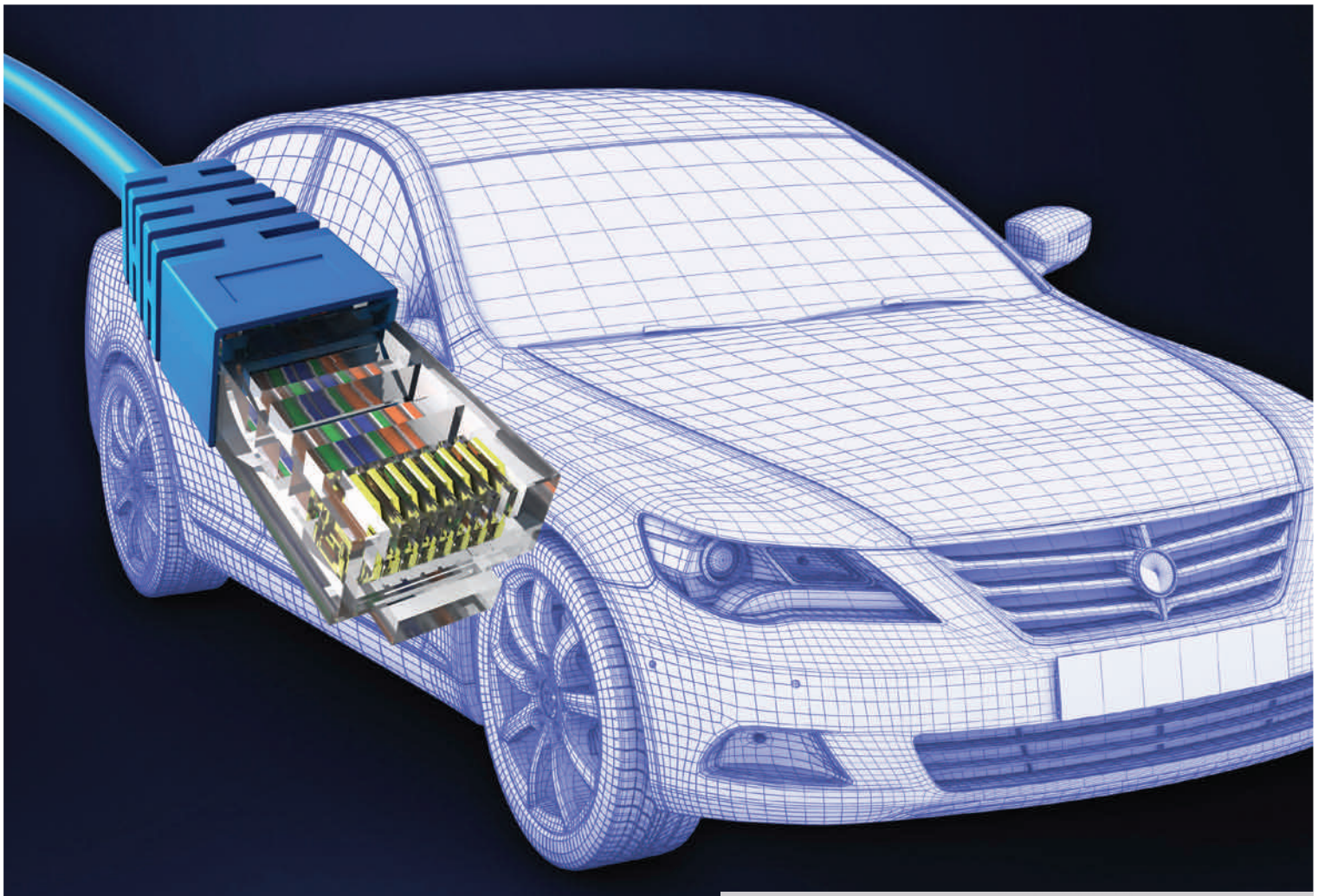
7.2015 Issue 89
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Network Connectivity



Deterministic Ethernet & TSN for Automotive 8

IIoT Reference Architecture 18

Resilient IoT Network Infrastructures 28

Time Sensitive Networks: mission impossible? 32

Power Over Ethernet Procedures 36

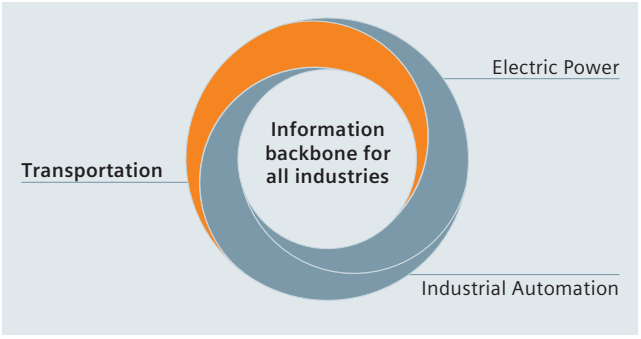
SIEMENS

Rugged communications for transportation systems

E20001-F680-P820-X-7600

With a combined portfolio of RUGGEDCOM and SCALANCE networking products, Siemens is taking a leading role in transportation networks around the world. We offer best-in-class, end-to-end networking solutions for road and rail that are able to withstand the harshest conditions.

Improved mobility, efficiency, safety and sustainability are just some of the benefits enjoyed by Siemens customers.



siemens.com/communications-for-transportation

GET CONNECTED...

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

Focus on security initiatives ...

With the Internet of Things pressing into our consciousness at every turn, technical decision makers are more and more focused on security. And as a result, work is being poured into technical reference architectures that will provide a framework for network security in the future.

Rockwell Automation and Cisco recently announced new additions to their Converged Plantwide Ethernet (CPwE) architectures to help both operations and information technology professionals address constantly changing security practices.

Core to the new validated architectures is a focus on enabling OT and IT professionals to utilize security policies and procedures by forming multiple layers of defense. A defense-in-depth approach helps manufacturers by establishing processes and policies that identify and contain evolving threats in industrial automation and control systems. The new architectures leverage open industry standards, such as IEC 62443, and provide recommendations for more securely sharing data across an industrial demilitarized zone, as well as enforcing policies that control access to the plantwide wired or wireless network.

In this issue, we also are reporting on the new Industrial Internet Reference Architecture (IIRA) developed by the Industrial Internet Consortium. This group, which includes participation of the biggest technology companies in the world, has produced a technical document that will help your organization to better understand the technical requirements, methodologies and roadblocks to adoption. Download a copy here: http://www.iiconsortium.org/IIRA.htm.

According to the Reference Architecture document, it "initiates a process to create broad industry consensus to drive product interoperability and simplify development of Industrial Internet systems that better fulfill their intended uses, are better built and integrated with shorter time to market."

"We have identified what we believe are the major architecture issues and we have examined these issues based on a formal architecture framework. We believe we have arrived at a reasonable statement of what the most important architecture components are, how they fit together and how they influence each other. This first version is an opportunity to gather early feedback from industry participants, especially across industrial sectors, so we can improve it quickly in its subsequent versions."

We hope many of you will also become engaged in this process as well, and create an effective voice for the users of Industrial Ethernet and other networking technologies that are shaping this exciting new future.

Al Presher

Contents

Industry news	4
IoT solution increases safety and efficiency in busy seaports	7
Deterministic Ethernet & TSN: automotive and industrial IoT	8
Real-time historical mobile data collection and reporting	12
Synchronizing mechatronics using FPGAs and POWERLINK	14
Aircraft component manufacturing automation	17
Implementation of an Industrial Internet Reference Architecture	18
Defense-in-depth protection for electrical grid substations	22
Network security concerns extend to production systems	24
Renewing the energy efficiency of existing facilities	26
Building resilient IoT network infrastructures	28
PROFIBUS network provides reliability and robustness	31
Time Sensitive Networking: impact or mission impossible?	32
Reliable fiber optic connections for industrial and outdoor use	34
Using Power over Ethernet procedures for effective designs	36
Mission-critical redundant serial-to-Ethernet data	38
Nonstop IP surveillance using optimized Ethernet networks	41
Secure remote maintenance for automotive manufacturing	44
New Products	45
Private Ethernet	50

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2015**
Deadline for editorial: August 7, 2015 **Deadline for artwork:** August 28, 2015

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, both the printed and online version. 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: map Mediaagentur Ploner, info@iebmedia.com
Tel.: +49-(0)8192-933-7820 · Fax: +49-(0)8192-933-7829
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

Industrial Internet Consortium

The Industrial Internet Consortium is celebrating its one-year anniversary, and the Consortium's first technical deliverable, publishing of an Industrial Internet Reference Architecture.

THE NEWLY PUBLISHED Industrial Internet Reference Architecture (IIRA) document is divided into three parts. The first is a set of "Key System Characteristics" to which a system must adhere, such as upholding privacy expectations, reliability, scalability, usability, maintainability, portability and composability.

The second part is a set of "viewpoints" that enables discussion from different perspectives such as the business, system usage, functional components and implementation. A third part is a set of concerns that span the system as a whole which relate back to the key system characteristics.

Key components of IIoT

The key system characteristics of the Industrial Internet are addressed in three parts. First, there is a context into which the system must fit. Second, there is the actual engineering of the system from conception through implementation. Third is the assurance that the system performs as it claims. This includes, obviously, testing and validation, but it also includes demonstrations of compliance and engineering processes.

On top of these are multiple key system characteristics shown as layers. Of these, three are key to the discussion of Industrial Internet systems because of their criticality in ensuring the core functions, rather than the efficiency, of these functions, of the system:

Safety: the condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

Security: the condition of the system operating without allowing unintended or unauthorized access, change or destruction of the system or the data and information it encompasses.

Resilience: the condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties.

Viewpoints

Having multiple stakeholders involved, each representing unique concerns, calls for a framework to classify the concerns into appropriate categories so that they can be evaluated and addressed systematically across the full lifecycle of the system.

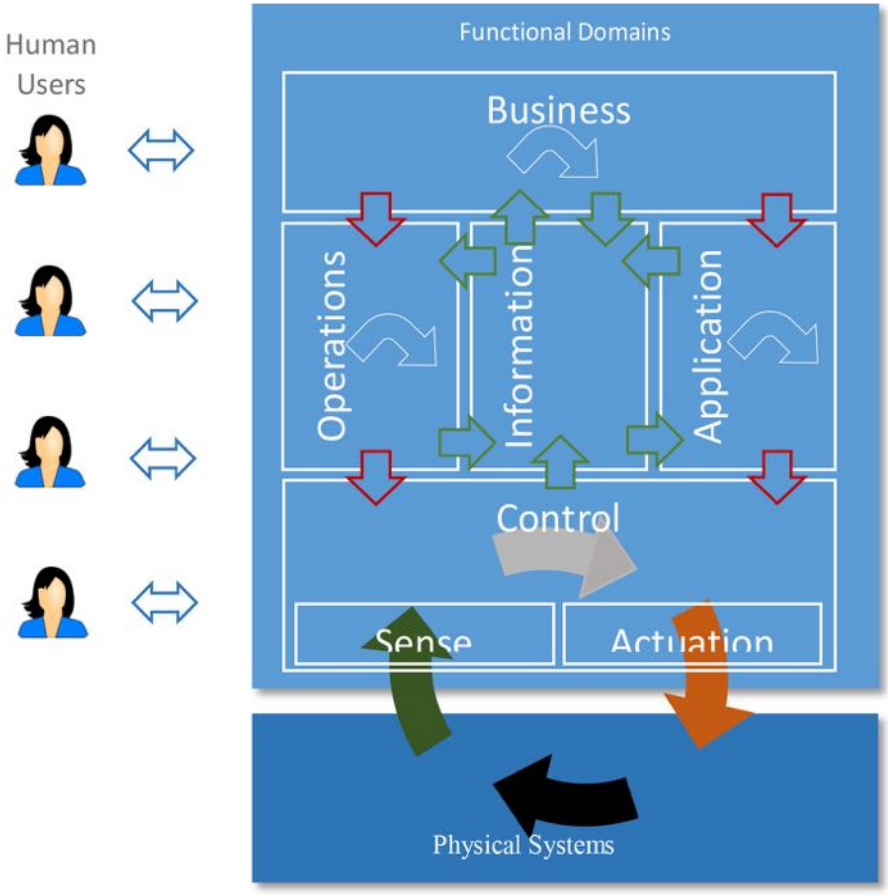
The members of the Consortium have defined an architecture framework that describes the conventions, principles and practices based on ISO/IEC/IEEE 42010:2011 that facilitates evaluation, and systematic and effective resolution of stakeholder concerns, and guides communication about the IIRA.

The document defines four main categories:

- The business viewpoint covers concerns related to the busines
- The usage viewpoint covers how the system is used by operators
- The functional viewpoint outlines the main functional block
- The implementation viewpoint covers deployment details and practices

The functional viewpoint contains the functional blocks that make up the system. An organization developing an Industrial Internet system may not use all the blocks, but should at least consider whether the functional blocks apply in their system.

In other news, the Vocabulary Task Group has produced a glossary of all the terms used in the IIRA. The Use Case team is has delivered a simplified use case template that helps to reveal architectural concerns. On the Testbed front, the Consortium Steering Committee has approved the sixth IIC testbed.



SOURCE: IIC

Chart shows major factors indicated by respondents in the 2014 study that caused data unavailability.

Smart factory testbed

The goal of the Smart Factory testbed is to manage handheld power tools in manufacturing and maintenance environments. This involves tracking and tracing the usage of these tools to ensure their proper use, prevent their misuse and collect data on their status.

Communication and control testbed

The energy testbed re-architects the power grid system into a series of distributed microgrids that control smaller areas and support load, generation and storage. Microgrids will operate independently from the main grid but will still interact with existing infrastructure.

This testbed introduces the flexibility of real-time analytics and control to increase efficiencies in the legacy process of traditional power grids, ensuring that power is generated more accurately and reliably.

www.iic.org

Universal high-speed Ethernet.

PC- and EtherCAT-based control technology from Beckhoff.

www.beckhoff.com/EtherCAT-System

PC-based Control
- bus connection directly to Ethernet port
- software replaces hardware: PLC and Motion Control on the IPC

EtherCAT I/Os
- real-time Ethernet down to each I/O module
- large choice of components for all signal types (IP 20, IP 67)

EtherCAT Drives
- highly dynamic Servo Drives
- integrated fast control technology

IPC
I/O
Motion
Automation

EtherCAT®

New Automation Technology **BECKHOFF**

Test lab for automotive OEMs

A strategic partnership between Belden and ASKOM is delivering a test center for factory floor communication infrastructure, leveraging close cooperation to respond to automotive customer needs.

A NEW AUTOMOTIVE TEST LAB located in the main building of ASKOM in Wolfsburg, Germany, is a joint venture between Belden Inc. and its strategic partner ASKOM, a specialist in communication technology.

The test lab is able to demonstrate a complete communication infrastructure around applications in the factory floor, and was established to meet the increasing demand for closer geographical support from Automotive OEMs and their suppliers - with a focus on the Volkswagen (VW) group.

The lab is equipped with a large range of products from various Belden brands, such as Lumberg Automation, Hirschmann, Tofino Security and Belden. They include EAGLE One security products; MACH4000, MACH1000 and MSP30 backbone switches; MS20/30 field switches; patch cord and IO box connectivity solutions; and HiVision software for industrial network management.

Speaking at the formal opening, Andreas Schleicher, general manager of ASKOM said: "This new test lab allows us to offer a range of services to the automotive industry cluster in Northern Germany and enables us to respond quickly to customer needs. VW and other suppliers can rely on us to test their communication infrastructure networks intensively and train their employees in the most critical technologies for implementing the latest networks."

SOURCE: BELDEN

From left to right: Steve Biegacki, senior vice president Belden sales and marketing, Andreas Schleicher, general manager ASKOM, Wolfgang Schenk, vice president of industrial sales Belden EMEA.

Belden Wolfgang Schenk, vice president of industrial sales for EMEA said: "Our partnership with ASKOM enables us to support VW with Belden technology as well as product training for automotive applications at a location that is close to the production facilities of VW."

Industry news from Belden and ASKOM.

RFID in healthcare expands into smart cabinet systems

Cloud-based RFID cabinet solutions accessed using Web and mobile apps set to grow, finds Frost & Sullivan.

RADIO FREQUENCY IDENTIFICATION (RFID) is rapidly making headway into the healthcare and pharmaceutical industries, especially in assets tracking, supply chain management, and inventory management. In particular, the need for inventory management to reduce instances of loss or misplacement of medical equipment, supplies or drugs, along with efforts to minimise errors and improve patient safety, drives the market for RFID smart cabinet systems.

New analysis from Frost & Sullivan, Market Opportunity for RFID Smart Cabinet Systems in Healthcare, finds that the uptake of RFID smart cabinets is likely to gather momentum over the next three to five years.

"The low infrastructure costs and quick returns associated with RFID smart cabinets encourage their adoption in hospitals," said Frost & Sullivan Healthcare Research Analyst Shruthi Parakkal. "End users prefer RFID smart cabinets with cost-effective architecture that eliminates redundancies – such as multiple paths – and reduces interference."

Unproven business models and resistance to changing the status quo are major factors limiting investments in RFID smart cabinet systems. Since countries decide the frequencies used for RFID according to their spectrum and bandwidth availability, RFID device manufacturers also face the challenge of designing solutions that are compatible across regions.

Moreover, the lack of a long-term vision on the evolution of RFID application from the perspective of policy makers, vendors and end users could stall the development of this promising technology. To pave the way for large-scale deployments, suppliers must focus on technical capabilities such as range of uninterrupted RFID, automation and integrated analytics.

"In the long run, virtual management and managed services that involve minimum capital and overhead expenses will gain traction over the outright purchase of cabinets," added Parakkal. "RFID cabinets with cloud-based integrated analytics that can be accessed through Web applications will become popular, facilitated by the Internet of Things and Near Field Communications."

Continued and growing recognition of the technology's potential to improve outcomes and efficiency in a healthcare environment will keep the RFID smart cabinets market on track towards swift growth.

Market Opportunity for RFID Smart Cabinet Systems in Healthcare is a Market Insight that is part of the Connected Health Growth Partnership Service program. The study focuses on RFID smart cabinet systems that track equipment and medical supplies in a healthcare environment.

It aims to analyse the technological advancements in RFID smart cabinet systems and includes the business models of key market participants in this space. The research also covers the market adoption of RFID smart cabinet systems and discusses the factors that impact such adoption.

Industry news from Frost and Sullivan.

IoT solution increases safety and efficiency in busy seaports

M2M connectivity and digital security technology that leverages IoT communications technology is increasing the safety and efficiency of Latin America's busiest seaports. A telemetry system uses robust modems to collect various ocean data from sensors deployed on buoys, piers and the seabed in the ports.

A real-time weather and oceanographic system provides an ability to monitor waves, currents, water depths, temperature and salinity to enhance port productivity.

M2M CONNECTIVITY IS AN ENABLING technology for an innovative Internet-of-Things (IoT) solution that monitors dynamic ocean conditions to optimize safety and efficiency in Brazilian ports.

Developed by HidroMares, a leading oceanography consulting firm, the real time weather-oceanographic information system (SISMO) monitors waves, currents, water depth, temperature and salinity to improve navigation safety, streamline ship traffic and increase port productivity.

SISMO telemetry system

The SISMO telemetry system leverages robust modems by Duodigit, a provider of telemetry and biometrics technology products, to collect various ocean data from sensors deployed on buoys, piers and the seabed in ports.

The modems use Gemalto Cinterion M2M Modules with embedded Java to process and send data via wireless networks and the Internet to a backend server. Port workers sign on securely to an intuitive interface and use the data to improve real time decision-making and optimize port productivity.

The solution is already deployed in Porto of Açu in Rio de Janeiro state, whose location near Campos Basin is strategic to the petrol industry in that region.

One challenge was creating a cost-effective solution that would ensure reliable communications in the extreme environment of a seaport

"Sampling of oceanographic data is done in extremely hostile environments requiring rugged durability of system components during installation and maintenance. The transmission of real time data demands a robust system that is reliable continuously in all conditions, 365 days a year," said Alexandre De Caroli, Technical Director of HidroMares.

"One of our biggest challenges was designing a cost efficient solution that could ensure reliable communication in the extreme environments of a seaport," said Luiz Henrique Correa Bernardes, Technical Director at Duodigit.

He added that a Java embedded module provides the required durability along with the processing power needed to analyze and store information locally in the device. The solution allows efficient communication as needed, which is critical for cost efficiency and preserving battery power in hard-to-service locations such as seaports.

"Optimizing supply chain logistics and improving productivity in distribution systems is key to the profitability of our increasingly global economy and it also improves fuel economy for positive environmental impact," added Rodrigo Serna, President for Latin America at Gemalto.

*Application story by **Gemalto.***

Deterministic Ethernet & TSN: automotive and industrial IoT

Deterministic Ethernet and Time-Sensitive Networking (TSN) provides a real-time platform for development of Internet of Things (IoT) solutions in automotive and industrial applications. The key is meeting the technology demands of implementing high-bandwidth, open and standard solutions for real-time systems.

THE INTERNET OF THINGS (IoT) is often discussed in terms of the business impact it is having, the exciting opportunities it creates and the growth in global GDP that it drives. But one area where the impact of the Internet of Things (IoT) is not yet fully being felt is that of real-time systems.

IT features such as analytics software and cloud computing rely on open, standard IP or wireless connectivity to gather data. However in the environments of automotive and industrial real-time applications, this type of connectivity is rarely found.

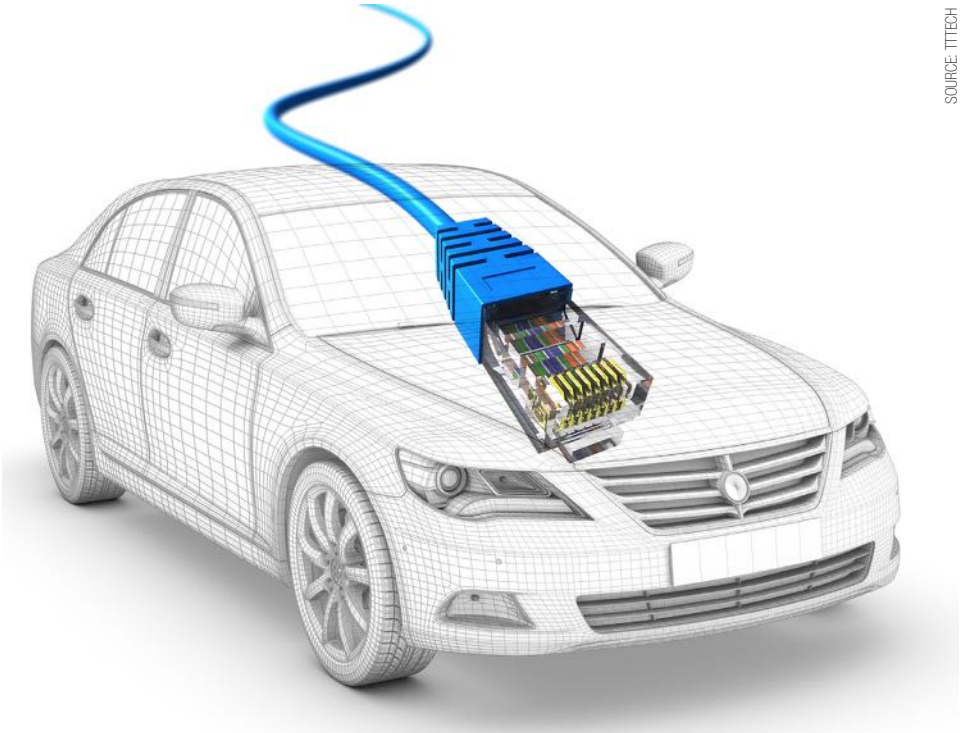
Potential of TSN sub-standards

In industrial automation and in energy production, for example, improved connectivity of robots, wind turbines or substations can lead to big increases in production efficiency, reduced system downtime and human-machine collaboration. To take advantage of the improvements in efficiency, uptime and functionality that IoT can deliver, the underlying networks must provide reliable and deterministic M2M and machine-to-cloud connectivity, at prices that only open standards can ensure.

Similarly in automotive, deterministic connectivity in vehicles will enable advances in remote diagnosis, car-to-X and autonomous driving. In response to the demands for a high-bandwidth, open and standard solution for real-time systems, the Time-Sensitive Networking (TSN) task group was formed in 2012 and is developing a set of TSN sub-standards in IEEE 802.1.

In the search for connectivity, networking technologies often migrate from one sector to another as complimentary solutions and benefits for alternative applications become apparent. This has been demonstrated in the case of the CAN bus protocol, which after being developed initially for in-vehicle communication was widely adopted for use as a fieldbus in industrial automation.

The transition was helped by commercial factors, such as the enviable efficiencies of scale found in the automotive industry, which led to the availability of low cost CAN controllers and processors for industrial customers. This process can be seen again today with Ethernet technologies. The new generation of Ethernet based in-vehicle communication which emerged through IEEE 802.1 Audio-Video Bridging (AVB) is now being developed into a set of fully Deterministic Ethernet standards in IEEE 802.1 Time-Sensitive Networking (TSN) which will play a key role in the Industrial Internet of Things and Industry 4.0.



SOURCE: TTTECH

Current technology developments are moving toward bringing Time-Sensitive Networking (TSN) to the automotive market, by integrating switch IP core technology into a cost-effective ASSP for automotive Ethernet switching.

The focus for automotive and industrial applications has turned to Ethernet with good reason, especially in regard to realizing IoT. Ethernet technology has proven incredibly successful as a ubiquitous method of communication in the IT world.

Ethernet is a very well standardized and open technology that is easily accessible to everyone, provides a wide range of bandwidth and physical layer options, and has significant support in a diverse range of application areas. Because of the open development of Ethernet standards, its technical functions and operational speed evolve rapidly, resulting in low-cost solutions – in particular with COTS (commercial-off-the-shelf) equipment. Ethernet was originally used as a platform for converging divergent IT networks. With a Deterministic Ethernet standard (TSN), automotive and industrial applications can now follow this same route of convergence for all applications, including those which have strict real-time communication requirements.

Ethernet in automotive

Ethernet has been used for automotive applications since 2008, mostly as a method for diagnostics communication and data download. Increasingly, the large bandwidth Ethernet provides compared to other automotive in-vehicle networking technologies makes it an obvious choice for emerging applications such as camera-vision systems and infotainment systems.

There is also a huge potential for Ethernet to be used for backbone network communication throughout the vehicle. This could even include safety critical applications which enable piloted and autonomous driving – a major trend in the automotive industry today.

The automotive industry has particular requirements for in-vehicle networking. For example, network solutions need to

SOURCE: TTTECH

The goal is to integrate a wide range of communication and traffic classes into a single in-vehicle backbone network.

take weight and cost of the cable harness into account and generally be as robust, serviceable, and efficient as possible. For this reason, technologies such as BroadR-Reach for 100 Mbit/s and RTPGE for Gbit/s connections are being developed and standardized. These unshielded twisted single pair cables can drastically reduce the weight and cost of in-vehicle infrastructures while still fulfilling automotive EMC requirements.

Another key in-vehicle network requirement is guaranteed communication latency and for this reason Ethernet is not used for controls communication in cars. While Ethernet can at best provide Quality-of-Service (QoS) for prioritization of traffic, there remain many control applications which require strict guarantees that critical messages will be delivered through the network in time. In order to fulfil these requirements, Ethernet with deterministic capabilities must be used. The Time-Sensitive Networking (TSN) standard offers the requisite latency guarantees for communication of critical controls traffic in vehicles.

Deterministic Ethernet standards are transforming the way that in-vehicle networks are being designed and built. The integration of Ethernet in vehicles can be broadly shown in 3 phases. Each phase brings new opportunities and new levels of value for manufacturers

Phase 1: Sub-system level

In the first phase, Ethernet is used as a high-speed in-car connection for applications with high-bandwidth requirements. Systems such as a video camera can be connected over regular Ethernet.

Example phase 1 applications:

- Surround sensing (video, radar, …)
- Diagnostics, Car2x (IP)

Phase 2: Architecture level

In the second phase, Ethernet is used as a scalable communication network. It can be used for the integration of the video camera with in-car infotainment systems.

Example phase 2 applications:

- Multimedia, infotainment (audio / video streaming)

Phase 3: Domain level

The third phase culminates in the integration of all traffic classes on a single in-vehicle backbone network. A driver assistance system with video top view (rendered then displayed on the infotainment screens) requires the communication guarantees provided by Time-Sensitive Networking (TSN).

Example phase 3 applications:

- Control loops (real-time, synchronous)
- Safety (real-time, synchronous, ISO 26262 ASIL D)
- Availability (Fail-Operational Systems)

As an example, time-scheduled Deterministic Ethernet is being deployed in Advanced Driver Assistance System (ADAS) hardware for autonomous driving, where functional subcomponents of the safety-critical system are connected on a shared network infrastructure. This system will be available in the next generation of automobiles released over the coming years.

TSN in industrial applications

Time-Sensitive Networking (TSN) also offers a solution to the challenges in industrial control and automation systems with increased connectivity requirements for M2M and cloud communication. The Industrial Internet of Things and Industry 4.0 are often described as a fourth wave of the industrial revolution. They are driven by the notion that with greater access to process and control related data, machines and processes can be made considerably more efficient.

Data must be sharable between machines for synchronization and control, and from machines to the enterprise space for analysis

What is TSN?

TSN IS A SET of IEEE 802 Ethernet sub-standards that are defined by the IEEE Time-Sensitive Networking task group. The new standards enable time-scheduling capabilities and therefore fully deterministic real-time communication within the 802 suite of standards.

Example TSN sub-standards currently being developed are:

- IEEE 802.1ASrev (PTP profile for clock synchronization in TSN)
- IEEE 802.1Qbv (timed message release)

TSN achieves deterministic real-time communication over Ethernet by using a global sense of time and a schedule which is shared between network components. By defining queues based on time, TSN ensures a bounded maximum latency for scheduled traffic through switched networks.

and optimization. This is being described as the convergence of OT (Operational Technology) and IT (Information Technology). In order for this to happen, the network must be open and standard to all, however as with automotive applications, there are strict real-time communication requirements that cannot be met by Ethernet in its current form.

In the world that Industrial IoT is set to revolutionize, single-purpose control networks using proprietary communication protocols are becoming islands, connected to one another via gateways, and with limited data access and usability.

As new functions and machines are added to systems, even more networks are installed, leaving industrial systems potentially containing tens of different networks using incompatible communication protocols. These systems are not flexible or reaching their maximum potential. In the world of IoT and interconnectivity, those who aren't accessing and using valuable data run the risk of being left behind.

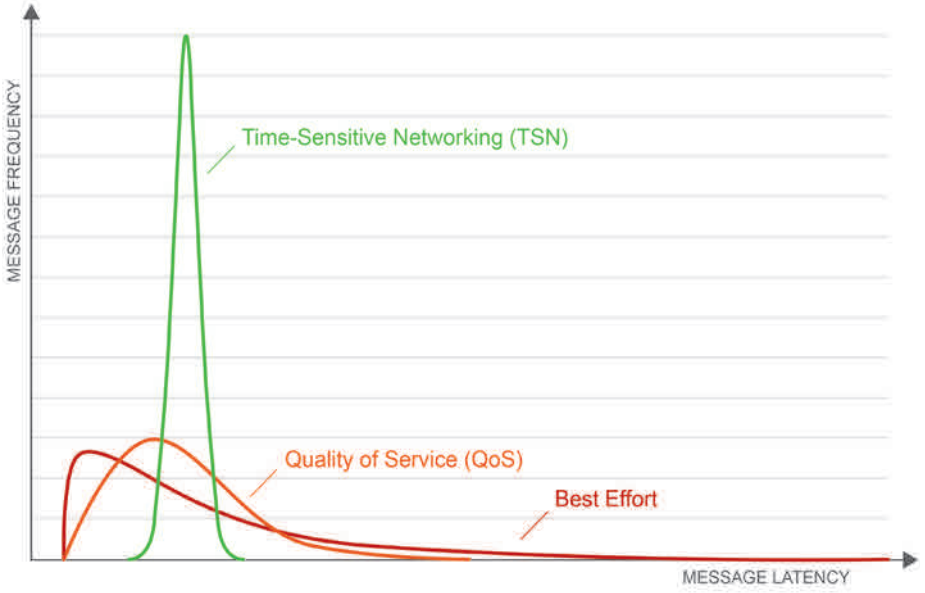
Ethernet is the obvious choice for Industrial IoT connectivity. It is open, standard and already used in enterprise networks, making data access much simpler. It is often implemented today in industrial environments for replacing non-critical bus networks or for high bandwidth camera and visualization applications.

Indeed convergence on Ethernet is already common for audio, video, and data services, and Quality of Service (QoS) solutions can be used for critical control over Ethernet. However the determinism provided by QoS does not scale well to the larger converged networks and open infrastructures that are being driven by the Industrial Internet of Things.

The Time-Sensitive Networking (TSN) extension to IEEE 802 Ethernet enables exactly the large scale convergence described in Industrial IoT and Industry 4.0. Low latency and guarantees for communication of even the most critical control traffic means that all applications are able to share a single communications network.

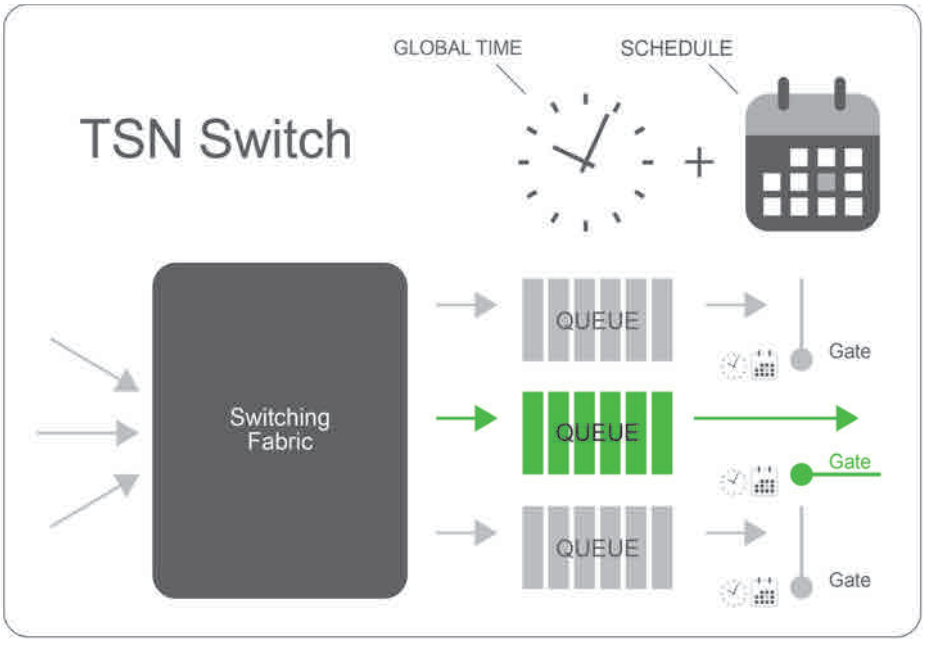
When critical and non-critical applications share the same communications infrastructure safely and securely, OT (Operational Technology) and IT (Information Technology) are brought together and data access is improved immeasurably. This will enable new business models, cut downtime, simplify system integration, and reduce the cost of maintenance.

As an example; consider a discrete automation plant with multiple robots working on production lines. Today these robots are controlled locally, with limited synchronization between them, and bottlenecks for data access from beyond the factory floor. Where there is connectivity, it is either done over proprietary networks or via gateways. By removing local control functions or converging non-critical traffic in the same network, one could jeopardize the guarantees for communication of critical messages.



SOURCE: TTTECH

A deterministic Ethernet network guarantees latency of critical scheduled communication. Time-scheduled traffic partitioned from other network traffic is immune from disturbances.



SOURCE: TTTECH

TSN messages are forwarded as part of scheduled queues (802.1Qbv) which enables guaranteed latency in converged networks.

Now consider a TSN connection between these robots. The controls communication is guaranteed across the network even when converged with non-critical traffic, and all robots are synchronized to the same global time. This means that controls networks can be integrated with data networks, and many control functions can be centralized away from the robot cell, where greater computing power can be utilized.

Importantly, huge amounts of data from the robots are now also visible to higher layer networks without the need for gateways, enabling Machine as a Service (MaaS) type business models – simultaneously improving service and maintenance from machine builders and lowering capital expenditure for end user manufacturing companies.

Use cases for Deterministic Ethernet standards like TSN can be found in a wide range of application areas beyond manufacturing.

For example in wind turbines, deploying control over Ethernet helps to cut downtime and increase production efficiency. And in railway applications, convergence of critical train control networks over Ethernet saves space, weight and power, in addition to improving system reliability.

Technology article by ***TTTech.***

IEEE 802 Ethernet Sub-standards

IEEE Standard Ethernet for guaranteed real-time communication achieves determinism using a global sense of time and shared schedule.

IEEE 802 Ethernet sub-standards are defined by the IEEE TSN task group. These standards enable fully deterministic real-time communication over Ethernet. TSN achieves determinism over Ethernet by using a global sense of time and a schedule which is shared between network components.

By defining queues based on time, Time-Sensitive Networking ensures a bounded maximum latency for scheduled traffic through switched networks. This means that in a TSN network, latency of critical scheduled communication is guaranteed.

In control applications with strict deterministic requirements, such as those found in automotive and industrial domains, Time-Sensitive Networking offers a way to send time-critical traffic over a standard Ethernet infrastructure. This enables the convergence of all traffic classes and multiple applications in one network.

In practice this means that the functionality of standard Ethernet is extended so that:

- Message latency is guaranteed through switched networks
- Critical and non-critical traffic can be converged in one network
- Higher layer protocols can share the network infrastructure
- Real-time control can be extended away from the operations area
- Sub-systems can be integrated more easily
- Components can be added without network or equipment alterations
- Network faults can be diagnosed and repaired faster

Key benefits

- **Standards-based:** Part of IEEE 802 standards suite
- **Partitioned:** Virtual separation of traffic classes, enables convergence of other protocols on one physical network
- **Compatible:** Integrates installed industrial Ethernet protocols including Profinet and EtherNet/IP
- **Scalable:** Scales from small to very large systems without compromising safety, security or performance
- **Secure:** Existing security standards and management features are implemented; partitioning prevents denial of service

Real-time historical mobile data collection and reporting

A new mobility solution for a rail transportation system uses remote monitoring to reduce downtime costs. The use of FactoryTalk Historian software helps LORAM rail grinders remotely collect performance data for real-time troubleshooting, maintenance and reporting.

RAIL GRINDERS ARE ESSENTIALLY ADVANCED factories on wheels, incorporating high power, flexible grinding modules with patented control systems. LORAM Maintenance of the Way, a leading supplier of track maintenance machinery and rail grinders, is constantly looking for new ways to save its customers money by maximizing efficiency, productivity and value from the rail asset.

To help streamline maintenance activities and improve visualization into operations, the company recently implemented a mobile remote-monitoring solution.

Mobile remote monitoring

LORAM rail grinders are highly automated machines, incorporating many different technological components and software. Each rail grinder requires an on-machine crew of approximately 10 that is responsible for operating the machines. Engineering and troubleshooting of the machines is managed by a team at the company headquarters.

In the past, if an issue occurred or corrective action for a component failure was required, the crew would have to contact the maintenance technicians at LORAM headquarters to diagnose the issue. Because all of the data from the control systems resided on the machines, the technical support staff was occasionally unable to diagnosis the problem without travelling to the machine.

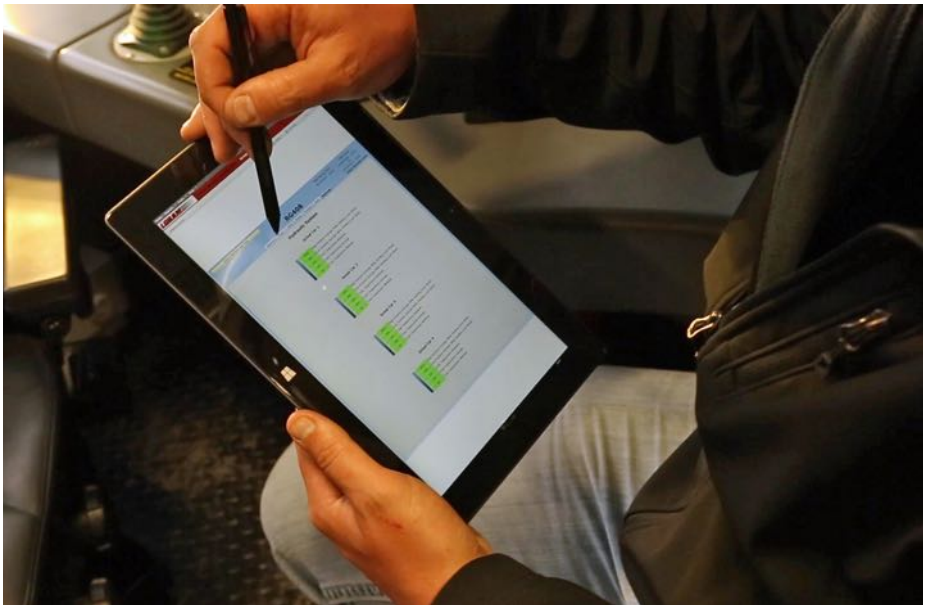
"Without easy remote access to machine data, troubleshooting and diagnostics on machines in the field were time consuming and difficult, relying on the technical support staff to walk the on-site team through the issue and potential fixes," said Nathan Moyer, field application technician for LORAM. "Larger issues would require the technical staff to travel to the grinder, extending downtime further."

One day of downtime for a rail grinder is very costly for the company, even before parts and service costs are added. In addition, performance data wasn't automatically collected through a centralized application, and was only accessible on-machine for 30 days.

With machines in the field for many years or their entire lifecycle, maintenance technicians from headquarters needed to proactively retrieve data from the machines, as the on-machine historians held up-to 30 days of data. When there are more than 80 grinding machines out in the field, collecting this type of data required resources that could be used elsewhere within the company.

SOURCE : ROCKWELL AUTOMATION

Rail grinders control systems produce more than 100,000 data tags. Technicians have visibility into 45,000 tags via HMI screens and can collect up to 2,100 data tags per electronic report.



SOURCE : ROCKWELL AUTOMATION

Plant management personnel can use easy-to-read dashboards and trend reports to dig deeper into data logs from the office, home or on the road using a Surface tablet with wireless connectivity.

"Retrieving data remotely was a time-consuming task – not to mention, all data was in PLC code requiring it to be retrieved and analyzed by a technician who could properly interpret the data," said Moyer.

"The data-log format wasn't easily readable, customizable or searchable. Due to the difficulty in understanding the data and manually developing reports, reports were only developed on an ad-hoc basis. We developed reports based on issues we had at any given moment, not for predictive maintenance," Moyer added.

Manufacturing intelligence

Partnering with Rockwell, LORAM implemented a manufacturing-intelligence system with remote-monitoring capabilities on its newest line of LORAM RG400 series rail grinders.

Allen-Bradley ControlLogix programmable automation controllers (PACs) manage machine automation with EtherNet/IP as the industrial communications backbone of the solution to provide seamless communication between the various pieces of equipment on the rail grinder.

Leveraging FactoryTalk Historian software, LORAM remotely collects critical performance data from each rail grinder for real-time troubleshooting, maintenance and electronic reporting. Data points cover component temperature, engine run hours, historical generator loads and other KPIs. Surface tablets running the FactoryTalk VantagePoint mobile app allow LORAM technicians to see machine data and troubleshoot issues from any location in real time.

"Now when I get a call about an equipment issue on the rail grinders, I can pull up easy-to-read dashboards and trend reports to dig deeper into data logs from my office – at home or on the road using the Surface tablet with wireless connectivity. I can also tap into all necessary on-machine HMIs via FactoryTalk View software," said Moyer. "Locating necessary information for troubleshooting that used to take a significant amount of my time, now only takes a few minutes."

Using FactoryTalk Historian software and the FactoryTalk VantagePoint GPS time module, LORAM now tracks North American rail grinders through wireless connections, and displays machine location and status on Google Maps mapping service.

A global positioning system (GPS) mapping capability provides off-site technicians visibility of each grinder at all times. Technicians have the ability to see a street level view of each machine and link to individual machine KPI dashboards.

Real-time machine data

Remote access to real-time machine data provides LORAM rail grinder technicians the ability to see issues as they happen and to proactively plan for similar issues that could occur in the future. Utilizing remote diagnostics for predictive-maintenance activities has increased mean time to failure while reducing mean time to repair.

The control systems used on the RG400 series of rail grinders produce more than 100,000 data tags. Technicians have visibility into 45,000 tags via HMI screens and can collect up to 2,100 data tags of their choosing per electronic report.

"Our new remote capabilities have significantly reduced troubleshooting time and costs. Mobility provided by our Surface tablets and the FactoryTalk VantagePoint KPI mobile app can prevent considerable downtime – saving us significant costs in downtime avoided," said Moyer. "Additionally, this level of remote access gives LORAM and our customers a competitive edge."

New, electronic reporting makes accessing, searching and analyzing data much easier on the new system. Each rail grinder can now hold 137 days of local data storage before upload. All critical performance data can be conveniently retrieved from the field electronically and quickly.

Technicians and engineers now have the time to focus their efforts on monitoring and implementing proactive maintenance or even implementing next-generation design changes. This means LORAM can re-allocate resources for improved efficiency and increased uptime across its fleets.

*Application story by **Rockwell Automation.***

Synchronizing mechatronics using FPGAs and POWERLINK

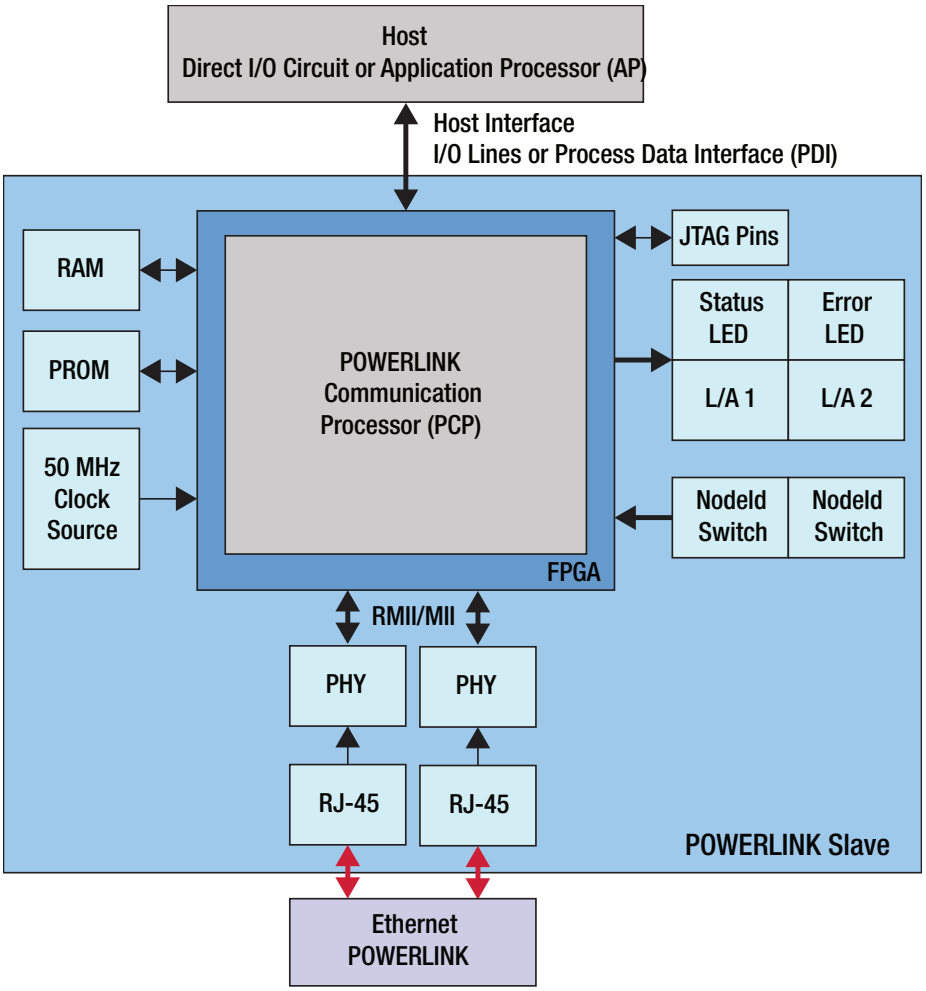
Implementing Ethernet POWERLINK protocol on FPGAs allows maximum system flexibility and performance at a cost-effective solution point. Options include using either a one-chip solution with the application processor embedded inside the FPGA, or the application processor may be implemented externally.

TRADITIONAL CENTRALIZED I/O SYSTEMS are inadequate for building large machines. Running high-speed I/O lines over long distances increases cabling requirements and errors due to signal noise with higher frequencies. Industrial Ethernet solves many of these problems by providing an accelerated and deterministic methodology to manage I/O systems, sensors, and actuators for high-frequency applications such as motion control.

Field programmable gate arrays (FPGAs) can provide a protocol for real-time deterministic jitter-free Ethernet communications, as well as reliable deterministic synchronization capabilities over large distances. This article presents an example implementation of using the open source protocol Ethernet POWERLINK implemented on an FPGA.

Industrial Ethernet adoption is expected to continuously increase in the upcoming years, and there are many different protocols available to meet the real-time Ethernet requirements for industrial automation.

Ethernet POWERLINK is a patent-free, Open Source protocol that is very efficient and effective at handling both time-critical real-time data and high-throughput best-effort traffic at the same time. It combines the requirements for minimum system jitter as requested by high-precision motion control with demands for bandwidth used in industrial vision applications. All data is transferred on a single wire, typically following the Cat 5e or Cat7 cable standards.



SOURCE : ALTERA

Ethernet POWERLINK FPGA Block Architecture.

How Ethernet POWERLINK works

The Ethernet POWERLINK cycle consists of the real-time isochronous phase and the non-real-time asynchronous phase. The cycle is initiated by the MN issuing a Start-of-Cycle (SoC) frame. This frame is used for network synchronization and indicates to each CN to sample its input data as well as to set active the latest received output data.

In the isochronous phase, the MN sends individual PollRequest (PReq) frames to each CN on a network. The addressed CN then responds with a PollResponse (PRes) frame. The response is sent as a multicast message, making the data available to all network nodes. This allows direct cross-communication between the CNs within a single cycle and guarantees the fastest possible synchronization between nodes.

After the isochronous phase, the MN grants permission to send a standard Ethernet frame to any station on the network. This asynchronous phase is used for non-time critical communication, such as network management, configuration, diagnose or web-traffic.

Poll response chaining

An automation network typically contains a variety of components requiring high frequency data updates such as drives and encoders, and devices requiring lower frequency updates such as sensors. Also, in some cases a centralized control approach is preferred, while in others a decentralized one fits best.

Ethernet POWERLINK offers a feature (Multiplexed Slot Assignment) allowing the master to poll slow stations every nth cycle. Another feature (Poll Response Chaining) combines all outgoing data from the MN into a single-frame request. The CNs will then send their responses at a specified point of time with fixed predetermined time delays.

PollResponse Chaining increases network performance when several nodes with small amounts of process data are connected, because all CNs receive a single Pres frame from the MN. This frame is sent as multicast instead of all the individual PReq frames in standard mode. PollResponse Chaining is ideal for situations where centralized control loops are used for robotics or Computer Numerical Control (CNC) applications.

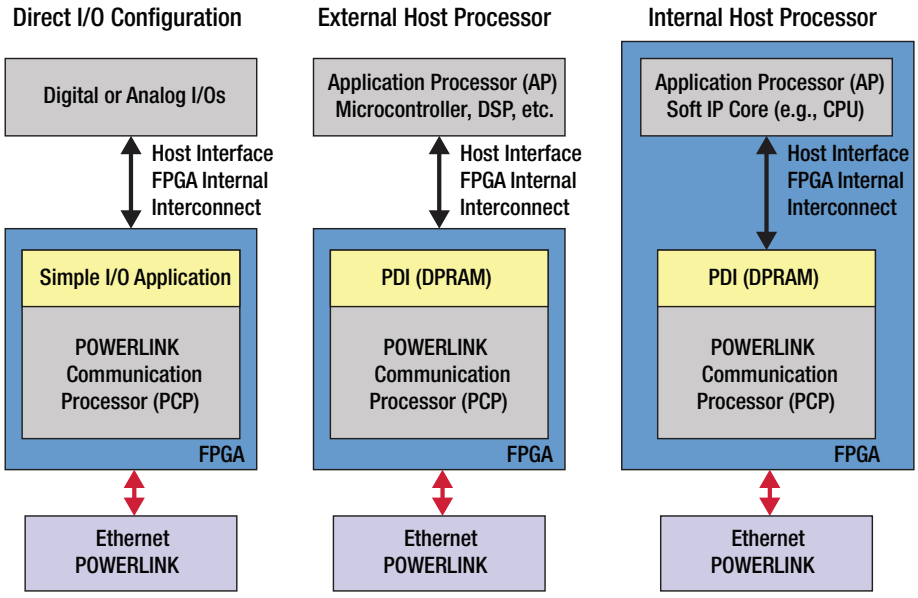
FPGA implementation of POWERLINK

A typical POWERLINK slave implementation on an Altera Cyclone-family device. In this configuration, the POWERLINK slave consists of the following hardware components:

- Altera FPGA (e.g., Cyclone IV device)
- Clock source (quartz crystal oscillator)
- Non-volatile memory (PROM)
- Volatile memory (RAM)
- Ethernet physicals (PHYs)
- Ethernet jacks (RJ45) + transformer
- Diagnostic LEDs
- Node ID switches
- Debugging interface (JTAG)

The Ethernet POWERLINK protocol is implemented in the POWERLINK Communication Processor (PCP). The PCP internally parts into a Soft-IP-Core (POWERLINK IP-Core) and a software stack running on a standard Nios II embedded microcontroller within the FPGA.

Required hardware components for booting and running the PCP consist of volatile memory (RAM) to run the software stack, non-volatile memory (PROM) to store the firmware, and a clock source.Hardware parts that directly interact with the user include the Node ID switches, the diagnostic LEDs (STATUS, ERROR, and PHY LINK/ACTIVITY) and optionally (for debugging purposes) a JTAG interface.



SOURCE: ALTERA

Ethernet POWERLINK Slave Configurations

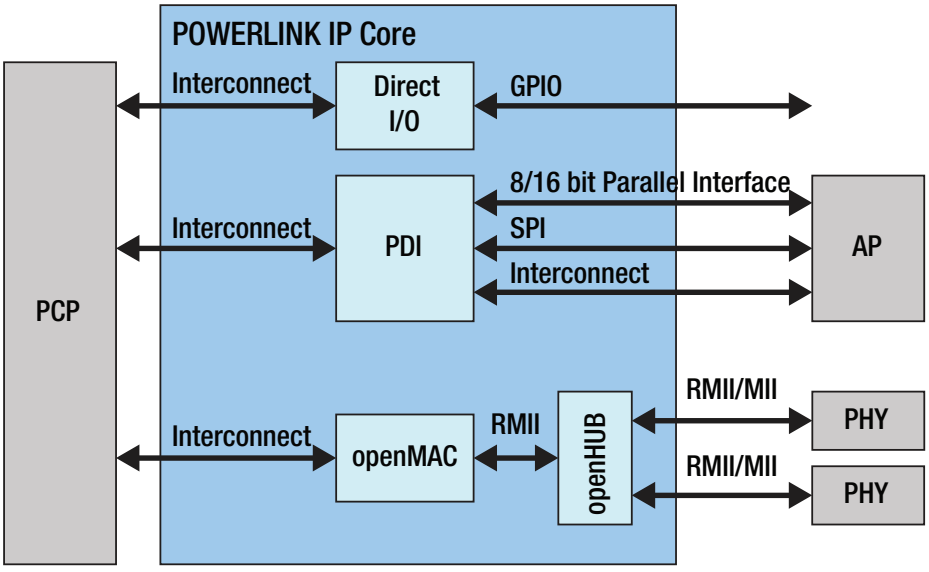
Ethernet POWERLINK options

There are three different configurations for the Ethernet POWERLINK slave:

- Direct I/O
- External host processor
- Internal host processor configurations

The direct I/O version consists of the PCP solely. It can be directly connected to up to 32 I/O lines. This configuration is used mainly for simple remote sensors interfacing with analog or digital signals.

Typical Ethernet POWERLINK devices require



POWERLINK IP-Core Block Diagram

their own application processor on which the main device firmware is run.

This application processor may be an external chip (micro controller, DSP) or reside inside the same chip (Dual Nios configuration, or the ARM cores of a Cyclone V SoC). The PCP is connected to the application processor via the process data interface (PDI).

Three variants are available for the user:

- Serial peripheral interface (SPI) for simple applications
- An 8 or 16 bit parallel memory interface for faster throughput
- Altera's on-chip Avalon memory mapped interface for single chip or SoC solutions

FPGA implementation benefits

Although there are software implementations of Ethernet POWERLINK that allow running the protocol on standard microcontroller units (MCUs) and processors, the hardware implementation of Ethernet POWERLINK produces the optimal performance.

The main reason for it is the Ethernet POWERLINK-aware MAC IPCore called openMAC, which offers hardware acceleration functionality. An additional benefit of the FPGA implementation is the included openHUB, an Industrial Ethernet hub, that enables placing two (or more) external Ethernet jacks on a device to set up line or ring topologies in the POWERLINK network without a need for further infrastructure components. The PDI is part of the FPGA IP-core. It should be noted that the PDI and Direct I/O are mutually exclusive.

SOURCE : ALTERA

openMAC Hardware Acceleration

To understand why hardware acceleration at the Ethernet MAC layer is key to the design, a deeper look into the architecture is necessary. A main factor for speeding up the automation processes is reducing the overall reaction time of the nodes in the network.

In Ethernet POWERLINK, the reaction time of a node is determined by the gap between receiving the PReq from the MN and the start of transmission of the PRes frame: The shorter the gap, the faster the slave. openMAC now allows to automatically transmit a pre-assembled PRes frame as soon as the PReq is received and recognized. As this is all done in the FPGA logic, the minimum possible gap of 960 ns (the so-called Inter Frame Gap as given by the Ethernet standard) is reached. This auto-response mechanism together with extended filtering on the MAC layer optimally accelerates POWERLINK slave implementations.

In addition, frame transmissions can be scheduled by openMAC (time-triggered sending), which allows Ethernet POWERLINK slaves to operate in PollResponse Chaining mode and Ethernet POWERLINK masters to reduce the system jitter to below 1 microsecond.

With these optimizations inside the FPGA, fastest cycle times and lowest jitter are possible, as shown in the table.

Conclusion

The Ethernet POWERLINK implementation showed combined with FPGA technology make Industrial Ethernet an attractive solution for modern automation systems.

The Ethernet POWERLINK protocol implemented on FPGAs allows maximum system flexibility and performance at a cost-effective solution point. With an FPGA, there are various options of implementing Ethernet POWERLINK.

This is achieved by using either a one-chip solution with the application processor embedded inside the FPGA, or the application processor may be implemented externally. Furthermore, by using field programmable gate array techonology, it becomes possible to embed additional system functionality such as motor control or programmable logic controller (PLC) functionality into the FPGA to reduce system complexity and the overall system bill of material (BOM) costs.

Technology report by Sari Germanos, Technology Marketing Manager, ***Ethernet POWERLINK Standardization Group,*** *Wolfgang Seiss, Manager Open Automation Solutions,* ***B&R Industrial Automation*** *and Elias Ahmed, Sr. Strategic Marketing Manager,* ***Altera.***

POWERLINK Performance Specifications in Altera FPGAs

Feature	Master	Slave
Interfaces	Parallel (16/32 bit) PCIe Avalon	SPI Parallel (16 bit) Avalon
Cycle time	250 µs	250 µs
Jitter	< 1 µs	< 1 µs
Response time	1 µs	1 µs
Supported modes	Standard Poll response chaining	Standard Multiplex Poll response chaining
Virtual Ethernet interface	Yes (for tunneling IP traffic)	Yes (for tunneling IP traffic)
Remote update	-	Yes (via POWERLINK master)
FPGA resource utilization for standard configuration	9K LEs 286 KB RAM	7K LEs 286 KB RAM
IP access details	openpowerlink.sourceforge.net	openpowerlink.sourceforge.net

Summary of performance specifications using POWERLINK implemented within the FPGA.

SOURCE : ALTERA

Aircraft component manufacturing automation

A large sensor and measuring instrument manufacturer offers an innovative factory automation capability for industrial manufacturers and warehouse distribution centers. Optimizing efficiency and increasing productivity through mechanization and industrial innovation is the goal.

An industrial production company creating aircraft parts received a plan from a factory automation integrator to streamline a floor process in the warehouse. The specific assembly process was responsible for etching numbers onto finished parts and readying them for shipment.

Included in the assembly, the sensor manufacturer's laser marking machine etches part numbers onto the completed projects. A robotic arm then receives each etched piece and packs it properly for shipping. This configuration is integrated and controlled by a PLC, PC application and Comtrol's DeviceMaster UP 2-Port 2E with its DualConnectPlus feature. This manufacturer needed to connect the raw/ASCII laser marker over serial RS-232 to an EtherNet/IP enabled PLC.

Conversion to EtherNet/IP

The laser marker is connected to the DeviceMaster UP via RS-232 serial. Data is transmitted from the laser marker through the DeviceMaster UP where conversion to EtherNet/IP takes place to route the data to the PLC.

The DualConnectPlus feature was utilized to ensure that connection between the laser marker and the DeviceMaster UP was operating correctly, before moving on to troubleshoot the connection between the DeviceMaster UP and the PLC.

DualConnectPlus technology connects raw/ASCII devices (serial and/or Ethernet) to PLCs and/or applications simultaneously. String, RFID, and barcode data filtering eliminates redundant data while extracting the RFID and barcode parameters. It opens communication to the SCADA system and can provide troubleshooting information for individual steps of the communication process.

This information can determine PLC, device and sensor health, along with helping to yield consistent communication and successful integration. The manufacturer was able to correctly identify where the communication process in this system was initially failing by using DualConnectPlus and the company's engineering technical support team.

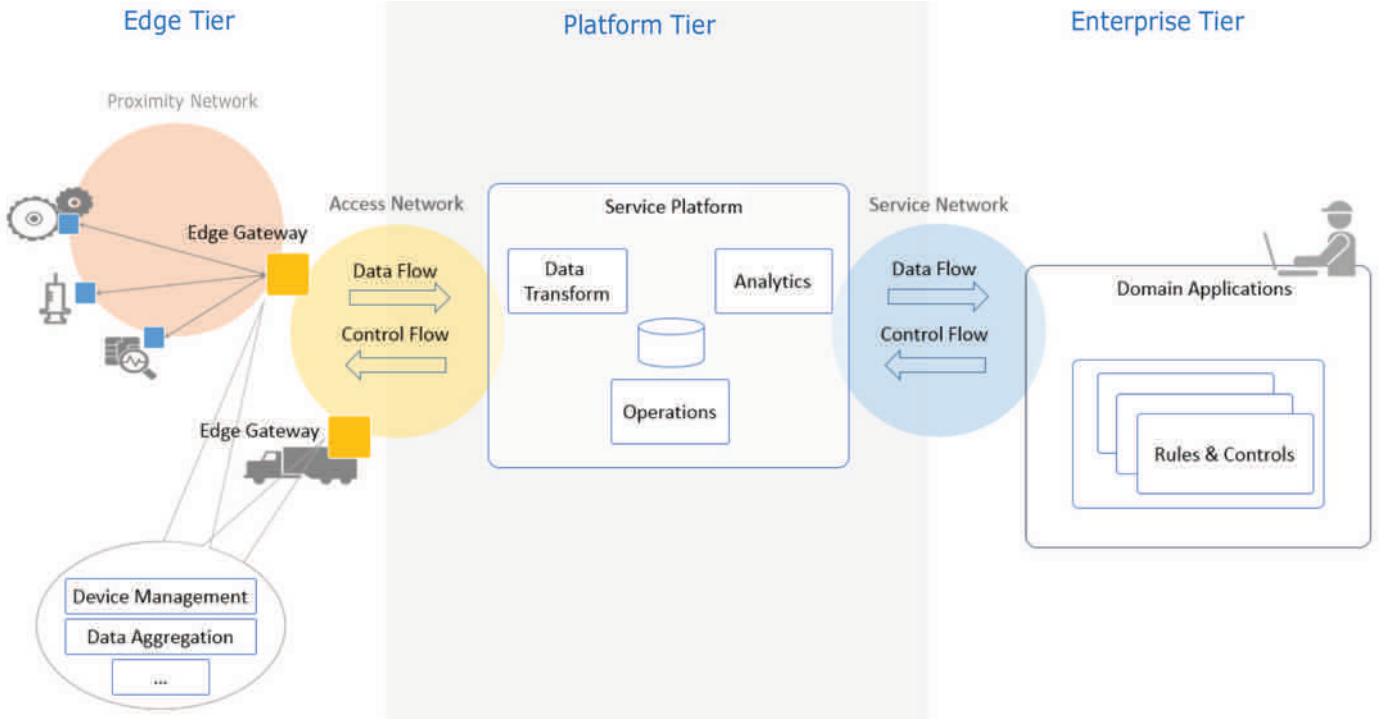
The DeviceMaster UP DB9M 2-Port 2E Ethernet gateway operates in a -37° to 74°C temperature range and variable power input eliminates the need for power converters.

DeviceMaster UP technology provides EtherNet/IP, Modbus, and PROFINET IO connectivity to a wide variety of devices. It can enable you to quickly connect PLCs, SCADA, OPC servers and applications to devices such as barcode scanners, RFID readers, weigh scales, vision systems, printers, encoders, HVAC and sensors.

Application story by ***Comtrol.***

Implementation of an Industrial Internet Reference Architecture

The IIoT reference architecture recently released by the Industrial Internet Consortium identifies key system characteristics and end-to-end properties common across activities that need to be enforced globally for successful IIoT implementations.



SOURCE: IIC

System diagram of three-tier IIS architecture.

IMPLEMENTATION OF AN IIoT REFERENCE Architecture is concerned with the technical representation of an Industrial Internet System (IIS), along with the technologies and system components required to implement the activities and functions prescribed by the reference architecture's usage and functional viewpoints.

The IIS architecture and the choice of the technologies used for implementation are also guided by the business viewpoint, including cost and go-to-market time constraints, business strategy in respect to the targeted markets, relevant regulation and compliance requirements and planned evolution of technologies. The implementation must also meet the system requirements including those identified as key system characteristics that are common across activities and must be enforced globally as end-to-end properties of the IIS.

The implementation viewpoint describes:

- The general architecture of an IIS: its structure, the distribution of components, and the topology by which they are interconnected.
- A technical description of its components, including interfaces, protocols, behaviors and other properties.
- An implementation map of the activities identified in the usage viewpoint to the functional components, and from functional components to the implementation components.
- An implementation map for the key system characteristics.

Architecture patterns

Coherent IIS implementations follow certain well-established architectural patterns:

- Three-tier architecture pattern
- Gateway-Mediated Edge Connectivity and Management architecture pattern
- Edge-to-Cloud architecture pattern: This contrasts with the gateway-mediated pattern as it assumes a wide-area connectivity and addressability for devices and assets.
- Multi-Tier Data Storage architecture pattern: This supports a combination of storage tiers (performance tier, capacity tier, archive tier.
- Distributed Analytics architecture pattern.

An architecture pattern is a simplified, abstracted view of a subset of an IIS implementation that is recurrent across many IIS systems, yet allows for variants. For example, an implementation of the three-tier pattern in a real IIS does not exclude multiple implementations of every tier (e.g. many instances of the edge tier as well as many to many connections between instances of a tier and instances of the next tier). Each tier and its connections will still be represented only once in the pattern definition.

The Three-tier and Gateway-Mediated edge patterns are key to this discussion because of their stronger prevalence in IIS systems.

Three-tier architecture pattern

The three-tier architecture pattern comprises edge, platform and enterprise tiers. These tiers play specific roles in processing the data flows and control flows involved in usage activities. They are connected by three networks.

The edge tier collects data from the edge nodes, using the proximity network. The

SOURCE: IIC

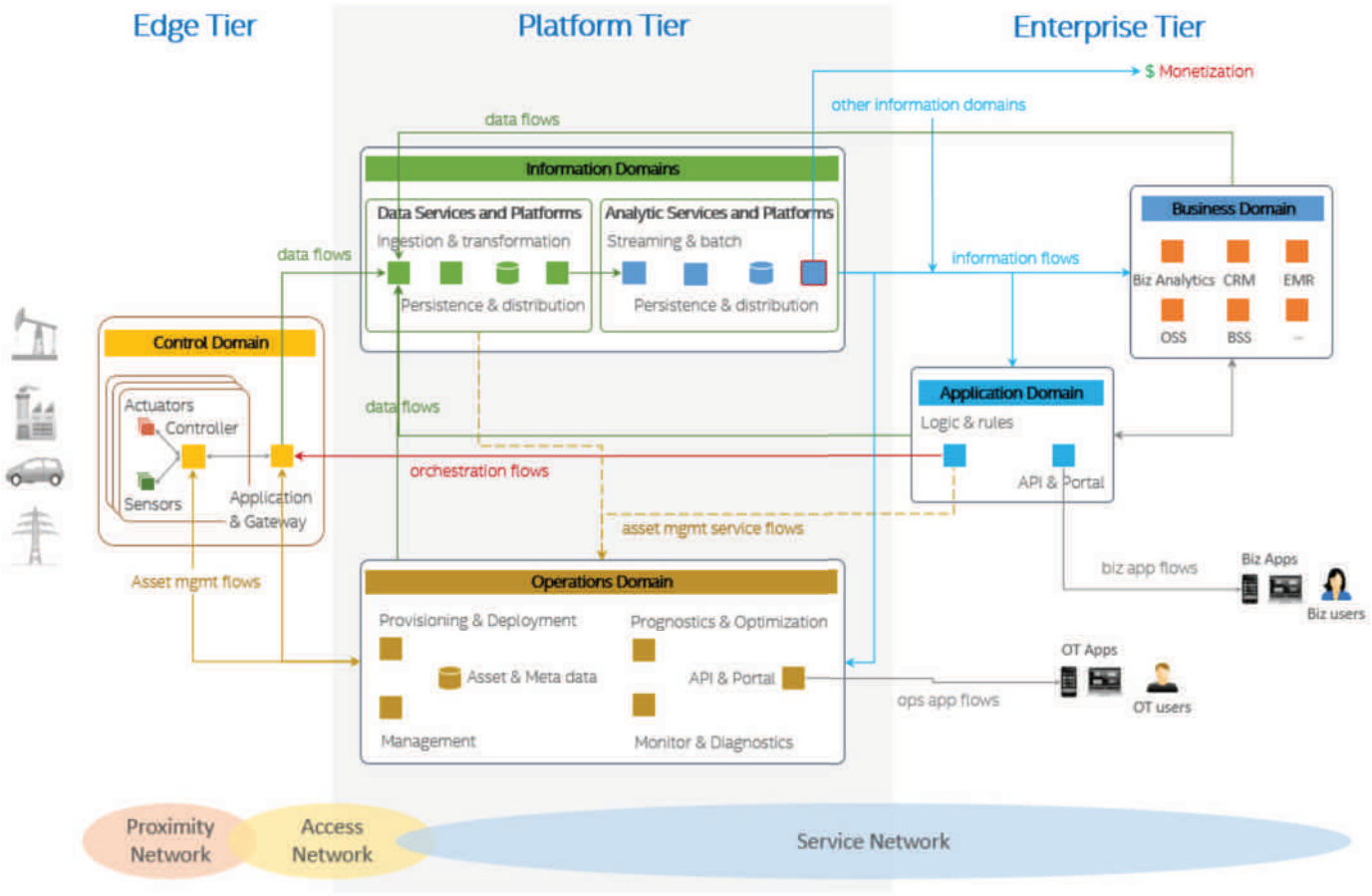


Diagram shows mapping between a three-tier architecture and the functional domains.

architectural characteristics of this tier, breadth of distribution, location, governance scope and the nature of the proximity network, vary depending on the specific use cases.

The platform tier receives, processes and forwards control commands from the enterprise tier to the edge tier. It consolidates processes and analyzes data flows from the edge tier and other tiers. It provides management functions for devices and assets. It also offers non-domain specific services such as data query and analytics.

The enterprise tier implements domain-specific applications, decision support systems and provides interfaces to end users including operation specialists. The enterprise tier receives data flows from the edge and platform tier. It also originates control commands to the platform tier and edge tier.

Functional blocks in each tier are indicative of the primary functional vocation of the tier, yet are not exclusively assigned to that tier. For example the 'data transform' function in the platform tier could also be found in the edge tier (e.g. performed by a gateway) although it would be implemented in a different way and for a different purpose. For example, 'data transform' at the edge is typically done in a device-specific manner through device-specific configuration and interfaces, unlike in the platform tier where it is usually supported as a higher-level service that operates on data that has been abstracted from any device source or type.

Different networks connect tiers

The *proximity network* connects the sensors, actuators, devices, control systems and assets, collectively called edge nodes. It typically connects these edge nodes, as one or more clusters related to a gateway that bridges to other networks.

The *access network* enables connectivity for data and control flows between the edge and the platform tiers. It may be a corporate network, or an overlay private network over the public Internet or a 4G/5G network.

The *service network* enables connectivity between the services in the platform tier and the enterprise tier. It may be an overlay private network over the public Internet or the Internet itself, allowing the enterprise grade of security between end-users and various services.

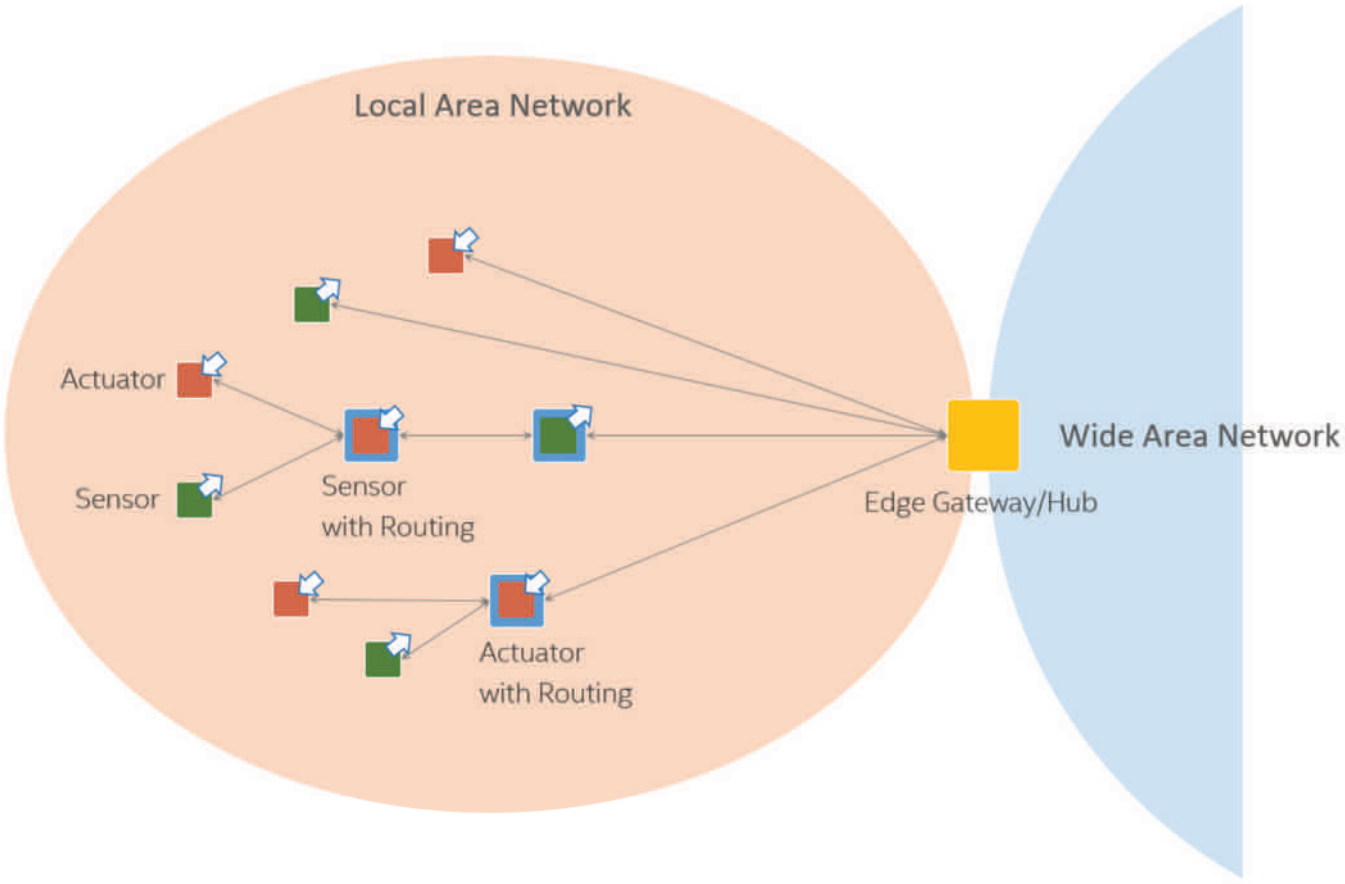
The three-tier architecture pattern combines major components (e.g. platforms, management services, applications) that generally map to the functional domains (functional viewpoint). From the tier and domain perspective, the edge tier implements most of the control domain; the platform tier most of the information and operations domains; the enterprise tier most of the application and business domains. This mapping demonstrates a simple functional partitioning across tiers. The actual functional mapping of IIS tiers is usually not as simplistic and depends on the specific of system use cases and requirements. For example, some functions of the information domain may be implemented in or close to the edge tier, along with some application logic and rules to enable intelligent edge computing.

Another reason why implementation tiers do not generally have an exclusive mapping to a particular functional domain is that these tiers often provide services to each other to complete the end-to-end activities of the IIS. These services—e.g. data analytics from the information functional domain—then become supportive of other functional domains in other tiers. For example:

The asset management flows is an expression of the operations domain component of the platform tier to manage assets in the edge tier. The operations domain component of the platform tier itself provides services to other components, either in the same tier or in another.

For example the data services (information domain) component of the platform tier may request services from the operations domain component for:

- The verification of asset credentials received in data flows from the edge tier.
- The query of asset metadata so it can augment the data received from the assets



SOURCE: IIC

Gateway-mediated edge connectivity and management pattern.

before the data are persisted or fed into analytics in the next stage of processing.

Similar operations domain services can be provided to the application domain components in the enterprise tier as well. Conversely, the operations domain components may use data services from the information domain component in order to get better intelligence from asset data, e.g. for diagnostics, prognostics and optimization on the assets.

As a result, components from all functional domains may leverage the same data and use analytic platforms and services to transform data into information for their specific purposes.

Edge connectivity and management

The gateway-mediated edge connectivity and management architecture pattern comprises a local connectivity solution for the edge of an IIS, with a gateway that bridges to a wide area network. The gateway acts as an endpoint for the wide area network while isolating the local network of edge nodes. This architecture pattern allows for localizing operations and controls (edge analytics and computing). Its main benefit is in breaking down the complexity of IISs, so that they may scale up both in numbers of managed assets as well as in networking. However, it may not be suited to systems where assets are mobile in a way that does not allow for stable clusters within the local network boundaries.

The edge gateway may also be used as a management point for devices and assets and data aggregation point where some data processing and analytics, and control logic are locally deployed.

The local network may use different topologies. In a hub-and-spoke topology, an edge gateway acts as a hub for connecting a cluster of edge nodes to each other and to a wide area network. It has a direct connection to each edge entity in the cluster allowing in-flow data from the edge nodes, and out-flow control commands to the edge nodes.

In a mesh network (or peer-to-peer) topology, an edge gateway also acts as a hub for connecting a cluster of edge nodes to a wider area network. In this topology, however, some of the edge nodes have routing capability. As result, the routing paths from an edge node to another and to the edge gateway vary and may change dynamically. This topology is best suited to provide broad area coverage for low-power and low-data rate applications on resource-constrained devices that are geographically distributed.

In both topologies, the edge nodes are not directly accessible from the wider network. The edge gateway acts as the single entry point to the edge nodes and as management point providing routing and address translation.

The edge gateway supports the following capabilities:

- Local connectivity through wired serial buses and short-range wireless networks. New technologies and protocols are emerging in new deployments.
- Network and protocol bridging supporting various data transfer modes between the edge nodes and the wider network: asynchronous, streaming, event-based and store- and-forward.
- Local data processing including aggregation, transformation, filtering, consolidation and analytics.
- Device and asset control and management point that manages the edge nodes locally and acts an agent enabling remote management of the edge nodes via the wide area network.
- Site-specific decision and application logic performed within the local scope.

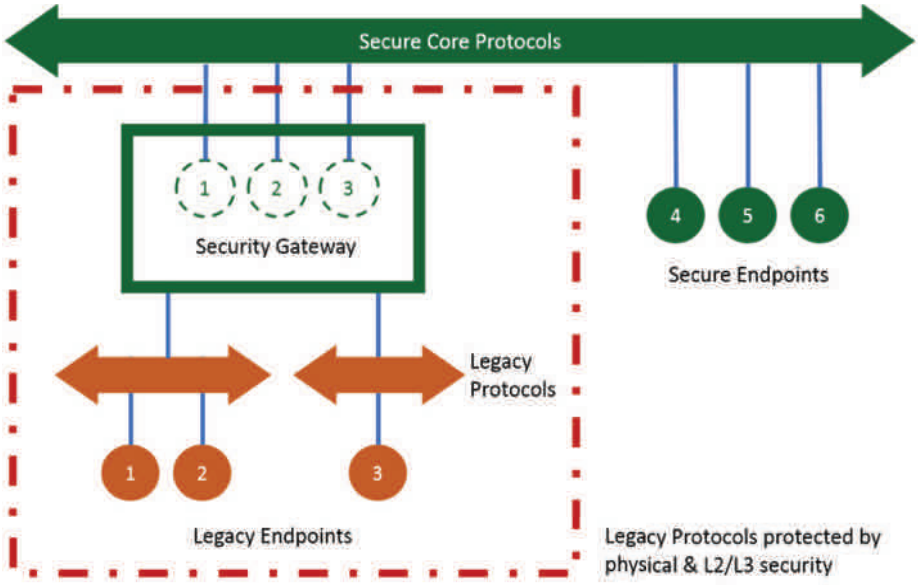
Secure implementations

To secure an Industrial Internet System, we outline a number of important and common security issues to be addressed in its implementation.

End-to-end security: To offer end-to-end security, an implementation must provide:

- Protected device-to-device communications
- Confidentiality and privacy of the data collected
- Remote security management and monitoring

SOURCE: IIC



Security gateway deployment pattern.

- Simultaneously addressing both existing technologies as well as new technologies
- Seamless spanning of both information technology and operational technology subsystems without interfering with operational business processes.

This effort requires building in security by design rather than the often-failed paradigm of bringing it in as an afterthought.

Securing legacy systems: Most IIS systems incorporate legacy systems due to the effort and capital expense involved in replacing or retrofitting these systems. Often legacy endpoints implement limited or no security capability in processing and in the protocols they use, and they are not modifiable to add the requisite security capability. Security of the overall system requires minimizing the attack surface of these legacy systems.

The use of security gateways is an approach to secure legacy endpoints and their protocols. A security gateway acting as proxies for the legacy endpoints bridges the legacy protocols supported by the legacy endpoints and their counterparts used by new endpoints. A security gateway isolates the attack surface introduced by legacy endpoints and their protocols to the links from these endpoints. However, isolating the attack surface is insufficient, as we still need to detect attacks. We want to detect security attacks by analyzing the data for anomalies and possible abnormal behavior within the threat surface. Not all attacks will be routed through the gateway.

Security for architectural patterns: Every architecture pattern has its own security requirements and challenges. In the three-tier architecture pattern, there are four critical areas and operations to secure:

- end-points
- information exchange
- management and control
- data distribution and storage

End-point security: Many IISs need to embed security capabilities and policy enforcement directly in end-point devices. It includes enablement of remote management of end-points for near real-time security responses during an attack as well as for proactive security measures prior to an attack.

The end-point should have the ability and autonomy to defend itself and must remain resilient even when disconnected from the external security management systems. Endpoints must be able remain secure and resilient even when adjacent peer endpoints are compromised. The embedded security measures should include mitigating controls, countermeasures and/or remediation actions defined by security policies to minimize the risk of being compromised and the impact when being compromised.

IIoT reference architecture

Information exchange security: Communication and data exchanges within an IIS must be protected for authenticity, confidentiality, integrity and non-repudiation. Security solutions and practices in information technologies can be applied to network segments and applications that are built on information technologies-based infrastructures in an IIS. In some industrial environments, legacy communication technologies, protocols and processing capability may limit the full security implementation for information exchange. A security gateway approach may be employed to protect the information exchange between the local legacy environments and the broad systems while enforcing logical isolation and physical protection for the local environments until the inadequate legacy systems re-phased out over time.

*Technology report by the **Industrial Internet Consortium.***

Defense-in-depth protection for electrical grid substations

A holistic approach to security recognizes a range of threats and that protective systems must integrate both physical and cyber security solutions. But even then, best practices need to evolve and incorporate a dynamic approach to systems, solutions and processes.

THE INCREASING CONNECTIVITY OF SUBSTATIONS in electrical grids has been both a boon and a challenge for network managers. Positive results include greater efficiency, responsiveness and integration. The downside has been an increase in the complexity of protecting the information network, given that greater connectivity also means greater vulnerability.

Meeting this challenge requires a holistic approach to security that recognizes the wide range in types of breaches, acknowledges that no solution can create 100 percent protection and integrates physical and cyber security solutions.

How has the landscape changed?

Electrical substations were once islands where the security of the network was less of a priority than safety, reliability and ease-of-use. This isolation is no longer the case and networks in electrical substations are most likely to include one or more of the following:

- Commercial off-the-shelf technology
- Ethernet and TCP/IP-based protocols
- Open IEC60870-5-04 and IEC61850
- Integration of legacy industrial protocols (DNP3) and Modbus TCP
- Remote connections
- Interconnection with company IT systems
- Use of public networks

Interconnected with systems across entire countries, networks are more prone to mistakes and failures. Protecting these networks requires robust cybersecurity policies designed first to prevent denial of service (DoS) attacks.

Preventing DoS attacks is prioritized based on the critical role that the network plays in the operation of high and medium voltage grids and the reality that a DoS attack may lead to service disruption and financial losses. Other objectives include protecting confidentiality and ensuring information integrity by preventing unauthorized modification or theft of information.

Five levels of security

Cybersecurity requires network managers to continuously evaluate conditions and threat sources to ensure that systems and policies remain current and effective. To manage this iterative process, it's helpful to understand the differences between risks, threats and vulnerabilities:

Networks in electrical substations now need to include the latest technology for physical and cyber security.

- A risk is the likelihood that something will happen to cause harm to an information asset, including loss.
- A vulnerability is a weakness that could be used to endanger or cause harm to an information asset.
- A threat is anything (caused by nature or man-made) that has the potential to cause harm to an information asset.

Protecting against these various hazards requires a multi-layered approach to cybersecurity designed to protect and mitigate from harm in the event of a breach. There are five layers of security for optimizing protection and threat mitigation:

1. Preventive security: Intended to prevent incidents from occurring and reduce the number and type of risks and vulnerabilities. Methods include strong password policies and preventing external USB devices from accessing open ports.

2. Network design security: Minimizes vulnerabilities and isolates them so an attack doesn't affect other parts of the network. A "zones and conduits" model can help limit the number of connections between network zones, lowering the risk of an attack spreading across the network.

3. Active security: Includes measures and devices that block traffic or operations that are not allowed, or expected, on a network. Examples include encryption, protocol-specific deep packet inspection, Layer 3 firewalls and antivirus use.

4. Detective security: Identifies an incident in progress or after it occurs by evaluating activity registers and logs, including log file analysis and intrusion detection system monitoring.

5. Corrective security: Aims to limit the extent of any damage caused by an incident, such as configuration parameter backup policy and firewall and antivirus updates.

Best practices for cybersecurity

Grounded now in the types of hazards, and the types of security and network solutions that can protect and mitigate threats, operators can design security strategies that go far beyond single point of defense solutions.

The Defense in Depth model is based on multiple, overlapping layers of protection for critical infrastructure. Defining policies and procedures based on an integrated view of physical, network, computer and device security, Defense in Depth is the best way to manage both external and internal threats.

The model draws on three concepts to ensure fast detection, isolation and control, limiting the impact of an error or breach, regardless of where or how it happens on the network:

1. Multiple layers of defense: If one is bypassed, another layer provides defense.

2. Differentiated layers of defense: If an

By building multiple layers of security protocols, any system failure or breach can be contained to limit damage.

attacker finds a way past the first layer, they can't get past all the subsequent defenses, since each layer is slightly different than the one before it.

3. Threat-specific layers of defense: Designed for specific risks and vulnerabilities, these solutions defend against a variety of security threats the electric power system is exposed to, such as computer malware, angry employees, denial of service (DoS) attacks and information theft.

Integrating security

As part of a multi-layered Defense in Depth model, physical and cybersecurity should be used together to create more robust protection for critical infrastructure. Physical protection systems include card readers at critical assets, such as transformer cabinets and control rooms, and security cameras that monitor access.

A systematic approach to network security should include the following elements:

- Routers and firewalls between the corporate backbone and substation network.
- Stateful or Deep Packet Inspection.
- Clearly demarcated zones between the operational and telecom network.

When physical security is combined with layers of network security, utility operators gain a coordinated monitoring system for the protection of both physical and cyber assets.

The electrical grid including substations and feeders is an increasingly attractive target for hackers. The potential for losses due to breaches, whether malicious or accidental, is significant and makes the mandate for a rigorous integrated cybersecurity strategy all the more compelling.

Vigilance is key

Implementing these changes from the historical approach to security may seem like a daunting task, but utility operators can manage the process with a few tenets. First, prioritize to ensure that mission-critical systems are secure. Second, create a culture of security with information and education. Third, keep risk assessments current. Finally, do not be tempted to deploy a one-size fits all solution; the threats, risks and objectives are varied, so the solutions must be as well.

Cybersecurity threats will evolve over time, making it essential that those charged with managing the protection systems continuously evaluate systems and processes. Answering a few questions can ensure that, as the landscape for threats evolves, so do the best practices:

- Do we know the topology protocols and type of traffic on the network?
- Do we know how and where components are connected, so we're allowing necessary conduits for traffic and can establish effective security zones?
- Do we require that any new device connected to the network be validated by an administrator and trigger a review of all documentation?
- How frequently do we change network passwords?
- Are we staying current with upgrades?

Ideally, network managers would be able to guarantee 100 percent protection, but the reality is that level of protection is simply not possible. Whether intentional and malicious or accidental, breaches will happen and so the objective must be to limit their effect on the system.

By building multiple layers of security protocols, any system failure or breach can be contained, making it easier to control efficiently and limit damage. Most importantly, the Defense in Depth model for cybersecurity protection ensures that in spite of any breach, the remaining portion of the system remains safe and high-performing.

*Germán Fernández is global vertical marketing manager, Power Transmission and Distribution for **Belden**.*

Network security concerns extend to production systems

Production control system network security is more important than ever to protect against potential threats. Looking at the complete network hierarchy provides insights into how to guard against vulnerabilities.

NETWORK SECURITY FOCUSED ON ENTERPRISE systems, until a few years ago, relied on firewalls to prevent viruses from arriving electronically. Now there is increasing realisation that the production control systems need to be protected too, and that viruses can be uploaded by many means.

Industries as diverse as manufacturing, processing, refining, power generation, and food and drink processing are all considering ways to improve the security of their plant and control systems and look at how to mitigate potential threats.

Ethernet network security issues

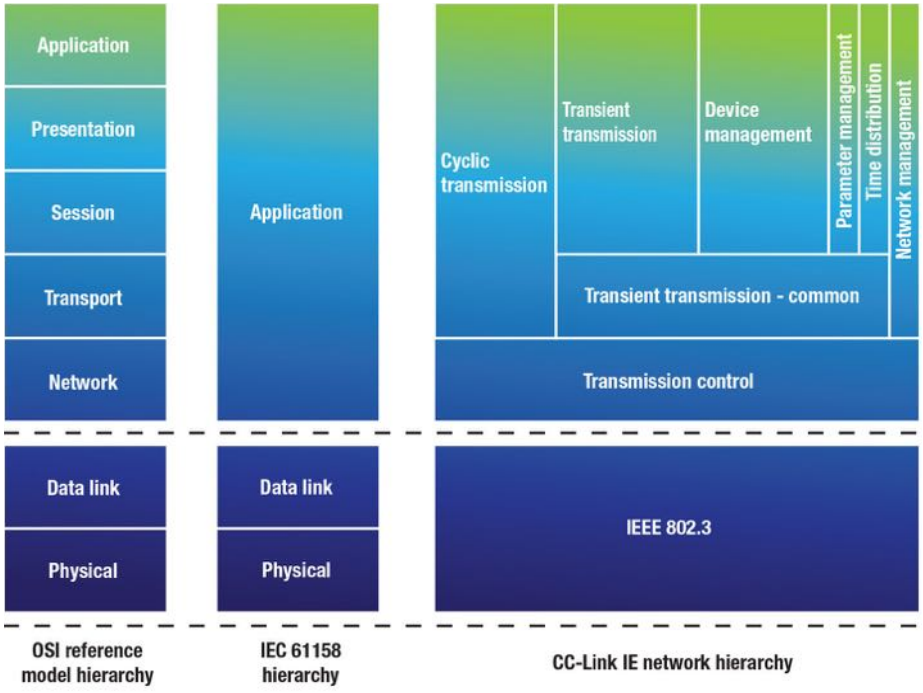
As Ethernet becomes the de facto industrial network of choice, installers and users can be seduced by the advantages the technology brings and give insufficient consideration to network security. However, given some recent high profile situations there is now a growing awareness that there is the very real possibility that networks can be compromised by both the electronic importation of a virus and from within, either accidentally or maliciously.

The problems of hacking from within a company are as much a personnel security issue as a general network security issue. Security considerations need to consider both deliberate acts of sabotage and the possibility of personnel making an unintended mistake.

Further, companies are increasingly adopting systems that allow remote access to plants – and reaping great benefits. However, monitoring processes typically use standard web browsers, which open the system up to the possibility of abuse of the network by third parties.

It is now well understood that SCADA (supervisory control and data acquisition) and other plant floor control systems have weaknesses and vulnerabilities when it comes to security. Therefore many companies are reassessing their traditional methods for moving information around between the plant/asset and the enterprise level.

The point of attack can be at the enterprise system level, plant control level or even the individual field device level. Top end attacks have previously been the main concern, with the result that very sophisticated security measures are available. Vulnerable field devices are relatively easy to protect with local measures.



SOURCE: CLPA

Plant security initiatives need to look at all of the layer in the OSI seven layer model because all it takes is for one layer to fall to an attack before the whole communications system is compromised – potentially without the other layers even being aware that there is a problem.

Security of PC-control systems

However in the 'middle ground' of plant control, we frequently see PC-based control systems with little or no security measures in place. There are even cases of some technologies still being utilised despite known vulnerabilities.

Security problems at this level and at plant floor device level are exacerbated by the fact that there is often limited collaboration between a company's IT department and the control engineering departments. In addition, within the control and engineering community, there is not always adequate recognition of the automation system security threats and liabilities. In particular, the business case for automation system security is not established, and there is limited understanding of the automation system risk factors.

The drive towards open network technologies generally, and towards Ethernet in particular, as a means of giving companies the freedom they want to choose best-of-breed control technologies has exacerbated the security threat. Users want standardisation, flexibility and choice, and this has been delivered through standardised open protocols. The trade-off, though, which is only just coming to be realised, is that these open protocols are less robust and more susceptible to attack. By contrast, the old proprietary networks were highly robust by virtue of their non-standardisation, but they were far less flexible and they ultimately limited product choice.

Looking at what the ideal industrial network would offer, we can build a wish list that offers the robustness of the old combined with the flexibility of the new. This wish list might include common cabling, standard connectors, open standards, ease of configuration, flexibility, highest possible security and reduced susceptibility to attack.

Deploying Ethernet solutions

In looking at how we might be able to adapt industrial Ethernet to meet the requirements of this wish list, it is worth revisiting our definition of Ethernet, because nowhere in networking parlance has a single word been so misused as an umbrella term for so many disparate standards, technologies and

applications. And the best place to start for that is with the OSI seven layer model itself.

Layer 1, the Physical Layer, defines all the electrical and physical specifications for devices. In particular, it defines the relationship between a device and the physical medium. Layer 2 is the Data Link Layer, providing the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. It is here that Ethernet is defined as a network protocol under the IEEE 802.3 standard.

Over the years, Ethernet has become synonymous with the TCP/IP suite, but one does not necessarily imply the other. IP is defined under the Network Layer (Layer 3) of the OSI model. This Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks. The Transport Layer (Layer 4) provides transparent transfer of data between end users, and defines the likes of TCP and UDP.

The Session Layer (Layer 5) controls the connections between computers, whilst the Presentation Layer (Layer 6) transforms the data to provide a standard interface for the Application Layer (Layer 7) at the top of model. It is here that you find typical applications such as FTP, HTTP, RTP, SMTP, SNMP and others. In short, when it comes to operating as a communication architecture for industrial networks, Ethernet is capable of very little without the layers that sit above it.

Not all industrial Ethernet offerings implement the Ethernet stack in the same way. Within the Application Layer the different industrial Ethernet organisations implement their own kernels and protocols which define much of the functional benefits of their technologies. From a security point of view, though, what is really of interest are the more vulnerable lower layers.

Under the seven layer model, all it takes is for one layer to fall to an attack before the whole communications system is compromised potentially without the other layers even being aware that there is a problem. Security is only as strong as the weakest link.

Controlling cost and complexity

There are a number of discrete security products available, and these work well, but one of the biggest problems in the industrial arena lies in implementing tightly integrated security systems without incurring excessive costs and without imposing a level of complexity that makes the system difficult to maintain and support. Further, standard commercially available security solutions are rarely up to the rigours of life in challenging industrial environments.

In terms of network technology, much work has been done to make Layer 2 more secure, but in classic implementations of industrial Ethernet little has been done to address weaknesses in the Network Layer (Layer 3) and the Transport Layer (Layer 4). Like the office Ethernet implementation, the vast majority of industrial Ethernet technologies are still built around IP within Layer 3 and TCP/UCP within Layer 4.

Most industrial Ethernet network installations implement perimeter security (firewall services) at points where they connect to other networks to provide protection at these vulnerable layers.

Firewalls filter on source and destination IP addresses and protocol port numbers (for example TCP and UDP ports) to further restrict the traffic permitted to enter an Ethernet network.

Packet filtering may be implemented even among known network communities, and in some cases filtering deals with very specific device addresses and application ports to provide a layer of access security unique to an attached device and application. Despite this however, in classic industrial Ethernet implementations, Layer 3 and Layer 4 are still highly vulnerable to attack.

CC-Link IE Security

CC-Link IE (Control and Communication Link Industrial Ethernet) combines the best of many existing technologies, and applies them to optical or copper-based industrial networks with a redundant architecture that enables extremely high-speed and reliable data transfer between field devices and other controllers via Ethernet links and a signalling rate of 1Gbps.

CC-Link IE technology differs from conventional implementations by defining an open "Real-Time Protocol" within the stack layers. By taking this approach to implementing these layers within the Ethernet stack, CC-Link IE realises the benefits of our network technology wish list.

It uses standard Ethernet connectors, but most importantly from a security point of view, it inherently offers the highest possible security and is less susceptible to attack. The key distinguishing factor is an open, but controlled knowledge base for the network technology.

Security requirements for industrial Ethernet networks are continuing to evolve, with sophisticated requirements increasingly migrating from Enterprise networks to process control and other industrial environments. Wherever there are network installations, companies need to look at the probability of attacks to the network, and the risk associated with any attack. In every case, as security becomes more important, companies must look at ways to mitigate the risk, reduce the risk or eliminate the risk as appropriate within each branch of the network topology.

*John Browett is managing director of CLPA, the **CC-Link Partners Association.***

Renewing the energy efficiency of existing facilities

Automation systems can help to significantly improve the carbon footprint of buildings and plants. Retrofit projects in particular call for innovative, wireless technologies that can be easily installed and operated at relatively low cost.

SOURCE: ENOCEAN

Energy harvesting wireless technology and self-powered wireless sensors capture values that can significantly reduce and optimize the energy needs of a modern HVAC system.

INDUSTRY ACCOUNTS FOR ABOUT ONE THIRD of all the energy consumed in the United States, all together 24.0 quadrillion Btu, according to the U.S. Energy Information Administration's Annual Energy Outlook 2013. Newly constructed plants typically incorporate energy-efficient buildings and equipment, but existing facilities are often less efficient and face greater retrofit challenges.

Sensor-based data collection

The intelligent control of energy requires sensors to collect the relevant data from several points of measurement and receivers to process the information. A larger system can comprise hundreds to thousands of these sensing devices requiring power and communication.

This is an obvious instance where wireless sensors and switches are the most cost effective solution: particularly in retrofits, in situations where project timing is critical, where there is an abundance of glass fenestration (making wiring difficult) and where it is desirable to have device maintenance kept to a minimum.

There are already established technologies, primarily in the field of building automation, which can be a driver for intelligent energy management. In a building automation system, for example, thousands of sensors measure data from many different points, recording data on temperature, CO2, light or room occupancy to enable a central controller to optimize the building environment and meet individual requirements. It is not much of a stretch to go from building automation to an energy management system. Therefore, building automation principles can be the basis for energy automation processes in industries.

A major challenge is how to network an increasingly large number of individual wireless nodes or sensors that can communicate with long-range wireless networks. Different wireless standards can be used for this purpose, for example GSM, Bluetooth or IP. These standards support applications where large volumes of data must be transmitted quickly, for example in smart metering systems. However, high data rate comes at the price of high energy demand at the remote node, requiring a continuous supply of power either over cables or via large capacity batteries.

Drawback of cable and batteries

For smaller devices, such as sensors for data collection, these technologies are suitable up to a point. This is particularly true when measured data from many different points must be available to an intelligent controller. Here, however, power cables or batteries can prove to be a drawback in complex applications. Batteries last

for only a limited time, depending upon the application, and must be replaced regularly and disposed of properly. In such a highly connected energy control system, demanded in industrial plants, this can be costly and lead to downtimes.

Energy harvesting wireless technology can overcome these problems, connecting a large number of batteryless and maintenance-free sensors into existing Wi-Fi or mobile networks that process data for intelligent energy control.

SOURCE: ENOCEAN

A major challenge for energy management systems is how to network an increasingly large number of individual wireless nodes or sensors that can communicate with long-range wireless networks using GSM, Bluetooth or IP.

Harvesting flexibility

Energy harvesting wireless technology stems from a simple observation – where sensor data resides, sufficient ambient energy exists to power sensors and radio communications. Harvestable energy sources include motion, indoor light and temperature differentials. These ever-present sources provide sufficient energy to transmit and receive radio signals between wireless switches, sensors, actuators and controllers, sustaining vital communications within an energy management system. Instead of batteries, miniaturized energy converters generate power for the wireless communication of devices, keeping the maintenance effort to a minimum enabling a highly flexible installation.

For optimal indoor RF effectiveness, the 902 MHz frequency band in North America offers fast system response and elimination of data collisions. RF reliability is assured because wireless signals are less than one millisecond in duration and are transmitted multiple times for redundancy. The range of energy harvesting wireless sensors can be about 900 feet in open air and up to 90 feet inside buildings. A non-profit technical organization of 350 manufacturing company members, defines standardized application profiles for batteryless wireless devices. This ensures that solutions from different vendors can be wirelessly connected in a system, enabling system planners, integrators or facility owners to find the right pieces of equipment for their individual requirements.

Energy saving effects

Energy management, by definition, is the process of monitoring, controlling and conserving energy in a facility. Energy management systems that utilize energy harvesting wireless building automation and control technology hold are ideal for retrofitting existing spaces and with no batteries, there is virtually no maintenance. Such a solution controlling HVAC and lighting can be expected to save between 20 to 40 percent on energy. For example, if a sensor detects that a room or area is no longer occupied, lights can be automatically switched off and the HVAC systems automatically controlled, saving an average of 30 percent energy compared to a non-automated system. Alternatively, if enough natural sunlight is entering a room then lights can be automatically programmed to dim or switch off completely.

Integrated system approach

Based on batteryless technology, an intelligent system can be realized by interconnecting automated thermostats, window contacts, humidity sensors, occupancy sensors or CO_2 sensors. These are examples of the products in place, to regulate climate control automatically. In an intelligent automation system, for example, a room controller receives information related to temperature, humidity, window position or CO2 from the respective sensors and controls the heating or cooling accordingly. At the same time, the room controller sends information to an energy controller. This automation calculates the demand as a function of outdoor temperature and flow temperature to control energy generation.

The more complex a cooling or heating installation, the more information it takes to control it. This is where the self-powered technology creates advantages. Room controllers with energy harvesting wireless technology and the integration of self-powered wireless sensors to capture values can significantly reduce and optimize the energy needs of a modern HVAC system. Information can be transmitted wirelessly to a HVAC regulator or programmer, without batteries and with no need for maintenance or servicing.

Information from everywhere

Wireless and batteryless technology facilitates energy monitoring and control with little impact on the infrastructure. The wireless devices are highly flexible to install so that individual components can be easily networked to form a deeply connected system without complex cabling, especially in retrofit projects. Due to these characteristics, standardized batteryless technology is ideally suited for the last communication level in energy management, providing data from each measurement point optimizing control and enabling a comfortable user experience together with a fast ROI between two and seven years at the same time.

*Graham Martin is Chairman of the **EnOcean Alliance.***

Building resilient IoT network infrastructures

The Internet of Things is making it an absolute necessity for manufacturers to develop a more resilient network infrastructure. Given this reality, companies should complete a series of steps to understand its network bandwidth and cabling requirements.

THE INTERNET OF THINGS (IoT) encompasses everyday devices including smartphones, tablets, video cameras embedded with technology that enables these devices to interact in new ways. The IoT also broadens outside the production space to connect Operations Technology (OT) with Information Technology (IT), opening the door to an array of new applications and enhancing existing ones. These new capabilities are further bolstered by a standard Ethernet network, which manufacturers are now adopting on the plant floor as they migrate from proprietary networks.

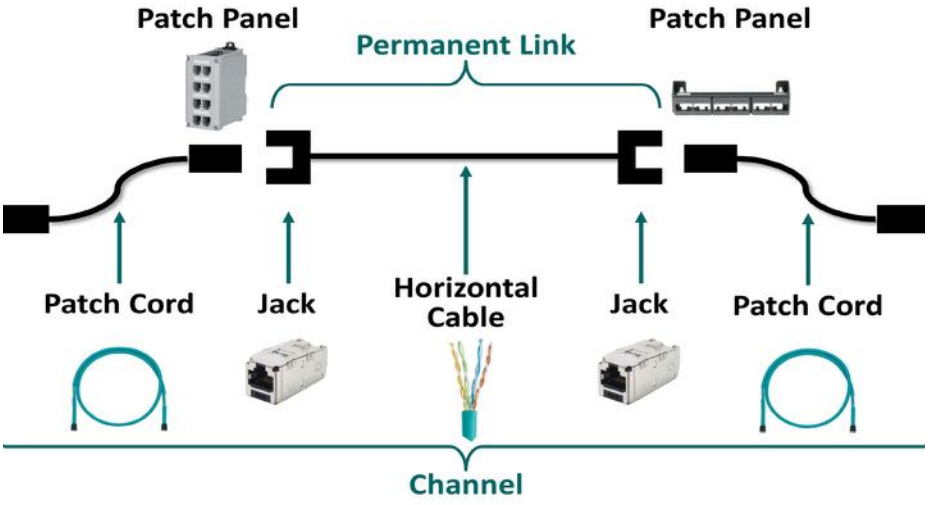
IoT and network reliability

The IoT revolution is expected to create tremendous business opportunities by 2022, especially in the industrial automation market. This translates into a value of $3.88 trillion linked to manufacturing, according to Industrial IP Advantage, and invites speculation on whether the physical cabling network infrastructure will be able to withstand the IoT flood of data flow.

The right design and cable installation are critical to overall network reliability. According to Gartner, the average cost of network downtime is estimated to be $5,600 per minute, which is well over $300,000 per hour.

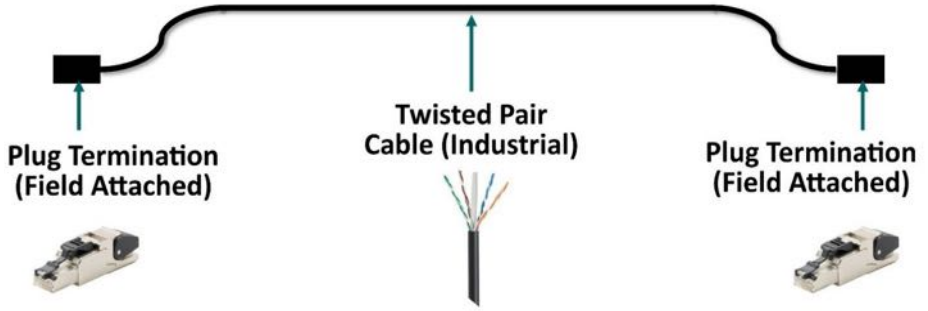
Manufacturers are acutely aware of the repercussions of downtime. In addition to the direct costs associated with down machines tied to the network, challenges exist even when machines are running. Although a plant may be able to produce manufactured goods, the company may not be able to ship or sell because it lacks quality-controlled electronic documentation, product serialization to track and trace, inventory management, and regulatory compliance data.

Enterprise applications, plant floor software, asset management and quality control applications, predictive analytics, and virus protection systems need a reliable network to work effectively. More importantly, the necessary network is comprised of more than communication protocols. The actual physical infrastructure (i.e., the cables, connectors, wires, cabinets, and panels) is often overlooked. This existing hardware —most of which has been in place for decades—will soon be overtaxed by an influx of networked devices resulting from the IoT movement.



SOURCE: PANDUIT

Simplified example of copper structured cabling



SOURCE: PANDUIT

Simplified example of point-to-point cabling

As manufacturers standardize on Ethernet across the organization, they create synchronicity and visibility between the plant floor and the enterprise to achieve gains in efficiency and output. Still, plant managers worry that their existing reliable, proprietary configurations could be degraded in an Ethernet network upgrade. Therefore, it is critical for every CIO, plant manager, and systems integrator to assess each element of the network, from communication protocols to cables, and proactively focus on future needs as they expand or upgrade their network infrastructure.

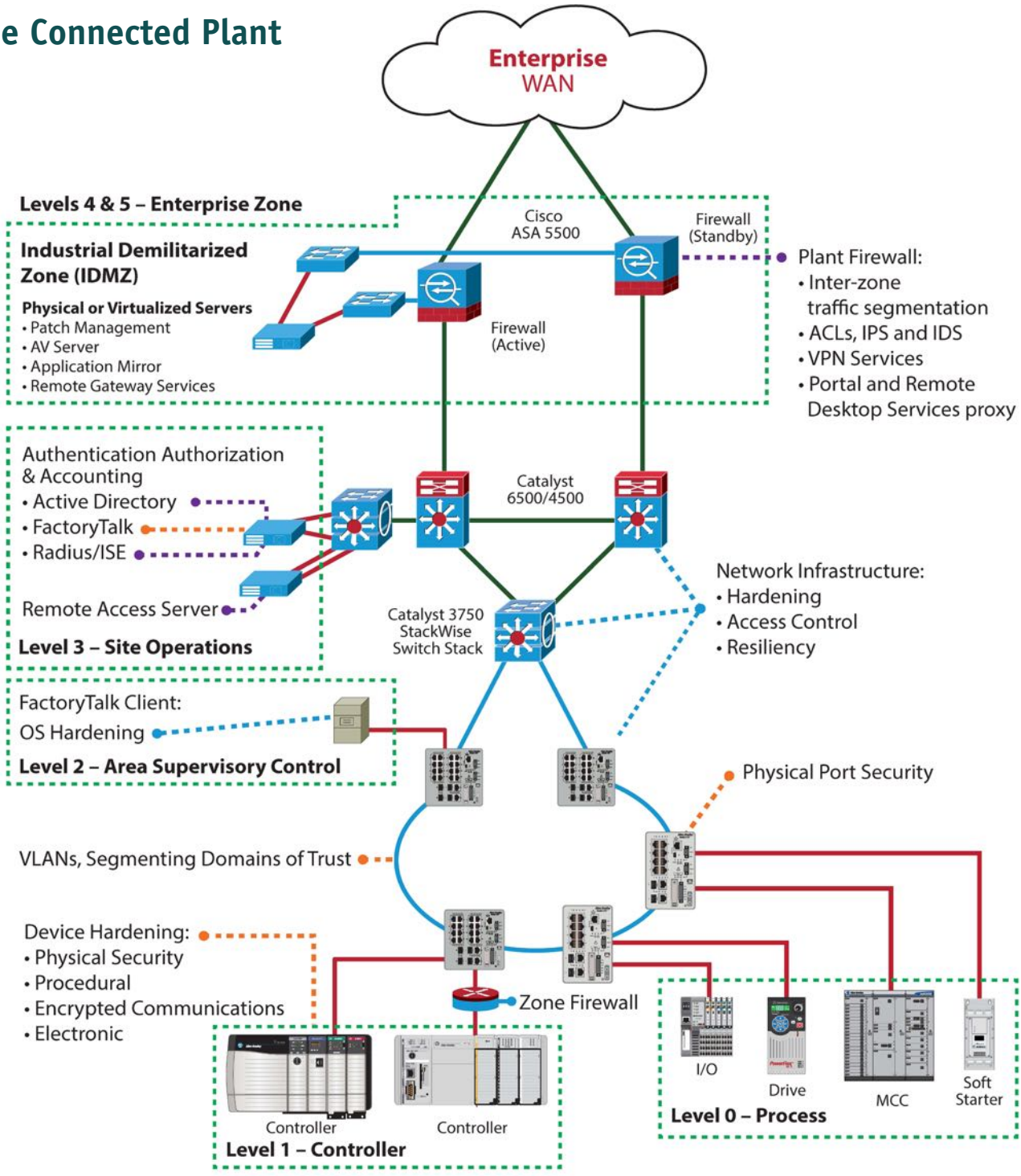
Historically separate domains

The plant floor and the enterprise have remained separate domains in the past. However, with changing market dynamics that demand just-in-time manufacturing, scalability, and operational visibility, companies are now connecting these disparate networks.

Rockwell Automation and Cisco have developed an architectural model that safely merges the two standards-compliant Ethernet networks. The model, called the Converged Plant-wide Ethernet (CPwE) architecture, is a set of best practices referring to a logical network architecture that extends to the physical layer.

This architecture uses VLANs to efficiently segment traffic across the Layer 2 and Layer 3 network infrastructure; however, all plant control traffic stays below the Demilitarized Zone (DMZ) layer, while any information needed in the enterprise zone is accessed through a server in the DMZ rather than allowing direct traffic

The Connected Plant



Converged Plant-wide Ethernet (CPwE) architecture.

between the enterprise and manufacturing compute systems. This setup allows the IT network and the operations network to share data, but they remain virtually isolated, so if the enterprise is breached or a virus is introduced, it cannot reach the production environment.

In addition to security, CPwE also considers planned and unplanned future growth of the network. As Ethernet expands into the manufacturing environment and as a unified architecture is put in place to manage all networking and to control traffic, facilities that have well-planned and structured physical networks will be best positioned to improve overall operational efficiency, productivity, and flexibility.

The new manufacturing model

Today, organizations are challenged to transform due to disruptive technologies. From the proliferation of IoT to the globalization of manufacturing, the pressure is on to achieve lower costs, and deliver to new markets.

Manufacturers in the best-in-class category put a greater emphasis on network management, network reliability, and resilience. They build redundancy into network paths as a backup and map out a wiring strategy to ensure that data speed is maximized across the plant network. In other words, the "best-in-class network blueprint" plots every aspect of the infrastructure—down to the wire.

In this environment, it pays to be forward-thinking with your physical infrastructure. Deploying the right media will help avoid performance issues and keep costly upgrades to a minimum. Late in the game, when the network is already deployed, it is very

expensive to fix issues. Something that costs $10 in the planning stage may cost $10,000 to fix in the field.

To turn the reliable, resilient network vision into a reality, companies are defining physical designs and establishing global standards. But before they can proceed, they must conduct an environment evaluation, otherwise known as an assessment.

Five key assessment steps

Manufacturers should complete the steps outlined below to understand their bandwidth and cable requirements.

1. **Number of Ethernet Devices:** Start the assessment by tallying all the Ethernet devices that require connectivity not only for today, but for the next 10 to 20 years. This may include machines, sensors, cameras, controllers, drives, and switches.
2. **Environmental Risks:** Next, consider the environmental risks to the infrastructure. For example, caustic, wet conditions could affect cable jacket material, and areas with high electrical noise may compromise copper cable. The assessment is also the time to identify obstructions to cable routing and to optimize cable run lengths. Refer to TIA-1005-A for more information.
3. **Bandwidth Consumers:** After assessing environmental risks, consider the kind of traffic flow to determine bandwidth needs. Examine all the packet-producing devices and estimate data, control, video, and VoIP output needs.
4. **Downtime:** To properly architect the network, it is important to determine the cost of downtime to help establish network investment needs. High downtime costs require design considerations for greater resiliency, cable protection, and pathways.
5. **Security:** The industrial network is not an island. As part of the assessment, manufacturers should determine how to connect with the enterprise network, which has greater security needs due to the number of security attacks.

The convergence of enterprise IT and the industrial network means a hacker could wreak havoc in a company's ability to manufacture. Therefore, it is important for companies to adhere to best practices, and build a bullet-proof security scheme when converging its IT and plant floor networks. This in-depth defense scheme should cover everything from protocols to port physical security.

Industrial network of the future

Traditionally, industrial networks have been set up in a point-to-point configuration, with a single cable terminated to plugs (i.e., a long patch cord). Structured cabling is emerging as a more robust and sustainable infrastructure because it better facilitates growth and troubleshooting, factors that are important to manufacturing. However, there are pros and cons to each approach, depending on the implementation.

Point-to-point is ideal for short cable runs in an enclosure or small ring applications. However, plugs can be hard to terminate. Another consideration is stranded vs. solid cables. Stranded cables lead to reduced distance because of higher attenuation, while a solid conductor cable can break due to flexing. More importantly, fixed length, point-to-point cables cannot be readily extended or reconfigured as a structured approach with patch panels. In addition, some network test equipment excludes connections to the tester, therefore the entire channel is not tested.

Structured cabling is preferred for longer and more critical runs, such as connecting enclosures, machines, test equipment, and cameras, as it provides a means for troubleshooting and testability, growth, and reliability. Utilizing patch cords, jacks, and horizontal cabling creates an optimized network channel. Also, the horizontal cable is easier and faster to reliably terminate to a jack versus a plug. By installing network cabling to create spare network channels for growth, technicians can connect to a different channel when adding equipment or in the event of a network cabling failure.

While there is a focus on channel resiliency, the value of structured cabling is its systematic approach to planning and deploying cabling and cable management based on the Telecommunications Infrastructure Standard for Industrial Premises (TIA-1005-A).

Media selection

Cable media is influenced by cable reach, harsh environments, electrical noise, bandwidth, and switch convergence. For example, proper copper channel cable transmits 100m while single-mode fiber optic cable can reach distances of many kilometers, depending on the transceiver selection.

Corrosive, wet, and oily environments all impact network cable jackets, causing degradation. There are a variety of outer jacket coverings such as polyurethane, polyvinyl chloride (PVC), and thermoplastic elastomer (TPE), which have varying levels of cable protection. The toughest jacket covering, polyurethane, is abrasion- and tear-resistant, and resistant to oil, radiation, fungus, oxidation, and ozone. Beneath the outer jacket, metallic foil or braid may be used to suppress electrical noise. However, the ultimate in electrical noise immunity is the deployment of fiber.

Another media consideration is bandwidth, especially for large data consumers such as interswitch links and cameras. Bandwidth requirements may necessitate higher category copper such as Category 6 and perhaps multi-mode and single-mode fiber that can transmit up to 10Gb/s.

Recovery time from a network interruption impacts manufacturing downtime. This time can be minimized by deploying fiber cable for interswitch links in rings or redundant star configurations. With fiber the switches recognize loss of signal faster than copper interfaces, and can recover communications much faster than copper. In less complex, smaller networks, copper may be suitable, but the recovery time for network faults needs to be weighed against downtime costs.

Mapping out network necessities

At this point, the network assessment is complete, the network topology is settled, the location of the point-to-point and structured cabling, and the cable construction/media have all been decided. Now it is time to design and deploy the infrastructure, starting with the plant drawing to overlay the logical network architecture on the physical layer.

By having a visual diagram of the network in place prior to the deployment, decisions can be made on routing and the environmental impact on cabling infrastructure. The ISO/IEC 24702 standard has a methodology to assess the environment with four factors - mechanical, ingress, climate, and electromagnetic (M.I.C.E).

M.I.C.E disruptions can be mitigated with the proper cable jacket covering and shielding to suppress electrical noise.

Keep the following in mind when assessing, designing, and deploying the physical infrastructure:

- Standards-compliant configurations (from TIA cabling to EtherNet/IP)
- Cabling methods, (i.e., structured vs. point-to-point)
- Network topology affecting media selection
- Fiber optic and copper cabling applications
- Appropriate jacket covering and shielding for harsh environments

Infrastructure matters

If approached in a systematic manner using standards-compliant methodology, cabling infrastructure can be a scalable solution that marries the evolving aspects of the logical and physical networks and can adapt to an ever-changing dynamic industry. Data continuity involves media, wire covering, and topology. In addition, leveraging best practices and certified techniques outlined by technology vendors allows for an efficient and cost-effective installation.

The network must withstand the test of time. Wire it right from the beginning.

*Andy Banathy is a Solution Architect for **Panduit**.*

PROFIBUS network provides reliability and robustness

Using multi-functional network components enabled a water treatment facility to overcome network interruptions and achieve a reliable, high quality network with high uptime.

THE BARWON WATER BIOSOLIDS DRYING FACILITY is a fully enclosed thermal drying operation in Australia. The facility provides an environmentally sustainable, long-term solution for reclamation of 100% of the biosolids produced at the Barwon Water's Black Rock and smaller regional water treatment facilities. In order to keep the PROFIBUS system going, Barwon Water uses PROCENTEC ProfiHubs. By using these multi-functional network components the facility is continually assured of the most reliable, high quality and robust PROFIBUS network with the highest uptime.

The Barwon Water biosolids drying facility utilizes PROFIBUS for the entire production process. The network has a combination of PROFIBUS DP, fiber optics, DP/DP couplers and a wide range of PROFIBUS PA devices. After a few years in operation, interruptions within the PROFIBUS network began to appear. To get the PROFIBUS network at peak operation again, Barwon Water called in PROCENTEC's valuable distributor Pentair PICC to assist. They visited the site and carried out a detailed network audit, through the use of PROCENTEC ProfiTrace. This innovative tool enables engineers to check the quality of the PROFIBUS network within a few hours. After the network audit, Pentair PICC realized the PROFIBUS installation at Barwon Water biosolids facility was not operating according to the PROFIBUS guidelines and that the physical layer of the network needed urgent attention as a few devices were on the verge of dropping from the network.

PROFIBUS network upgrade

In order to make the PROFIBUS network more stable and reliable, Pentair PICC recommended detailed actions to upgrade the PROFIBUS network. The PROFIBUS network upgrades were executed accordingly during a planned three-day site shut down. First, PROCENTEC ProfiHubs were installed on the PROFIBUS DP network, with critical devices isolated on separate segments to achieve galvanic power surge isolation, isolated spur lines maintenance, and reduced potential junction failure.

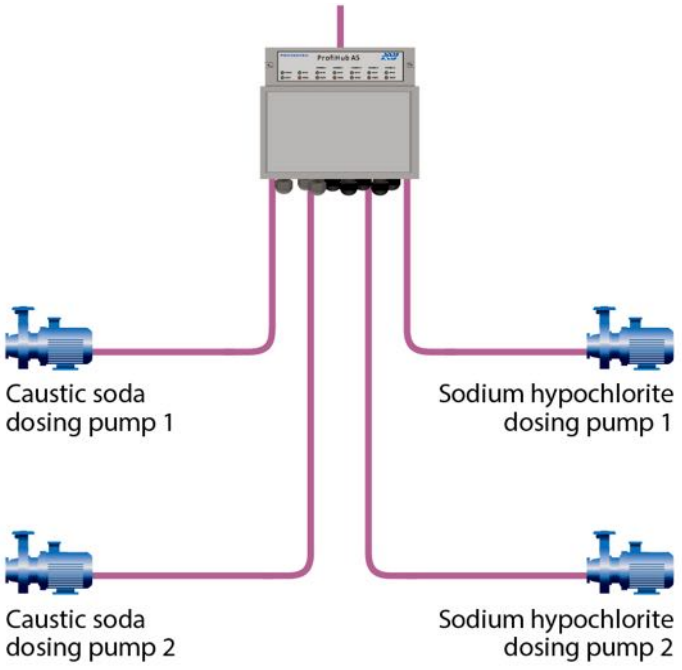
ProfiHubs were installed in various MCC cabinets to allow separation of main channels entering into the dosing pump areas. Further, the ProfiHub was utilized to connect transmitters, level sensors, remote I/O, gateways and DP/PA links within the facility.

The second recommendation was a baud rate reduction from 1.5Mbits/sec to 500kbits/sec. The baud rate was changed at the master PLC by the system integrator, allowing for increased cable lengths. Unused devices were disconnected from the network and hardware configuration on the PLC updated accordingly.Poor connections were reconfigured, improper termination was corrected, and damaged connecters were replaced. These recommendations all feed into increased operational capabilities, eliminating the poor signals that were affecting this network.

Reliable PROFIBUS network

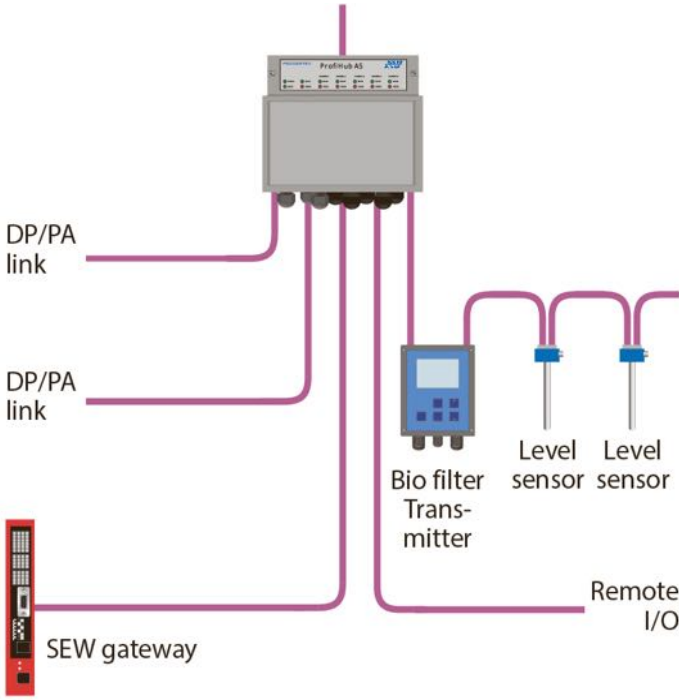
After the network upgrade, a PROCENTEC ProfiTrace report was generated showing the improved network health. The PROFIBUS network has improved remarkably compared to earlier reports. The modifications made to the network have made a significant difference in quality of the signal and the strength of the PROFIBUS network, making the network very robust and stable.

*Application story by **PROCENTEC**.*



SOURCE: PROCENTEC

PROCENTEC ProfiHub enabled new cables to be laid for each dosing pump segment.



SOURCE: PROCENTEC

The ProfiHub was also used to implement a wide range of network connections.

Time Sensitive Networking: impact or mission impossible?

Two years ago, the Time Sensitive Networking task group was established, seeking to make Ethernet usable for time-critical applications. IEEE 802 does not offer a complete solution, but instead provides standards for the data transfer layer that then requires integration into an application concept.

THE MAJOR SHORTCOMING OF ETHERNET often boils down to a lack of real-time capability but the IEEE task group, Time Sensitive Networking (TSN), intends to change this. The intention is for real-time to become an integral part of the Ethernet standard, rather than a non-standard-compliant add-on. But does that really make sense?

IEEE 802 task group

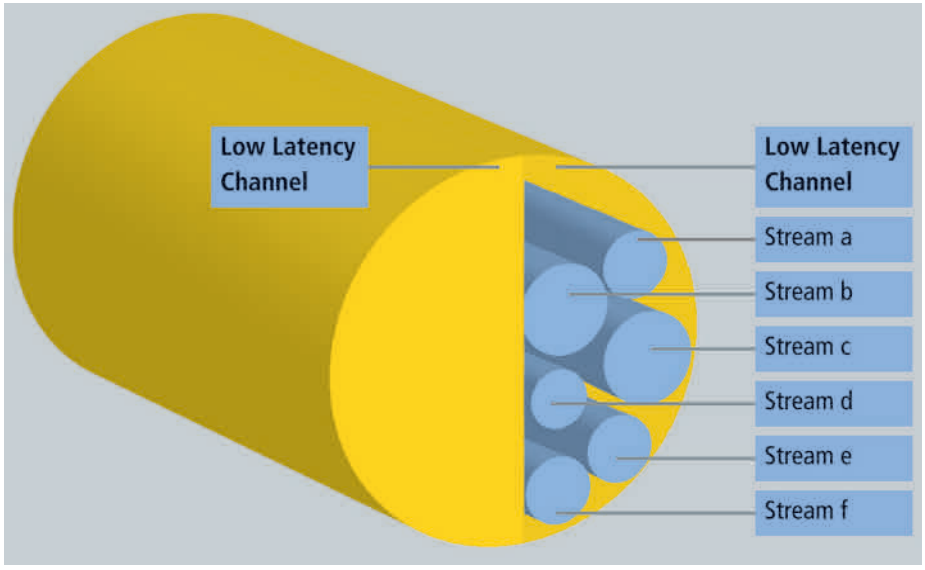
Ethernet is specified and continually developed in the working groups of the IEEE 802 project. Two years ago, the Time Sensitive Networking task group was established, seeking to make Ethernet usable for time-critical applications. However, IEEE 802 does not offer a complete solution, but instead provides standards for the data transfer layer that then requires integration into an application concept.

The original plan envisioned that the projects of the Time Sensitive Networking task group would be completed by the end of 2016. In addition to the six originally proposed extensions to the Ethernet standard, further projects are under discussion. The group is developing a procedure that involves forwarding time-critical messages only to the immediate neighbour during each cycle (IEEE 802.1Qch) which is advantageous if the cascading depth is low. The approach can help integrate wireless devices or other components with latency that is difficult to determine, and is more robust than time control.

An additional aspect discussed by the experts is how to limit the effects of nodes that act incorrectly. To this end, the incoming side (ingress) of the nodes must monitor the partners. Ethernet itself is also subject to changes; particularly noteworthy is the new two-wire transmission technology (100 Mbps: IEEE P802.3bw, 1 Gbps: IEEE P802.3bp) which can use unshielded cables. The main drivers for these new projects are car manufacturers. If the forecasts of half a billion Ethernet ports installed in vehicles by 2021/2022 come true, this will also have a lasting effect on other markets, not just direct suppliers.

TSN in automation applications

The procedures defined in TSN are not suitable for efficient distribution or gathering small data quantities. Compared with an EtherCAT solution, for a typical data volume below 10 bytes per device, TSN would result in a tenfold increase in protocol overhead, even in a best-case scenario.



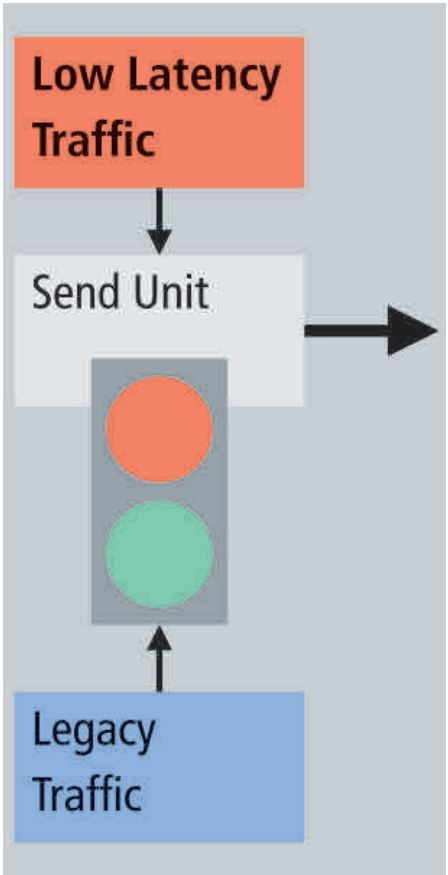
SOURCE: BECKHOFF

The data streams must be organized like the timetable of a rail network, but without transfers.

The TSN approach, with its significantly poorer efficiency, is therefore not really suitable for conventional I/O or drive applications. However, it can have advantages in heterogeneous environments with data quantities of more than 100 bytes per transfer. Such an environment can be found, for example, in the networking of controllers, in robot cells, or in the integration of camera systems into automation systems.

Since standards are unable to take into account individual cases and special requirements, some functions may not be particularly suitable for specific automation applications. For example, although IEEE802.1Qca includes a provision for the distribution of topological information, this protocol contains so much functionality that there is significant transfer and memory overhead.

The lack of scalability limits the usability for simple nodes, as the important information regarding the topology could be distributed with significantly lower overhead. In addition, degrees of freedom for synchronisation were limited in IEEE 802.1AS. Yet there is no restriction on the temporal behaviour of the individual nodes, which may have a very negative impact on cycle control. For example, delayed adjustment of the time in



SOURCE: BECKHOFF

A "traffic light system" can be used to avoid delays in data streams due to low-priority traffic.

the individual nodes at critical moments may cause increased inaccuracy.

Although time control can eliminate the influence of other protocols on time-critical tasks, the remaining real-time traffic would have to be controlled in such a way that cyclic data exchange can be realized without delays. However, this is a complex optimization problem. Even with a modest number of data streams, it is not possible to determine the optimum method within a reasonable time.

IEEE 802 only deals with data communication. In addition, a so-called application layer is required, in order to integrate communication into operations. However, at cell level the proprietary protocols of individual control system manufacturers dominate these days. There are standards at the I/O level, which are offered in a similar way in different systems; the addressing volume is usually limited, however, which can be a hindrance in structured architectures. CANopen-based protocols with certain extensions, such as those used in EtherCAT, would be suitable as intermediate level. This would facilitate the transition to the I/O protocol world and would therefore be efficient, both in the cyclic and acyclic range.

TSN – a success story?

Industrial communication has been a key driver for progress in automation technology. However, it has also produced a number of "development dead ends", such as the Manufacturing Automation Protocol (MAP), or the attempt to network with .NET components. All failed approaches were characterized by unnecessarily high complexity of protocols with relatively low efficiency and a lack of focus on the needs of automation vendors. TSN also has a tendency towards more complex procedures. Nevertheless, there are quite a few companies that have a strong interest in standardized real-time Ethernet. However, at the field level, workable solutions that are adapted to automation are already available today, so the willingness to establish an additional fieldbus will likely be limited. Still, TSN could well play an important role higher up in the automation pyramid.

It therefore makes sense to grapple with TSN and associated activities, even if many key questions remain. Automation companies and automation providers should build on the achievements at the I/O level to-date. If TSN is to become a successful model for automation in a heterogeneous cell infrastructure, there is a need to agree on an application protocol and to select appropriate real-time mechanisms from the TSN pool.

Dr. Karl Weber is Senior Technology Expert, Technology Marketing for ***Beckhoff Automation.***

TSN real-time standards

To date, the TSN group has initiated six standardization projects:

Improved synchronization behaviour (IEEE 802.1ASbt)

The previous version of IEEE802.1AS had already specified a synchronization protocol for the timing of distributed clocks, based on the IEEE 1588 standard. It had promoted the integration in a standard Ethernet environment. However, compatibility with other 1588 Ethernet profiles was lost. The main area for improvement right now is the response to error situations, such as failure of a communications line or the master. The new version should also be able to deal with different time domains in a device.

Interruption (preemption) of long frames (IEEE 802.1Qbu)

A major problem for deterministic transfer of time-critical messages is time-uncritical data streams present on the same network segment, whereby an individual frame can be more than 1,500 bytes long. This can result in delays of up to 125 µs per node cycle. The problem can be addressed by means of a frame interruption mechanism (specified within the IEEE working groups in Ethernet project P802.3br). Ultimately, this mechanism will require not only new network components, but also new Ethernet blocks.

Time control of the transmission equipment (IEEE 802.1Qbv)

The time control of send operations plays a key role in TSN. Just like in 'real life', there may be traffic jams on information highways, and even with high-priority real-time data and preemption, there may still be some variation in transmission times. Since the time-sensitive streams are transmitted cyclically, largely undisturbed communication can be realized by blocking less time-critical data. The procedure is comparable to traffic light control.

Identification of network topology and path selection (IEEE 802.1Qca)

In order to get from A to B as quickly as possible, you need a map and a route planner. Just like in everyday life, a network requires one to capture the way in which components are arranged and determine how to select the communication routes in the most efficient manner. The protocol should preferably be based on the "Intermediate System to Intermediate System" (IS-IS) concept, which is also used by routers. It involves gathering all the topology information for neighbouring nodes and distributing it through further channels. After several iterations, all nodes have all the topology information from the entire network. If there are several possible routes that lead to the destination, the procedure can be used to find the shortest one. It can also be used to identify redundant routes.

Smooth redundancy (IEEE 802.1CB)

Although the IEC already provides specified protocols for smooth redundancy such as High-availability, Seamless Redundancy (HSR), or the Parallel Redundancy Protocol (PRP), they require that the complete data exchange between stations be designed for redundancy. This can cause problems, because the order of the messages is not respected in the event of a fault. In addition, troubleshooting is quite complex. For IEEE 802.1, it was therefore decided to explicitly apply smooth redundancy only to individual critical data streams. This makes it possible to reduce the protocol overhead, and critical points are easier to identify.

Bandwidth reservation (IEEE 802.1Qcc)

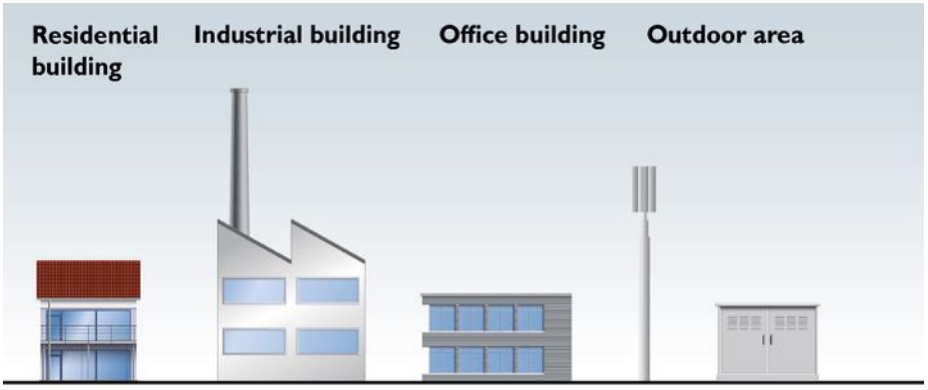
A major problem with Ethernet is found with overload situations, such as when data are received through two channels and forwarded over a single output. A large memory is also sub-optimal, since the dwell time increases with the filling level. In automation technology, this delay (best effort) cannot be controlled by increasing the response time. In order to eliminate this behaviour, real-time data streams are treated preferentially. However, this results in a risk that overload situations are intensified even further, if the proportion of real-time communication becomes too large. For this reason, the required bandwidth is determined precisely, and then firmly reserved. The protocol enables a real-time load of up to 80% of the bandwidth. It is an extension of the existing reservation protocol.

Reliable fiber optic connections for industrial and outdoor use

For wide area networks and fiber optic plug-in connectors used for industrial and outdoor deployment, what defines reliability? In diverse environments including processing plants and robotic production cells, professional fiber optics provide numerous advantages.

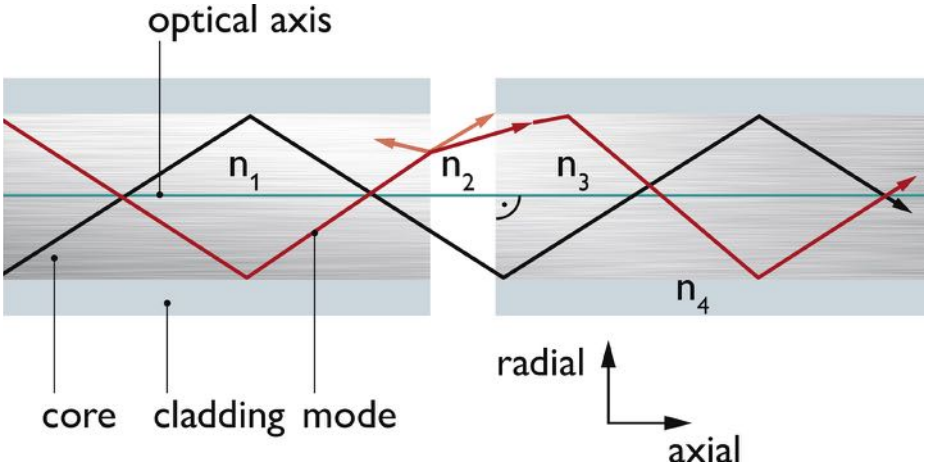
STARTING WITH WIDE AREA NETWORKS for telecommunications, fiber optics have become the data transmission medium of choice in many different areas of application. The industrial sector has been deploying fiber optics very successfully for many years. No matter if it's expansive plants in the processing industry or production cells based around robots – professional fiber optics provide numerous advantages.

Optical fiber of all types remains unaffected by electromagnetic interference and surge voltages. Thanks to electrical isolation, parasitic voltages and equalization currents are also avoided. Depending on the type of fiber, fiber optics can provide much higher transmission distances than electrical data transmission.



SOURCE: PHOENIX CONTACT

With fiber optic plug-in connectors being tested, reliability will largely depend on their design and on environmental conditions.



SOURCE: PHOENIX CONTACT

The modes inside the optical fiber are affected by unfavorable refraction indices, foreign objects, and humidity – bad field conditions can disrupt the transmission.

Not parallel to the optical axis

In order for data transmission to be reliable, there are a few technological factors to consider. Transporting light-based signals along fiber-optic cables is a highly specialized process. Individual light beams – which are also described as modes – are introduced into the optical fiber by means of a light source such as LEDs or a laser. Once inside, these modes travel along the fiber. Depending on the type of fiber being used, a single-mode fiber only transports one mode; all other fiber types are multi-mode. The modes do not travel in parallel to the optical axis, which means that they are reflected off the fiber's cladding and then take a different direction.

With a plugged connection, there are two optical fiber ends facing each other. The light exiting the first fiber enters the second fiber, where its transport continues. However, this transition is prone to several types of disruption. For example, the fiber surfaces are never completely flat when they meet, which means there is a minute air gap between the fiber ends; this changes the refraction index and thereby causes an altered light path.

In this case, some modes may be diffracted so much that they cannot be transported any further down the second fiber, which results in a decrease in optical intensity. In addition, the modes are reflected at the fiber boundary, which causes individual modes to be diverted back down the fiber. These modes therefore also become unavailable for transporting the signal along to the target – and if a laser is used at the source, they can also interfere with system operation.

Lastly, when there is a radial offset between the optical fibers, some of the modes exiting the first fiber connect to areas of the second fiber that are not suitable for transporting the modes. Again, this causes an attenuation loss.

Light path and refraction index

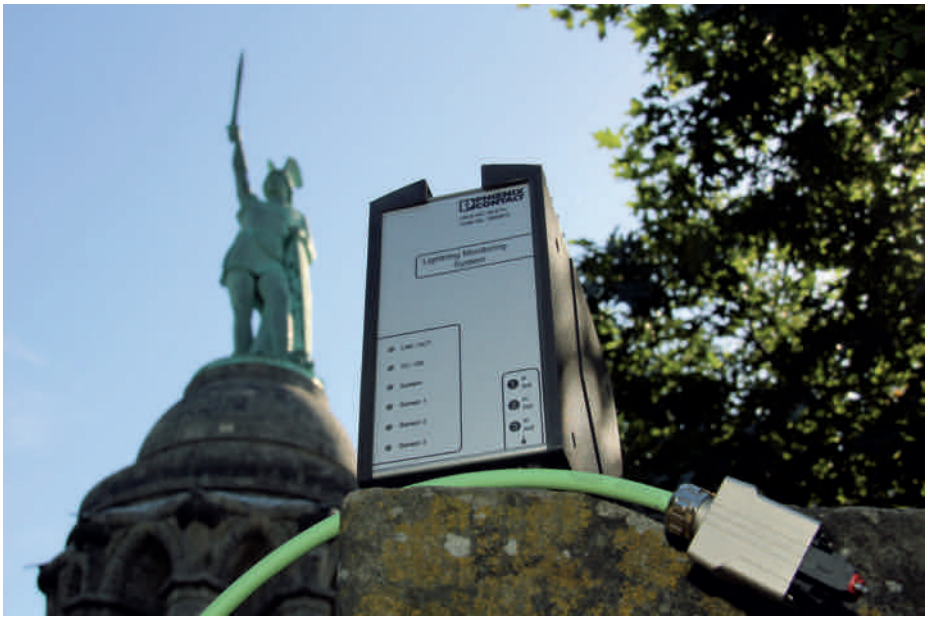
Due to the issues inherent to the optical fiber ends touching, there is a risk of dust and other foreign objects getting between the fiber ends, as well as humidity, which may be caused by condensation. This can interrupt the modes. Similarly the light path may be diffracted by an unfavorable refraction index, which means the modes travel back into the first fiber.

Manufacturers of plugged connections for fiber optics and preassembled cables do their best to design their products as precisely and tidily as possible so as to avoid these side effects. On-site technicians are also trained to install fiber optics as professionally as possible. The quality of the products and their installation is usually documented by an acceptance test following installation.

Once a system goes live, it is subject to real-world environmental conditions. As these often do not yet apply during acceptance testing, the data transmission quality may still decrease considerably if the effects outlined above occur at the plug connections for the optical fiber ends. Mechanical stresses such as shocks and vibrations, for example, may temporarily cause an exaggerated axial and

SOURCE: PHOENIX CONTACT

Fiber optic plug-in connectors transmit data securely and reliably, and users also benefit from innovative connection methods and industrial-level designs.



SOURCE: PHOENIX CONTACT

One field application using fiber optic transmission, a lightning monitoring system being used to measure lightning currents, reliably deploys fiber optic plug-in connectors in an outdoor setting.

radial offset of the fiber ends. Humid heat and temperature changes, as well as direct exposure to liquid, can cause a moisture layer between the fiber ends. This further attenuates the optical transmission path, and in the worst case, the data transmission breaks down completely. In addition, aggressive substances, gases, and UV light may damage the housing materials. This compromises the mechanical integrity of the devices, making them more vulnerable to liquids and foreign objects.

Type testing simulates stresses

With fiber optic plug-in connectors for industrial and outdoor deployment, the connector design crucially determines the suitability of the components (Figure 3). Depending on the type and extent of the stresses to be expected, the products are divided into different environmental categories. Products from Category C, for example, are intended for deployment in offices and similar environments, whereas products from Category I are intended for high-stress industrial environments.

Type testing is applied to the components to simulate the environmental stresses to be expected for each category. The components are subjected to tests that represent typical real-world scenarios: shocks and vibrations; forces acting on the plug-in connector; movement of the connected cable; temperature and humidity changes; as well as exposure to liquids and gases. The tests ensure that the optical transmission characteristics, particularly the attenuation and return loss, are not degraded to a level where the data transmission may break down.

When planning for data transmission via fiber optics, then it is of paramount importance to be familiar with the environmental conditions to be expected and to select the components accordingly. Only then will it be possible for the tested transmission path to function securely and reliably in real-world operations.

Fiber optics for data transmission has provided lasting success in the realm of industrial automation technology and outdoor deployment. Their reliability for a range of different purposes is granted by using the appropriate environmental categories. The technology has been deployed in these sectors for many years, and is known for its long-term reliability and effective data transmission.

Bernd Horrmeyer is Senior Specialist for ***Standardization at Phoenix Contact.***

Connector categories for different environments

Different areas of application necessarily entail different environmental conditions. Both the design and testing of fiber optic plug-in connectors are heavily informed by the environmental conditions they are subjected to, be it inside an air-conditioned office or in an underground cable duct. The applicable standardization committees have established a system of categories that classify the deployment of fiber optic components in different environmental conditions. These categories are described in the IEC 61753-1 standard. Each component is subjected to a series of environmental tests based on the different categories, and if it passes these, it is certified for the most suitable category. This way, users who are familiar with the category definitions can easily identify the components most appropriate to their requirements.

In differing areas of deployment, fiber optic plug-in connectors are certified according to IEC 61753-1 using type testing for different environmental categories.

Many of today's fiber optic components are deployed in air-conditioned rooms inside office buildings and data centers. Category C, which is associated with this, therefore only accommodates low environmental stresses. In the past, the plug-in connectors used outdoors or in challenging environments were mostly designed for indoor use. This has now changed with the inclusion of Category I in the IEC 61753-1-3 standard to represent industrial environments. This category specifies the component requirements – such as those for plug-in connectors – in such a way that they can also be deployed outdoors (Figure sidebar text). Technicians and developers in the automation technology sector therefore now have access to common definitions of the environmental compatibility of fiber optic components to be deployed outdoors or in challenging industrial settings.

Using Power over Ethernet procedures for effective designs

802.3at-2009 provides procedures for manufacturers that ensures compatibility, and serves as a guide for PoE applications. It also describes how to signal the power requirement from the powered device to power sourcing equipment for effective allocation of power.

INSTALLING A SEPARATE POWER LINE for devices such as IP phones, IP cameras, code readers or WLAN access points is not a requirement if the user supplies power and data via the same cable. Both can be provided by using an Ethernet switch and procedure called Power over Ethernet (PoE) which can help achieve the goal of distributing the required power to all consumers with fewer voltage supplies.

PoE standards and procedures

Because manufacturers do not always offer devices that supply and consume PoE at the same time, it is of utmost importance that all manufacturers adhere to one definition. The IEEE 802.3at-2009 standard for Power over Ethernet describes a procedure for all manufacturers that ensures compatibility with devices from another manufacturer.

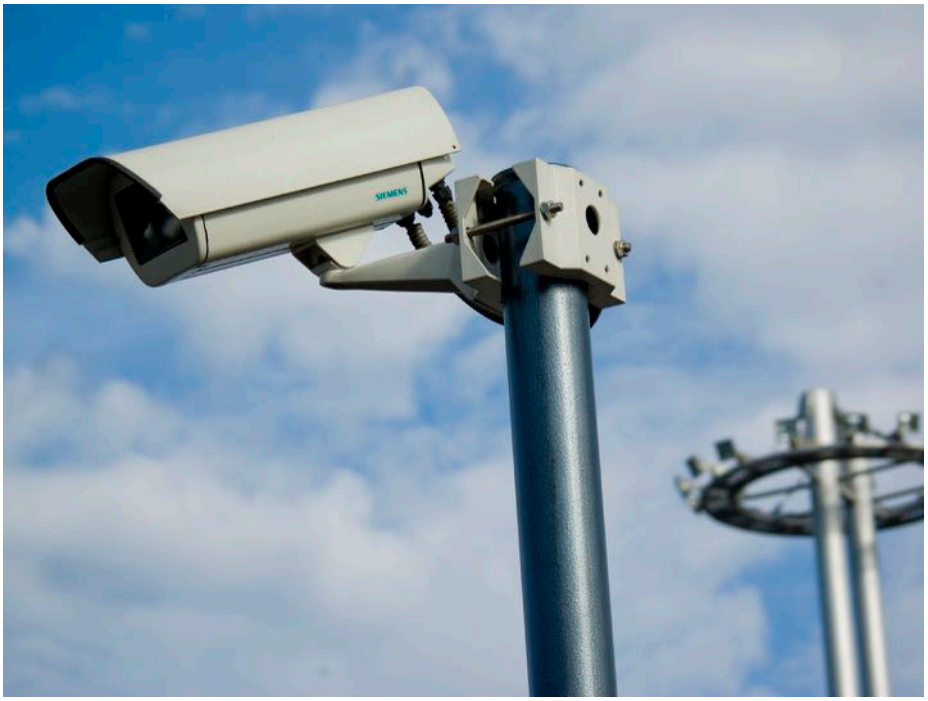
A device supplied with power is a PD (Powered Device). A device supplying power is PSE (Power Sourcing Equipment). The practical challenge is to use the resources efficiently. It starts with dimensioning the voltage supply and ends with the required number of PoE-capable ports at the switch. In most cases, existing power is not used to its full potential.

There are two procedures in the standard describing how to signal the power requirement from the PD to the PSE to allocate this power. Electrical energy is not transmitted unless the PD has successfully registered as consumer.

Classification into power classes

The first procedure of classification takes place on the lowest layer, the physical layer. This procedure meets the older standard, IEEE803.2af, and is referred to as Type 1 in the current IEEE802.3at standard. Many devices on the market only support this type. Five power classes (0, 1, 2, 3 and 4) are defined for a PD. Because the value of class 0 corresponds to the value of class 3, we often only refer to four different power classes. Class 4 must be supported by a powered device according to IEEE802.3at Type 2.

The PD assigns itself to one of these power classes when connecting to the PSE. The PSE classifies the PD by measuring the classification current. A Classes 3 (6.49 W to 13 W) and 4 (13 W to 25.5 W) in particular cover relatively wide ranges, so that unused power must be reserved and is not available to any other PD.



SOURCE: SIEMENS

Power over Ethernet is used when no power outlet is available on-site such as with a camera mounted to a mast.

Optimizing power demand signal

The second procedure is classification via the data link layer (layer 2 of the OSI layer model). The PD informs the PSE via LLDP (Link Layer Discovery Protocol) about its electrical requirement. This procedure has finer power resolution that goes beyond the defined power classes. The connected PDs usually reserve the maximum power they need at full load.

However, if this power is not used by the consumer device because devices seldom run continuously at peak performance, this power is not available to any other consumer according to the rigid scheme.

Because the current requirement values can be transmitted from the PD to the PSE even after initial registration, this procedure is superior to the one using power classes. Thanks to the fine granularity and the dynamic demand signal, more PoE consumers can be operated on one switch at the same available overall power than if each were to statically reserve the maximum power draw for its class. However, this procedure cannot be applied to devices of the "old" communications standard (IEEE802.3af).

Only a PD according to IEEE802.3at Type 2 must support classification via LLDP and via power classes. A PSE, on the other hand, must only support one of the two classification procedures. This ensures that each PSE can always be used with any PD.

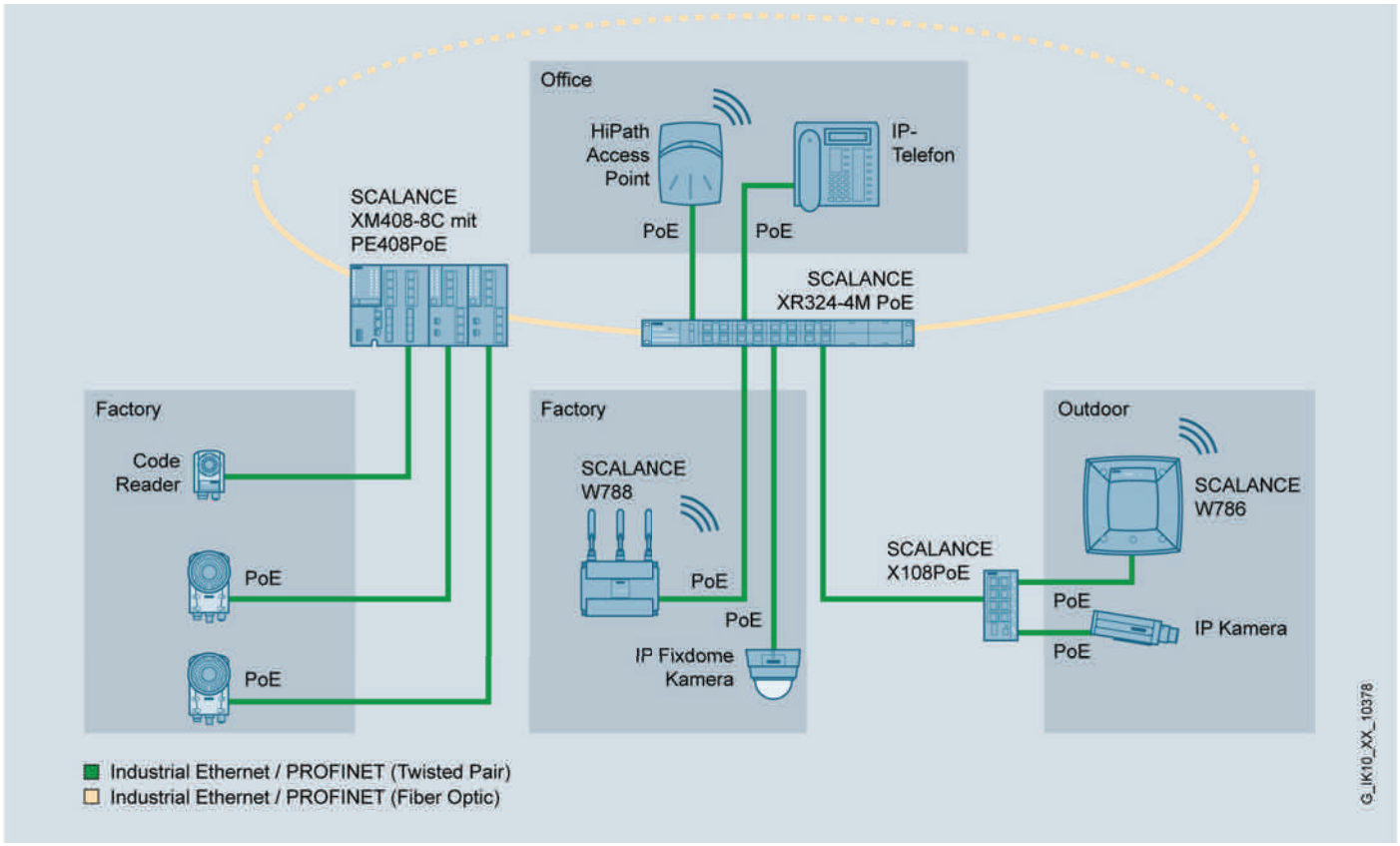
Power management in extreme cases

But PoE power management involves even more. If all connected PDs require more power than is available at any given time, a prioritization has to take place. Three stages (critical, high and low) are available in this case. The standard stipulates that the PSE is not to distribute any electrical power to a PD if the demand exceeds the power that is available. As a result, the PD is switched off.

If a device with a higher priority is added to an existing system and if the total available power would be exceeded by this step, a PD with a lower priority is switched off so that the PD with the higher priority is supplied. A user should keep this in mind and come up with a useful prioritization that determines which device is most important and which device could be switched off first in case of need.

Because standards usually represent a compromise between the many parties

SOURCE: SIEMENS



Users do not have to install a separate power line for IP phones, IP cameras, code readers or WLAN access points if they supply power and data via the same cable.

Class	Power output by PSE in watts	Power received by PD in watts
0	15.4	13.0
1	4.0	3.84
2	7.0	6.49
3	15.4	13.0
4	30.0	25.5

involved, there is frequently a need for a solution that expands this standard for individual applications. Another option for power distribution is to specify a static maximum power limit for each port on the PSE. The static PoE power distribution can also be used for PDs that only support the older standard, IEEE802.3af. The user sets the maximum power available per port at the PSE. Due to the finer granularity, this is better than power classification to the standard in which the range within a class can be rather wide. Static power distribution does have its limits, of course.

If a specific power is reserved for a port and a PD, it cannot be used by any other consumer even if the PD is not connected at all. Users need to be much more familiar with the requirement in this case, and may find information on power requirements in the technical specification of a PD or determine it by conducting their specific measurements.

Calculating the potential savings

Let us conclude with a practical example, which illustrates the savings potential of PoE power management. A major difference between the power that is drawn by the devices and the power that is reserved according to the power classification may add up to rather large amounts with multiple PDs.

The difference may be so large that additional PDs could be supplied with static power distribution compared to the standard power classification. If a WLAN Access Point consumes a maximum of 8W, for example, it must reserve 13W according to its classification (Class 3). The result is a difference of 5W that is reserved but never used. This means with a total available power of 30W with static power distribution a total of three instead of only two of these WLAN Access Points could be supplied. This also means that there is no need for an additional switch, which otherwise would possibly be required for the third access point. Scalance technology includes switches that are power sourcing equipment, as well as WLAN Access Points that are powered devices.

The standard is a good basis and enables easy compatibility across all manufacturers, but offers only limited options especially for devices that are not of IEEE802.3at Type 2. These devices are still widely used even though the standard was adopted in 2009. PoE Power Management enables optimal use of available power even when you use devices that do not support IEEE802.3at Type 2. The topic of efficient power distribution is becoming increasingly important due to growing power requirement caused by higher data rates.

Outgoing vs. incoming power

Let us now point out the difference between the power that is output by the PSE and the power that is received by the PD. We have to deduct the effective power loss caused by the transmission across the Ethernet cable with a maximum length of up to 100m. In addition, Ethernet cables have never been optimized for low power loss. While 15.4W have to be output for Class 3 at the power sourcing equipment, we are only expecting 13W to be received by the consumer. The loss is even greater for Class 4 where the output by the PSE is 30W while no more than 25.5W is received by the PD.

*Anja Adling is Product Manager for Industrial Ethernet switches at **Siemens**.*

Mission-critical redundant serial-to-Ethernet data

Redundant serial-to-Ethernet device servers can eliminate single points of failure for networked devices, while also assuring data redundancy supports data transmission with dual-independent host connections simultaneously.

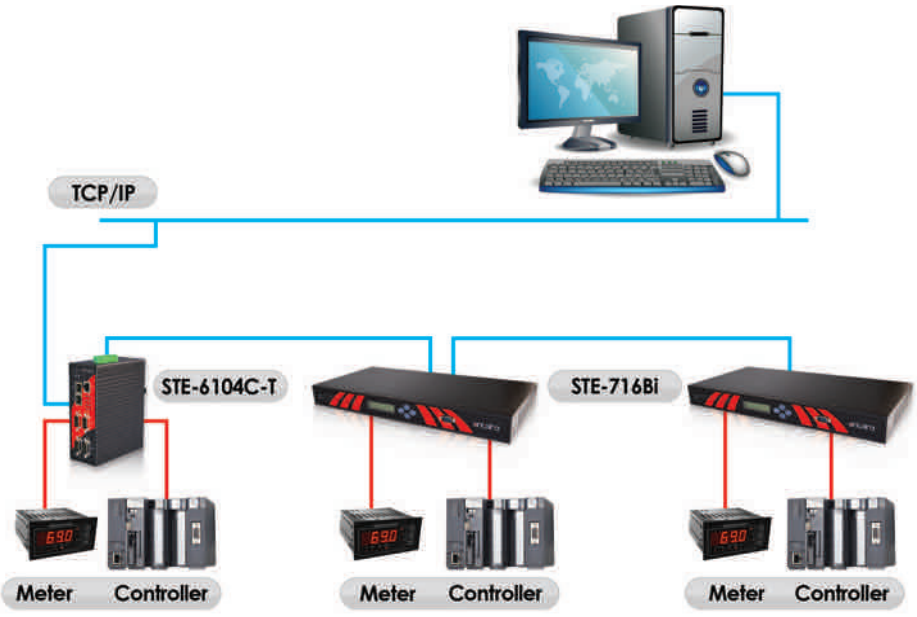
SERIAL DEVICES STILL PLAY A MAJOR¬ ROLE in many applications worldwide to collect or report process data. No matter the industry, from Power/Utility, Water Wastewater Treatment, Oil/Gas or Mining, Transportation, Factory or Process Control Automation, Medical, to Security, many applications are still equipped with legacy serial equipment, such as PLCs, sensors, meters, barcode scanners, display signs, security access controllers, and CNC controllers for processes, that are not yet Ethernet ready for a TCP/IP network.

Why redundancy is important

Today, in these industries, it can be challenging to connect serial devices to an Ethernet network. Serial-to-Ethernet technology has been approved since the late 1990's, and represents a paradigm shift. Data transmission which was previously tied to a 45-foot RS-232 serial cable can now be made available across TCP/IP Local Area Networks (LANs), Wide Area Networks (WANs) and even the Internet.

It benefits the limited transmission distance of serial-based connections and can be extended to essentially any distance with Ethernet. Serial-to-Ethernet can also benefit engineers in many applications to centralize remote management for easily and efficiently accessing, controlling and/or monitoring the status of field serial devices.

As engineers start to depend on access to these islands of information, issues such as the environment, connection reliability (uptime), and accessibility become top concerns. Thinking of redundancy as a design paradigm is important, especially, mission-critical applications that cannot afford data to be lost by any network downtime. Building a reliable redundancy system with a primary and secondary remote host PC or Server will allow field devices to exchange data simultaneously through a dual-network infrastructure. With this setup, engineers will have no need to worry about any failures occurring because the primary and secondary hosts will continuously communicate with field devices.



SOURCE: ANTAIRA

Daisy chain solution for LAN bridge mode.

SOURCE: ANTAIRA

Ethernet switching solution for LAN bridge mode.

Serial-to-Ethernet redundancy

Typical Ethernet networks consist of many links between hosts and Ethernet switches, and form a tree topology with hundreds of point-to-point wired connections. Any link failure in the network could bring the entire operation to a critical halt. A redundant ring network allows a small portion of the network to be kept idle until another part of the network fails, at which point the "redundant" portion is activated to maintain the flow of data. However, building a reliable redundancy system can create other challenges to engineers, due to specific hardware and the costly software development.

Technology is now available to address the redundancy needs of users, incorporating new features in industrial redundancy device servers including:

- **LAN Bridge Mode Solutions –** A dual LAN port solution that allows engineers to perform daisy chaining.
- **LAN Redundancy Mode Solutions –** Redundancy serial devices support IEEE802.1D/W Spanning Tree or Rapid Spanning Tree Protocols, and open standard ITU-T G.8032/Y.1344 ERPS (Ethernet Ring Protection Switching) Protocol to provide a single-ring redundancy network solution.
- **LAN Dual Subnet Mode Solution –** This technology will enable engineers to setup the device servers to connect two independent networks with different IP addresses for data redundancy solutions. It involves creating a complete backup to the Ethernet network.

Device server overview

Device servers represent the segment of product also known as Serial-to-Ethernet converters, which essentially allow any serial device with a serial port to communicate with an application across an Ethernet IP network. Serial device servers provide Virtual COM operation mode and TCP Socket connections that allow an application to communicate with a remote networked serial port as if it were attached locally.

Types of connections to device servers:

- Raw TCP Socket
- User Datagram Protocol (UDP)
- Serial Tunneling (a pair connection)
- Virtual COM

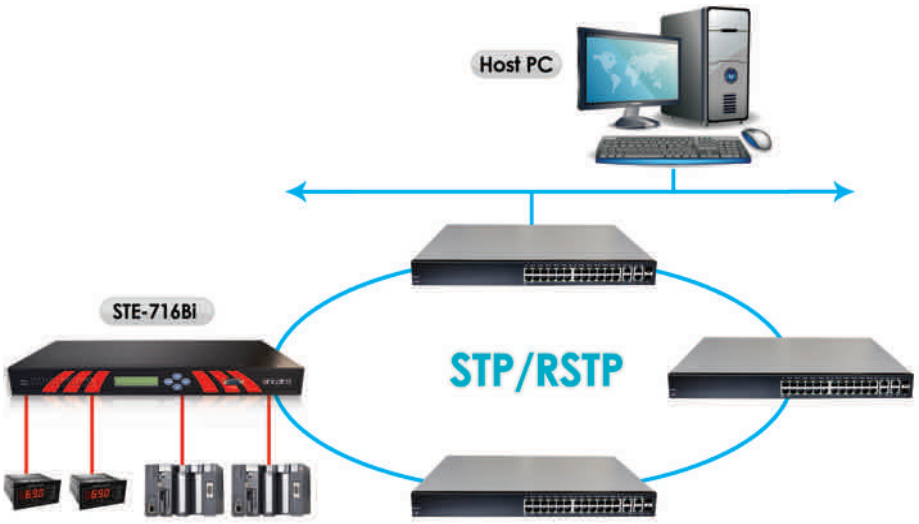
LAN bridge mode

Dual 10/100Tx LAN ports allow engineers to connect multiple serial devices in a single location through the Ethernet network. Engineers can enable LAN Bridge Mode to cascade multiple serial device servers through a second LAN port. When enabling this feature, LAN 1 and LAN 2 can use the same IP address setup.

In many manufacturing automation applications, Ethernet-based devices are now being incorporated on the plant floor with a variety of legacy serial-based devices. By enabling LAN bridge mode, the device server can also allow engineers to apply a second LAN port as a switching port to connect with the Ethernet-based device, instead of buying an additional Ethernet switch for the application.

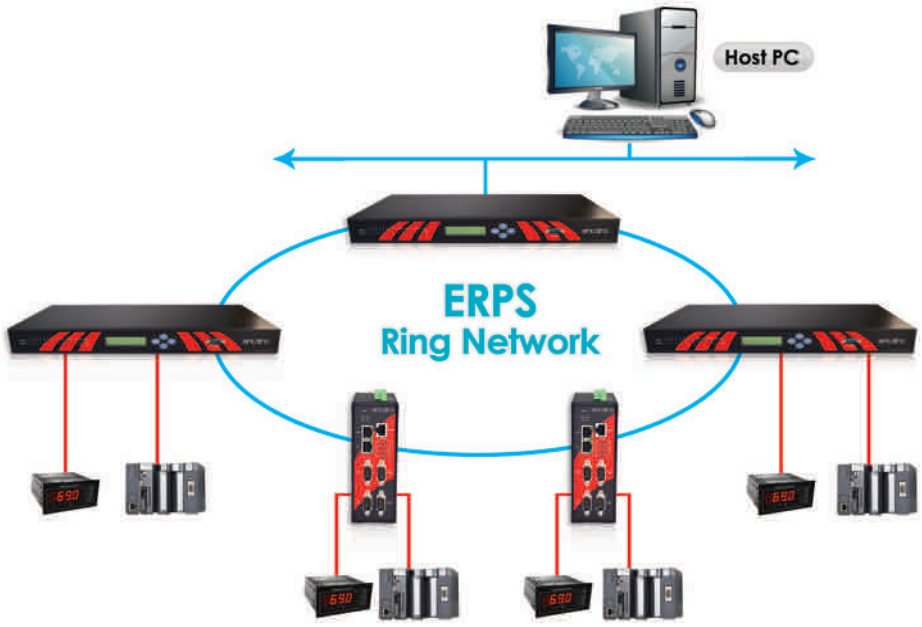
LAN redundancy mode

LAN redundancy mode allows users to setup a single-ring redundancy network with all device servers. This technology uses a physical link in the network as a backup path, and the built-in software allows devices within the ring network to transmit data to the next connection link in one direction. The data transmission will be routed to the backup path direction if the built-in software does not detect data transmission in an uplink port, eliminating any network downtime concerns. Redundancy serial device servers can provide two types of open standard network recovery protocols to support a redundant ring network: IEEE 802.1D/W and ITU-G.8032 ERPS.



SOURCE: ANTAIRA

Daisy chain solution for LAN bridge mode.



SOURCE: ANTAIRA

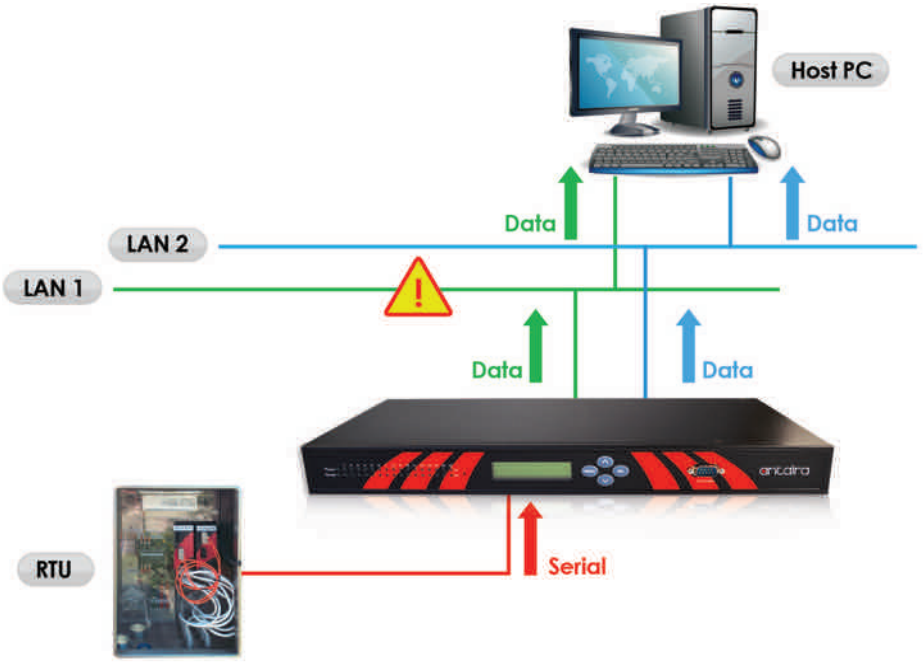
ERPS protocol for LAN redundancy mode.

Spanning tree protocols

IEEE 802.1D, Spanning Tree Protocol (STP) was introduced in 1990 to protect the network from broadcast storms caused by unintended loops, and to reduce network crashes caused by failure of a single link in the network. IEEE 802.1w, Rapid Spanning Tree Protocol (RSTP) is an enhanced version of STP released in 1998. Both STP and RSTP detect duplicate paths in the network and then block data from being transmitted across those duplicate paths.

The STP/RSTP protocol is a typical setup for a tree or star topology network and can be used with complicated mesh-type networks. The advantage of setting up mesh-type networks is that there is no need to worry about loops. The STP/RSTP algorithm analyzes the network automatically to determine if any loops exist. If loops are discovered, the algorithm determines which links in the loops should be blocked, and the blocked loops are then reserved for use in the event that an active link is broken. Meanwhile, the STP/RSTP algorithm springs into action by activating one of the redundant links in the network.

However, there is also a drawback to using STP/RSTP within an industrial network; slow recovery time. The STP protocol can take up to 30 seconds for network recovery, and



SOURCE: ANTAIRA

Dual-network redundancy.

RSTP can take up to 3~5 seconds. Since data transmission from device to device is in a matter of milliseconds, the slow recovery time of STP or RSTP protocol can run a potential risk of losing data between 3~5 seconds.

Ethernet ring protection switching

ITU-T G.8032/Y.1344 ERPS (Ethernet Ring Protection Switching) was introduced in 2008 by the International Telecommunication Union (ITU). ERPS defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. It was defined to protect the point-to-point, point-to-multi-point and multipoint-to multipoint connectivity within a ring network topology.

Antaira's STE-6104C-T and STE-700 series supports an Ethernet Ring Protection Switching (ERPS) protocol for Ethernet layer ring networks without requiring extra managed Ethernet switches. By enabling the ERPS function, users can connect all serial device servers to a ring topology network. In a ring topology, each ring node is connected to an adjacent ring node participating in the same ring using two independent links (i.e. two ways).

Loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any given time. This particular link is called a Ring Protection Link (RPL). A control message called an R-APS coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the owner node, which is referred to as the blocking state. In case of a network failure, the RPL owner node will be responsible for unblocking the RPL to allow it to be used for forwarding, hence why it's called the protection state.

The RPL becomes the backup link when a link failure occurs. Ethernet Ring Protection Switching (ERPS) provides a highly reliable and stable protection within the ring topology, and supports a network recovery time <50ms.

LAN dual subnet mode

Dual independent LAN ports simplify setup of dual-network redundancy architectures, in order to perform data redundancy for mission-critical applications. LAN dual subnet mode can be used to set up a redundant LAN between serial devices connected to the device server and the host computer.

The redundant structure involves using the device server's two LAN ports to set up two independent LANs that connect the device server to the host computer. If any LAN port link fails, the other LAN link will continue transmitting packets between the serial devices and the host, with the packets passing through the device server. As a result, LAN dual subnet mode performs a zero data loss mechanism to support data redundancy applications.

Redundancy options

In a multi-host setup, serial device servers can establish TCP connections to the serial port at the same time, duplicate the serial data, and transmit the data to all hosts at the same time. Ethernet data is sent on a first-in, first-out basis to the serial port when data comes into the device server from the Ethernet interface.

By setting up a LAN dual subnet mode, the device server can provide a highly redundant network structure that takes advantage of built-in dual LAN ports, dual IP addresses, and dual MAC addresses. Engineers can setup two remote host PCs or servers with two independent networks to connect to the redundancy serial device server. The remote redundancy system sets one host PC up as a primary host and another PC as a secondary host as a backup system.

When the primary IP fails, the backup IP will take over by using a switching library. However, this type of setup will only allow the primary host IP to transmit data bi-directionally to the device server, and the secondary IP to receive data from the device server.

Data redundancy in substations

Within power substations, engineers cannot afford data loss from any piece of equipment. Building reliable systems and dual-network architectures for remote data acquisition and access control become mission-critical. There are so many serial-based devices, such as protection relays, controllers, switch gears, and RTUs that require integration with major redundancy systems and networks which can become a challenge because traditional redundancy systems and networks require costly software development and specialized hardware.

LAN dual subnet mode allows engineers to setup dual-network redundancy architectures without requiring a front-end redundancy system to connect all bay level legacy serial devices and exchange data simultaneously with remote dual-host servers.

Although there are a variety of Ethernet-based or USB-based devices in the market, they are more for consumer, commercial, or enterprise type equipment that thrive only in indoor or air conditioned environments. Most industrial application measurement devices are still being developed by device manufacturers which means serial is still prevalent in today's automation world and applications require real-time and accurate data exchange between field serial devices and remote control management maintenance system.

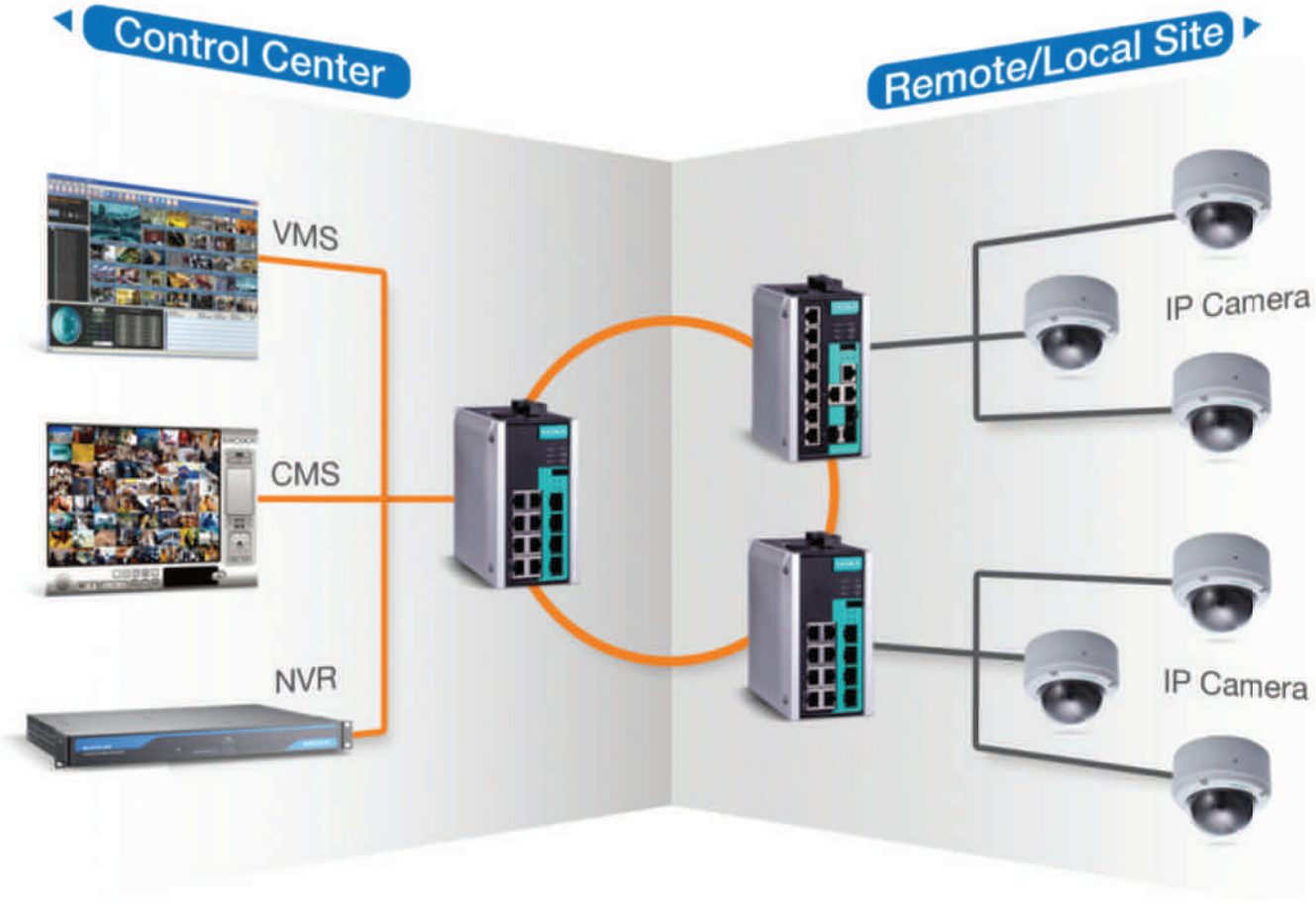
Industrial serial device server technology provides high industrial grade, environmentally proven design, and features that can assist in a number of mission-critical applications for data assurance and accuracy solutions.

- **LAN Bridge Mode –** applications can be applied as daisy chain connections, or Ethernet switching solutions.
- **LAN Redundancy Mode** - includes STP/RSTP protocols for mesh-type topologies, and the open standard TU-T G.8032/Y.1344 ERPS (Ethernet Ring Protection Switching) protocol for ring network topology solutions, and supports a standard network recovery time <50ms.
- **LAN Dual Subnet Mode –** supports dual-network setup to transmit serial data simultaneously to remote redundancy servers.

Brian Roth is a Marketing Product Engineer for ***Antaira Technologies.***

Nonstop IP surveillance using optimized Ethernet networks

Video surveillance systems are playing an increasingly important role in mission-critical infrastructures. Technical challenges can be effectively addressed using multicast configurations that can save an impressive amount of bandwidth for the entire network.



SOURCE: MOXA

Network video surveillance system

WHAT COMES TO MIND when you hear the term "mission-critical infrastructure?" Depending on your experience and background, you might think of oil and gas production fields, railway station monitoring systems, power generation facilities, or highway traffic systems. The term "mission-critical" should not be taken lightly since it is used to describe networks that, once they experience instability or transmission problems, could result in serious damage to equipment and facilities, or even injuries or loss of life. In recent years, video surveillance systems have played an increasingly important role in ensuring the reliability and safety of mission-critical infrastructures.

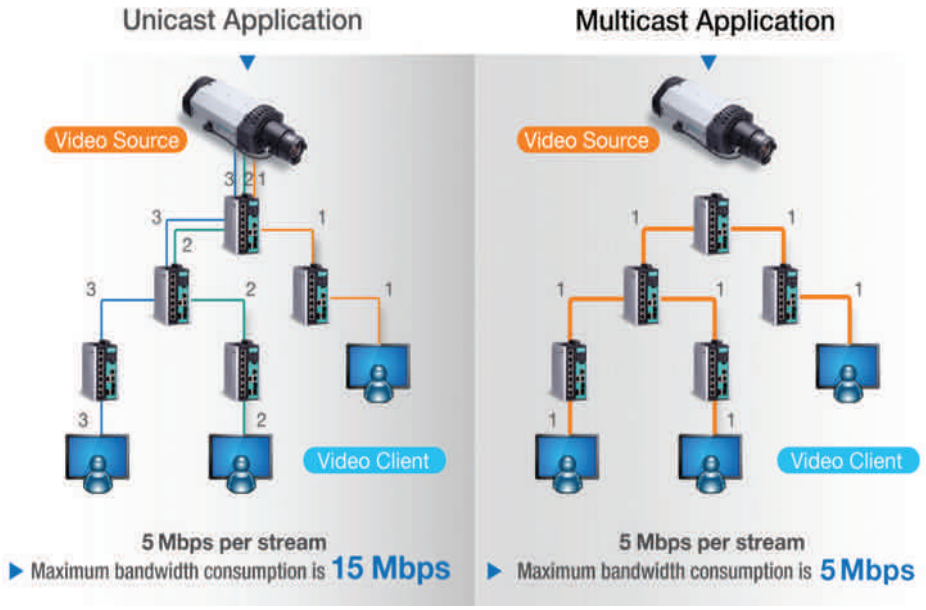
Video surveillance now standard

Video surveillance systems use "images" to allow security personnel to monitor an entire facility, or even a collection of facilities, from a central location, 24 hours a day, 7 days a week, instead of hiring a large contingent of security guards to man a large number of guard stations. Surveillance systems are certainly not new, but in recent years there has been a big change in how they are implemented. A basic system might simply save all of the images onto a hard drive for future analysis when the need arises. More advanced systems, however, use intelligent cameras that support extremely sophisticated features, including the ability to recognize scene changes in critical areas (e.g., if someone leaves a backpack unattended in an airport), or identify specific types of objects. It goes without saying that a video surveillance system is already a must have standard system for any type of mission-critical facility, both for monitoring events in real time, and for providing a library of images that will be available for future analysis.

Commercial-grade video surveillance systems are used in almost every public facility, including supermarkets, offices, and schools. But when it comes to installing a video surveillance system in a mission-critical industrial application, pay special attention to the following issues.

Data vs. Video Transmission

Transmitting video streams presents unique challenges that you may not need to consider with basic data transmissions. At the IP packet level, data and video use the same TCP/IP technology to ensure large scale, fast data transmission. But at the application level, video surveillance normally involves establishing and managing network access



SOURCE: MOXA

Comparison of unicast and multicast video transmissions

between multiple devices. For example, an NVR (Network Video Recorder) and a VMS (Video Management System) operating in different control rooms may want to save or show the same video stream at the same time, while a CMS (Central Management System) may want to display images from the same video stream on a large LCD screen. For this kind of scenario, the IP camera would usually need to send the video streams separately. For the particular case shown below, the IP camera would be required to send three video streams over the Internet.

As the number of cameras increases, the need to transmit so many video streams over the same network will occupy a huge amount of the backbone network's bandwidth. In order to reduce the amount of bandwidth used by all of these video streams, we normally configure video streams as "multicast" type. Multicast means that each IP camera only needs to send one video stream at a time, and uses Ethernet switches to reproduce and forward the same video stream to multiple receivers automatically. Using a multicast configuration can save an impressive amount of bandwidth for the entire network.

To further illustrate how multicast streaming can save bandwidth, an actual project used 400 HD IP cameras as well as 20 video clients. When configured for unicast based transmission, engineers found that the cameras and video clients could consume up to 46,000 Mbps. However, when configured for multicast streaming, the bandwidth consumption was reduced to only 2,000 Mbps.

Lack of data redundancy

Most CCTV surveillance networks use a "star" or "daisy-chain" topology to connect and expand the number of IP cameras connected to the network. However, star topologies are not designed to recover from single points of failure. If only one network cable gets disconnected, or one network device crashes, that single point of failure could result in the disruption of a huge number of video streams.

Designers might recommend using "trunking" technology to aggregate multiple Ethernet ports and cables into one transmission path. In this case, if one cable is disconnected, video data will continue to be transmitted through other ports and cables. This design can't prevent interruptions to data transmission due to single node failures, as would be the case if an Ethernet switch stopped working due to a power outage in the field.

Network management efficiency

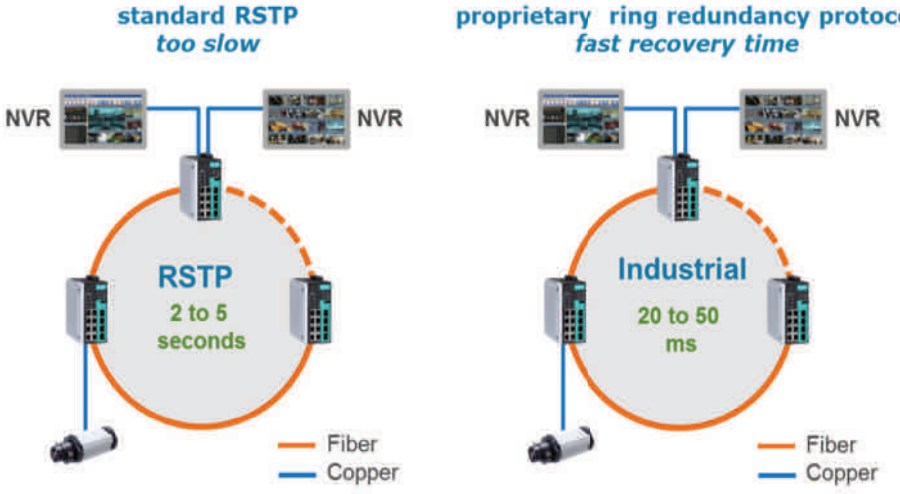
As your network gets bigger, you will probably want to use network management software to monitor and manage the status of your network and network equipment. Experience has shown that if you have more than 50 Ethernet switches on a single (or extended) network, you should consider using an NMS (Network Management Software), since you can save a lot of time on network management tasks. However, there are three features you should consider when you choose an NMS for a video surveillance network.

Real-time monitoring: How fast can the NMS receive and then display alarms from large numbers of network devices? Many enterprise NMSs use traditional "polling" methods to check the status of each network device. However, with polling, the amount of time between when an alarm is triggered and the NMS notifies security personnel will increase as you add more and more devices to your network.

A good industrial-grade NMS will use a "push" or "active" method to ensure that security personnel can receive alarms as soon as they're triggered. In this case, instead of requiring the NMS to continually poll devices in the field, switches installed at remote parts of the network will be smart enough to sense when an alarm is generated by a device connected to the switch, and then immediately send the alarm to the central NMS.

Visualization: When network alerts appear on your screen, how quickly can you locate the root cause? For example, when an alert is triggered, can your NMS determine if the problem is most likely due to a problem with an IP camera, a network device, or a cable? And if the problem is with a cable, how easily can you determine which port on which device it's connected to? A well designed industrial-grade NMS will make the field operator's or maintenance engineer's daily routine easier and more precise.

Integration: Intelligent systems rely on close



SOURCE: MOXA

Mission-critical CCTV applications require an extremely fast recover time.

Recovery Times

Failure Mode		Not Optimized (Traditional Ring Network with RSTP Protocol)	Optimized (Redundancy Protocol Optimized for Video Streams)
Media Failure	Min.	1,280 ms	1.8 ms
	Max.	**11,040 ms**	**37.6 ms**
	Avg.	3,620 ms	6.7 ms
Node Failure	Min.	390 ms	2.5 ms
	Max.	**63,300 ms**	**41.5 ms**
	Avg.	7,320 ms	7.9 ms

SOURCE: MOXA

system integration and message exchange to ensure that your NMS can determine if end devices (IP cameras, for example) are alive or not, and provide meaningful information to higher level central management systems in the control room. However, traditional network management systems focus on the network devices themselves (Ethernet switches and routers, for example); generally speaking, they don't have the capability to support message exchanges or monitoring of third party devices.

Leveraging network technology

For mission-critical network applications, you can consider using industrial grade network technology to overcome the challenges outlined above. Compared with an enterprise network solution, an industrial-grade solution focuses more on hardware reliability, network redundancy, and easy field management. For example, the hardware would be designed to work reliably in harsh environments, where "harsh" could refer to both cold and hot temperatures, as well as environments subject to high EMC (electromagnetic compatibility) radiated emission levels. In addition to hardware reliability, three industrial-grade network technologies that can help you optimize your mission-critical CCTV surveillance network are worth mentioning.

Fast Ring Network Recovery

As we mentioned above, "star" and "tree" topologies are prone to single point of failure events, which occur when only one cable or network device fails. For industrial networks, "rings" and "redundancy protocols" are commonly used.

The Ethernet switches are configured to use RSTP (Rapid Spanning Tree Protocol). RSTP identifies a certain number of network connections as redundant, and then blocks network transmissions through those connections to avoid looping.

If one of the active network cables or switches fails, RSTP activates one of the blocked connections to ensure that all of the devices connected to the network can continue to transmit data to the required locations. However, the typical recovery time for RSTP is 2 to 5 seconds. What this means is that you could lose 60 to 150 frames (assuming 30 frames per seconds) of CCTV surveillance images. However, some industrial network device manufacturers have developed proprietary ring recovery protocols that support recovery times between 20 and 50 ms, which is a much more acceptable recovery time for mission-critical CCT surveillance networks.

If your CCTV system uses multicast transmission over a redundant ring, then even if your ring redundancy protocol is able to activate backup paths in a fraction of a second when a disconnection occurs, it could still take more than 2 minutes for your multicast video streams to recover.

This is because a number of different protocols—including IGMP (Internet Group Management Protocol) and PIM-DM (Protocol Independent Multicast - Dense Mode)—are implemented to transmit your video packets around the network, and these standard protocols are not designed for mission-critical applications.

For example, since the IGMP protocol updates multicast group tables every 125 seconds, if a network cable gets disconnected or an Ethernet switch loses power, your multicast video streams will not be redirected to the backup path immediately. "Optimizing your network for video stream transmission" means implementing an appropriate non-standard proprietary protocol that makes up for IGMP's sluggishness. Without optimization, a multicast video stream can be disrupted for an unacceptably long period of time, until the next multicast paths are negotiated between the network's Ethernet switches.

Keep video streaming

Let's take a look at some actual test data to see just how important it is to optimize your network for video streaming. The data compares recovery times between the standard RSTP redundancy protocol, and the V-ON (Video-Always-On) redundancy protocol which is optimized for video stream transmissions.

The two surveillance networks used for the test were set up in the following way:

- 16 HD IP cameras were connected to each network
- Multicast transmission was used to transmit video streams to two NVRs
- Redundancy Protocol: Network 1: Traditional Ring network with RSTP redundancy protocol Network 2: Network with redundancy protocol optimized for video streams
- SPIRENT SPT-9000A Ethernet package measuring equipment was used to measure video stream recovery times
- Two scenarios were simulated: Scenario A: Media failure due to a disconnected cable Scenario B: Node failure due to loss of power to one Ethernet switch

Video stream recovery times after media failure and node failure, with and without optimization.

From the above data, it should be obvious that RSTP is not designed for multicast video stream redundancy. In fact, in at least one case it took more than one minute for the video streams to recover. Compared with the traditional RSTP protocol, when using the optimized protocol, recovery took less than 50 ms for all of the cases tested, which shows that V-ON technology can optimize the network for video streams and mission-critical IP surveillance applications.

With video surveillance now standard for industrial mission-critical infrastructures, it is important to choose the best technology for your network. Two of the most important aspects of this problem are the standard protocol and industrial network management.

Standard Protocol: Although RSTP and IGMP are often used, both of these protocols are not optimized for mission-critical surveillance networks. In fact, your video stream transmission could hang for up to two minutes as the standard protocol responds to single point of failure events. A better choice is new proprietary protocols designed to optimize networks for video stream transmission, ensuring that a data stream transmission can recover in under 50 ms for layer 2 networks and in under 300 ms for layer 3 networks.

NMS: Network management software can make a big difference in the success or failure of your mission-critical network. An NMS that relies on traditional "polling" technology to check the status of network devices can delay the reception of important warning messages by several minutes for networks comprised of hundreds or thousands of devices.

Users can save a lot of time and effort by choosing an NMS that supports visualization (allowing personnel to see the devices and structure of your network onscreen), real-time notification, and easy integration with SCADA systems.

*Ray Hsu and Alvis Chen are Product Managers for **Moxa**.*

Secure remote maintenance for automotive manufacturing

Automotive manufacturers and suppliers such as FRIMO expect quick troubleshooting and maximum availability of machines from plant and equipment manufacturers. Remote maintenance solutions proposed for that purpose, however, often fail to fulfill the high security standards of IT departments.

FRIMO specializes in the development and manufacturing of production systems for high-quality plastic components for a wide range of applications. The company already has many years of experience with remote service, especially in the automotive environment. Even 20 years ago, machine operators were supported by a remote service technician in the event of machine downtime via analog modems and telephone links. Despite the limited bandwidth of the analog 56 kbit/s modems, access to programmable logic controllers (PLCs) in the machines was still relatively efficient.

"Increasingly powerful industrial PCs have since taken over more and more functions in our machines. Analog connections are no longer sufficient to ensure remote maintenance for these computers," said Axel Starflinger, IT Administrator at FRIMO.

SOURCE: DEVICEMASTER

The security requirements for a remote service solution are very high in the automotive sector.

Troubleshooting and remote services

Analog technology has meanwhile been replaced with broadband Internet access, which is used to establish tap- and manipulation-proof connections through VPN (virtual private network) tunnels.

Thanks to the faster data connection between the customer's plant and the manufacturer's service technician, the machines' industrial PCs too can now be conveniently operated. Using VNC (virtual network computing) software, the entire screen content of the remote computer is transmitted and can be used by the service technician like a local PC.

FRIMO primarily utilizes remote service for rapid fault clearance. Expanded services are also available. As the support needs of its customers are continually rising, FRIMO intends to expand its remote service over time.

"We adapt our machines to the specific requirements of our customers. With fast and secure VPN connections, we have access to all the devices in the machine. For example, our service allows us to remotely set up an extra checkbox in the PC's visualization system, or adjust the parameters of a frequency converter," Starflinger said.

Configuring VPN router in minutes

If a machine needs to be equipped for remote maintenance, FRIMO uses mGuard technology from Innominate. To set up the remote maintenance solution, a complete configuration template is read into the mGuard via an SD card. This defines almost all the required parameters. Then only customer-specific entries for the VPN connection, the customer network's default router and the machine's IP addresses need to be added.

Address conflicts are avoided by mapping the real addresses of the machine network onto virtual IP addresses through the 1:1 NAT (network address translation) function of the VPN router. Additional adjustments to the machine's internal address space are no longer necessary.

At its headquarters, FRIMO is deploying an mGuard bladeBase for up to 12 mGuards in a 19-inch standard rack system. All technical parameters and authorizations are already set up, so a new machine can simply be added and connected, without any additional entries having to be made. All FRIMO locations are connected to headquarters via an internal MPLS network. When servicing is required, a technician from any location obtains remote access to the customer's machine via the blades in headquarters using the VPN connection depending on their authorization level.

High security standard in automotive

The administrator confirms that machine operators are generally skeptical or hostile towards the idea of external access to their production networks. This is especially true for manufacturers and suppliers in the automotive sector. "Security concerns are initially high. However, the benefits of rapid troubleshooting and the security features of our mGuard solution are very convincing."

"The mGuard solution is suitable for industrial use. It is secure and easy to administer," Starflinger said. "Support staff are dedicated and will find a solution, even for complex problems. For example, we recently had a large accumulation of open sessions in our MPLS network and suspected a remote service problem." A specialist checked the log file of the central mGuard, and an analysis helped find the problem within hours.

Application story by ***Innominate.***

Gigabit Ethernet industrial switches

Red Lion: The addition of 18 new compact models to its N-Tron series NT24k managed Gigabit Ethernet industrial switch platform includes over 100 mixed copper, fiber, SFP and PoE+ configurations that provide a full range of connectivity options.

The new NT24k 10-to-14 port DIN-rail mountable switches feature Fast Ethernet, Gigabit or dual-mode fiber ports alongside eight Gigabit copper ports with optional IEEE 802.3af/at Power over Ethernet Plus (PoE+) support. With the large group of mixed-media configuration options, the NT24k platform combines the benefits of noise-immune fiber with the versatility of 10, 100, 1000Base copper connectivity to provide a robust migration path across varying industrial applications.

Newest NT24k switch models include the following options: NT24k-FX switches offer eight all-Gigabit copper and 2, 3, 4 or 6 100Base fiber ports that are available with SC or ST connectors in multimode or single mode; NT24k-GX switches provide eight all-Gigabit copper with 2, 3, 4 or 6 Gigabit fiber ports that are available with SC connectors in multimode or single mode; and the NT24k-DM4 switches offer 8 all-Gigabit copper ports with 4 SFP expansion slots for optional 100Base or Gigabit SFP transceivers.

Modbus couplers

WAGO: New Modbus couplers enable use of

Modbus RTU or Modbus ASCII communications within a distributed I/O architecture.

These fieldbus couplers serve as a gateway between a WAGO-I/O-SYSTEM and higher level devices including PLCs and PCs.

The 750-315/300 and 750-316/300 Modbus Couplers carry a full complement of worldwide certifications including hazardous location ratings and marine approvals making them ideal for a variety of applications. The speed of data transmission can be configured between 1.2 Kbaud to 115.2 Kbaud.

The couplers also support over 247 node addresses providing abundant connectivity to multiple devices on the network. Available in two versions (RS-485 or RS-232) the Modbus Couplers support over 500 WAGO I/O modules.

Performance for optical networks

Schweitzer Engineering Laboratories: A new addition to the SEL wired communications product line is designed to cut the rack-mount space in half.

The ICON cube chassis offers the same functionality as the full-sized, 19-inch chassis, but with a smaller footprint. Its reduced size allows wide-area communications to be brought to locations that are space-constrained, such as pad mounts, repeater sites and oil/gas platforms.

The ICON offers a new approach to solving voice and data communications network design. The ICON combines superior deterministic SONET transport technology with flexible Ethernet and TDM drop interfaces to provide an integrated protection, data, and voice communications solution in a single platform.

Designed and built to address demanding communications needs and operate in extreme environments, the SEL ICON cube chassis is well-suited for utilities, light-rail and highway transportation, manufacturing, petrochemical plants, pipelines—anywhere dependable communication is required to support critical applications.

New automation platform

MKS Instruments: The company's new automation platform offers a modular, scalable and configurable solution for comprehensive control that improves operational and productivity efficiencies. It provides a low total cost of ownership and improves utilization of existing tools and assets.

The Automation Platform integrates with other MKS products, and its library of process routine templates and function blocks to facilitate faster implementation.

The platform's hardware and software are both scalable and flexible due to its modular and open architecture, as well as its support for many fieldbuses and control networks. It consists of two programmable automation control options (MKS PAC 100 & PAC 1000); a variety of IO modules for interfacing to any type of sensor, actuator, valve, etc.; and the MKS Controls Workbench software for configuration, process monitoring, tuning, and data storage. MKS integration services assist in recipe and logic development, integration and training.

The platform leverages MKS Umetrics advanced analytical solutions to drive improved automation via real-time actionable data insights. It is highly suitable in a variety of applications, including open and fully programmable automation control, remote or distributed IO, multi-zone temperature control, and remote process control.

Wireless Ethernet serial modems

Weidmuller: Two new licensed frequency data modems offer powerful long-range communications (up to 40 miles) to extend Ethernet networks into difficult-to-access locations.

Unique design features built into the new wireless Ethernet modems provide dynamic network optimization and intelligent routing for high reliability, lower latency and deterministic power management. They support 360 to 512 MHz and 928 to 960 MHz configurations and can operate in an Access Point/Client configuration. The units can also function as a network Bridge/Router or serve as a Serial Server (RS232/485).

The new modems feature node-to-node deterministic mesh network repeatability for

extended range, and multiple channel spacing options to increase network scalability. These licensed modems are optimized for throughputs of up to 25.2kbps, providing secure wireless communications in challenging outdoor environments and over obstructed paths – typical of remote monitoring and control applications. The integrated Modbus server capability offers seamless integration with smart sensors, RTUs or I/O expansion through the use of expansion modules.

Secure firewall for OPC Classic

Phoenix Contact: A new license for Phoenix Contact's FL mGuard security devices can protect OPC Classic applications. While traditional firewalls do not offer protection for this protocol, users of mGuard firmware version 8.1 and beyond can now upgrade to the OPC inspector license.

The OPC inspector firmware looks into transmitted data packets, analyzing and modifying them as necessary. The OPC inspector dynamically creates firewall rules matching the ports and directions used by OPC traffic. It identifies and blocks all non-OPC traffic and permits use of network address translation procedures such as masquerading or 1:1 NAT routing.

Instead of using fixed TCP port numbers, OPC Classic negotiates new port numbers within the first open connection. This means that intermediary firewalls can only be used with wide-open rules, greatly reducing the security and protection they provide. The mGuard OPC Inspector license counters this problem by using a deep-packet inspection for OPC Classic.

USB-to-CAN V2

IXXAT: USB-to-CAN V2 is the next generation of the company's USB-to-CAN interfaces. With up to two CAN High Speed channels, one CAN Low Speed channel, and a LIN channel depending on the device variant, a wide variety of applications can be addressed in both the industrial and the automotive sectors.

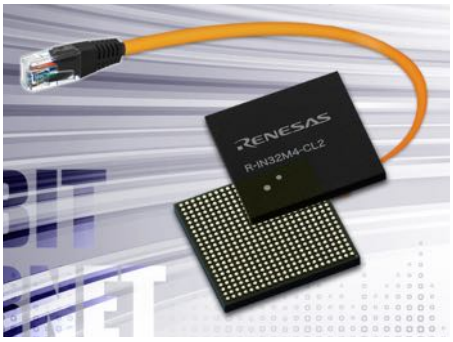
By using powerful hardware and connecting over USB 2.0 Hi-Speed (480 MBit/sec), these interfaces achieve very high data throughput with minimum latency and low power consumption. This allows them to provide the reliable, loss-free transmission and receipt of

messages in CAN networks at high transmission rates and bus load. The messages are also timestamped and can be filtered and buffered directly in the USB-to-CAN V2.

The current versions of the IXXAT driver packages for Windows and Linux (VCI and ECI) support the new USB-to-CAN V2, permitting its use in existing applications with no need to modify software. The APIs for CANopen and SAE J1939 also support the new USB-to-CAN V2 device family.

The USB-to-CAN V2 is available in different variants. In the USB-to-CAN V2 compact variant, the CAN connection is implemented as a sub-D9 plug or alternatively as an RJ45 connector. For devices with two CAN interfaces, these are implemented as RJ45 connectors. Adapter cables to sub-D9 plugs are included with the devices. Additional options include galvanically isolated CAN interfaces, bulk variants, and support for ISO 11898-3 low-speed CAN and LIN.

IC Supports CC-Link IE Field

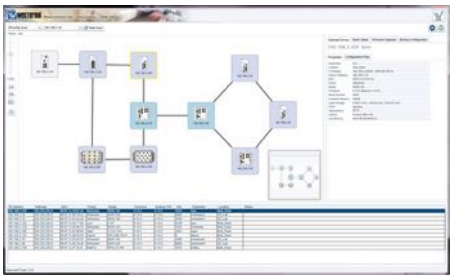


Renesas Electronics: the R-IN32M4-CL2 industrial Ethernet communication application specific standard product (ASSP) with integrated Gigabit PHY is designed to support the network and factory productivity needs of Industry 4.0.

With Industry 4.0, the number of sensor nodes in the factory will increase exponentially, driving the need for more bandwidth in the network to move more data and improve analytics. Gigabit-level industrial networks will become the norm, as the current standard industrial network of 100 Mbps will be inadequate for next-generation networks, and transition to a 1 Gigabit standard is under consideration.

The new IC extends the company's R-IN32M3 platform by incorporating hardware accelerators and supporting real-time operating system (RTOS) performance, as well as Ethernet packet handling. It improves network performance by up to five times faster than conventional implementations. The R-IN32M4-CL2 is enhanced with a new ARM Cortex-M4 processor with FPU core running at 100 MHz, and a single precision Floating Point Unit (FPU) for computationally demanding and complex requirements to support process controllers, gateways, and IO controllers.

Network configuration/management



Westermo: The latest version of the ompany's WeConfig software tool enables easy and secure configuration of large networks

WeConfig 1.2 enables time consuming and complex configuration of large networks to be implemented reliably in just minutes, simplifying both the initial installation and the ongoing maintenance after commissioning.

Using WeConfig 1.2, both the initial configuration and network commissioning can be performed much quicker than before and, over the lifetime of a network, hundreds of man hours can be saved. Regular configuration backups can be performed and stored automatically. Firmware upgrades can be managed in a controlled and reliable manner. Network failures can be visualised and diagnostic information displayed at the click of a button to assist in rapid and effective maintenance.

WeConfig 1.2 provides powerful VLAN configuration functions, allowing quick and easy creation of secure networks. In addition, WeConfig provides security settings on network interfaces, protecting networks from potential vulnerability.

HART multiplexers

Eaton: New HART multiplexers provide an overall communication solution for plant safety and monitoring.

A wide range of MTL HART multiplexers provide a reliable link between field devices and plant control systems. They enable users to reduce unscheduled plant downtime and increase reliability through predictive maintenance diagnostics as part of a plant asset management strategy.

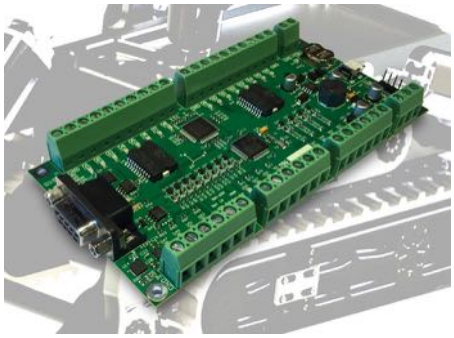
Three new multiplexers, the MTL4851, MTL4852 and MTL4854 are designed to communicate with process instruments supporting the latest HART Standard.

Creating a simple interface between

smart devices in the field to HART enabled communication systems, the MTL4851 and MTL4852 multiplexers provide a scalable solution from 16 to 256 channels/node in a compact, easily configurable package. With auto-detection of communication parameters, no switches on the modules, and up to three times faster scan than comparable products, users can make significant savings in commissioning time, associated costs and reduce project risk.

When combined, the MTL4851 and MTL4852 multiplexers provide a communication system for access to device health and process data and the modules can be connected on one network giving access to approximately 8,000 devices. Simply connected to Ethernet networks with the ET-485 accessory, the multiplexers offer a low cost per channel in the MTL range.

Intelligent I/O module



Roboteq: An intelligent I/O expansion card with an optional Inertial Measurement Unit is intended for use in robotics navigation, unmanned vehicles, machine control, industrial automation and any other applications that need interfacing to the real world.

The IO eXtender module (RIOX), seamlessly integrates with PCs via its USB interface, or with PLCs via its CANbus or RS485 interface. RIOX also directly interfaces with most Single Board Computers, such as Aduino, Raspberry PI, or Beagle Boards. RIOX can drive, or be driven by, all Roboteq Motor Controllers. The module includes a 32-bit ARM MCU for processing and buffering I/O and managing the communication with the host PC/PLC/SBC, motor controllers or other system components. The processor can be configured to perform conversion, capture, filtering, or conditioning on the I/O.

MOST networking technology

K2L GmbH: Version 4.2.0 of the company's MOST PCI Tool Kit eases the simulation of MOST technology-based automotive infotainment systems and devices for rapid prototyping, verification and test.

This new version features significant enhancements, including support for MOST150 coax (cPHY) and the addition of the MOST Stream software tool with an intuitive graphical user interface (GUI) that speeds the setup of synchronous and isochronous streaming connections. These streaming connections transmit audio and video data with unprecedented convenience, using MOST networking technology.

With MOST Stream, received audio and video data can instantly be played back over connected speakers and a GUI-integrated, open-source multimedia cross-platform VLC player, or stored on the hard drive. Support for multi-channel, 7.1 surround sound with control/configuration bytes was also added. Additionally, the VLC player can be directly used for the immediate playback of Digital Transmission Content Protection (DTCP)-free, isochronous video data with a length of up to 196 bytes per frame and PCR timing.

Network-based control system

Yokogawa: The new STARDOM version reduces

communication costs and ensures highly reliable monitoring and control. These enhancements meet a variety of needs in upstream oil and gas development and production.

STARDOM network-based control systems consist of FCN/FCJ autonomous controllers and either a VDS or FAST/TOOLS SCADA server. FCN/FCJ controllers are ideal for the monitoring of oil and gas field installations, pipelines, and other widely distributed facilities that rely on satellites and other types of communications platforms for the transmission of data. In addition to eliminating communications delays and achieving high quality communications, the companies that operate such facilities are seeking to reduce communications costs by limiting the volume of data that needs to be transmitted.

Personnel in central monitoring rooms rely on process data to monitor and control production facilities in the field. As all the process data are sent to the SCADA server at regular intervals, communications costs are high. To address this and other needs, the FCN/FCJ controllers now support the DNP3 unsolicited response function and thus are able to immediately transmit only the most essential data to the SCADA server in the central monitoring room. Without impacting the reliability of monitoring and control, this reduces the amount of data that needs to be transmitted and helps to hold down communication costs. DNP3 is an open communications protocol for use with facilities that are distributed over a wide geographic area.

Handle drives or motion profiles

HMS Industrial Networks: By offering a solution for handling profiles, targeting drives and motion applications, an extension to the CompactCom 40-series enables manufacturers to comply with common profile specifications such as PROFIdrive, EtherCAT DS402 and transparent DS402 on other networks.

Drive profiles or motion profiles are supported by the Anybus concept through a Profile Driver Package, a software stack which is implemented into the drive during development. Ready-made source code can be integrated into the processor of any drive. Consequently, the profile-specific data is not actually "translated" inside the CompactCom. Rather, it passes through the module's transparent channel unchanged and the conversion is done in the drive utilizing HMS' Profile Driver Package. The DS402-based Profile Driver can be used to handle any CAN-based profile – not just drives and motion profiles – on any network.

LTE industrial cellular gateway

Moxa: A new LTE industrial cellular gateway helps M2M system integrators maximize reliability and minimize latency for Video-Over-LTE applications.

In the fast changing wireless landscape, several converging trends have encouraged industries to adopt the LTE (Long-Term Evolution) cellular standard for M2M applications: the gradual decommissioning of legacy networks, the cost-benefits of LTE technology, and the increased demand in rich media and real-time monitoring.

The OnCell G3470A-LTE unit features an integrated, high-speed 4-port Gigabit Ethernet switch that allows up to 4 devices to be connected with the ability to NAT and route between the cellular connection and the wired ports. To enhance reliability, it is equipped with built-in power and antenna isolation to fight against EMI, along with Dual SIM support for cellular connection redundancy, dual power input, and innovative GuaranLink technology for connectivity. Together these features ensure uninterrupted video streaming over LTE networks in harsh and demanding industrial environments.

Radio communication analyzer

Anritsu: The MT8821C addresses the need for measurement tools that support wider bandwidths using LTE-Advanced CA and higher-order MIMO technologies.

As well as supporting LTE-Advanced, the all-in-one MT8821C operates as network simulator supporting LTE, W-CDMA/HSPA, GSM/GPRS/EGPRS, TD-SCDMA/HSPA, and CDMA2000® 1X/1x EVDO technologies to run RF TRX tests in compliance with the 3GPP and 3GPP2 standards, as well as parametric tests.

The easy-to-operate MT8821C makes setting and operation errors a thing of the past, simplifying configuration by using preset measurement parameters for test items specified by the 3GPP RF test standards. Additionally, parameters for all tests can be set and changed easily using the all new highly advanced Graphical User Interface, which includes touch screen operation. An advanced parameter search function enables complex user test settings to be quickly and reliably configured, and automatic PASS/FAIL judgment of measured results according to test specification speeds up testing, leading to greater cost efficiencies.

Library of PLCopen function blocks

B&R: With the SafeDESIGNER library for press applications, B&R offers a complete set of the function blocks specified in PLCopen part 4. As a result, users working with safety-critical press applications will have a solutions for setting up the necessary safety functions

Over the past several years, PLCopen has worked intensively on a specification for function blocks in press applications. The result is part 4 of the PLCopen safety specification, which defines safety aspects of mechanical, electrical and hydraulic presses. Also defined in this specification were the corresponding vendor-independent function blocks for the safety application.

Modules for higher data rates

HARTING: A number of new modules to the Han-Modular industrial connector family, expanding its potential range of applications in new market sectors. Users will now benefit from higher data rates, more mating cycles and greater safety.

The Han USB 3.0 module enables data rates of up to 5 Gbit/s to meet the USB 3.0 standard. The data rate of the new module is increased by a factor of ten over the existing product.

The connector portfolio is also expanding in the RJ45 area, including new variants that offer the options of preLink or insulation displacement terminations. These variants make the Han-Modular RJ45 solutions even more versatile and flexible.

The Han 200A protected crimp module, with its integrated finger protection, puts a strong emphasis on safety. The modifications to the new double module ensure that accidental touching in the unplugged condition is impossible.

CP1L-E with Embedded Ethernet

Omron: The CP1L-E provides a solution for remote access and communication over different protocols simultaneously.

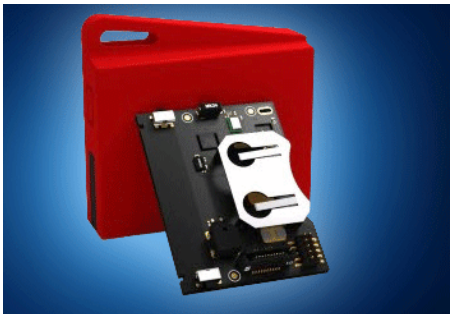
The new controller offers embedded Ethernet that connects seamlessly to the Internet, providing remote access, monitoring and data logging that can reduce an end-user's technical support costs and provide faster diagnostic response. An embedded Ethernet port with socket services (typically available only in larger, modular PLCs) enables OEMs to adopt whatever protocol their application requires, including UDP, TCP, Modbus TCP and the Omron FINS Ethernet protocol for simple connection to other Omron PLCs and HMIs.

The CP1L-E's Automatic-Connect function saves set-up and programming time. It connects instantly over a default IP address to a switch or directly to computer or HMI without a crossover cable – as quick and easy as USB. There are currently three Ethernet-enabled versions of the CP1L-E available, offering 20, 30 or 40 I/O points (expandable to 160 I/O points).

These models include two embedded 1-10V analog inputs. If more analog I/O is required, the unit can be expanded with modules to add two additional inputs and outputs. All models of the CP1L series provide four high-speed encoder inputs and two high-speed pulse outputs, as well as several ready-to-use function blocks for easy positioning.

Expansion capability includes options for digital and analog I/O, temperature inputs and serial interface boards.

Multi-standard development kit



Mouser Electronics: The SimpleLink multi-standard SensorTag development kit (CC2650STK) enables quick and easy integration of sensor data with wireless cloud connectivity.

SensorTag helps jump-start development for Internet of Things (IoT) applications by offering flexible development with multiple wireless connectivity options, including Bluetooth low energy (BLE or Bluetooth Smart), 6LoWPAN and ZigBee.

SensorTag application technology enables developers to get sensor data online and up to the cloud in less than three minutes. The TI SimpleLink SensorTag, available from Mouser Electronics, comes equipped with a SimpleLink CC2650 ultra-low power wireless microcontroller - a 48MHz ARM Cortex M3 core paired with a 2.4 GHz RF transceiver compatible with Bluetooth Smart, ZigBee, 6LoWPAN and other IEEE 802.15.4 protocols. This wireless microcontroller platform provides very low power, and along with a low active RF and run current requirements, the SensorTag provides 75 percent lower power consumption than previous Bluetooth Smart products.

Protection for automation networks

Siemens: The Scalance S615 is the latest addition to the Siemens security module product line, and protects industrial networks and automation systems against unauthorized access.

The S615 security module has five Ethernet ports that offer protection for various network topologies via firewall or virtual private network VPN (IPsec and OpenVPN) and enable flexible implementation of security concepts. Users can configure up to five variable security zones with individual firewall rules. With the autoconfiguration interface, the device can be easily integrated and parameterized with the Sinema Remote Connect management platform. The management platform lets users conveniently manage network connections and access widely distributed plants and machinery.

The new security module has various configuration, management and diagnostics options via web-based management (WBM), command line Interface (CLI) and simple network management protocol (SNMP). As a dynamic host configuration protocol (DHCP) server and client, the device can be used in any virtual local area network (VLAN) security zone.

Coaxial cable-to-board solutions

Molex: Multi-Port RF (MPRF) coaxial cable-to-board solutions provide printed circuit board (PCB) designers and test and measurement engineers with a secure electrical connection suitable for high vibration conditions.

Featuring a rugged single housing design with dual latches to support the weight of the coaxial cables, the MPRF solution ensures a secure multi-port RF I/O connection. The compact connectors also meet space demands for shrinking electronic devices in a variety of industries including telecommunications and networking, data communications and computing, medical, along with aerospace and defence.

With a 3.75mm-pitch, the connectors accept 2.10mm cable diameters (RG-316) for PCB space savings. The robust outer shell can withstand a minimum of 500 mating cycles, while the 1.00mm contact wipe ensures proper engagement under extreme conditions.

Small radio data transceiver module

Satel: The Satelline TR4 compact UHF transceiver offers transmitting power of 1,000 mW, and is compatible with a variety of protocols including Pacific Crest, Trimble and Satel.

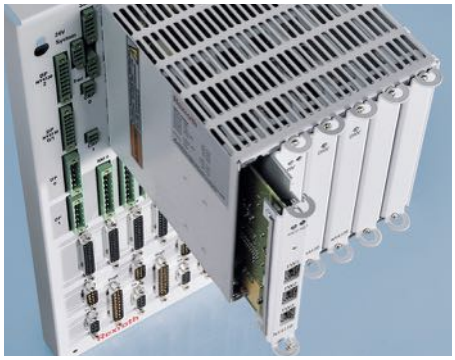
The TR4 is designed for integration into end devices that are intended for international use. The unit offers a weight of only 18 g, transmitting power of 1,000 mW and an "ver the air" data transmission rate of 38,400 bps.

With dimensions of 56 mm x 36 mm x 6 mm, it is designed for easy integration. Robust UHF frequencies (400 MHz - 470 MHz) are a reliable basis for the communication of self-sufficient stations even in the event of unknown

topology. In addition, the new TR4 features all of the advantages of the Satelline EASy and 3AS modems including channel scanning, and error correction.

With license-free frequencies becoming more popular (869 MHz in Europe and 915 MHz for the American market) transceiver modules of identical design will follow. The identical footprint and the standardised communication commands will minimise integration costs. Later it will only be necessary to insert the corresponding radio module for the destination, and the end device will be ready to use.

Motion control system



Bosch Rexroth: The NYCe 4000 multi-axis motion controller offers an integrated set of control and drive hardware in an extremely compact housing. The hardware is designed to handle complex operations, combining an open software architecture and Sercos automation networking to provide a platform for motion solutions and simple integration into the automation landscape.

High-level programming languages allow users to write complex motion control programs. Extremely high-speed control loops with 32 kHz bandwidth deliver maximum precision and dynamic performance.

The motion control system can handle up to 120 digital and analogue I/Os in parallel in real time for implementing complex process operations on standardized hardware. Pre-defined software algorithms ensure zero-vibration and zero-backlash.

Cyber security goes mobile to protect your bicycle

Experts estimate, that each year nearly two million bicycles are stolen around the world. Bicycle theft is often seen as a low police priority, but the Center for Problem-Oriented Policing points out that this picture is misleading. When viewed at the aggregate level, bicycle theft represents a much larger problem, one with harmful economic and societal effects that warrant greater attention.

SEVERAL STUDIES SUGGEST THAT fear of cycle theft may discourage bicycle use and that many bicycle theft victims do not buy a replacement. Combating bicycle theft is therefore a necessary step toward increasing the use of this sustainable form of transport. Advanced wireless networking technology comes to the rescue.

Clearance rates for bicycle theft remain consistently low. For example, in Sweden, only 1 percent of bicycle thefts are cleared by arrest. One reason for this is that there typically exists little relationship between the victim and the offender, and hence it is difficult to identify suspects. A further problem is proof of ownership. Even when crimes are reported to the police, the majority of bicycle owners cannot supply sufficient details to assist in an investigation. As a consequence, even when an offender is detained for cycle theft, if the owner cannot provide proof of ownership for the retrieved cycle, then the suspect may be released without charge and may even have the stolen bike returned on release.

Advanced wireless networking technology comes to the rescue.

Keyless locks

While most cheap bicycle locks are constructed using soft alloys, quality products are made from hardened steel, and they're impervious to hacksaw and bolt cutter attempts.

So while the bicycle thief would need an angle grinder to cut through the steel, it's often quite easy to pick the lock. If you search the Internet (no, I will not post the link here) you will find video instructions on how to pick a cycle lock with no other tools than a simple Bic pen.

PHOTO: BITLOCK

PHOTO: LOCK8

BitLock overcomes this problem by replacing the bike key with a smart phone, bringing keyless entry technology to your bike. Using Bluetooth 4.0, BitLock detects your presence as you come within 3 feet of your bike.

BitLock uses Bluetooth to bring keyless entry technology to your bike.

Without the need to interact with your phone, you can lock and unlock by simply pressing the button on BitLock.

But what if the battery on your phone dies just as you want to unlock your bike? The BitLock app allows you to set a unique 4 digit combination code. In case your phone dies, punch in the code as a sequence using the two push buttons on BitLock to authenticate yourself and unlock your bike.

The manufacturer claims that thanks to an intelligent power management, advanced battery technology, low power radio and actuation system, BitLock can perform more than 10,000 lock/unlock operations on a single battery. This would be enough to provide a 5-year battery life under average usage. Once the battery level is low, you get a notification on your phone to replace the battery.

bitlock.co

Solar charging

Skylock offers similar functionality to BitLock, but has a built-in solar panel that recharges the battery. According to the manufacturer, 12 hours of sunlight provide enough power for six months.

In case that you ride your bicycle mostly at night, there is also a micro-USB charging port.

Another neat feature is the integrated 3-axis accelerometer. All manufacturers admit that any lock can be cut with the right tools and enough time. Also, the lock may be made from hardened steel but the structure to which you locked your bike is most likely not. A thief could easily cut the fence or pipe, haul your bike away and then take all the time he needs to open the lock.

Skylock will sense if your bike is being

PHOTO: SKYLOCK

Skylock uses its accelerometer to notify you that your bike is being tampered with. It can also detect many types of serious crashes and can notify anyone in your trusted network.

tampered with and can automatically send an alarm to your smart phone. You can even adjust the sensitivity of the accelerometer, e.g. if you live in a busy city where pedestrians will frequently be bumping into your bike.

The accelerometer can also be used for crash detection. While you are riding with the lock onboard, Skylock monitors your movements. If you have an accident, the accelerometers will record a sudden spike and the app will ask you if you are okay. If you don't respond it will automatically call emergency responders and give them your position. To avoid false alarms, Skylock cross-references the data from the lock with the data from your phone's accelerometers.

www.skylock.com

Bike sharing

Lock8 is another GPS tracked, alarm secured cycle lock, but it focuses more on the bike sharing aspect.

Unlike Skylock or BitLock it is not a traditional U-Lock. The 'Sharkfin' is mounted directly to the chainstay of your bycicle. The frame-mounted design has several advantages. For one thing, there is no need to worry about battery life and charging. The kit comes with spoke reflectors that feature built-in magnets, which constantly charge the device through induction every time you ride.

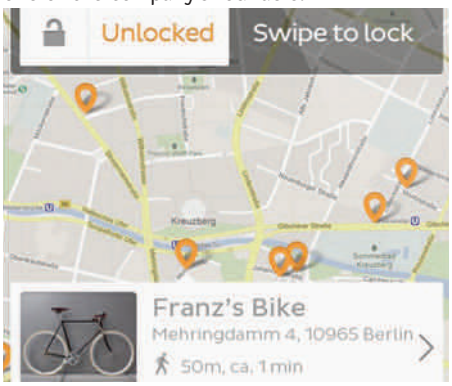
As the integrated GPS is fixed to the frame it will transmit the location at all times. This comes in very handy if the bike gets stolen.

Lock8 combines a three-axis gyroscope, accelerometer, temperature sensor and a steel cable with smart-wire cut detection to secure your bicycle.

To avoid this in first place, Lock8 comes with a hot-wired steel cable, gyro-accelerometer, motion and temperature sensor. The latter is there in case a bicycle thief would use a blowtorch or freezing to break the lock. If the sensors detect that the lock is being tampered with, a notification is sent to your phone and it can also be set to sound a 120 dB alarm.

Lock8 makes it easy to share your bike with friends and family. You simply send them an e-Key via Facebook or over your phone.

If you're looking to earn some extra money, you can use the 'Rent offer' button. This allows other verified Lock8 app users to rent out your bike. You can set your price and the times when it's free, and also define a geo-fenced drop-off zone where the bike is returned. "It's like Airbnb for bikes," says Franz Salzmann, one of the company's founders.



lock8.me

The ultimate theft protection

If you don't trust all these smart sensors and electronics, here is the perfect solution to protect your bike.

It doesn't need a smart phone, yet you can be sure that no one else but you gets to your bike. If someone tries to steal your bicycle - which is highly unlikely - it will sound a very loud alarm. If the thief should actually get away with your bike - which is even more unlikely - he will be tracked down and won't get very far. This anti-theft device needs neither batteries nor a mounting bracket.

Take a look at the video below to find out about the ultimate theft protection:

Scan the QR code to watch a video of the ultimate bike theft protection.

Leopold Ploner

Service

industrial ethernet book

Reader Service Card

IEB issue 89 - July 2015

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

Return by mail to:	Or fax back to:	Or use our online reader service at:
IEB Media Bahnhofstr. 12 86938 Schondorf Germany	+49 8192 933 7829	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: _____