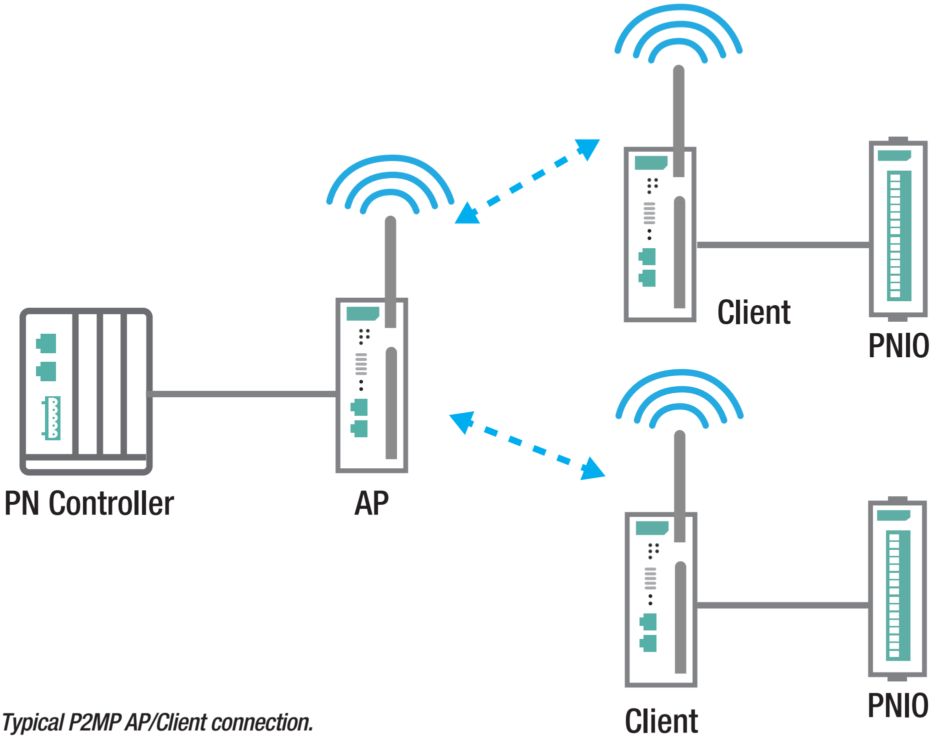
AP/Client architecture

Point-to-point (P2P): In a P2P AP/Client configuration, a dedicated wireless connection is established between the PN controller and a single PNIO through an access point (AP) and the client's wireless interface. In this scenario, the PN controller and PNIO are connected to the wireless devices using Ethernet. This type of topology is usually preferred in situations where bandwidth is not shared between clients and where each wireless connection runs on a different, non-overlapping channel.

Point-to-multipoint (P2MP): In a P2MP AP/Client configuration, a single AP supports multiple clients with each client supporting a maximum of one PNIO connected to it. It is one of the most commonly adopted wireless configurations for connecting multiple clients in a shared bandwidth environment. In some circumstances, the AP will need to serve a combination of PNIO clients and standard Wi-Fi clients such as laptops and tablets.

Bridge architecture

Point-to-point (P2P): In a P2P bridge configuration, a dedicated wireless bridge between a pair of wireless devices is created to connect multiple PNIOs to a PN controller. Since bridge architecture works at the data link layer (L2) of the OSI model, it allows more than one PNIO to be connected to either wireless device over the same bridge.



Typical P2MP AP/Client connection.

This topology can be seen as a wireless extension of a wired backbone, bridging the wired devices on both sides of the wireless connection into a single L2 network. A classic example of a P2P bridge connection is the Wireless Distribution System (WDS).

Point-to-multipoint (P2MP): Similar to its AP/Client counterpart, the P2MP bridge topology is a type of deployment that is commonly adopted by system designers that want to integrate multiple mobile PNIOs. In a multi-bridge topology, several wireless bridge connections are established, converging to a single wireless device to connect multiple PNIO systems to a PN controller.

Both the P2P and P2MP bridge topologies are frequently used by AGV machine builders as it allows one wireless device to act as the wireless adapter for multiple PNIOs installed onto the AGV such PLCs for sensors, motors, and cameras.

Whether using an AP/Client or Bridge architecture, PROFINET system designers generally adopt WLAN infrastructure for the benefits of rapid deployment and device mobility. Therefore, candidate wireless solutions are also expected to support seamless roaming to ensure mobile PNIOs can easily move between access points without interrupting the connection.

Once you have identified a suitable WLAN architecture for your PROFINET application, the following sections will explore the challenges presented by each architecture, and the solutions to address these challenges in order to implement a robust industrial wireless network capable of supporting PROFINET WLAN applications.

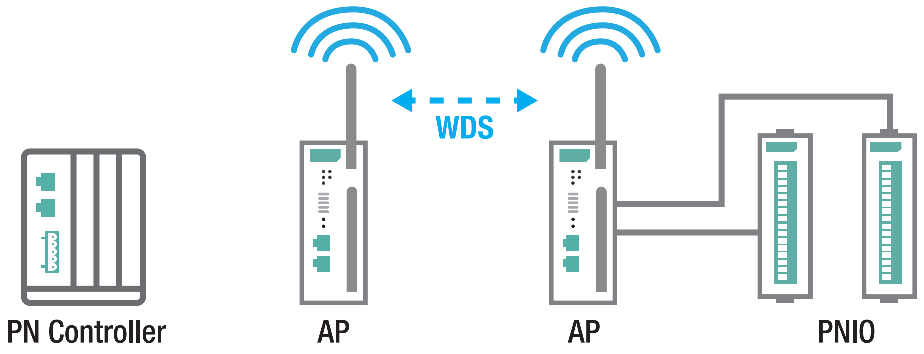
WLAN infrastructure challenges

As wireless solutions gain in popularity, they are gradually becoming an integral part of the industrial network infrastructure designed to support PROFINET-based communication. Below is a quick summary of the key points:

1. PROFINET real-time (RT) communication requires the underlying network infrastructure to be Layer 2 transparent in order to forward data frames correctly.
2. Wireless infrastructure differs from wired infrastructure. Additional considerations need to be addressed to increase network reliability and availability, such as enhanced functionality to adjust for the additional complications of mobile applications, and RF environment analysis to create a reliable, deterministic wireless network.
3. The most common wireless installations can be categorized into AP/Client or Bridge architectures. Which topology to adopt depends on several factors including the scale of the network and the number of PNIOs that need to be integrated.
4. When using standard WLAN solutions in industrial settings, integrators may experience some complications concerning functional requirements.

AP/Client configurations

In AP/Client P2P or P2MP configurations, when a PNIO is wired to a wireless client,



SOURCE: MOXA

Typical P2P wireless bridge connection

L2 transparency ends at the client device's wireless interface.

This means that when using standard Wi-Fi client connectivity without enhanced functionality, the PN controller will not be able to forward data frames to the PNIO as it cannot identify the MAC address of the connected PNIO. Refer to Appendix 1 for more details regarding this technical limitation.

Challenge 1: Since the communication between the PN controller and the PNIO happens on the data layer, the boundary of L2 transparency must extend beyond the wireless client's Ethernet interface, while maintaining compatibility with standard AP/Client connections to allow other Wi-Fi devices to connect to the AP.

Bridge configurations

One example of a typical bridge connection is the Wireless Distribution System (WDS), which, by its technical specification, is a L2 transparent wireless link connecting two APs. A layer 2 wireless bridge setup is preferred in cases where multiple PNIO devices need to be connected to one wireless device.

However, commercial WDS solutions are unable to fulfill the needs of more complex industrial applications. WDS is statically configured and is not designed to support bridge roaming to accommodate moving devices such as AVGs. Furthermore, WDS does not support hybrid bridge/AP functionality by default to serve standard Wi-Fi clients such as laptops and tablets used by on-site engineers.

In cases where multiple wireless bridges are necessary, system designers can set up additional WDS bridge links to create a P2MP configuration. However, each bridge link needs to be configured manually. This makes deploying conventional P2MP wireless infrastructure very time- and resource-intensive and more prone to network issues due to configuration conflicts.

Challenge 2: Commercial wireless solutions have out-of-the-box limitations that make them unable to meet the functional requirements of industrial wireless PROFINET applications.

Bridge devices should support multipoint bridge topologies, bridge mobility, and be able to act as a hybrid bridge/AP to connect additional standard Wi-Fi clients.

Latency, jitter, and RF management

Wireless connectivity occurs through electromagnetic waves that are sent within an ISM band. This physical characteristic of communicating over a shared medium is inherently susceptible to interference from various devices operating in overlapping channels within that spectrum. As a result, WLAN components are more likely to suffer from latency or jitter. The amount of additional latency compared to a purely wired network depends on the type of WLAN technology, antenna performance, and the channel utilization within the network environment.

Therefore, employing a set of best practices when evaluating and configuring the RF environment and wireless coverage are key to yielding optimal wireless performance and establishing the foundation for a more deterministic WLAN infrastructure.

Outlined below are several important RF best practices for reference.

Wireless spectrum:

- Select the radio bands most appropriate for the application considering the network environment and signal penetration.
- Reserve the 5 GHz frequency band for critical communication as this band has more channels available and is generally less congested compared to the 2.4 GHz band.
- Use the 2.4 GHz frequency for farther signal penetration.
- Avoid configuring Dynamic Frequency Selection (DFS) channels on the 5 GHz band (channels 52 to 140) for critical communications to prevent interference from radar signals.
- Perform on-site RF spectrum analysis to identify and allocate devices for different applications to free, non-overlapping channels.

Wireless coverage:

- Maintain an unobstructed line of sight when installing antennas to avoid signal degradation caused by nearby physical objects.
- Select suitable antennas for the environment to ensure a good signal-to-noise ratio (SNR).
- However, performing RF analysis and configuration relies on experienced personnel with extensive knowledge of wireless networking. In the industrial sector, it is often difficult to dispatch qualified individuals on a readily available basis.

Challenge 3: RF optimization is a complicated process that relies heavily on highly experienced personnel. Therefore, integrators should look to provide an accessible, easy-to-use solution for on-site personnel with limited WLAN knowledge to perform wireless coverage site surveys and to identify and configure optimal RF channels during installation and maintenance.

Another major benefit of using wireless networks in mobile applications is the ability for wireless clients to roam across different BSSIDs within the network. Roaming involves a client device disconnecting from one access point as it moves out of range and dynamically establishing a new connection with a nearby higher signal quality BSSID. However, this process unavoidably generates additional communication latency as clients constantly transition between APs. Industrial applications can only tolerate a very low margin for latency to ensure smooth and uninterrupted data transmission. As a result, WLAN solution manufacturers are required to optimize their products to mitigate the additional latency generated by the roaming process.

Challenge 4: Wireless mobile applications such as AGV automation and control processes rely on stable and highly responsive networks. Achieving millisecond-level wireless roaming handover times therefore becomes a necessity to minimize latency and avoid impact to operations.

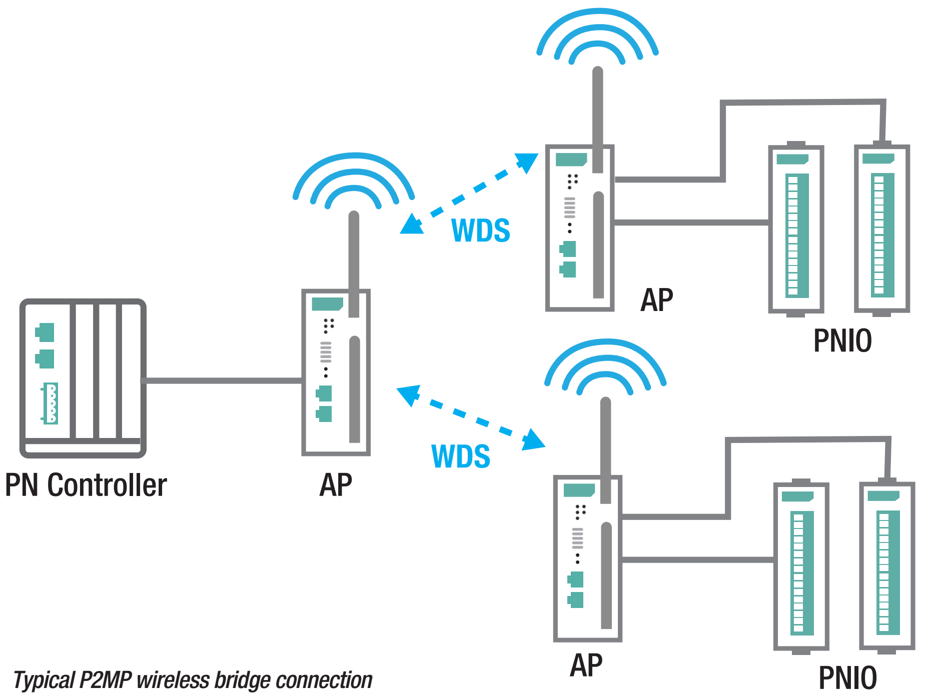
WLAN Infrastructure Solutions

The following section describes how Moxa's AWK Series WLAN technology help address each of the challenges defined in the previous section.

MAC Cloning

Challenge 1: Extend Layer 2 transparency beyond the client's Ethernet interface in an AP/Client configuration so that the connected PNIO is addressable by the PN controller.

The AWK Series' proprietary MAC Cloning technology is designed to extend L2 transparency to a single PROFINET IO device connected to the wireless client by cloning the MAC address of the PNIO to the client it is connected to. By doing so, the PN controller is able to communicate with the PNIO through



Typical P2MP wireless bridge connection

SOURCE: MOXA

the client using its cloned MAC address. MAC Cloning can be used in either Auto or Static mode, depending on the application.

Auto: The AWK client automatically copies the MAC address of the PNIO device connected to its Ethernet interface. Only one device should be connected to the client when using this method to avoid MAC address translation conflicts.

Static: The MAC address of the AWK client is manually configured to use the MAC address of the PNIO. This is useful in cases where multiple devices need to be connected to the same client. While this method supports more than one device to be wired to the client, only one PNIO device can be connected to one client at any given time.

Master/Slave Bridge

Challenge 2: Bridge devices should support multipoint bridge topologies, bridge mobility, and be able to act as a hybrid bridge/AP to connect additional standard Wi-Fi clients.

Master/Slave mode is a variation of the wireless bridge mode exclusively available on Moxa's AWK Series that allows multiple bridges from a single Master device to several Slave client devices, with each Slave client supporting multiple PNIO devices. Moxa's Master/Slave bridge configuration is simple and intuitive, adopting a configuration process similar to setting up an AP/Client connection. This eliminates the complicated and issue-prone setup procedure that plagues conventional bridge setups such as WDS.

In addition, Virtual Access Point (VAP) functionality can be enabled on the designated Master AWK Series device, enabling it to broadcast its SSID to concurrently support additional standard Wi-Fi client connections.

AeroMag

Challenge 3: RF optimization is a large and complex activity that requires experience and knowledge to execute. Accessible tools should be available to enable less experienced on-site personnel to:

1) perform wireless coverage surveys to determine optimal deployment and antenna density, and
2) analyze the wireless spectrum to determine the best wireless bands and channels.

Moxa's AWK Series features AeroMag technology, which helps alleviate the complexity of RF optimization by automatically configuring basic Wi-Fi settings and performing RF spectrum analysis to identify optimal bands and channels. AeroMag is a useful tool throughout the entire Wi-Fi network lifecycle. During the installation phase, AeroMag helps streamline network operations by dynamically analyzing and adjusting radio channels depending on your current operating environment. When configuring network devices, AeroMag's one-step setup establishes Wi-Fi connections quickly, significantly reducing deployment times.

Moxa's AWK Series industrial WLAN AP/Bridge/Clients support AeroMag functionality in AP/Client mode. Once the RF and channel settings are configured using AeroMag, the device can be switched to bridge mode and will automatically carry over the RF and channel settings.

While AeroMag simplifies the RF optimization process, it does not substitute a full analysis of the wireless environment. To ensure maximum availability and deterministic performance, a complete independent site survey should still be conducted to generate the best wireless coverage and most suitable RF configuration for the target environment.

Turbo roaming

Roaming behavior is configured on WLAN clients. Standard WLAN clients without any roaming enhancements usually maintain an established connection regardless of changes in environment or signal quality. This often results in the device disconnecting before attempting to find the next available BSSID. As industrial applications require seamless communication to avoid interruptions to operations, conventional WLAN client roaming solutions are inadequate.

Challenge 4: Establish millisecond-level wireless roaming to avoid any impact to industrial operations.

WLAN Client products support the proprietary Turbo Roaming technology. This function actively scans the wireless environment to identify and roam to nearby APs with optimal signal quality before the original connection deteriorates beyond a predefined threshold. By constantly monitoring and connecting to the best available AP, Moxa's Turbo Roaming feature increases WLAN reliability and availability through fast millisecond-level roaming handover times.

Turbo Roaming is available in both AP/Client and Master/Slave bridge topologies. A customizable AP signal quality indicator or roaming threshold can be set to cater to different environmental conditions. In addition, the intuitive Turbo Roaming Analyzer utility tool is available to help network designers visualize and confirm that the roaming logic behaves as intended within the set performance margins.

Summary

There are two key challenges to address when attempting to build a stable PROFINET application over a WLAN infrastructure.

1) The selected WLAN solution must support L2 forwarding in different configurations.
2) Wireless latency and jitter need to be minimized to meet the requirements of the PROFINET application.

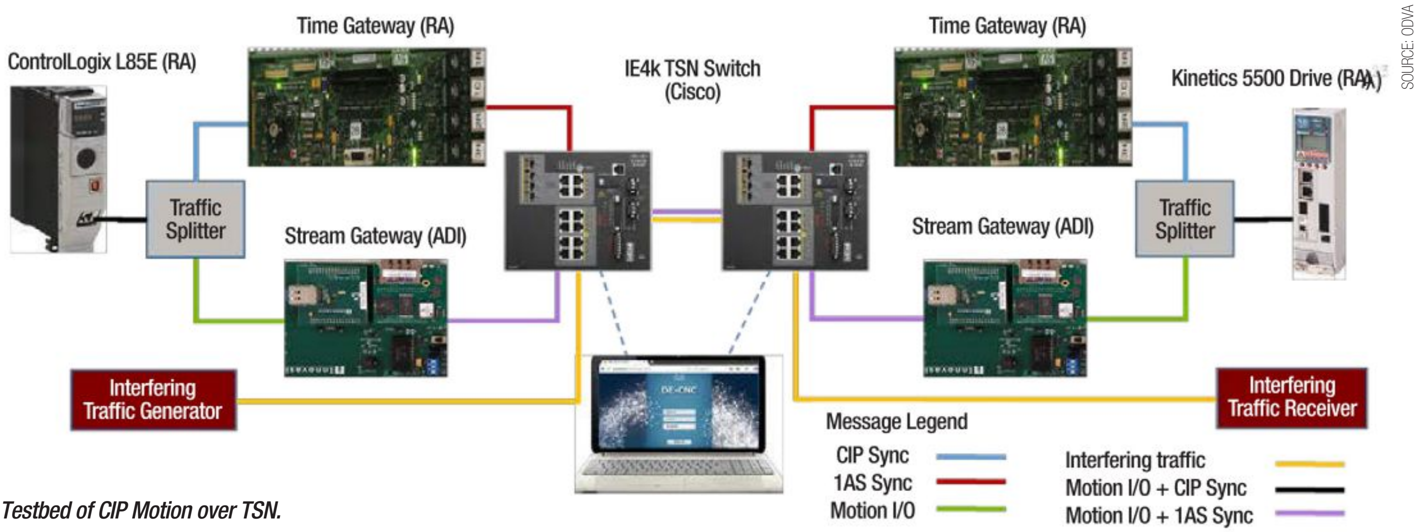
The limitation of L2 transparency terminating at the client level can be overcome by using Moxa's proprietary MAC Clone and Master/Slave bridge technology.

The remaining challenge that comes with designing a stable PROFINET application over WLAN Infrastructure is to account for the impact of additional latency from wireless communication and roaming activities. Moxa's AeroMag functionality simplifies RF configuration by performing automatic spectrum analysis and channel optimization while Turbo Roaming enables millisecond-level roaming capability.

Tony Chen, Product Manager, ***Moxa.***

Test bed results: integrating CIP Motion into TSN network

Test bed consists of TSN-capable network bridges, embedded device prototype gateway boards and CIP Motion capable end nodes (PLC and Drive) with prototype firmware supporting TSN. Based on evaluation results, the text bed demonstrated feasibility of integrating EtherNet/IP into networks deploying TSN.



SOURCE: ODVA

Testbed of CIP Motion over TSN.

THERE HAS BEEN SIGNIFICANT ACTIVITY recently in the market around Time Sensitive Networking (TSN) culminating with both CC-Link IE and Profinet proposing new work items in IEC for TSN extensions to their technologies.

In preparation for work on extending the EtherNet/IP specifications to support TSN, member companies have developed EtherNet/IP TSN test beds. This article will give a report on the lessons learned from the test bed of CIP Motion over TSN.

The test bed consists of TSN-capable network bridges, embedded device prototype gateway boards and CIP Motion capable end nodes (PLC and Drive) with the prototype firmware supporting TSN. The key TSN features supported in this test bed include:

- IEEE 802.1Qbv which specifies a time-aware shaper to schedule traffic. The CIP Motion traffic is inserted into a scheduled part of the network bandwidth.
- IEEE 802.1Qcc which enhances the stream reservation protocol (SRP) and operates at the network control plane
- IEEE 802.1AS which provides peer-to-peer precision time clock synchronization, and is a profile of IEEE 1588 (while CIP Sync uses the default IEEE 1588 profile without peer-to-peer synchronization)

Presented below is an evaluation on the aspects of the TSN adoption method and the performance of TSN adoption for a CIP system. Based on the evaluation results, we demonstrate the feasibility of integrating EtherNet/IP systems into networks deploying TSN. We also propose enhancements and requirements for TSN incorporation into CIP technologies and EtherNet/IP specifications.

Testbed topology and application

As TSN technology mostly impacts critical traffic applications like motion control, we take CIP Motion control as the study case for this testbed. For evaluation of the TSN Scheduling in a converged network, interfering traffic is injected in the system alongside the motion traffic.With reference to test bed terminology, clarifications include the following.

Time Gateway is a prototype implementation that provides the single same time scale for all the components in the system. It is the foundation for scheduling the isochronous type of critical application traffic across the network and application components.

Stream Gateway is a prototype implementation that provides the TSN stream's scheduling functionality based on Stream Conversion. It can integrate the legacy system traffic into the TSN network and protects critical traffic with scheduled transmission slots.

Traffic Splitter could be a managed switch which is configured to route CIP Sync and CIP Motion messages through different paths. It is used on the present testbed because the Stream Conversion and time translation are separately implemented in the independent Stream Gateway and Time Gateway.

IE4k TSN Switches create a TSN network, which implements the prototype of TSN standards including 802.1AS time synchronization, 802.1Qbv (Enhancements for Scheduled Traffic) and 802.1Qcc (Stream Reservation Protocol (SRP) Enhancements and Performance Improvements).

DE-CNC implements prototype TSN configuration interfaces that are compliant with 802.1Qcc (Stream Reservation Protocol (SRP) Enhancements and Performance Improvements) and can configure IE4k TSN Switches via NETCONF.

Controller and drive represent the user motion control application entities. On the present testbed, only one motion axis is controlled.

Traffic Path Clarifications: Different types of traffic are represented in different colors in figure above. The communication paths for these messages are controlled by the Traffic Splitter and IE4k TSN Switch. The static MAC address table is configured for the path control. STP (Spanning Tree Protocol) is turned off since all static MAC address tables are configured for path control. Since the STP is turned off, communication loops in the

► Security System

► Transportation

► Data Center

► Robotics

► Communications

► Factory Automation

Test Case	TSN Features	Interfering Traffic Enabled	C2D Msg mean delay (us)	C2D Msg Jitter (us)	C2D lost packet counts	C2D late packets counts[1]
1	802.1AS time sync	No	208	38	0	0
2	802.1AS time sync	Yes	375	105	0	0
3	802.1AS time sync, 802.1Qbv TSN scheduling	No	578	14	0	0
4	802.1AS time sync, 802.1Qbv TSN scheduling	Yes	578	28	0	0

SOURCE: ODVA

[1] *Lost and late packet counts are reported by the CIP Motion implemented application and reflect packets that were not acted on by the application.*

system are prevented by access-list control configuration in each IE4k TSN Switch.

Test cases and TSN evaluation

We conducted several test cases to evaluate the components' capability and the whole system's performance when integrating TSN technologies into CIP Motion control. The detailed test cases and verification results will be presented in this section.

These efforts are advisory to interest holders who are concerned with the TSN technology benefits and adoption key points for automation control applications.

For all the test cases, common configurations of applications and networks include:

Except as noted, all test cases are run on the "100 Mbits/s" Ethernet for two hours without application connection disconnection.

In test cases, the CIP Motion I/O messages are assumed to have a conservative maximum frame size of "100 bytes", although the variant packet size depends on the specific motion connection parameters.

One CIP Motion axis control is configured with the application cycle of "10 ms", and the TSN network is configured with the network cycle of "10 ms". That is to say, the Reduction Ratio is "1".

Both CIP Motion controller and TSN network components are configured to start their cycles at the integer times of seconds, i.e. "Top of Second". By this means, all the components in the system are aligned to the same start point of cycles.

The interfering traffic is generated by a test tool in order to artificially bring the system to the point of CIP Motion system failure, with selected parameters:

- The packet frame size is of "1500 bytes" on the wire
- The messages are transported on UDP, the transport protocol for CIP Motion I/O traffic
- The message is set with DSCP value of "55", which is same as that of CIP Motion I/O traffic
- The pps (packets per second) is set with value of "8000". With this setting, the interfering traffic roughly needs the network bandwidth of "96 Mbits/s".

Test Case 1: CIP Motion Control System over Time Gateway

In this test case, the TSN network of the testbed is enabled with the 802.1AS time synchronization features. Since the legacy CIP Motion application operates CIP Sync protocol (default profile of IEEE1588), the Time Gateway is needed for translating between CIP Sync messages and 802.1AS time synchronization messages.

The performance data is the same as that of the normal CIP Motion application on a standard Ethernet network. And especially in the side work of observing the internal 1PPS (1 Pulse per Second) signals on the both controller and drives, we measure the time synchronization offset with the value around "200 ns".

This case demonstrates that migration from IEEE 1588v2 default profile to IEEE 802.1AS clock synchronization is viable and can be implemented in a heterogeneous system with both techniques used for different devices.

Test Case 2: CIP Motion Control System over Time Gateway with Interfering Traffic

In this test case, the TSN network of the testbed is configured with Time Gateway as in test case 1 and injected with the interfering traffic in the C2D direction.

The performance degradation (both delay and jitter) validates previous analysis and shows that it is questionable to establish a converged network for both critical applications and interfering traffic with quality of service tags set to the same values.

Test Case 3: CIP Motion System over TSN

In this test case, the TSN network of the testbed is enabled with the features of 802.1AS time synchronization, 802.1Qbv compliant TSN Scheduling and 802.1Qcc compliant TSN Configuration. The TSN Configuration (covering Stream Conversion and TSN Scheduling) is performed in the Stream Gateway and TSN Switch with the stream schedules calculation performed by the DE-CNC.

Stream Conversion is configured in Stream Gateway based on the identification parameters of the application flows of interest and TSN stream identification rules on the bridge networks. Taking CIP Motion I/O traffic for instance, it is communicated on UDP with DSCP of "55" as defined in "3-7.5 Mapping CIP Traffic to DSCP and 802.1D". So, it is preferred to identify the CIP Motion flows by using tuple-set of {IP address, DSCP}.

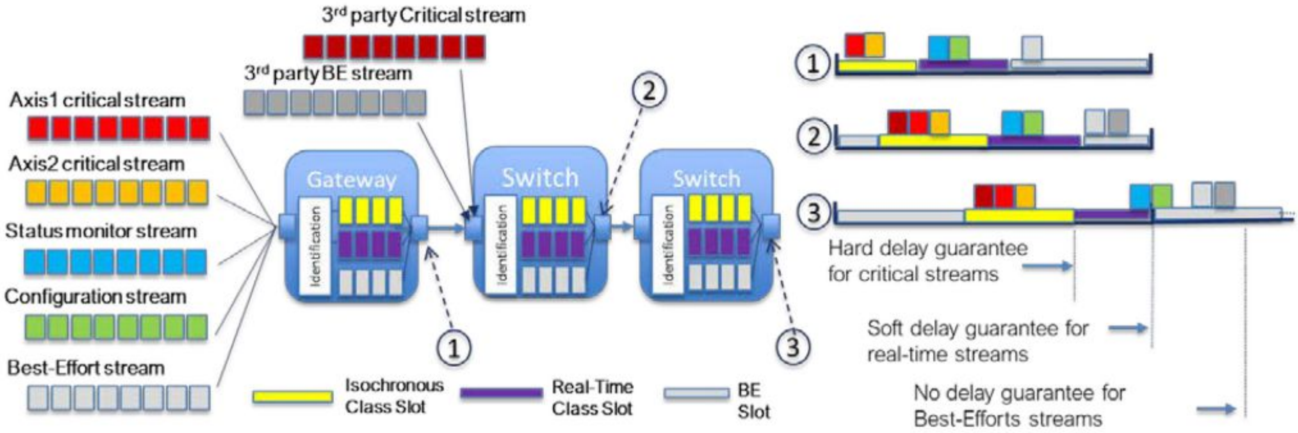
In terms of TSN stream identification, it can be identified by the rules as defined in 802.1CB. Among available TSN identification rules, the "Null Stream Identification" rule is simple and implements a passive stream identification function that operates on a tuple-set of {Destination MAC address, VLAN} of stream packets, which is used to identify TSN streams on this testbed.

TSN Scheduling configuration is compliant with 802.1Qcc and needs the user to input application flows requirements together with the system topology.

The system topology can be automatically discovered by LLDP protocol or manually established by users. By using the DE-CNC on this testbed, the IE4k TSN Switch can be automatically discovered but not the Stream Gateway. So, we have to manually add the Stream Gateway.

After the semi-automatic process of establishing system topology, we will input the user application traffic requirements including cycle time, maximum frame size, maximum latency, earliest transmit offset, and latest transmit offset etc. On this testbed, the prototype CIP Motion control has the requirements of Two-Cycle model for Isochronous Motion Control. Specifically, the C2D transfer is expected at beginning of each application cycle and D2C transfer is expected at the half time point of each application cycle.

With user inputs, the DE-CNC calculates the schedules for the TSN streams converted from user application flows and downloads the configurations (e.g. time slot offset and size) into the TSN Switch via NETCONF. In absence of CUC on this testbed, we had to manually configure the Stream Gateway with the schedule and TSN Talker/Listener traffic specification as calculated by the DE- CNC. Although there is no interfering traffic, the performance indicators are worse than that in



SOURCE: ODVA

Class-based Scheduling Idea.

test case 1. This situation could be caused by:

Factor 1 -- Earliest Transmit Offset (application traffic requirement)

EarliestTransmitOffset, according to 46.2.3.5.5, specifies the earliest offset within the Interval at which the Talker is capable of starting transmission of its frames. As part of the TSN-defined Status group, the network will return a specific TimeAwareOffset to the Talker (within the earliest/latest range), which the Talker uses to schedule its transmit.

Ideally, the CIP Motion C2D message is sent at the beginning of the cycle, i.e. earliest Transmit offset is "0 µs".

However, Stream Gateway needs additional time to process Stream Conversion and Stream Scheduling. So, it will introduce additional delay. This delay was measured as about "300 µs". The earliest transmit offset should be about "300 µs".

Factor 2 -- Latest Transmit Offset (application traffic requirement)

The variable LatestTransmitOffset , according to 46.2.3.5.6, specifies the latest offset within the Interval at which the Talker is capable of starting transmission of its frames. As part of the Status group, the network will return a specific TimeAwareOffset to the Talker (within the earliest/latest range), which the Talker uses to schedule its transmissions.

Ideally, we could determine the latest Transmit offset by adding earliest Transmit offset with the jitter of "38 µs". However, the present DE-CNC only allows the minimum of "300 µs" difference between the earliest and latest Transmit offset. So the latest Transmit offset is set to "600 µs".

Factor 3 – Time slot size (CNC output)

The Latest Transmit Offset and Earliest Transmit Offset that are input by the user will affect the scheduled time slot size calculated by CNC. (Note there are other important factors affecting time slot size, e.g. the application payload size, and the guard band size that is used by CNC to prevent the in-transmission interference traffic). In a preceding hop in the network, the scheduled time slot represents the time span for egressing the packets and in the following hop, there needs a same size of time slot for ingressing the packets.

As all the packets within the time slot are valid for user's time-sensitive applications, the larger the time slot is, the more addition latency (in the worst case, the packet arriving at the last time point of time slot will still be valid and it will endure the delay equal to time slot size) will be introduced during a switch forwarding process. For instance, in our test, it takes the time slot of "130 µs". Compared to strict priority transmission where no time slot is used, the most additional latency could be "130 µs".

Factor 4 -- Max Latency (application traffic requirement)

This is an input parameter depending on applications, e.g. C2D messages are required to arrive at drives before half of the cycle. The looser the value is, the easier it is successfully calculate schedules along the communication path for streams. But a loose value also means a big latency.

DE-CNC has the limitation of minimum "500 µs" for this parameter. Since this value is used in the schedule calculation, it will determine the additional latency that is introduced in the form of the time slot size or switch processing time. Its impact on schedule calculation is determined by the scheduling algorithm of CNC.

Factor 5 -- Switch Processing Time

When scheduled streams go through a TSN Switch, there is an offset between stream ingress and stream egress,reserved for packet forwarding inside switches. In DE-CNC schedule calculation, it takes a variable conservative value for each IE4000 TSN Switch. Node latency is respectively 80 µs and 20 µs.

Based on these impacting factors, we can roughly calculate the End-to-End latency (by assumption of neglecting the link delay) introduced by TSN Scheduling as: Factor 1 + Factor 2 + Factor 3 + Factor 4 + Factor 5 = 300 µs + 2*130 µs + (in form of Factor 3) + (in form of Factor 3) + 100 µs = 660 µs. Analysis of this delay indicates that at least 360µs is due to known limitations of prototyping equipment such as software-implemented functions like switching that would normally be in hardware and configuration parameters not having full accessibility in software tools. While for non-TSN situation, the End-to-End delay (by assumption of neglecting the link delay) is 94 µs.

The addition latency by TSN Scheduling is 564 µs. This value could explain the experiment observation of additional delay introduced by adoption of TSN Scheduling.

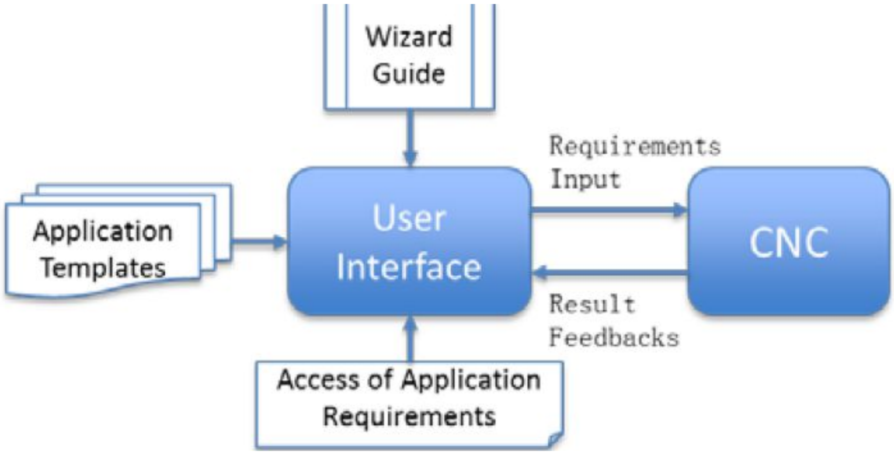
The performance degradation compared to Test Case 1 demonstrates that where there is no interfering traffic (with the same QoS tag values) adding TSN functionality to the network architecture delivers no significant performance benefit to any individual axis and by increasing the mean delay may result in a reduction in the number of axes supported in a given system.

Test Case 4: CIP Motion Control System over TSN with Interfering Traffic

In this test case, the TSN network of the testbed is configured with TSN features as in test case 3 and injected with interfering traffic in C2D direction.

With TSN Scheduling enabled, the critical CIP Motion traffic maintains the same performance even in the condition of interfering traffic. We also tested interfering traffic of "9000" pps (i.e. 108Mbit/s bandwidth). When TSN Scheduling is enabled, CIP Motion traffic still maintains the same performance. While in the case without TSN Scheduling, the communication connection will break down.

With no performance degradation for CIP Motion traffic compared to Test Case 3 we have demonstrated that where there is interfering



SOURCE: ODVA

traffic (with the same QoS tag values) adding TSN functionality to the network architecture can ensure consistent CIP Motion operation in applications where there would have been either performance degradation or system failure using traditional Ethernet technique

Conclusions: TSN Adoption for CIP

In this section, we will conclude the experiment experience and propose the enhancements or requirements for incorporating the TSN technologies into CIP and EtherNet/IP technology.

Time Gateway is required for adopting TSN technology in the CIP Motion control system that uses CIP Sync for time synchronization. On this testbed, we proved the prototype Time Gateway can achieve a high precision of time synchronization between two endpoints and make the legacy system run over the Time Gateway without performance loss.

Time Gateway needs to handle two time domains of default IEEE1588 and 802.1AS profiles on two ports, involving functions of:

- Time Gateway's timing port in 802.1AS profile domain needs to support Peer-to-Peer synchronization at layer 2.
- Time Gateway's timing port in default IEEE1588 profile domain needs to support End-to-End synchronization at layer 3.
- Time Gateway needs to synchronize two time domains to same Grandmaster Clock

The Time Gateway function is preferred to be combined with Stream Gateway function in one implementation entity. Otherwise, the system topology will be complex. The Traffic Splitter has to be used for routing time synchronization messages and control data streams via two separate paths.

Stream conversion & TSN scheduling

Stream Conversion between CIP flows and TSN streams is expected to leverage the "IP address + DSCP" rule. But this method has some issues. This kind of "per-stream" identification is applied for connection with specific peers' IP address. So, it will require too much work for configuring a complex system with many endpoints.

Since multiple CIP Motion I/O connections' messages are not sent from the controller in a fixed order, it would be impossible to assign time slots for each motion connection by the "per-stream" identification and scheduling method. If only referring to the DSCP or alike for identifying certain traffic classes and neglecting the specific endpoints' IP addresses, the "class-based" identification and scheduling mechanism is preferred in the case of multiple CIP Motion axes control.

This is in compliance with the traffic classification by DSCP tag in the "3-7.5 Mapping CIP Traffic to DSCP and 802.1D" of EtherNet/IP specification.

The "Class-based Scheduling" idea includes the identification of traffic class. Another point is about the schedules and guaranteed End-to-End delay for each class of traffic. For instance, each egress port of bridges will assign an isochronous slot for the class of critical traffic. Although the sequence of streams are not fixed, the scheduled isochronous slot can ensure the worst-case End-to-End delay guarantee for all streams of this class.

Regarding TSN stream identification, it needs more study about the simplest rule of tuple-set {(multicast) Destination MAC address, VLAN}, considering potential questions:

- Whether there are limitations when applying the stream identification for the "class-based scheduling" function in bridges. If we should use the extended tuple-set of {MAC address, VLAN, extended tags} like the work in 802.1CBdb?
- Whether the Destination MAC address should be multicast or managed. What are the benefits or challenges for different allocation mechanisms of the Destination MAC address?

TSN Scheduling requires a modification to the CIP Motion isochronous application model; it requires the application cycle be synchronized with the isochronous network cycle. Although the "Top of Second" practice can meet this purpose, it has some limitations. The application cycle period has to be a value that is divisible by an integer into 1 second. That is to say, the cycle period can only be "1/n" second, where "n" is an integer.

The "Top of Second" practice is not a standardized rule, which might cause compatibility issues. Actually in "8.6.9 Scheduled traffic state machines" of 802.1Qbv, definitions already exist for the "AdminBaseTime" and related attributes that can be used to set the network cycle's start point by the state machine.

If taking this approach, all the components need to implement the standard compliant state machines and protocols. Most probably, the applications will be responsible for coordinating the application cycle with the network cycle by the management interfaces.

TSN Configuration and 802.1Qcc

The stream schedule calculation by CNC is an interactive process between applications configuration and CNC calculation. In this process, there are some issues.

The process lacks efficient configuration guidance and most times the user must input multiple different application settings to achieve successful scheduling results by the CNC. It would be desired to design a wizard that can help users to efficiently figure out application requirements either by means of advisory template or parameter tuning suggestions based on CNC feedback.

For now, there are no available interfaces in applications to fetch the required parameters for CNC calculation. Taking the "Earliest Transmit Offset" for instance, we only get the value of about "300 µs" by additional side work. So the next urgent work for application vendors is to define and expose the interfaces for CNC to fetch application requirements.

Future work

This article introduces a testbed that adopts the subset of TSN features (i.e. 802.1Qbv, 802.1Qcc and 802.1AS) into the CIP motion application. It considers existing challenges and suggests a migration path of existing CIP Motion applications using TSN implementations and standards.

In future work, it is desired to improve the testbed by solving known issues and prototyping solutions with TSN enhancements to solve motion application such as Class-based scheduling, 802.1Qbv based application and network cycle start alignment, combined time and stream gateway and native TSN end stations etc.. Based on this evolving testbed, it will be able to verify the TSN migration of EtherNet/IP technology with more comprehensive and solid proofs.

*Paul Brooks and Yi YU, **Rockwell Automation**, Paul Didier, **Cisco Systems** and Jordon Woods, **Analog Devices.***

FRER vs. PRP protocol in Time Sensitive Networks

The availability of a network is the probability that the network is in service and available for use at any instant in time. A comparison between PRP/HSR and FRER solutions discussed in this article, used to achieve static redundancy reveals critical technical differences in both system costs and performance.

VARIOUS PROTOCOLS CAN BE USED TO PROVIDE high availability in EtherNet/IP systems. The protocols focused on in this article are the Time Sensitive Networks (TSN) feature Frame Replication and Elimination for Reliability (FRER) defined in the IEEE 802.1CB-2017 standard; and the Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) protocol, both defined in the IEC 62439 standard.

Critical system applications are often required to maintain high availability of communication network components. For critical infrastructures and time sensitive processes, downtime is never allowed. The protocols focused on here (FRER, PRP, HSR) provide zero recovery time. We will compare and contrast these protocols in reference to network topology, frame structures, network convergence and cost to deploy.

High availability

High availability is based on the concept of availability. The availability of a network is the probability (in percent) that the network is in service and available for use at any instant in time.

High availability is represented as a percentage, usually referred to as the 9s. If the availability metric is specified as five nines, it is understood to mean that the network should be functional for 99.999% of the desired duty cycle (24-hours/day).

Availability is expressed using the following measures of reliability.

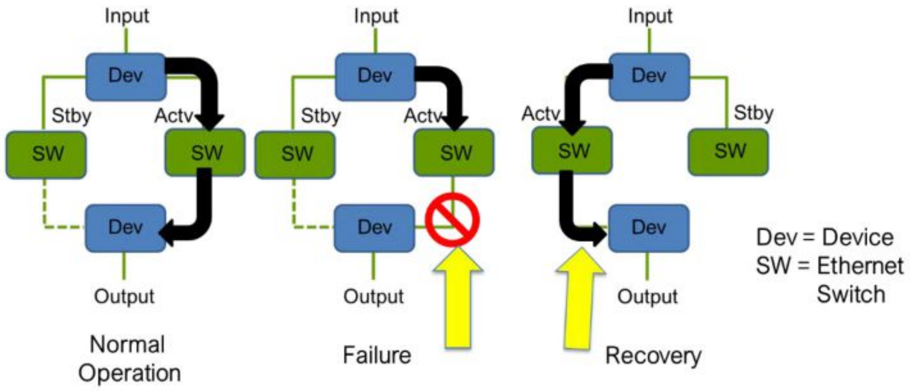
Availability = MTTF / (MTTF+MTTR) (1)

where

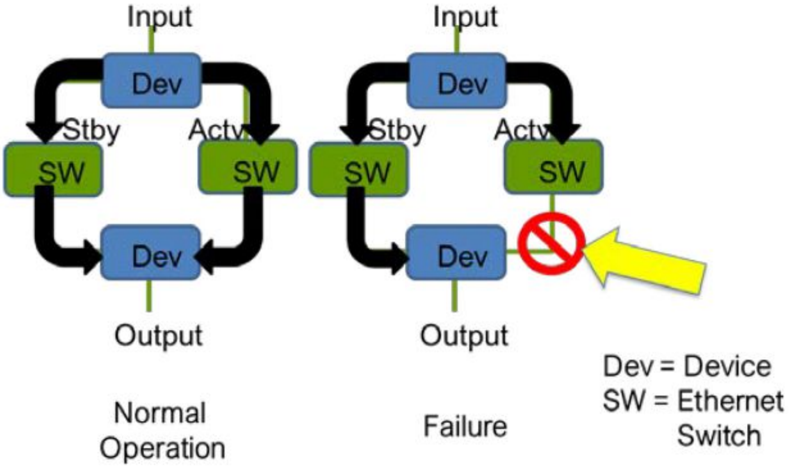
MTTF is the mean time to failure; a measure of the reliability of a network, otherwise known is its failure rate. The MTTF is the interval in which the network or element can provide service without failure.

MTTR is the mean time to repair; a measure of reliability that represents the time it takes to resume service after a failure has been experienced.

As equation above shows, the availability of a network can be increased by designing network elements that are highly reliable (high MTTF), and/or by reducing the time required to repair the network and return it to service (low MTTR).



Dynamic Redundancy.



Static Redundancy.

SOURCE: SCHNEIDER ELECTRIC

Since it is impossible to create networks that never fail, the key to high availability is to make recovery time as brief as possible. Availability is increased in networks by introducing redundancy.

Redundancy

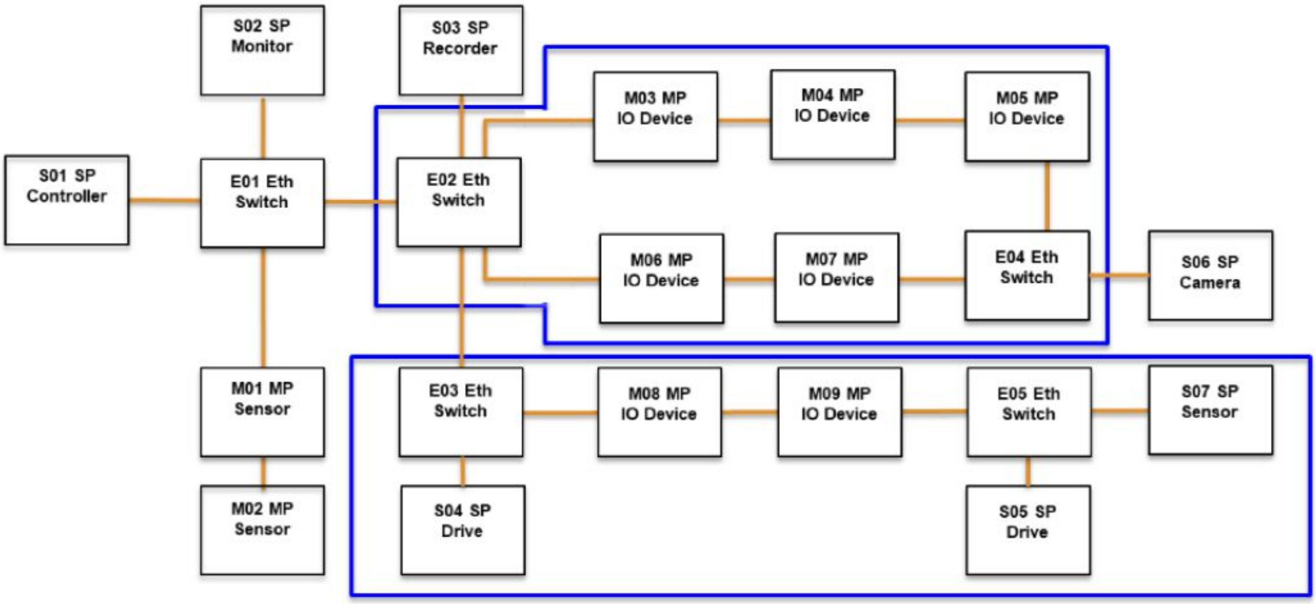
High availability can be achieved economically by using techniques that detect points of failure and avoid service interruptions through redundancy in the system. There are two forms of redundancy, dynamic and static.

In dynamic (standby) redundancy the replicated components activate after a failure has been detected. Dynamic redundancy does not actively participate in the control. Switchover logic determines when to insert and activate redundancy.

In static (parallel) redundancy the replicated components are active concurrently. Static redundancy usually participates in the control. No special processing is needed on errors. This provides bumpless (0 ms) switchover, with continuously exercised redundancy and increased point-of-failure detection with fail-safe behavior. Static redundancy is provided at the cost of duplication.

The two set of protocols discussed here provide Static Redundancy. They are:

- Parallel Redundancy Protocol (PRP) and Highly-available Seamless Redundancy (HSR) protocol, both defined in the IEC 62439-2 standard;
- Frame Replication and Elimination for Reliability (FRER) defined in the IEEE 802.1CB standard.



SOURCE: SCHNEIDER ELECTRIC

Sample Target Solution

A Sample Target Network shown above will be used as illustration for the comparison of PRP/HSR and FRER.

The Sample Target Network is a complex network consisting of the following: a basic Star network centered around the E01 Ethernet Switch; A Ring network with the Ethernet Switch E02 as the Head of the Ring; and a Line network with Ethernet switch E03 at the Head of the Line.

The Sample network includes control applications consisting of Single Port Sensor and Drive devices (Sx), Multiple Port Sensor and IO devices (Mx), Ethernet Switches (Ex), and cables. A video monitoring network (Camera, Monitor, and Recorder) has be converged with the control network.

IEC 62439-3 PRP/HSR Solution

The IEC 62439-3 standard specifies two redundancy protocols designed to provide seamless recovery in case of single failure of an inter-bridge link or bridge in the network, which are based on the same scheme: duplication of the LAN, and/or duplication of the transmitted information. Further improvements in recovery time require managing of redundancy in the end nodes, by equipping the end nodes with several, redundant communication links. In general, doubly attached end nodes provide enough redundancy.

Conversion of the Ring

The conversion of the Sample Target Network the Ring portion of the network will be converted to an HSR Network. The Multiport Devices will be converted to Doubly Attached Nodes with HSR Protocol (DANH) and will stay arranged as a ring. These Dual Attached Nodes within the ring are restricted to be HSR-capable bridging nodes, thus avoiding the use of dedicated switches.

Single-port Devices, known as Singly Attached Nodes (SANs) cannot be attached directly to the ring, but need attachment through a Redundancy Box (RedBox). Ethernet Switch (E04) will need to be replaced with an HSR Redundancy Box (R06) to connect the Single-port Camera (S06).

Each DANH has two identical interfaces, port A and port B. For each frame, the source node sends one copy over each of its two ports. The source node removes the frames it injected into the ring. Each node (between source and destination) relays a frame it receives from port A to port B and vice-versa, except if already forwarded. The destination node consumes the first frame of a pair and discards the duplicate. If the ring is broken, frames still arrive over the intact path, with no impact on the application. Loss of a path is easily detected since duplicates cease to arrive. HSR is not defined in this CIP specification but defined in the sub-clauses 5 and 7 of the IEC 62439-3 standard (IEC 62439-3:2012-7).

Star and Line Networks

The Star and Line Networks will be converted to two duplicate line networks and implement the PRP redundancy protocol. The PRP redundancy protocol implements redundancy in the devices such as Double attached nodes implementing PRP (DANPs) and Redundancy Boxes (Red Box).

A DANP is attached to two independent Local Area Networks (LANs) of similar topology (LAN_A [Blue] and LAN_B [Red]) which operate in parallel. One DANP (a source) sends the same frame over both LANs to another DANP (Destination) who receives it from both LANs, consumes the first frame and discards the duplicate. The same mechanism of duplicate generation and rejection can be implemented by a Red-Box. A Red-Box does the transition between a Singly Attached Node (SAN) and the doubled LANs (LAN_A and LAN_B). The Red-Box mimics the SANs connected behind it (called VDAN or virtual DANs) and multicasts supervision frames on their behalf. The Red-Box is itself a DANP and has its own IP address for management purposes, but it may also perform application functions.

The two LANs are identical in protocol at the MAC-LLC level, but they can differ in performance and topology. Transmission delays may also be different, especially if one of the networks reconfigures itself, for example using RSTP, to overcome an internal failure. The two LANs follow configuration rules that allow the network management protocols such as Address Resolution Protocol (ARP) to operate correctly.

The two LANs shall have no connection between them and are assumed to be fail-independent. Redundancy can be defeated by single points of failure, such as a common power supply or a direct connection whose failure brings both networks down. Refer to the installation guidelines in the IEC 62439-3 standard (IEC 62439-3:2012-7) to provide guidance to the installer to achieve fail-independence. PRP is not defined in the CIP specification but defined in the sub-clauses 4 and 7 of the IEC 62439-3 standard (IEC 62439-3:2012-7)

IEEE 802.1CB FRER Solution

FRER is a static (parallel) redundancy high availability capability as defined in the IEEE 802.1CB-2017 standard. This solution is illustrated by transforming the Sample Target Network into an FRER supported network.

The additional network interconnections needed within the network are representing by the dashed lines. These interconnections change an existing network into a Mesh network.

FRER provides increased reliability (reduced packet loss rates) for a Stream by using a sequence numbering scheme, and by replicating every stream packet in the source. FRER also eliminates those replicated stream packets in the destination. FRER provides:

- Packet replication: sending replicated frames on separate paths, and then using inserted identification information to eliminate replicates, reducing the probability of frame loss.
- Multicast or unicast: A path on which a Stream is sent can be a point-to-point path or a point-to-multipoint tree.
- Latent error detection: some means of detecting a failure to deliver copies of each packet is provided at the point that the replicated packets are discarded.
- Interoperability: a small number of controls are provided that make interoperation with other standards possible.
- Backward compatibility: To provide the ability to be connected to a network that is not aware of FRER, and for a network of conformant relay systems to offer these benefits to unaware end systems.
- Zero congestion loss: provide a Stream with zero (or very low) packet loss due to congestion.

The FRER protocol provides increased reliability (reduced packet loss rates) for a Stream by using a sequence numbering scheme, and by replicating every stream packet in the source end system and/or in relay systems in the network. FRER also eliminates those replicates in the destination end system and/or in other relay systems. The devices types described in the standard are:

End Systems (ES): End Systems may contain a Talker component, a Listener component, or both. End Systems are represented by: The Single-Port Devices (Sx): Controller; Drives, Sensor; IP Camera; Camera Recorder; and Monitor.

Relay Systems (RS): Relay Systems will either transfer packets belonging to redundant streams, or act as a proxy Talker or Listener for End Systems not capable of handling redundant streams. Relay Systems are represented by the Ethernet Switch(es).

Relay-End Systems (RES): Relay-End Systems are not defined in the IEEE Standard but are elements within the EtherNet/IP Network. The Rely-End System is created by combining the FRER End system and Relay System capabilities. Relay-End Systems are represented by the Multi-Port IO Device(s) and one Multi-Port Sensors.

PRP/HSR Topology Performance

This section will discuss to operations within the HSR Ring in the sample PRP/HSR network as comparted to a similar operation within the FRER Mesh. One key to the technology is the message flow between the MP IO Device (D08) and the SP Controller (D01).

The message from IO Device (D08) is duplicated along two paths. The messages transition to the HSR Redundancy Boxes whose job it is to transfer the messages to the respective PRP networks. The message traverses the two separate PRP networks until reaching the PRP Redundancy Box supporting the SP Controller (D01).

The messages will also traverse back through the HSR Network to their source to be removed from the network. This is demonstrating the need to account to double the bandwidth for messages within an HSR Network

One message traverses 8 hops, while the second message only traverses 7 hops. The one message will arrive at R01 first and be selected to generate the message to the D01 controller. The other will be dropped once it reached R01, as it has arrived later.

An error may occur within the HSR Ring. The error in this example is a break in the cable between R02B and D06 MP IO Device.

The message from IO Device (D08) is duplicated along two paths. One message has stopped transitioning due to the cable break, but the second message continues to the HSR Redundancy.

One message continues to traverse the 8 hops, while the other has been stopped. The first message will be used this time by R01 since it is the only message to arrive, though it will arrive 1 hop later.

Device	Sample	IPRP/HSR	TSN-FRER
Single-port Devices [Sx]	3500	3500	3500
Multi-port Devices [Mx]	9000	9900	9900
Ethernet Switches [Ex]	5000	5000	5500
Red Boxes [Rx]	0	7700	
Cable	1050	1300	1150
Total	18550	27400	20050
Cost Difference		48%	9%
[(S-T)/S]			

Cost Comparison: PRP/HSR vs. TSN-FRER

FRER Mesh topology performance

This section describes the use of FRER in an EtherNet/IP network example. The mesh network is supported by any of the Network Control Protocols defined in the IEEE 802.1Q-2018 Standard (i.e. RSTP, MSTP, SBB, etc.).

In this scenario the D08 MP IO Device is an End System (RES) acting as a Talker that transmits a redundant stream to the D01 SP Controller (ES). The Talker proxy will generate redundant streams:

- Sequencing information in frames;
- Replicates each frame passed to it, assigning each replicate a different stream handle, at most one of which can be the same as the original passes unchanged;
- Triggers the sending of one stream (Blue) before the other (Red) to keep the propagation delay within the network the same at the destination (7 hops).
- Encodes the sequencing information into the frame in a manner such that it can be decoded by its peer.

The S01 Ethernet Switch (RS) are connected to the D01 SP Controller and acting as Listener for the Redundant stream from D08 MP IO Device. When the Listener proxy receives redundant streams:

- Extracts and decodes the sequencing information from a received frame.
- Examines this sequencing information in received frames packets and discards frames indicated to be a duplicate of a frame previously received and forwarded; Also monitors the variables to detect latent errors of streams.

An error may occur within the Mesh Network. The error can be illustrated as a break in the cable between So2 Ethernet Switch and D06 MP IO Device. The network recovery time of these control protocols is irrelevant due to the seamless redundancy nature of the FRER protocol.

In this scenario the D08 MP IO Device is an End System (RES) acting as a Talker that transmits a redundant stream to the D01 SP Controller (ES). The Talker proxy will generate redundant streams:

- Sequencing information in frames;
- Replicates each frame passed to it, assigning each replicate a different stream handle, at most one of which can be the same as the original passes unchanged;
- Triggers the sending of one stream before the other to keep the propagation delay within the network the same at the destination (7 hops).
- Encodes the sequencing information into the frame in a manner such that it can be decoded by its peer.

George Ditzel, Ethernet Architect, ***Schneider Electric.***

Lean PLC and HMI system offers facility automation solution

Small and medium facility operators can obtain a comprehensive facility automation system delivering the capabilities they need by choosing the right hardware and software solution. Standard PLCs and HMIs can meet the needs of the facility without complex and expensive server hardware, or a datacenter environment.

A PATIENT CARE FACILITY NEEDED SECURITY but was plagued by the challenges of aging infrastructure. Upgrading to a modern setup of integrated door security and intercom functions was not a question of if, but when. But the facility was hard-pressed to achieve the functionality it needed at reasonable cost.

Fortunately for this end user, a systems integrator was able to design and program an ideal system: a lean programmable logic controller (PLC) and human machine interface (HMI) automation system based on IDEC hardware and software—complete with datalogging and enterprise-zone management—without the cost, complexity, and power-consuming burden of server infrastructure in a datacenter.

Legacy system at end of lifecycle

This customer's previous arrangement used hardwired relay logic and an old computer system to control the doors and intercoms. Not exempt from the fate of system lifecycles, these two separate systems—one for door security and another for call connectivity—had served their purposes well for the facility but were becoming increasingly prone to the frailties of aging equipment.

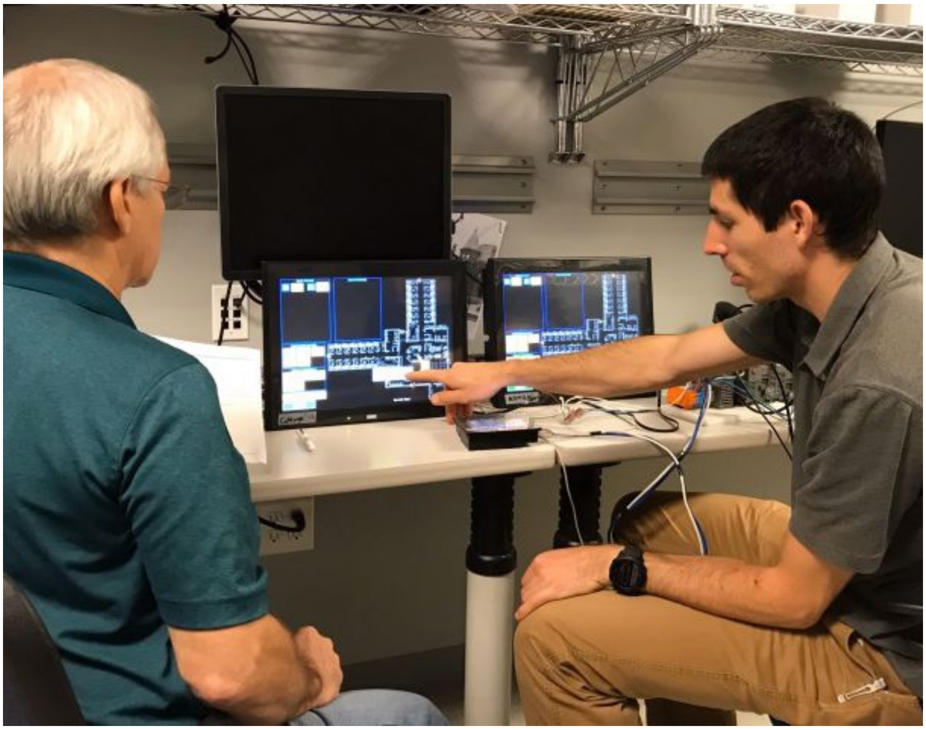
The difficulty for the facility was not finding a system to meet their technical needs as the industrial control systems market is dominated by overdesigned hardware and software solutions able to translate data across languages, protocols, networks, and platforms. Some were relatively open, while others were proprietary and industry-specific.

Instead, the challenge was finding the required functionality in a user-friendly platform, designed to fit their requirements without unneeded frills. The facility needed to combine the door security and intercom systems to operate in tandem and ensure accurate logging of all events, but they did not want a proprietary, overdesigned solution.

Additionally, they needed a system that would recover quickly following a power failure and come back online more rapidly than those using enterprise servers.

Capable PLCs and HMIs

To meet their goals, facility personnel engaged the help of an integrator with prior experience using IDEC PLC and HMI hardware.



SOURCE: IDEC CORPORATION

Integrator configures MicroSmart PLCs and HMIs to meet door security and intercom requirements.

After brainstorming with the stakeholders and engineering a prospective system architecture, the team confirmed MicroSmart FC6A PLCs and HG series HMIs would meet the precise needs of the facility.

The team took advantage of the MicroSmart's multi-communication protocol capability:

- To translate ASCII RS-232 serial data sent and received by the existing administration building intercom master
- Modbus TCP/IP data used to connect PLCs to each other for transfer of information and passwords
- Ethernet was also used for communication between the deployed PLCs and HMIs

HG series HMIs offer built-in event logging, which the team configured so the primary administrative HMI kept a record of event history for viewing on the facility's PC. Because all monitoring, control, and historizing functionality was performed by the PLC and HMI, system recovery following loss of power was quick, typically requiring only about 10 seconds. This is in contrast to a system architected with a PC-based HMI, where reboot times could range into minutes.

It was necessary for control functions to be available from HMIs at each local building and also from the main administration building, coordinated so they would not interfere with each other. This included all door control, alarm and motion device monitoring, and intercom connections. For example, if a call was taken from the administration building, the cottage HMI would show the call was active and no longer needed to be answered.

Therefore, the team created a system design with PLC and HMI at each location, and then networked the two locations together. One PLC interfaces with the intercom system, which also uses its own network connections. In case of network communication loss between the administration building and a local cottage, each cottage control area maintains full control of its equipment. This approach provides the required control even if there are localized failures.

The integrator also incorporated multiple digital devices into the automation system architecture. Each resident room has a call button, multiple indicator lights, a magnetic lock bond sensor, and a keyswitch.

When a resident requires assistance, they press their room's call button, which engages a digital input (DI) at the local cottage PLC. That sends a confirmation to the resident that their request has been received by energizing a digital output (DO) to illuminate a band around the button. The PLC simultaneously sends a signal over the Ethernet network to the cottage's HMI, and to the master PLC and HMI in the administration building.

It is then up to an operator, either in the cottage or administration building, to respond to the call request by pressing a button on the HMI. If the call is answered from the cottage, the local PLC sends an Ethernet command to the cottage IP intercom master to establish a link with the resident's intercom where the call was placed. If the call is answered from the administration building master HMI, the master PLC sends a serial ASCII message over the RS-232 interface to the analog intercom master to establish a connection with the cottage IP intercom master, which connects to the resident's intercom.

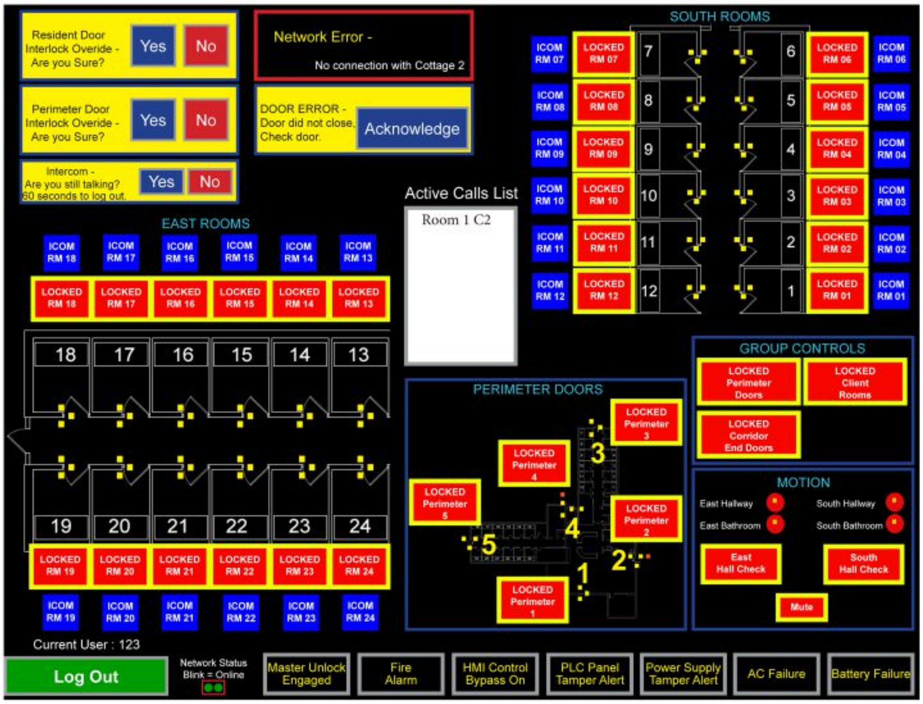
Once the endpoints of the intercom are connected, the PLC energizes a DO illuminating a green light in the resident's room to notify him or her that the call is active. Depending on the call, the operator has the choice to unlock the resident's door (de-energizing the magnetic lock device holding the door closed) or to end the call, activating either via an HMI touchscreen button. A door unlock command triggers the cottage PLC maglock DO, and a command to end the call is routed over the network to the intercom devices in the same manner as when the call was first initiated.

The current status of each door with a magnetic lock bond sensor can be monitored at the HMI, and the HMI generates an alarm if a door which is supposed to be locked is found to be open. Each hallway motion sensor status is also displayed on the HMI.

In addition to the ability to remotely unlock a resident's door through the HMI, an operator may also unlock a door locally using a keyswitch, which causes the local cottage PLC to deenergize the maglock on the particular door. Perimeter doors utilize additional I/O, allowing staff with RFID keycards to unlock exterior doors via badge and card readers. The card readers reside on a separate network and, if presented with proper credentials, trigger a DI detected by the local cottage PLC, causing the appropriate door maglock to disengage.

All of the call request, call answer, remote unlock, keyswitch unlock and card reader unlock events are stored in the HMI's native database and are viewable on the HMI or via the administration PC.

As important as it is to prevent unauthorized door unlocks, the team also needed to ensure safety of residents and personnel in the case of a catastrophic event. To achieve this, the integrator connected the fire alarm for each building into the PLC network. As this is a multi-building deployment, only the doors in the building impacted by a fire are unlocked, while the other buildings maintain normal operation.



Resident Door Interlock Overide - Are you Sure?

Perimeter Door Interlock Overide - Are you Sure?

Intercom - Are you still talking? 60 seconds to log out.

Network Error - No connection with Cottage 2

DOOR ERROR - Door did not close. Check door.

Active Calls List

Room 1 C2

Current User : 123

Network Status Blink = Online

SOURCE: IDEC CORPORATION

HMI screenshot based on geographical CAD drawing layout indicates door lock, motion detection, and call status of several resident rooms and hallways.

Upon a return to normal conditions and when the fire alarm condition has been cleared, an operator presses the fire alarm reset button on the HMI to resume the standard door lock protocol

Programming flexibility

The IDEC Automation Organizer software includes a rich variety of graphical and programming functions and features. It is also easy to use, customize, and modify.

This benefited the team, as shortly after the system went "live" in full operation, the end user decided a different HMI arrangement would suit them better. The integrator was able to make some quick adjustments in the HMI designer and produce a set of graphics directly in line with the site CAD layout, which was the arrangement the end user preferred.

Added benefits

To prevent unauthorized system access, the integrator created a database capable of allowing access by over 100 authorized users, with password protection. A user must be logged in to answer calls or unlock doors from the HMI.

After the signed-in user logs out or an auto-timeout period elapses due to inactivity, the HMI reverts to view-only mode, requiring an operator to log in prior to allowing user control. The user repository and the previously mentioned event log database are features of special note that are normally only available in PC-based platforms.

Interfacing directly with the facility's legacy analog TouchLine intercom was possible because of the built-in communication capabilities of the IDEC PLC. This is noteworthy in any PLC, let alone in a compact model. Most compact PLCs support fewer protocols and might require separate gateway devices to translate additional protocols, adding to hardware and configuration complexity and cost.

Into the future with confidence

The team was able to architect an agile automation system using MicroSmart FC6A PLCs and HG series HMIs to meet the needs of the facility without complex and expensive server hardware or a datacenter environment. The programming is easy to configure, adjust, and scale—and the automation system comes back online quickly following a power failure, a key feature for the end user.

Following the success of this project, the end user is eager to deploy similar setups in their other facilities. This deployment serves as an example of the advanced automation and datalogging possible without the implementation of a high-cost, maintenance-heavy, and slow reboot server infrastructure. IDEC PLC and HMI products provide most of the capabilities of such a system, and added benefits important for this facility.

Scott Hudson, Production Resources, and Gregory Hess, ***IDEC Corporation.***

Gateway

HMS Networks: To enhance control and cabling, a new line of Anybus Communicator high-performing gateways can be used for connecting devices and machines to industrial networks using EtherNet/IP.

All 2nd generation Communicators are powered by the Anybus NP40 industrial network processor used in all HMS' embedded solutions, which ensures that the Communicators will match demanding requirements in terms of performance, reliability, and security. Depending on use case, data cycle times are up to 10 times faster than with the first generation Communicators thanks to the new hardware and software.

Users can also benefit from significantly increased data exchange support as up to 1,448 bytes can be transferred from the connected PLC to the gateway, as well as from the gateway to the PLC.

Control cabinet inverters

NORD Drivesystems: The NORDAC PRO SK 500P frequency inverters are equipped with an integrated multi-protocol Ethernet interface, a multi-encoder interface for multiple axis operation and a USB interface for voltage-free parameterisation.

The new control cabinet inverters cover rated motor powers from 0.25 to 5.5 kW and high levels of connectivity, functionality and versatility. Various device versions can be optimally allocated to various application requirements. Plug-in control, safety and option modules ensure maximum flexibility and the compact book-size design format enables space-saving installation in control cabinets.

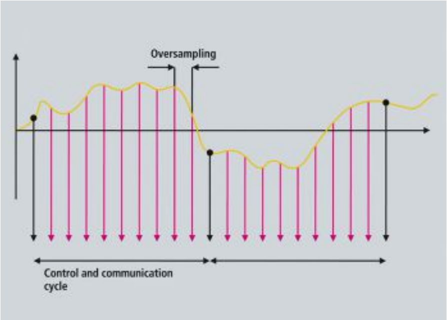
The series is equipped with an integrated universal Ethernet interface that enables the use of the major real-time Ethernet standards via one single interface. Whether for Profinet, EtherNet/IP, Powerlink or EtherCAT, the required protocol can be easily set by means of parameters.

Variable speed drives

Yaskawa: The HV600 family of drives employs the latest advancements in variable speed control for HVAC applications. In addition to its wide product range, users enjoy effortless setup with HV600's high contrast display and connectivity with Android mobile devices. Whether users need simple fan control with integrated BAS communication, advanced bypass control, or multiplex pump control, the HV600 family can help meet a wide range of variable speed needs in building automation.

Standalone HV600 drives include the following features: high-resolution multi-language display with setup wizards and data logging, DriveWizard Mobile for convenient and easy interaction, programming without main power via embedded USB port and enhanced embedded BAS protocol communications.

Multi-axis servo system



Beckhoff: The high-performance AX8000 multi-axis servo system is characterized by extremely high dynamics and very short cycle times. The motor current is scanned in µs cycles and the minimum adjustable EtherCAT cycle time is 62.5 µs. Through the support of oversampling technology, process data can now even be scanned several times within a communication cycle if required and transferred to the controller via EtherCAT.

With the new system, new setpoint values can be transferred every 62.5 µs from the motion controller in the Industrial PC to the servo drive. Comparable control systems usually operate with a cycle time of only 1 ms. Now the AX8000 firmware additionally supports oversampling technology familiar from EtherCAT I/Os.

This enables multiple sampling of process data within a communication cycle with an oversampling factor of up to 128 and the transfer of all data in an array via EtherCAT. This enables the higher-level controller to transmit several setpoint positions or speeds to the drive within one communication cycle, which the drive then follows.

PLCs add EtherNet/IP support

IDEC Corporation: An update adds EtherNet/IP communications to the MicroSmart FC6A Plus PLC. This update provides more options for end users, designers, and OEMs to integrate the FC6A Plus with many types of I/O systems and intelligent automation devices.

The FC6A Plus is already expandable to support up to 2,060 I/O, for controlling machines or small-scale manufacturing operations. With the addition of industry-standard EtherNet/IP scanner capabilities, the FC6A Plus can now connect with, monitor and control any I/O, variable speed drive, motor controls, or other intelligent automation device using this popular industrial protocol. In addition, the FC6A Plus can be configured as an EtherNet/IP adapter, allowing it to interact with other peer and supervisory systems, such as PLCs and HMIs.

All new FC6A Plus CPUs will ship with the latest firmware and EtherNet/IP connectivity already installed and ready for use. For FC6A Plus CPUs already in service, users can obtain the current WindLDR software (version 8.15.0 or later) for free, and then use it to easily perform the upgrade.

Once a new or upgraded FC6A Plus CPU is deployed, Ethernet port 2 can be configured with the EtherNet/IP protocol. This enhanced connectivity gives users new options for architecting their machine and manufacturing operations.

New I/O Modules

WAGO: New 750-564 analog output modules can be configured to feature either voltage or current outputs. These 4-channel modules offer individual configuration, making it suitable for applications that require multiple signal types. Each channel also provides diagnostics that include wire break, short circuit and field power supply information.

With under 3 ms of conversion time, a 16 bit resolution and high accuracy of .05% upper range, the 750-564 offers high performance, precision and resolution for all user applications. These modules also have the ability to adapt to signal types without the need for users to change hardware.

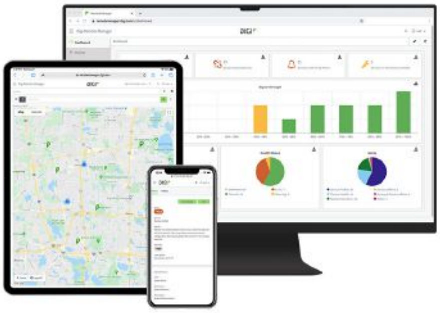
IO-Link smart sensors

Balluff: This new capacitive sensor operates in both IO-Link or standard mode. Balluff designed the new block-style capacitive smart level sensor with IO-Link for applications with highly conductive fluids like acids and bases, using smart level 50 technology to compensate for foam and deposit build up. And thanks to its IO-Link interface, it delivers expanded application and setting options.

IO-Link's automatic parameter setting allow the user to see the upper and lower hysteresis values allowing easy and precise adjustments that aren't possible with a potentiometer. Once unplugged, the sensor goes into standard I/O mode (SIO).

This capacitive sensor reliably detects fluid levels through non-metallic containers up to 10 mm thick, making it well suited for a wide variety of industries including packaging, food and beverage, metalworking and general factory automation.

Remote manager



Digi International: Digi Remote Manager expands its ability to simplify device deployment and maintenance, ensure network uptime and security, and provides new levels of network management so that the network team is not required to change their business processes to accommodate rigid network tools.

Digi Remote Manager is a cloud-based platform that allows users to manage IoT devices and networks in any environment from anywhere in the world. With the ability to support applications from industrial IoT to branch connectivity, intelligent traffic management and everything in between, Digi Remote Manager unlocks the potential of IoT deployments across the board. It transforms dispersed IoT devices to a holistic IoT network, deriving operational and business value and delivering the secure, resilient network required by organizations today.

Device Configuration, Monitoring and Maintenance are the core of any device management software, but Digi provides key differentiators that simplify processes and provide additional value.

Digital service

Endress+Hauser: Digital commissioning application and Netilion turnover package provides added value services to ensure projects stay on time, on-budget, and up to date on project steps.

The digital service experience enables users to digitize projects for efficiency, eliminating time consuming manual coding and progress reports. Users are able to see project work progress across the field devices startup phases in real-time and can flag any potential issues on the commissioning app. Visibility to issues enables users to reallocate resources to keep the project on time. The web-based application workflow is tailor built to field technician and project manager user's needs for greater productivity.

Instead of manual loop folders, documentation is generated digitally and stored in the Netilion Library digital service application. This paperless storage eliminates manual retrieval to facilitate development of a turnover package complying with project deliverable requirements.

Netilion Library helps users organize asset records, drawings, pictures, files, and turnover package documents. It is a file sharing and data management service for the complete life cycle of an instrument. This saves significant time when carrying out maintenance or engineering activities since the often-tedious search for information is eliminated.

Remote sensor network connections

Maxim Integrated: The new DS28E18 extends links up to 100 meters and minimizes wiring to connect peripheral devices to a host microcontroller. By leveraging a 1-Wire protocol to interface with I2C and SPI-compatible sensors, the DS28E18 reduces complexity by connecting devices using only two wires compared to competitive solutions that require four wires for I2C or six for SPI.

Nowadays, most designers use serial interfaces to connect remote sensors in industrial and remote monitoring applications. However, the most popular protocols are costly and complex because they require up to five external switch extenders to reach devices at distances as long as 100 meters. In addition, some of the interfaces widely deployed today require six cables for connecting multiple extended sensors to a host microcontroller.

The DS28E18 enables both power and communications on a single wire, using Maxim Integrated's 1-Wire protocol to link with I2C or SPI peripheral devices over 100 meters with only two wires. The solution eliminates up to five extender and switch ICs, significantly reducing connection costs and software complexity. In addition, only one programmable I/O port from the host microcontroller is necessary to operate a network with 10 to 20 nodes.

I/O modules

Rockwell Automation: Industrial producers can more easily and efficiently connect to devices in hazardous areas using new Allen-Bradley 1718 Ex I/O modules. The intrinsically safe distributed I/O modules provide EtherNet/IP connectivity to field devices in Zone 0 and Zone 1 hazardous areas.

1718 Ex I/O modules can reduce wiring in industrial applications because they can be mounted in Zone 1, closer to field devices in hazardous areas. The I/O modules can also save space with a compact, chassis-based I/O design that contains the primary power supply and an optional redundant power supply in the chassis.

Different chassis options and slot sizes allow users to scale the 1718 Ex I/O modules to meet a wide range of system requirements. Add-on Profiles in the Studio 5000 Logix Designer application help ease configuration of the modules. And a dual-port EtherNet/IP adapter that enables a Device Level Ring (DLR) topology can help improve network resilience.

The 1718 Ex I/O modules are designed for hazardous applications found in industries like chemical, oil and gas, and food and beverage. An ATEX-certified enclosure is required for the 1718 Ex I/O modules to be mounted in an ATEX Zone 1 area.

I/O modules

HARTING: The RJ Industrial MultiFeature series provides integrated blades, which shorten the individual strands to the correct length when closing the connector. A built-in side cutter completely eliminates a time-consuming work step and the assembly is more than 25% faster.

While the classic RJ45 was not sufficient for every industrial requirement, the MultiFeature series meets all the requirements and challenges of a tough operating environment. While the classic RJ45 was a telecommunications development that was not enough for every industrial demand, the new units can cope with all the requirements and challenges of a hard-operating environment. Safe Cat. 6A performance, IP20 and IP65/67 housing combined with PoE power supplies IEEE802.3af (PoE 15.4W) / IEEE802.3at (PoE 25.5W) / IEEE802.3bt (PoE 100W) supply data and power for any device.

The suitability for flexible and solid wires from AWG 26 to 22, the robust cable fastening and angled connectors with variable cable outlet direction are further features with great benefits for customers.

Gigabit cellular router

Contemporary Controls: The EIGR-C3 VPN router allows for cellular, secure VPN connection to remote sites where a wired connection is not an option. The EIGR Series gigabit IP routers allow users to separate their IT and OT infrastructure, with VPN models allowing secure remote access to devices at a job site.

The EIGR line has been expanded with the introduction of the EIGR-C3, a 4G LTE cellular router that has been certified and approved for use on Verizon networks. It is a high-speed router that links cellular to 10/100/1000 Mbps Internet Protocol (IPv4) networks — passing appropriate traffic while blocking all other traffic.

One network is the local-area-network (LAN); the cellular is the wide-area-network (WAN). It also has an Ethernet port that can act as the WAN if cellular access is not required. The built-in stateful firewall passes communication initiated on the LAN-side while blocking WAN-side initiated communication. With Port Address Translation (PAT), LAN-side clients can access the Internet.

The EIGR-C3 incorporates a built-in CAT1 cellular modem, a real-time clock, and OpenVPN client functionality compatible with the Cloud-VPN service from Contemporary Controls. The EIGR-C3 operates over a 0 to 60°C temperature range and the EIGR-C3X operates over the –40 to +75°C range.

The router comes with a Verizon SIM pre-installed. Data plan options for 1GB, 3GB and 5GB monthly use are available. Depending on the application requirement, a plan that allows data overage (with overage charges) or a plan that prevents overages by shutting down data after reaching a monthly data limit can be selected. Static IP options are also available if required.

Multi-protocol drives

Control Techniques: High performance Unidrive M700 and M702 drives are now available with enhanced multi-protocol Ethernet ports that support PROFINET RT as well as EtherNet/IP, Modbus TCP and Control Techniques RTMoE (Real Time Motion over Ethernet). The new ports have the words "Multi-Protocol" printed next to the Ethernet sockets, the prior versions that do not support PROFINET RT do not have this marking.

This new hardware is being incorporated in standard drives manufactured on or after August 3rd, 2020. The date code can be viewed on the product label and will be 2032 for the new multi-protocol version. The model number for the drives is unchanged from prior versions.

While Control Techniques' drives have always been multi-protocol in their nature, being able to support Real-Time Motion over Ethernet (RTMoE) simultaneously with Ethernet/IP and Modbus/TCP IP communications, this new variant adds Profinet RT capability to the list of protocols supported by the Unidrive M700 and M702. The changes also bring about performance improvements to the Modbus and EtherNet protocols.

Building automation controllers

Siemens: New Desigo PXC4 and PXC5 automation controllers can help transform buildings into high-performing, energy efficient assets. The new generation of Desigo building automation controllers offers a wide range of benefits for automating small and medium-sized buildings to get the most flexible and scalable building automation.

Thanks to the new, licence-free Desigo Engineering Framework, devices can now be seamlessly integrated in the same framework for intuitive engineering. Features such as open by design for successful integration of different protocols and easy wireless access facilitate building automation. Both controllers were designed to expand and strengthen the Desigo portfolio and focus on one specific automation element - the Desigo PXC4 for HVAC plants and Desigo PXC5 for system functions and integration.

Widget for historical data

B&R: A new widget makes it easier to display historical process variable data in a machine's HMI application. Machine operators can constantly monitor and optimize their processes. A clear overview of machine performance enables early detection of irregularities and helps minimize maintenance costs.

The new OnlineChartHDA HMI element from the mapp View software package gives users valuable insight into how their machines are behaving. Process data is recorded constantly via the machine controller and made available to the widget automatically.

The solution is based on the OPC UA standard. Machine data is retrieved from an OPC UA server and displayed in the HMI application using a standardized interface, so the widget can use data from any device that has an OPC UA server. All settings, including the sampling time and buffer size, are configured on the server.

IP65/67 managed switches

Belden: The OCTOPUS family of managed switches provide IP65/67 waterproof and dust-tight protection as well as ratings for on-board rail, fire protection in trains, railway line use, ship use, and road vehicle use. For high bandwidth applications, the full Gigabit managed versions comes equipped with full Gigabit Ethernet capability on all ports. Some versions support Power over Ethernet (PoE).

Now available in compact models, the OCTOPUS 8TX Managed versions provide an effective solution for a fully manageable switch for mobile applications or cabinet-less installations on machines.

Wireless networking solutions

Westermo: Two LTE routers have been added to the Ibex range of wireless solutions for reliable and secure data communications within rail applications. The Ibex-RT-330 and Ibex-RT-630 are compact LTE routers developed to meet the growing demand for continuous coverage onboard trains, and support applications such as data offloading between stations, monitoring and remote maintenance access.

The LTE routers ensure reliable, continuous, high-speed remote access data communications in extreme operational environments, connecting the moving train with the signalling control centre over a mobile network.

The Ibex-RT-330 is a mobile LTE router offering high bandwidth to support multiple applications, such as data offloading and remote monitoring. The Ibex-RT-630 is a mobile LTE and WLAN router/gateway, which offers high performance and rugged internet connectivity back-up to enable hybrid train-to-ground installations with a single device. Both routers support hardware offloaded VPN, for high performance capabilities.

The routers support LTE CAT-12, which provides ultra-high data throughput and aggregation of carrier frequencies to serve the most bandwidth-demanding applications worldwide. Multiband GNSS (Global Navigation Satellite System) support enables the use of multiple frequencies for extremely high accuracy positioning and deployment worldwide.

Edge computers

Moxa: These new ultra-compact, high-performance rugged edge computers are designed for AIoT computing in extreme environments.

The Artificial Intelligence of Things (AIoT) is bringing AI to new frontiers in industrial applications. To reduce latency, lower data communication and storage costs, and increase network availability, businesses are moving AI capabilities from the cloud to the edge. In outdoor and harsh conditions that are typical of sectors such as mining, oil and gas, smart cities, and utilities, implementing AIoT technologies in real-world applications poses many challenges, including size, power, and environmental constraints.

The MC-1220 Series rugged edge computers feature high-performance Intel Core i7/i5/i3 processor and multiple expansion interfaces. The expansion interfaces can incorporate hardware accelerators, such as VPUs, and support Intel OpenVINO toolkit for AIoT application development.

Designed based on Moxa's extensive expertise in building rugged computing platforms, the computers can operate in a wide operating temperature range and are C1D2/ATEX Zone 2 certified for deployments in outdoor and hazardous environments.

Edge router

Lanner: A new outdoor wide-temperature edge router enables a 4G/5G virtualized, small-cell solution.

The demand within the global small cell networks market has been rising on account of the growing popularity of LTE networks. Small cell networks are essential to the functioning of 4G and 5G networks. And the other way around, the advance of LTE networks has also played a major role in the growth of the global market for small cell networks.

The NCR-1510 Series edge router is designed to be deployed in remote installations with a wide environmental temperature range (-40~70°C) and fanless cooling for many outdoor cabinets.

While initially targeted at vRAN applications, the NCR-1510 Series edge router is designed for industrial site monitoring, Internet of Things (IoT) gateways, and smart city applications as well as private cloud installations, both on-premise and remote.

Railroad evolution: From steam engines to hyperloop

Almost 200 years ago, the Stockton and Darlington Railway started what would soon become a true worldwide web, an interconnected network of railway lines that spans the continents on our planet. Like other networks, it was continously improved to offer larger capacities at higher speeds.

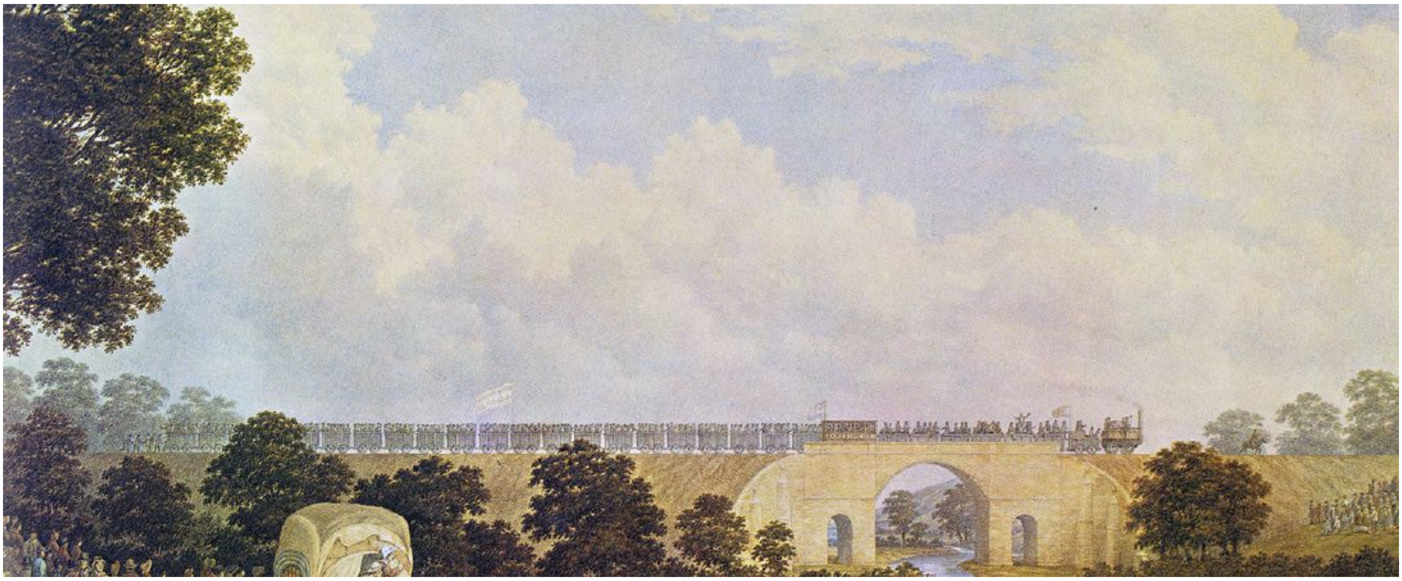


PHOTO: WIKIPEDIA

The Stockton and Darlington Railway

ON 27 SEPTEMBER 1825, THE Stockton and Darlington Railway was officially opened. It was the first public steam railway in the world. This sparked a transport revolution and today there are about 1.1 million kilometres of railway in the world.

The history of rail transport dates back to the 6th century BC. The "Diolkos" was a paved trackway near Corinth in Ancient Greece. Grooves in limestone provided the tracks for wheeled vehicles, which were pulled by animals.

Steam locomotives

This didn't change much for the next 2,500 years. Then in 1820 George Stevenson built the first public railway using no animal power, but a steam locomotive.

His invention was an immediate success, first in the United Kingdom and soon all over the world. Only 50 years after the 25-mile Stockton and Darlington Railway was opened, the First Transcontinental Railroad connected the east and west coast of the USA.

Steam continued to be the dominant railway power system for more than a century. The locomotives were constantly improved and the design reached its peak with the LNER Class A4, which was built in 1935 for the London and North Eastern Railway, and remained in service until the early 1960s. In 1938 the Class A4 locomotive "4468 Mallard" set a world speed record of of 126 mph, which still stands today.

PHOTO: WIKIMEDIA

Electric railways

In spite of this amazing performance, electric engines started to replace steam locomotives after World War II.

Electric railways were first used for inner city transport. In 1879, the German inventor Werner von Siemens built the world's first electric tram line in Lichterfelde near Berlin. A big step forward was the introduction of AC electric locomotives, which offered a much better power-to-weight ratio than DC motors. The first such locomotive was designed by Charles Eugene Lancelot Brown, who later became one of the founders of ABB. Brown's system was used on the first all-electric main line, the Valtellina line in italy, which opened in 1902. However, electrification projects were initially focused on mountainous regions, where electric locomotives gave more traction on steep lines, and hydroelectric power was readily available.

The 1960s saw the electrification of most main lines. By that time, electric locomotives were clearly outperforming even the most advanced steam engines. The LNER Class A4 mentioned above, weighed 170 tons and had a power output of 2,450 hp. By comparison, the German Class E 18 electric locomotive, which was built around the same time, weighed 60 tons less and produced 3,800 hp.

High-speed rail

Japan took a leading role in the advancement of rail transport when it introduced the first first high-speed rail system, the Tokaido Shinkansen, also known as the bullet train, in 1964. It reached a top speed of 130 mph and

PHOTO: WIKIMEDIA

sustained an average speed of 100 mph.

Within the first three years of operation, more than 100 million passengers used the Shinkansen.

Following this success, many countries started to build high-speed rail networks, e. g. the TGV in France, the Frecciarossa in Italy, or the ICE in Germany. All these trains reach speeds of 190 mph and more. China has the largest network, with a total of 17,000 miles of high-speed rail.

Maglev

To reach even higher speeds, operators looked at magnetic levitation (Maglev) trains. Except for the train itself, the system has no moving parts, but works with two sets of magnets. One pushes the train up off the track, and another set moves the elevated train forward. The lack of friction allows higher speeds and faster acceleration.

The concept goes back to 1907, when a US patent for a linear motor propelled train was awarded to German inventor Alfred Zehden. Germany later took a leading role in developing Maglev passenger trains. After a first prototype demonstration at the 1979 International Transportation Exhibition, a permanent, 20 mile test track was built for the so-called "Transrapid". Paying passengers were carried as part of the testing process, and the trains regularly ran at speeds up to 260 mph.

PHOTO: WIKIMEDIA

There were high hopes that the Transrapid would become an international success, once there was a first commercial implementation. That happened in the year 2000,when the Chinese government ordered a Transrapid to connect Shanghai to its Pudong International Airport.

However, other planned projects – in the US, Switzerland, Spain and Iran – failed to materialize, and the German test track was closed down in 2011.

Hyperloop

Like the Maglev, the Hyperloop idea dates back dates back more than a century. Rocket-pioneer Robert Goddard proposed a vacuum tube train (vactrain) for very-high-speed rail transportation already in 1904.

The idea of trains running at hypersonic speeds in partly evacuated tubes gained some popularity in the 1970s, but never progressed beyond the concept stage.

In 2013 Elon Musk, CEO of Tesla and SpaceX, published the "Hyperloop Alpha" paper, proposing a vactrain running from Los Angeles to San Francisco. The concept incorporates reduced-pressure tubes in which pressurized pods ride on air bearings, driven by linear induction motors and axial compressors. Hyperloop was likened to a cross between a Concorde, a railgun and an air hockey table.

The Hyperloop concept is "open source" and Musk has encouraged others to further develop the idea. Several companies and student teams are working to advance the technology. SpaceX has built a 1 mile test track in California, which is used for the pod design competition. During this competition in 2019, a capsule designed by students of the Technical University Munich demonstrated a top speed of 284 mph. An impressive performance, that showed the potential of the vacuum tube train.

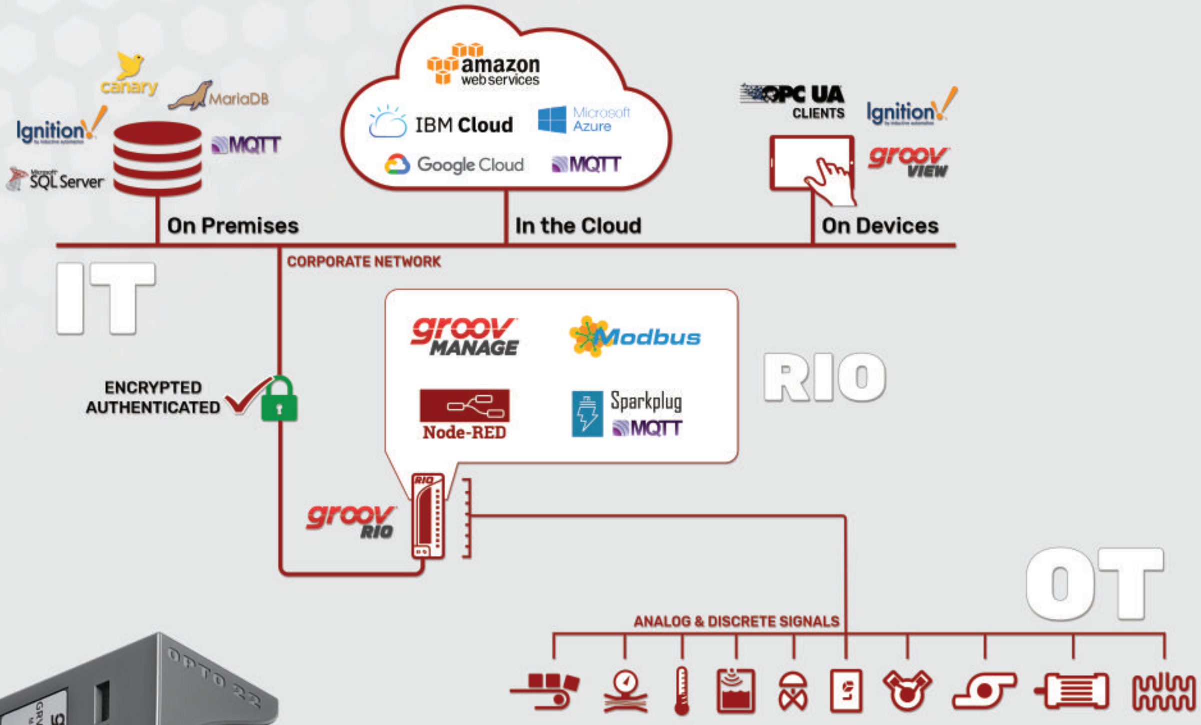
Time will show if the Hyperloop will be the "fifth mode of transport", as Musk called it, or if it will go the way of the Transrapid project.

Leopold Ploner

PHOTO: WIKIMEDIA

groov® RIO

I/O for the IIoT™



On Premises

In the Cloud

On Devices

IT

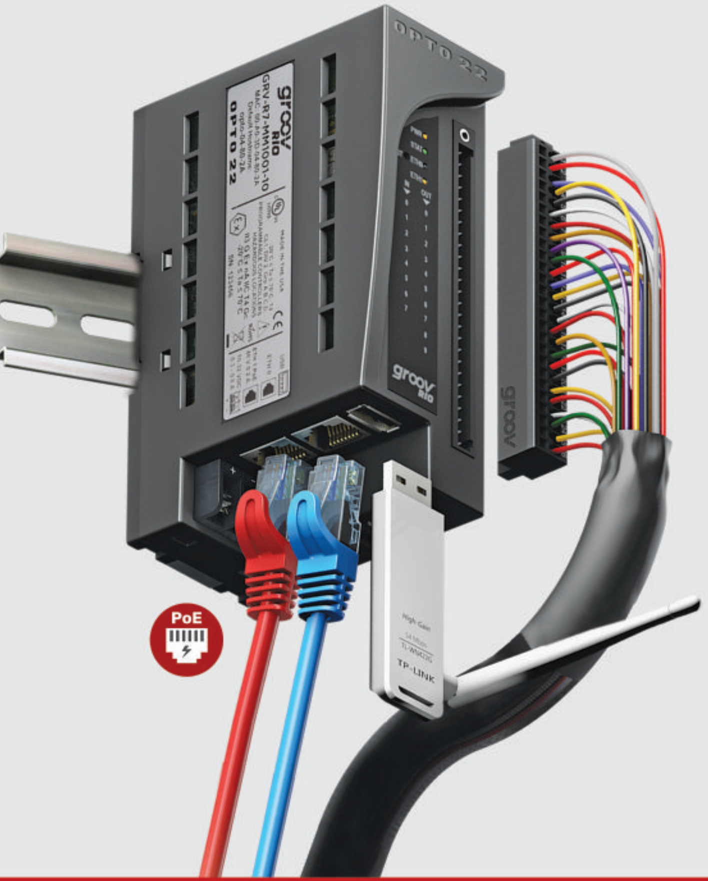
CORPORATE NETWORK

ENCRYPTED
AUTHENTICATED

RIO

OT

ANALOG & DISCRETE SIGNALS



Need field device data on premises or in the cloud? You've got it!

Collect and securely publish I/O data—no PLC or PC needed—to multiple destinations, simultaneously:

- Cloud services
- Ignition® SCADA
- MQTT brokers
- SQL databases
- USB mass storage
- Local power-fail-safe disk

This is *not* your father's remote I/O.

groov **RIO** is a standalone, industrial, PoE-powered Ethernet I/O module that supports nearly 60,000 unique signal combinations from a single unit, including all necessary software to democratize your OT data.

Learn more about *groov* RIO: **info.opto22.com/introducingRIO**

MADE IN THE USA

Made and supported in the U.S.A.
Call us toll-free at **800-321-6786** or visit **www.opto22.com**
All registered names and trademarks copyright their respective owners.

OPTO 22
The Future of Automation.