2.2015 Issue 86
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Network Connectivity

Moving into the era of IoT and Big Data 8

THE PFC200 CONTROLLER

Ultra-Fast and Highly Intelligent

PFC200

High processing speed

Programmable to IEC 61131-3

Configuration and visualization via Web server

Integrated security functions

Robust and maintenance-free

www.wago.com/pfc200

WE INNOVATE!

WAGO®

GET CONNECTED...

The new era of Big Data...

Of all the aspects of the Industrial Internet of Things (IIoT) and Industry 4.0, the one that has always been the most futuristic to me is Big Data. It's not hard to imagine an Internet of Things that could expand to extremely large numbers of connected devices, but what is somewhat harder to get my arms around is how vast amounts of data and advanced software algorithms will specifically create value.

At the Hannover Show in 2013, I distinctly remember attending an early evening press conference introducing Industry 4.0 by the CEO of Siemens. Much of what was talked about that night seemed very reminiscent of what all of us had experienced with networked automation over the last ten years. Large numbers of devices connected via networks. On one hand, it seemed very simple and doable, but all the talk was on a much more massive and more far reaching scale. Even now, it seems that maybe there will need to be a set of "killer apps" that emerge to drive the IoT higher. Maybe smart homes, connected cars or tools for a health care renaissance.

"Big Data analysis is the next big thing," Diane Bryant, senior vice president and general manager of Intel's Data Center Group, told the Silicon Value Business Journal late in 2014. She added that the total available market for IoT will be 41 billion devices in 2018, and there will be an explosion not only in chips, but huge software and services components as well. Her conclusion: that the number of conceivable connected machines out there is astronomical. None of that is especially hard to believe but still I think we're in a wait-and see-stage on the exact path forward

Recently, we've been learning about groups such as the Industrial Internet Consortium, which now has a member of 125 of the world's large technology companies focused on developing the reference architectures and frameworks required to take the IoT to the next level. This rethinking of fundamentals, especially security at all levels of the system, along with identifying current gaps in technology seems to be the right direction.

Internet Protocols were not originally developed with security in mind, and there is a need for a much higher level of cooperation, collaboration and a common vision among a vast array of technology suppliers to make the vision of a truly "industrial-strength" Internet a reality.

In the next 6-12 months, we will have a much better idea on specific technology initiatives and potential markets. But there is also no doubt that we will be seeing new examples of IoT enabling technology built into semiconductors, servers and a wide array of industrial components and systems that could also move the bar forward as well.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2015**
Deadline for editorial: February 13, 2015 Deadline for artwork: February 27, 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. All updates received by February **13, 2015** will be incorporated into **www.iebmedia.com** for the next issue.

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

NASA Orion Test Flight

Orion crew vehicle uses deterministic network technology, named TTEthernet (SAE AS6802), that combines commercially available Ethernet infrastructure with deterministic QoS Layer 2 enhancements and services.

THE ORION TEST FLIGHT successfully lifted off aboard a Delta IV Heavy rocket to perform its first flight test in space. The spacecraft is designed to carry astronauts on exploration missions into deep space.

A collaboration between NASA, TTTech and industry participants contributed to an open Ethernet-based standard suitable for the deployment in upcoming NASA programs and space systems, playing an important part in the Orion project. This Deterministic Ethernet network technology, named TTEthernet (SAE AS6802), combines commercially available Ethernet infrastructure with deterministic QoS Layer 2 enhancements and services. Those services are designed to enable the design of synchronous, highly dependable embedded computing and networking capable of tolerating multiple faults.

SOURCE: NASA

Orion Onboard Data Network provides system architectures for human-rated space flight based on TTEthernet.

With TTEthernet, robustly partitioned critical control data, graphics data streams and standard LAN messages can operate in one network without interference. This enables the handling of mixed-level criticality functions in complex Ethernet-based networks, effectively circumventing the limitations of Ethernet technology for the design of advanced integrated systems.

OPC UA Specification for Sercos

An OPC Unified Architecture (UA) companion specification for Sercos describes the mapping of the Sercos information model to OPC UA, so that functions and data of Sercos devices are made available and accessible via OPC UA. This initiative aims at simplifying the communication between machine and supervisory IT systems, supporting Industry 4.0 semantic interoperability.

The mapping rules can be used for different implementation approaches. On one hand, the OPC UA server functionality can be implemented in a Sercos master device (CNC or PLC). On the other hand it is possible to implement this functionality in a Sercos slave device. In the latter case, OPC UA accesses are executed in parallel to Sercos real-time communication or even without any Sercos communication.

In September, Sercos International launched a "call for experts" to invite members and specialists to contribute to this initiative. A draft of the Sercos OPC UA Companion Specification is available and is currently being reviewed by a technical working group consisting of manufacturers, technology providers and research institutes. The final specification will be available in April 2015.

http://sercos.org

Special Interest Group for EtherNet/IP

ODVA has announced a new special interest group for EtherNet/IP in the process industries. The SIG will leverage the strengths of EtherNet/IP to develop enhancements to its specification to address key use cases for automation applications in the process industries: field device-to-industrial control system (ICS) integration; field device-to-plant asset management (PAM) integration; and a holistic field-to-enterprise architecture.

The SIG's scope of work is founded on the overarching vision to proliferate adoption of EtherNet/IP in the process industries, and will focus initially on the integration of field devices with industrial control systems and related diagnostic services. The work of the SIG will result in a unified communication approach to process applications, enhancing the ability of users to exchange information to and from the field. The work of the SIG is expected to be completed in phases generally aligned with key use cases.

http://odva.org

PLCopen publishes packaging standards

PLCopen working with open standards organizations including the OPC Foundation have created an open standards ecosystem that simplifies the communications of packaging machines with other plant systems and the business enterprise. These standards leverage Service Oriented Architecture (SOA) technologies which is the fabric of today's computing. The PLCopen standards advance automation systems technology that has lagged behind general computing and software.

The Internet of Things, Industry 4.0, and Smart Factory applications are growing and implementation is simplified with PLCopen OPC UA function blocks. The open PLCopen standards improve automation system device interoperability, simplify sensor to enterprise, cloud, and Internet communications with PLCopen web services function blocks based on the OPC UA.

Today, there are many vendor-centric unique data exchange protocols that do not offer interoperability to transport information between controllers, systems, enterprise and the cloud.

http://plcopen.com

Plastic, stainless steel, die-cast zinc: the universal I/O system with IP 67 protection for all applications.

www.beckhoff.com/ip67

The wide range of extremely compact and robust Beckhoff I/O modules with IP 67 protected housings is designed for all industrial applications. The broad spectrum of signals ranges from standard digital I/O to complex analog technology to compact Drive Technology.

- **Fieldbus Box (plastic, IP 67):** 12 different fieldbus systems for universal application
- **EtherCAT Box (plastic, IP 67):** high-performance for all applications, directly on the machine
- **EtherCAT Box (stainless steel, IP 69K):** for hygienic applications in the food, chemical or pharmaceutical industries
- **EtherCAT Box (die-cast zinc, IP 67):** for harsh environmental conditions in "heavy-duty" industries

IPC
I/O
Motion
Automation

HANNOVER MESSE

Hall 9, Booth F06

New Automation Technology **BECKHOFF**

IHS Technology Industrial Automation Conference 2014

Ethernet and IP led the way with more than Big Data, and is undeniably good for business...but whose? IEB editor Frank Ogden reports on how technology is impacting advanced manufacturing and 3D printing.

IT WAS THE MAN FROM GE SYSTEMS, its chief of strategy for Intelligent Platforms, who said it all. Not the IHS chief economist who spoke with the clarity of 20:20 hindsight about the fortunes of the automation industry since the 2008 slump, unable to rule out another unseen cliff edge event because financial systems, like weather, are subject to chaotic behaviour.

Neither was it the ARM Holdings Internet of Things head who quite reasonably asked "Why connect everything? The network implications are colossal and you don't actually know why you are doing it... The idea [behind the use of internet protocol] is not that everything needs to be talking to everything else. The idea is that when you find something that needs to talk to something else, it is trivially easy to do this. You are buying the flexibility to use things in an entirely new way in the future".

And what did the man from GE say? Simply that one of his company's turbines could generate more process data in a day than the whole of the global Twitter network. Yes, Big Data is here and needs to be dealt with. And this is of course wonderful news, particularly if you are a management software giant such as SAP, or indeed any automation colossus in which your business is principally that of software with all its hooks and tie-ins from global enterprise level to distributed plant floors. And neither should one forget the data warehousing and security layer business models that run alongside Big Data. It promises a bonanza for everyone except possibly the end-clients.

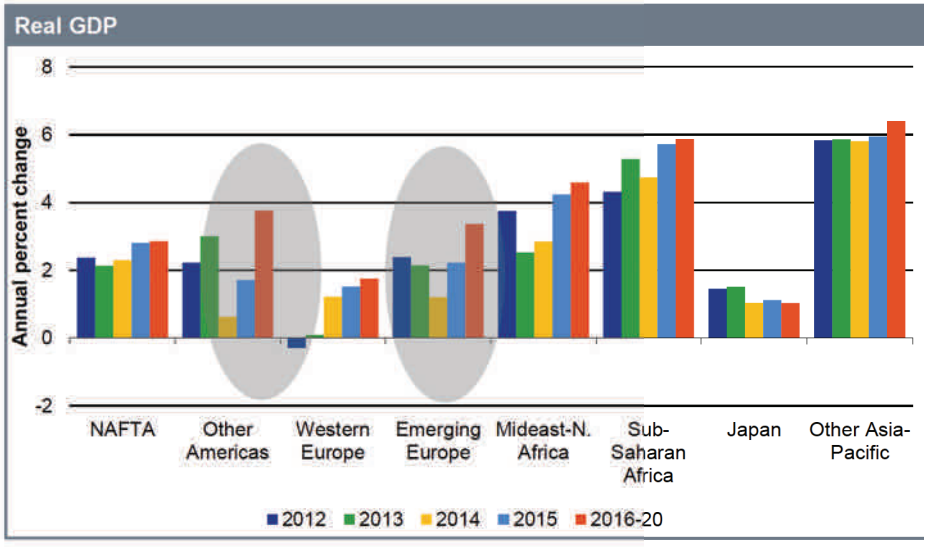
SOURCE: IEB

Energised chat during one of the IHS panel sessions. While the conference covered much of the well-trodden road to Big Data and industrial cybersecurity, it seemed to sidestep energy consumption and control topics.

At least this is the way it felt, having sat through a day and a half of presentations and discussions. Say 'Big Data', 'Internet of Things' and 'Industry 4.0' enough times and you too can sound as though you have a saleable vision of the future. In reality there is no revolution taking place across discrete and process manufacturing, simply a concatenated evolution built on increasing connectivity between machines, processes and people.

One should never lose sight that industrial infrastructure tends towards a 20-year lifecycle while process investment usually has even longer expectations of a positive ROI. This particularly applies to networks.

Even IHS' own analysts state that Ethernet accounts for no more than 30% of installed nodes some 15 years after the technology's industrial inception, the remainder being a fieldbus of one sort or another. Thus the man from GE quite rightly queried the best way to handle the potential wash of raw industrial data, possibly by finding of a better route to alarms and exceptions.



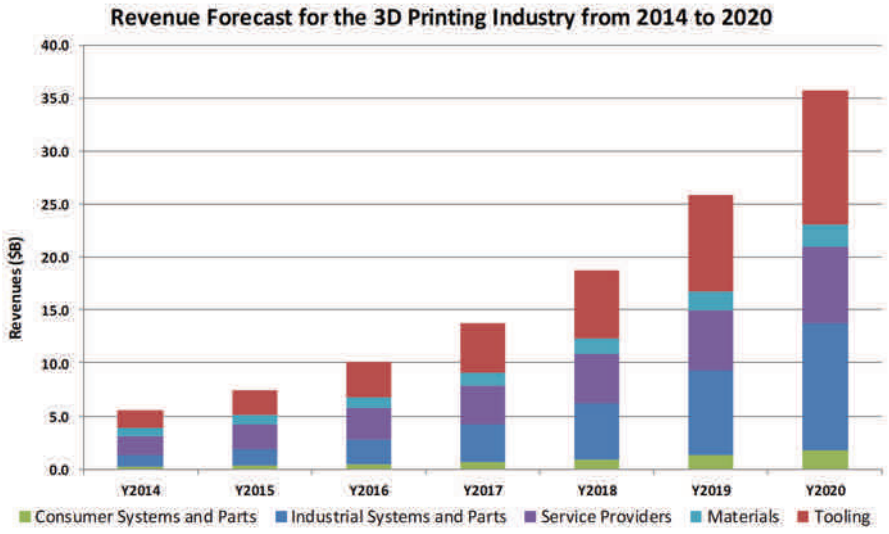
SOURCE: IHS

GDP does translate into projected business fairly closely. One of the the more surprising forecasts made by Elisabeth Waelbroack-Rocha, chief international economist at IHS in her opening presentation was that sub-Saharan Africa would join with ASEAN and the countries of new Europe in leading GDP growth up to 2016.

Batch quantities of one...

Once he had got past the torrent of massive IHS numbers which signified the size of global machinery and automation markets, senior principal automation analyst Alex Chausovsky delivered genuinely thought-provoking lecture on industrial 3D printing.

Building up physical structures through



SOURCE: IHS

IP can also mean Intellectual Property and Alex Chausovsky, principal IHS analyst for industrial automation reckons that 3D printing could be a game-changer. With key patents for selective laser metal sintering and other directed energy printing technologies about to expire, tool-making and small run metal fabrication batches will become big business for laser metal forming.

photo-polymerisation is of course not new; it has been around since the mid 80s. However, the advent of high energy laser sintering, electron beam melting and directed energy metal deposition technologies could make a difference to small batch, high value part manufacture. These processes offer precision solid metal 3D structural parts created directly from drawings, or from data gained by scanning an existing object to create an exact replica as might be the case with the production of obsolete parts.

Other arguments such as time to market, design innovation and the reduction of development cost could also be made for these rather exotic fabrication techniques. He added that patents relating particularly to sintered metal deposition are about to expire which could lend impetus to process adoption. While speed of fabrication would always exclude volume production, Chausovsky suggested that something akin to Moore's Law applied to 3D printing in that speed appeared to double every three years. He also cautioned that Intellectual Property design theft might become a factor with widespread object duplication availability.

He suggested that although the established printer companies such as Canon and Epson were in the running for the 3D printer market, the likes of Google, Amazon and Apple "with sufficiently deep pockets" might enter this embryonic business. Although other delegates at the IHS conference thought the prospect of 3D printing to be interesting, it has to be said that people to whom I talked were mostly sceptical about their future industrial impact.

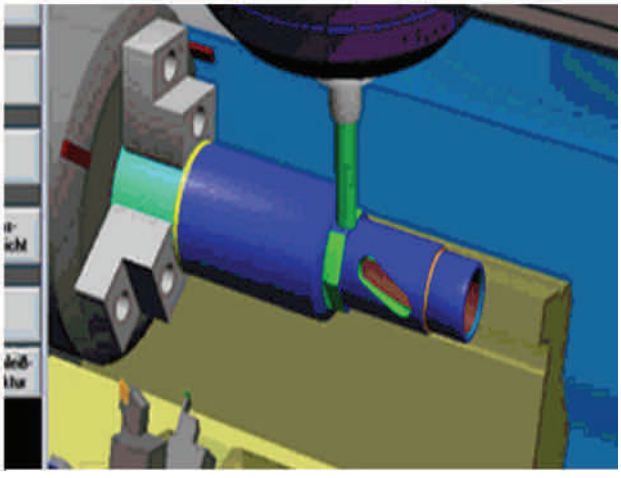
Industry 4.0

That slide which depicts the four stages of industrial automation – from mechanical to electrical, programmable and networked robotic control – made its appearance on a couple of occasions during the course of the conference, an aid to stating that unfettered connectivity within the factory will lead to new business models.

Wolfgang Dorst of Bitkom, Germany's ICT (information, communication technology) used the Uber taxi ordering service as an example of game-changing software, closely analogous to the pressures and opportunities available to highly connected manufacturing industry. He didn't actually say that a €3.99 app downloaded from Google's PlayStore could be used to order up your bespoke Audi direct from the factory but that was his general drift.

It fell to Siemens Prof. Dieter Wegener to add a practical dimension to Industrie 4.0, at least for his company's version aka Totally Integrated Automation.

Prof. Wegener described the twin track of virtual and real world manufacturing automation, and the way in which detailed software simulation could ease the path from product conception all the way through to production and beyond. As TIA applied to Process Automation, parallel simulation in association with real world plant could offer impressive walkthrough – literally – simulations for maintenance and service.



SOURCE: SIEMENS

Prof. Dieter Wegener, VP for advanced technologies and standards at Siemens offered what is probably the real shape of Industrie 4.0 in his presentation – computerised design automation from product concept to what comes off the end of the production line. Here he extols the benefits of the virtual machine and its simulation of the manufacturing process. Producing a 'digital twin' of a component in simulation can reduce the machine setup and installation costs by as much as 80% he claims. The simulation also assists with the calculation of manufacturing times.

Internet of Things

This, I am afraid, is where a personal cynicism crept into conference reporting. IoT generally means small comms processors and web servers, mostly wireless connected and battery powered, making plant, environment, location and maintenance data available to higher enterprise layers. All good, useful properties and a worthy aim for integrated factories, plants and homes.

Several would-be Messiahs offered presentations, generally changing the name to Industrial Internet of Things, all offering the prospect of connecting "isolated silos of automation" within a wider MES and ERP system. I have to tell them that field level web servers and other comms devices have been an integral part of both discrete and process automation for nearly all of the 12 years or so that I have been reporting on industrial networks. In that time both plant and line have been sending back volumes of data to enterprise both locally and remotely.

I also have to tell them that remote maintenance services, the subject of a separate conference presentation, has been a regular feature for forward-thinking plant managers, not least in the pages of IEB. Hmm. Indeed security concerns have inhibited the uptake of plant level servers in much the same way that reliability of wireless connections have limited the use of wireless machine nodes so nothing new here! How much more useful it would have been to have included a session on smart energy saving systems, a topic far more in line with the real cost of discrete manufacturing.

The next IHS Technology Conference will take place in Paris from June 10 to 12, 2015.

***Frank Ogden** is a contributing editor for the Industrial Ethernet Book.*

Engineering First Steps: Solutions for Big Data

Achieving the transformational objectives required to implement Big Data, Industry 4.0 and the promise of the Industrial Internet will require an unprecedented level of engineering collaboration and cooperation. In 2014, more than 125 of the biggest technology companies in the world joined to work together. This report looks into how the group is operating, the technical focus of its work and how you might become involved.

THE INDUSTRIAL INTERNET APPLIES "internet thinking" to industrial settings, covering the non-consumer side of the internet of things. It connects smart machines and devices and people at work, leading to better decision making through advanced analytics that result in transformational business outcomes.

The Industrial Internet Consortium brings together the organizations that will accelerate growth of the Industrial Internet by identifying, assembling and promoting best practices in ecosystems comprising industry, academia and governments. The scope, mission and status of the engineering work of the Industrial Internet Consortium (IIC) are focused on the needs of different audiences:

Members: What is happening in the engineering-related IIC Working Groups

Prospective Members: IIC engineering activities, and where members can engage the process

Standards Groups: What is being specified, and potential points of collaboration

Technology Focus

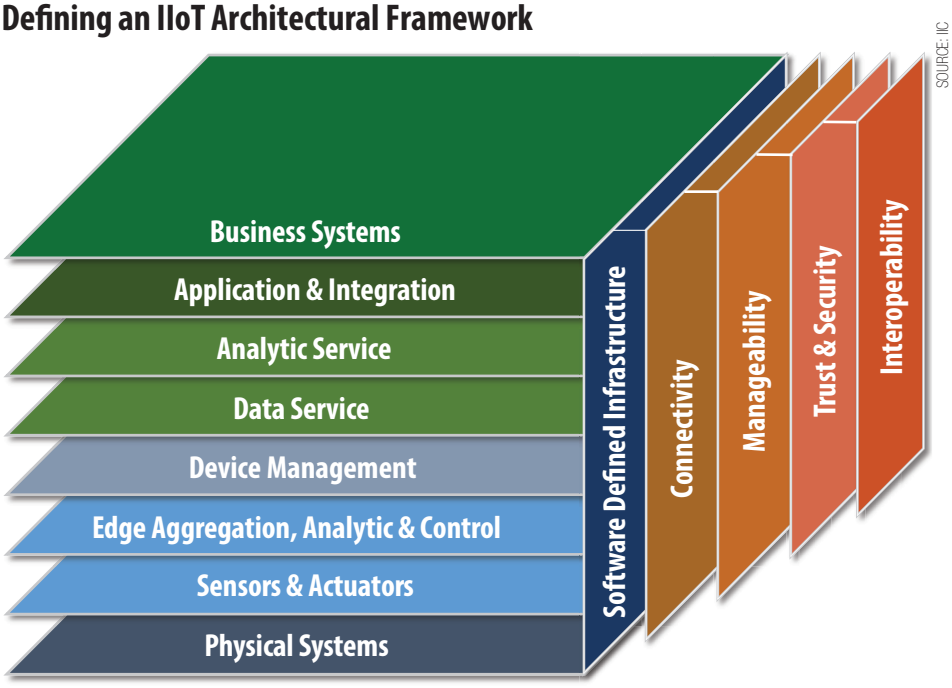
The Technology Working Group focuses on coordination of technical work and has an approved Charter and ten deliverables that it will create over time. It has created teams to work on three of these deliverables:

- Use cases
- Framework for the construction of reference architectures
- Vocabulary

Other deliverables include:

- Identification of elements that make up the Industrial Internet architecture
- Definitions of multi-view reference architecture(s)
- Identification of extant Industrial Internet technologies that can be integrated into such an architecture
- Evaluation of the identified technologies
- Proposals to standards organizations to fill in the technology gaps
- Review of testbed requirements to validate the architecture(s)
- Recommendation of adoptions to the IIC Steering Committee

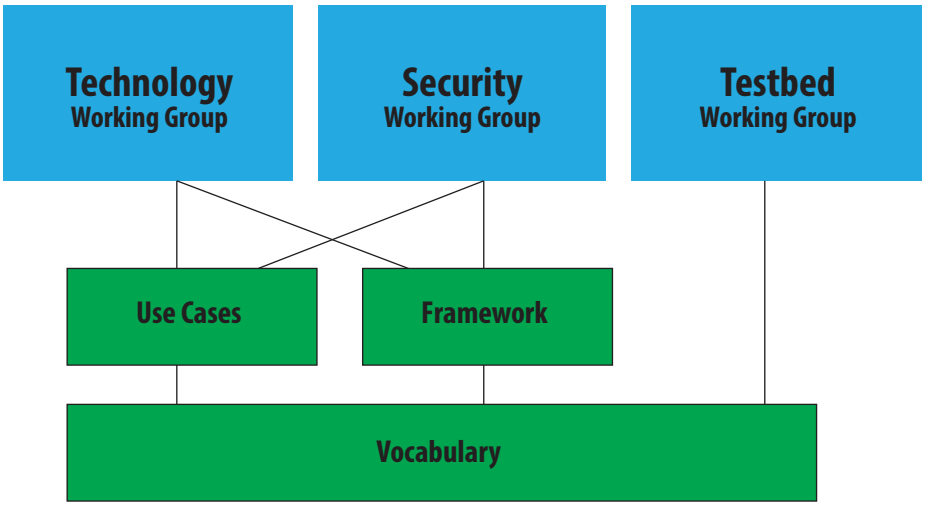
Defining an IIoT Architectural Framework



SOURCE: IIC

A key goal for the IIC is building a framework for expressing reference architecture(s). The framework must be easy-to-use and lightweight. and a vital precursor to the construction of the architectures for specific applications.

Structure and focus of IIC work groups



The focus of IIC development is on enabling technology, security and testbed projects that test application solutions.

DO YOU KNOW INDUSTRIAL ETHERNET?

TAKE THE QUIZ AND FIND OUT!

Go to www.iebmedia.com/Challenge or use the QR Code below to play the quiz.

PRESENTED BY

ETHERNET POWERLINK Standardization Group

OSADL Open Source Automation Development Lab eG

Use Cases

The Use Cases team is identifying architectural requirements and gaps to be filled in Industrial Internet applications and scenarios. Members identify and propose specific use cases based on their specific knowledge and needs. Sample IIC use cases are shown below:

Identity and Credential Lifestyle: Address the lifecycle identity (issuance, renewal and deactivation) of machines, users, groups, events and data that comprise the Industrial Internet.

Distributed Autonomy in Power Grid: Address the distributed control and rebalancing of the power grid resulting in optimum generation and distribution of power.

Security: A set of use cases describing specific aspects of the Industrial Internet Security ranging from policy management to detection

Web Application Developer: Improve the support for application developers to develop web applications that are built upon and use Internet of Things devices and protocols.

Component Pedigree and Chain of Title: Address the vulnerabilities of the semiconductor supply chain to counterfeiting that represents a threat to the health, safety and security of people around the world.

Device Management: Use cases specifying how devices connect, collaborate and organize themselves to achieve specific specified outcomes.

Data Management: Collecting, aggregating and sharing operational data for industrial machinery.

Use case development will be considered "complete" when the IIC has a sufficient range of use cases to specify the architectural requirements for the Industrial Internet, confidently and reliably. To do that, the IIC is mapping some use cases to an architectural framework.

Because architectural requirements will be driven by these use cases, the IIC is actively soliciting use cases from its entire membership in order to capture architectural requirements that work in vertical markets or with specific features of a platform. The use cases also have an important role in testbeds, covered later in this report.

Framework objectives

The Framework Team is building a framework for expressing the reference architecture(s). The framework must be easy-to-use and lightweight. It is a precursor to the construction of the reference architecture(s), not an end in itself. The framework must specifically support the Industrial Internet and enable the construction of an open architecture on which to build ecosystems for innovative products.

Collectively, the IIC Founding companies (AT&T, Cisco, GE, IBM and Intel) operate in all these areas and formed the IIC to ensure complete coverage of the stack comprising the Industrial Internet. The Framework Team is also working to ensure that this framework is not arbitrarily inconsistent with other frameworks. This listing of layers and definitions provides insight into specific framework definitions.

Physical Systems: The actual physical hardware including EPROMs and other chips that are necessary to represent or sense the environment. Physical systems are often "below" a Hardware Abstraction Layer which contains software interfaces to the hardware.

Sensors and Actuators: Environment sensors often abstracted by software components that manage the interface from the physical sensor to the overall controller software system.

Device Management: A set of services from in-factory provisioning and assignment of X.509 certificate to device de-provisioning, deactivation and un-deployment.

Data Management: This layer is responsible for ingesting data from sensors, devices and Gateways. Specific functions range from cleansing, filtering and checksum to sematic transformation.

Analytic Service: Provides a set of data aggregation and analytic across a domain of edge devices; logs information for Big Data analysis.

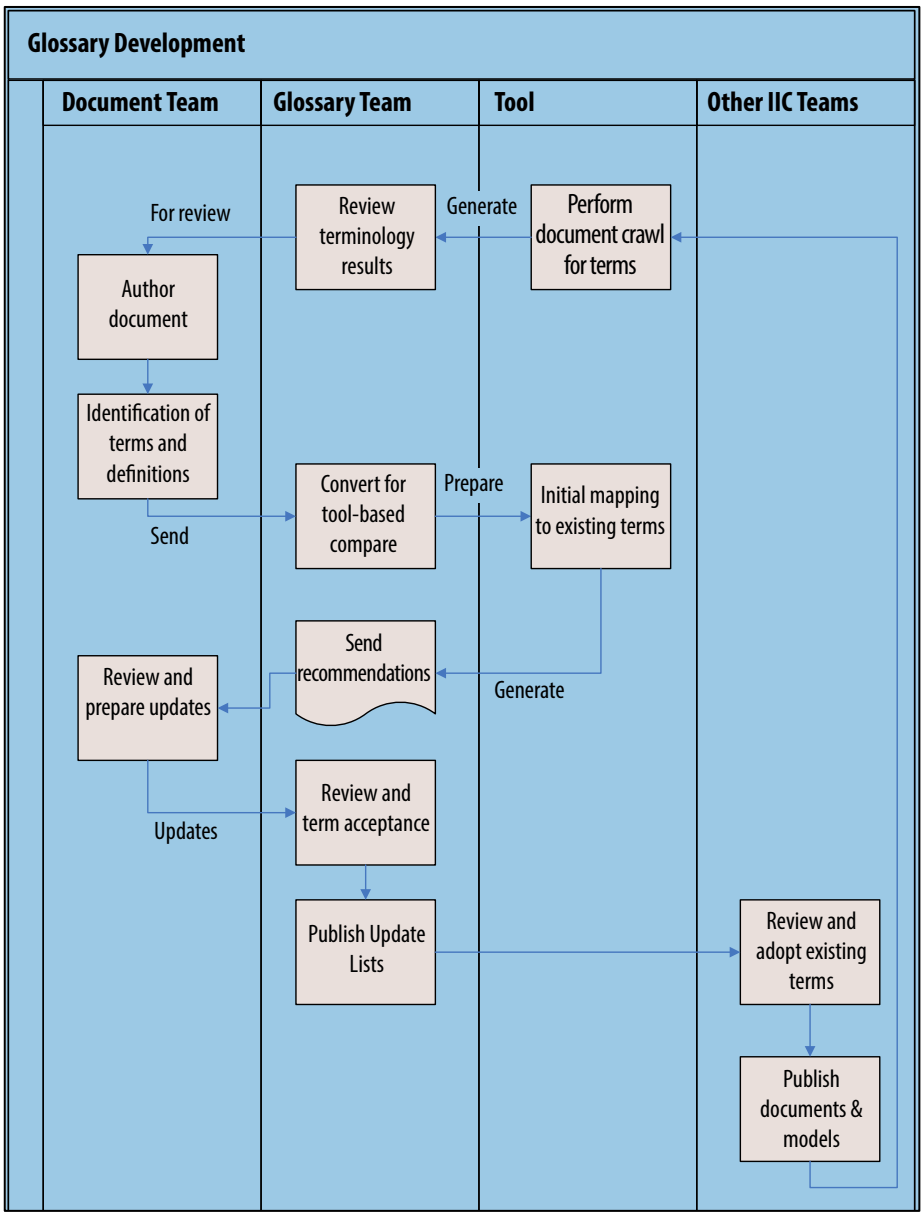
Application & Integration: Provides control and orchestration of a domain of devices and their software proxies.

Business Systems: Sets of services that permit connections to and incorporation of framework services into business systems.

Vocabulary

As with any complex and multi-faceted endeavor involving multiple organizations,

Process for Defining IIC vocabulary terms



SOURCE: IIC

Definition of terms becomes an important because IIoT solutions will be implemented by many organizations at all levels.

multiple backgrounds, and multiple points of view, the potential for ambiguity and misunderstanding is high. Every IIC Working Group and Team requires a common and reusable vocabulary of terms. This vocabulary includes standardized definition of terms—preferably from accepted sources such as IEEE, the OMG, or NSF, as well as usage of the term as it applies to specific IIC outputs.

There are four roles in vocabulary development:

1) The Document Teams (i.e. all teams that produce output) author documents and identify new terms, then rationalize specific terms to those in the dictionary;
2) The Vocabulary Team manages the review and incorporation of terms into the glossary. This team also scrapes existing sources for defined terms in order to reduce unnecessary duplication and difference.
3) Tools that automate the review of documents for the purpose of identification of new terms and synonyms/antonyms of existing terms.
4) Other IIC Teams review and use terms added to the glossary as a result of the work performed by a Document Team.

The goal is to create a set of documents that use consistent terminology throughout.

Security

The Security Working Group is focusing on systematically designing and incorporating security into the reference architecture(s) of the Industrial Internet from the start, as opposed to adding it as an afterthought.

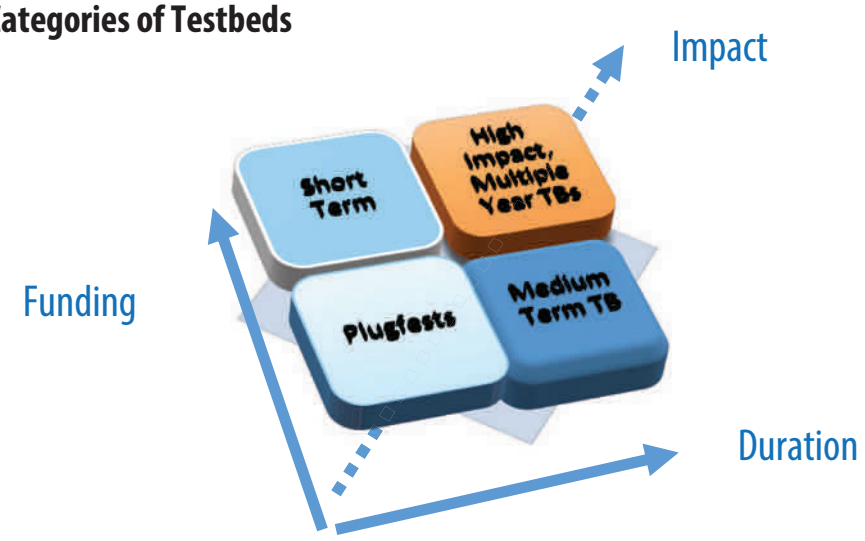
The team's first steps were to identify their deliverables, which included a set of use cases and a framework that could be applied to security. They also realized that their vocabulary had to be consistent with the work of the other teams. Consequently, the members of the Security Working Group are working with the Technology Teams on activities that were described in the sections above. They also meet separately to provide a "second pair of eyes" to IIC activities through a specific security lens.

The Security Working Group has divided into small, rapid teams to examine a general use case from three security-related points of view. They include (so far):

- Endpoint Security: A set of use cases designed to describe endpoint security, policy management, orchestration, and overall access control.
- Secure Communications: A set of use cases designed to describe secure communications between endpoints.
- Security Management and Monitoring: A set of use cases designed to describe secure provisioning and technical health and status of endpoints.

This list is being expanded to include topics such as data management to cover as much as possible in the evolving architecture. As that architecture takes shape, the IIC will apply security-focused use cases to the architecture so that these issues are considered.

Categories of Testbeds



SOURCE: IIC

Testbeds provide closed loop feedback to the technology groups as they attempt to implement specific solutions.

Testbeds

Testbeds are a primary focus area for the Industrial Internet Consortium. It is here that the innovation and opportunities of the Industrial Internet—new technologies, new applications, new products, new services, new processes—are initiated, thought through and rigorously tested to ascertain their usefulness and viability before coming to market.

A testbed is a controlled experimentation platform that:

1. Implements specific use cases and scenarios.
2. Produces testable outcomes to confirm that an implementation conforms to expected results.
3. Explores interoperability of untested or existing technologies working together in new ways.
4. Generates new (and potentially disruptive) products and services.
5. Generates requirements and priorities for standards organizations supporting the Industrial Internet.

Testbeds may be simulations or models, and they can be controlled from remote locations or onsite. The IIC divides testbed proposals into plugfest, short-, medium-, and long-term projects. Long and medium-term testbeds are expected to be 24 to 60 months in duration.

These longer-term initiatives are characterized by innovation that creates new markets and has an impact on the broader economy and society. They are often funded by institutions (governments, agencies, academia) in collaboration with industry.

Short-term and plug fest testbeds are of shorter duration (12 ~ 24 months) and focus on "go to market" product delivery. More than routine product testing, these IIC testbeds must demonstrate interoperability within an ecosystem (more than one company or proprietary technologies) and within the IIC roadmap. These testbeds are opportunities to open up new markets and to identify new applications during the development of multi-year testbeds

Because of the focus on new products and markets, these testbeds will often be funded by industry, and the funding organizations and testbed participants may choose to retain some or all of the intellectual property.

Testbeds are also driven by use cases in the sense that use cases specify desired business outcomes. IIC testbeds evaluate and test the functionality in the use cases. Consequently, as IIC testbeds are approved, new use cases are immediately solicited and identified to exercise the specific functionality that must be validated in the testbeds.

The IIC's priorities and activities for testbeds will continue to evolve. What will not change is its commitment to create and develop testbeds that support the goals of innovation and interoperability.

Conclusion

The market response to the Industrial Internet Consortium has been clear. With 125+ members four months into its existence, the Industrial Internet Consortium has become a significant player in the quest to systematically build the infrastructure for the Industrial Internet.

For more information on the Industrial Internet Consortium, visit www.iiconsortium.org.

***Stephen Mellor** is chief technology officer for the Industrial Internet Consortium.*

Cremation system uses smart phone as mobile HMI

DFW cremation systems are using new control technology to achieve energy efficient operation, extremely low emissions and a fully automated process. Their newest systems have also implemented a mobile HMI using a smart phone interface which enables use of a unique operator terminal that is very easy to use.

SOURCE: OPTO 22

DFW cremation ovens are highly energy-efficient and extremely low in emissions, and the whole process is controlled automatically.

MODERN MOBILE TECHNOLOGY is offering new levels of connectivity, convenience and performance to a maker of cremation systems, using a smartphone to implement a mobile HMI solution.

DFW Europe is an international producer and supplier of complete cremation solutions. They started as a central heating installer but grew into a machine manufacturer led by father and son, Jan and Bart Keeman. In the beginning, DFW gained experience in industrial gas heaters and filter systems during the construction of greenhouses. This was followed by a side-step into the installation of imported cremation ovens that would later prove to be all-decisive. Eventually DFW very successfully took control by providing the entire development, construction and final assembly of complete cremation installations.

They choose a programmable automation controller (PAC) control system from Opto22 because of its hardware and software flexibility, and the lack of licensing costs for the programming and HMI software.

The Challenge

With its newest system, DFW has designed a cremation installation with five cremation ovens with state-of-the-art technology for a crematorium in Ringsted, Denmark. But one of the requirements was that the brand-new cremation ovens could also be controlled by the operators with smart phones. DFW had already progressed far with a solution for scanning the cremation numbers with smart phones; however a separate IR remote control was required for operating the ovens. The challenge was to implement a new solution for this important project within a very short period.

The control system used for the cremation systems utilizes a programmable automation controller (PAC) as the solution for control and monitoring.

"Opto22 groov came out at the end of the project. It was exactly what we were looking for because the interface can be operated perfectly with a smart phone," said Jan Keeman.

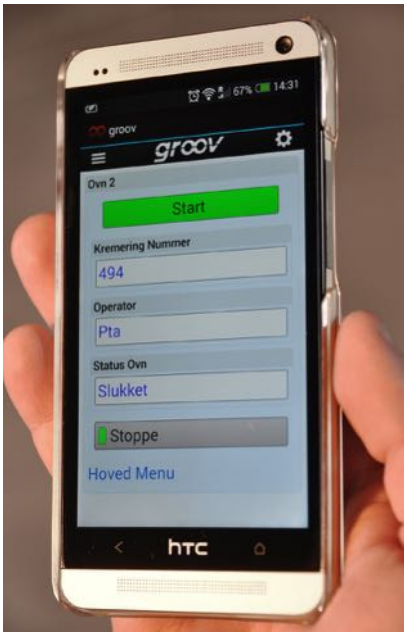
Smartphone control

Up until that point, the IR control was the only option for controlling the cremation ovens. But using the new product, a test set-up was developed in one morning using development tools and tag database. Testing could start after the training video had been watched,

the groov-box had been connected to the network and the connection with groov via a web browser had been established.

"We phoned on Thursday to ask if we could try a test set-up," said Bart Keeman. "We received it Friday morning and our first groov-interface was working in the test environment on Friday afternoon.

After a short testing phase, the engineers from DFW could quickly start programming the final user interface for the Danish crematorium. Within a couple of weeks DFW has been able to definitively implement the smart phone HMI in the production environment.



Operators can control the cremation process with a smart phone, along with monitoring the status of the oven at all times.

The result

The operators can now operate the whole cremation process with a smart phone and keep an eye on the status of the oven at all times. The interface developed here has been kept simple and basic. When the coffin is inserted into the cremation oven the operator only has to enter his name and scan the registration number of the coffin, and then press the start button. The whole process is then controlled fully automatically.

The DFW cremation ovens are very energy-efficient and extremely low in emissions due to the many technical innovations developed by DFW in the cremation process. Hundreds of homes, two schools and a swimming pool in Ringsted are heated with the recovered energy. The new crematorium is therefore known as 'Cremation 2.0' in the cremation market.

SOURCE: OPTO 22

Jan Keeman of DFW said that technology has allowed his company to refine and optimise the cremation process including mechanical design, instructions and installation.

According to Jan Keeman, "DFW has gone deeper into the technology to refine and optimise the process even further. As a company, the trick is to program all aspects of the cremation process in the machine and thereby combine the feeling for the mechanical side, the instructions and the installation."

***David Hill is** Marketing Communications Manager for Opto 22.*

SCADA cybersecurity – protecting critical infrastructure

The IEEE 1815 Standard known as Distributed Network Protocol 3 (DNP3) was originally developed without security. In today's connected world and for industrial SCADA systems, this is no longer acceptable and Secure Authentication (SA) is an addition to the standard that provides needed message authentication.

CYBER ATTACKS like the 86 million household and small business records stolen from JP-Morgan Chase Bank (Reuters, 2014) contribute to the 78% increase in financial impact of cybercrime in the past four years. In this same period, 40% of cyber-attacks have been directed against energy companies. The US government is focusing on the threat to the nation's critical infrastructure such as our electric grid, oil and gas pipelines, water and wastewater treatment facilities and transportation infrastructure like tunnels and bridges.

Executive Order 13636 addressed protecting the US critical infrastructure against cyber intrusions while directing the agencies responsible for the elements of the infrastructure to share information. The National Institute of Standards and Technology (NIST) has released the Cybersecurity Framework for systematically identifying the critical assets of the organization, identifying the threats and finally securing these critical assets. It is based on risk assessment techniques including periodic reassessment with the goal of identifying and neutralizing a threat before it occurs, but also recovery plans in the case of a successful attack.

The implementation of Cybersecurity under the NIST Framework is ultimately the responsibility of the SCADA Application owner and operator as it encompasses the entire system including the organization developing the SCADA application, the corporate networks and computers that it runs on and the control devices and instrumentation attached to it. However, the implementation of security standards and the capabilities of the software to implement security processes are the responsibility of the SCADA provider.

Three of the high-level security objectives of the modern electrical grid or Smart Grid are availability, integrity and confidentiality. These objectives apply to SCADA systems in all segments whether or not they are part of the Critical Infrastructure. The IEEE 1815 Standard commonly known as Distributed Network Protocol 3 (DNP3) was originally developed without security included in an era when the notion of "security-by-obscurity" was realistic. In today's connected world this is no longer acceptable and Secure Authentication (SA) is an addition to the standard that provides for message authentication. The DNP3-SA version 5 (SAv5) released as part of the IEEE 1815-2012 has a strong emphasis on addressing security concerns stemming from demonstrated vulnerabilities to denial of service attacks (DoS). The standard is under constant review and update to remain current to cyber threats.

Ten Most Common SCADA Vulnerabilities

SOURCE: PCMJE

VULNERABILITY	IMPACT
Un-patched Published Vulnerabilities	Most Likely Access Vector
Web Human-Machine Interface (HMI)	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

Critical infrastructure protection

In February 2013, with a growing awareness that cybersecurity is a critical defense against an attack which can potentially disrupt our power, water, communication and other critical systems, President Obama issued an Executive Order (EO) on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience. These policies reinforce the need for holistic thinking about security and risk management (Department of Homeland Security, 2013).

While these directives are focused on the US critical infrastructure, there is clear benefit of the approach when applied to other SCADA infrastructures.

NIST Framework

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity (NIST, 2014).

IEEE 1815 secure authentication

DNP3 was designed originally without any security mechanism. It is a protocol used extensively in North American substations, oil and gas pipelines, water and wastewater treatment, and transportation infrastructure. This makes it impractical to replace all of the DNP3 devices with security embedded. Instead, the standard has taken the approach to make secure authentication an addition to the DNP3 protocol.

DNP is designed to run over a variety of networks, even traversing serial links over radio and IP networks in the process of getting from the sender to the receiver. For this reason, it is not sufficient to secure only the network, but in fact the message itself must be secured which must be done at the application layer.

The mechanism used by DNP3-SA is to add a Hashed Message Authentication Code (HMAC) to the message to verify its integrity. This MAC uses a 'cryptographic hash" based on the NIST and ISO Secure Hash Algorithm (SHA) which requires a shared key to decode.

This approach is not based on encryption, rather it is based on verifying the sender of the message with assurance that the message has not been tampered with. An attacker can see the message since it's not encrypted, but cannot tamper with it or send unauthorized messages without the key.

There are three types of security that are commonly used in communication networks. These are Site-to-Site (such as Virtual Private Networks), Device-to-Device (e.g. TLS) and Application-to-Application (e.g. SA). All of these types of security can be deployed simultaneously for full protection. The reason that one type is not enough is illustrated by considering a VPN.

While VPN routers and protocols such as IPSec secure the link between two physical locations, it does not secure the networks at those locations leaving open the possibility that hacking into one network gives access to the other. TLS secures the complete TCP connection and is used in banking transactions today, but the difference to the SCADA environment is that it only works on the IP networks so if the DNP is crossing a serial link there is a vulnerability.

In developing SAv5, the operation of DNP3 SA has been reviewed by independent external security experts. A number of features were identified as being potentially vulnerable. Additionally, the Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) has a set of security criteria that must be met in order to permit IEEE 1815 to be adopted as a recommended standard for use in the Smart Grid. Some modifications that appear in SAv5 were included in order to meet SGIP security requirements.

SAv5 has several changes that reduce the impact of denial of service attacks responsible for the buffer overflow issue on the Idaho National Labs Top Ten List. Although DNP3-SA HMAC ensures that no unauthorized party can successfully communicate to a DNP3 device, the sending of improper HMAC creates a large amount of traffic in response to the bad message. Nearly half of the categories of changes in the SAv5 have a purpose of reducing the impact of DoS.

It's important to work in partnership with all stakeholders to ensure that cybersecurity concerns are addressed so that the operator is able to achieve a secure SCADA solution. The NIST Framework provides a way in which partnerships are more effective and cybersecurity prioritization is rationalized to meet the needs of the operator.

Edward Nugent is *Business Development Director for PcVue Inc.*

How OPC UA servers enable SCADA device data management

OPC Unified Architecture (UA) servers offer a step in the direction of Big Data by facilitating efficient SCADA device data management. In automation applications, Big Data means ever-increasing amounts of sensor data from the production process that needs to be effectively managed.

MODERN SCADA SYSTEMS can communicate directly with an OPC server which in turn communicates with PLCs, RTUs or remote I/O units to pass sensor readings and control signals back and forth between the OPC server and devices.

Where the more traditional OPC DA server uses a polling method which can use network bandwidth, newer OPC UA servers use a "report by exception" methodology to reduce the amount of information that the OPC server needs to send to the SCADA software. The combination of OPC UA with Active OPC server technology provides users with a seamless communication solution that can save an impressive amount of bandwidth usage.

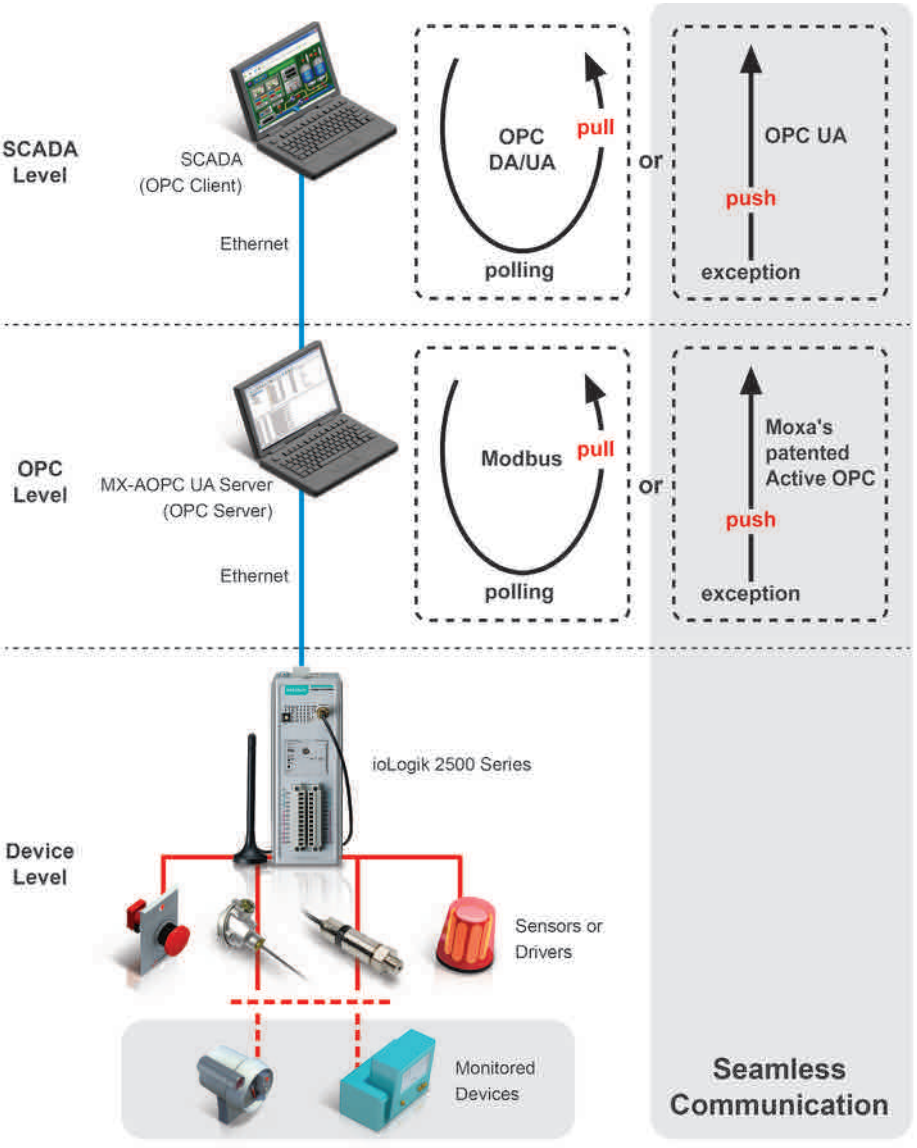
This article will explain the difference between "updating data by polling" and "updating data by exception," and give some general rules of thumb that users can follow to decide which method is suitable for various I/O devices, along with OPC UA server solutions.

Traditional SCADA architecture

For more than half a century, SCADA systems have given operators, located in a central control room, the ability to monitor and control multitudes of devices spread out over a wide geographical area.

The structure of a modern SCADA system has the SCADA software at the top, monitored devices at the bottom, and an OPC server in between. PLCs, RTUs, and/or remote I/O units are used to pass sensor readings and control signals back and forth between the OPC server and devices. The PLC/RTU and remote I/O provide the remote locations with a certain amount of autonomy, and are smart enough to implement local control schemes independent of the SCADA software itself.

SCADA software and OPC servers have traditionally been based on a client-server polling model. That is, the SCADA software polls the OPC server, which itself polls the system for current sensor readings, and then the SCADA operator issues commands in response to whatever information is provided by the SCADA software's user interface. Although some readings could be polled more or less frequently than other readings, sensors that monitor critical readings (e.g., whether or not a locked door is open or closed) may need to be polled as frequently as once per second to give operators enough time to take the necessary action (e.g., alert security personnel), and to ensure that the SCADA system is properly notified.

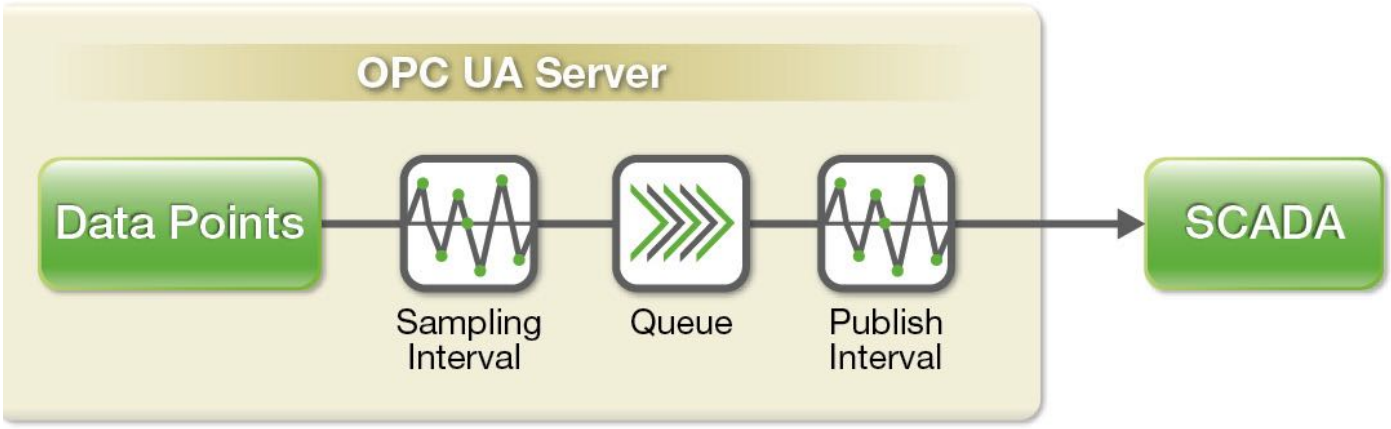


SOURCE: MOXA

Modern systems have the SCADA software at the top, monitored devices at the bottom, and an OPC server in between.

For example, if the door's status is polled once every five seconds, but the door is opened and then closed within a 4-second time interval, the SCADA system won't even know that the door was opened. If you only need to monitor the status of one door, then frequent polling may not be a problem. However, for SCADA systems that monitor the status of hundreds of doors, frequent polling of so many sensors could occupy a large amount of network bandwidth, and as a result slow down other applications that are connected to the same network.

About ten years ago, Moxa introduced its patented Active OPC concept, which is



SOURCE: MOXA

Report by exception uses a subscription and monitored item methodology. Readings that don't change aren't published, which forms the essence of the "report by exception" concept.

implemented by Moxa's ioLogik products. Put simply, Active OPC gives dumb I/O devices the intelligence they need to initiate a connection with the OPC server. In other words, since the I/O devices are connected to the ioLogik via local serial connections, the ioLogik can poll these devices as frequently as it likes without putting any burden on the Ethernet network, and only sends readings to the OPC server (over the Ethernet network) when certain pre-configured conditions are met. As illustrated by the diagram on page 16, the action of a traditional client-server polling model is sometimes described as a "pull" (since the OPC server "pulls" I/O readings out of the various devices), whereas the action of ioLogik's Active OPC is described as a "push" (since the remote I/O "pushes" I/O readings from the various devices to the OPC server).

In a more recent development, in 2008 the OPC Foundation standardized a "report by exception" methodology in the OPC Unified Architecture (OPC UA for short). OPC UA uses a "subscription and monitored item" model to control communication between the SCADA software and OPC server. OPC UA is completely new, in that it allows operators to work directly from their SCADA system to configure the way the OPC server interacts with the various I/O devices. In fact, since report by exception "pushes" readings from the OPC UA server to the SCADA software, using OPC UA in combination with Active OPC provides seamless communication by implementing what we could call a "push-push" strategy, which has the potential to save impressive amounts of network bandwidth.

Updates via polling or exception

For many years now "updating data by polling" has been the industry standard for communication between the OPC server and OPC clients (i.e., SCADA software).

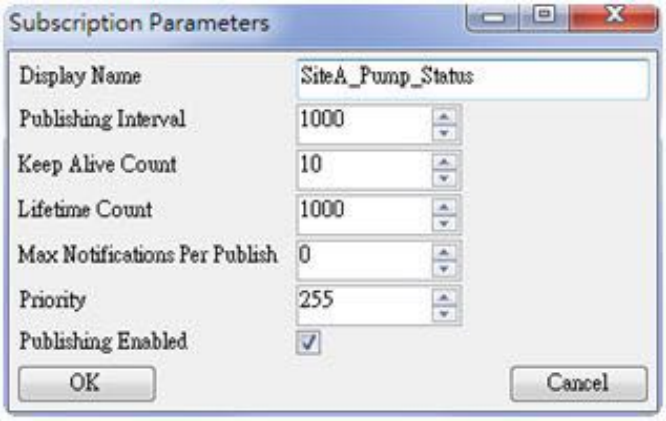
Now however, engineers can decide between updating data by polling and updating data by exception. Generally speaking, which option to choose depends on two factors: (1) the frequency with which sensor readings change, and (2) the urgency with which you need to know that a reading has changed. Sensor readings that change frequently need to be sampled frequently to get a true picture of how the sensor readings change with time. For sensor readings that don't change very often, you could end up wasting quite a bit of network bandwidth if you sample too frequently. But, if you sample too infrequently, you might completely miss critical data (such as that a door has been opened and then closed). Let's look in more detail at how updating works with an OPC UA server.

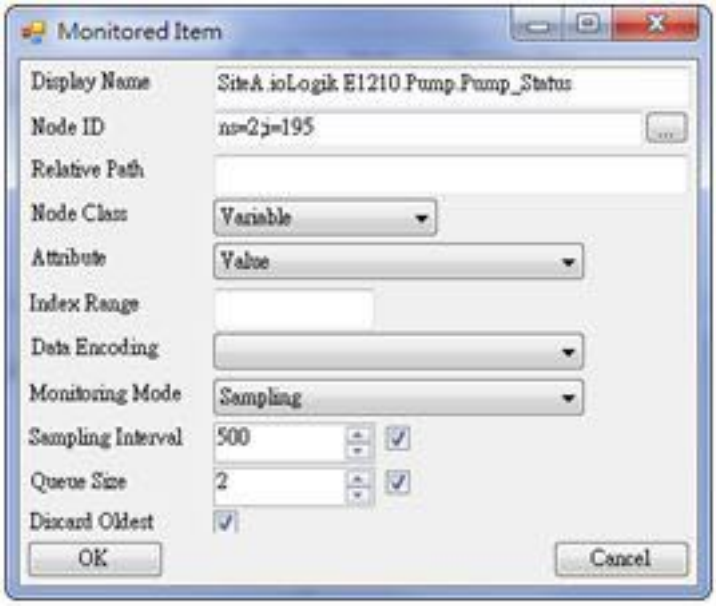
All OPC UA servers still support updating data by polling, with the configuration procedure and method of operation identical to more traditional OPC DA servers.

Updating data by exception

When configured for report by exception, an OPC UA server uses a "subscription and monitored item" methodology in which a SCADA client subscribes to a set of monitored items. The OPC UA server samples the data points at regular "sampling intervals," places the item's readings in a queue, and then publishes the readings at regular "publishing intervals."

A critical aspect of this operation is that if a sampled reading has not changed compared to the previous sample, the reading is not placed in the queue. What this means is that readings that don't change aren't published, which





SOURCE: MOXA

Two settings, the sampling interval and the publishing interval, need to be configured on the OPC client to enable updating by exception. The sampling interval defines the rate at which the server checks for changes in the monitored device readings; the publishing interval defines the rate at which the server sends notifications to the client.

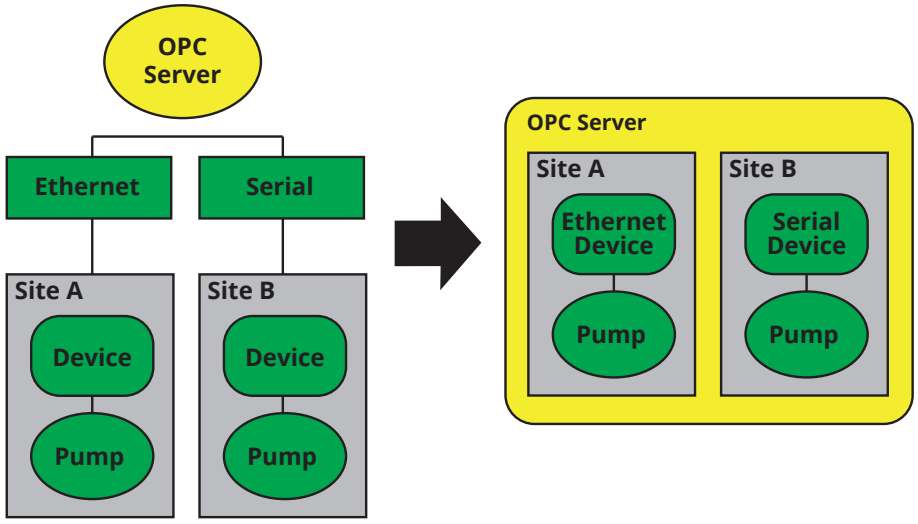
is the essence of the "report by exception" concept. Note, too, that OPC UA supports sending heartbeat signals during extended periods of inactivity so that each side of the connection will know that the other side is still alive, and consequently will not close the connection.

Two settings need to be configured on the OPC client to enable updating by exception: the sampling interval and the publishing interval. The sampling interval defines the rate at which the server checks for changes in the monitored device readings, and the publishing interval defines the rate at which the server sends notifications to the client. The sampling interval can be shorter than the publishing interval, in which case notifications are queued in the server until the publishing interval has elapsed. At that point, the server sends all of the notifications in the queue to the client.

With "update by exception," since I/O readings are not transmitted when the monitored system's status doesn't change, operators can greatly reduce the amount of network bandwidth that's required. This is especially true when the frequency of value changes is far less than the polling interval, such as is true when monitoring a door's open/close status. Report by exception also saves computing resources on both server and client computers for handling timeouts and retries.

If the frequency of value changes is higher than the polling interval and urgency is critical, updating data by exception is still the better way to go. However, report by exception may still cause a lot of data to be transmitted in a very short time, which could cause network congestion. The congestion can be relieved somewhat by setting an appropriate "dead band" for analog data, or by trimming down the amount of data with an appropriate numerical processing algorithm before data is sent out. On the other hand, if the frequency of value changes is higher than the polling interval and urgency is not critical (such as when monitoring the temperature of a liquid), updating by polling might be more appropriate.

Most OPC UA servers use a poll-type protocol, such as Modbus, to get data from their I/O devices. However, polling hundreds or thousands of tags is very inefficient. If both polling and exception options are available, you can determine the best approach by first categorizing device tags into one of four types, and then increase the efficiency of your operation by using poll-type methods on the high frequency but non-critical urgency tags to update data to the SCADA system.



SOURCE: MOXA

Changing from communication channel to application for tag naming.

Configuring tag names

Most OPC servers require tag names to start with communication type, such as Ethernet or serial, followed by device name, followed by I/O point name. For example, a tag name for a pump's on/off status might be Ethernet.Device.Pump_Status.

However, since the location of the sensor the tag name is associated with is not included in the tag name, and since a single SCADA system might include thousands of tags, it is difficult or impossible for operators to determine which device is being referred to just by looking at the tag name. For this reason, tags are often associated with more detailed descriptions, with the tag names and descriptions organized in an Excel worksheet.

One way to get around this problem is to include the device's location in the tag name by appending it to the device name. To illustrate, suppose the SCADA system uses the same model of I/O device to monitor two different pumps named PumpA and PumpB. If the two pumps are monitored by different I/O devices of the same model, you could write the tag names as Ethernet.Device_SiteA.Pump_Status and Ethernet.Device_SiteB.Pump_Status to differentiate between the two. But why should tag names start with communication channel?

If the tag names are based on the actual application architecture, it would be easier for users to construct the tag names. The difference in tag naming strategy is illustrated in the figure at the top of this page. The diagram on the left is less intuitive, and could get rather messy since if Site A also uses serial devices, then "Site A" would also appear under the Serial branch. The diagram on the right shows the same system organized by the application architecture. In this case, all devices at Site A will appear under the Site A branch, and the tag names could be written as SiteA.Device.Pump_Status and SiteB.Device.Pump_Status. These tag names are more readable, and make it easier to configure a SCADA system.

Data Changes \ Reporting Urgency	Critical	Non-critical
High Frequency	Update data by exception (with appropriate dead band setting)	Update data by polling (with short sampling interval)
Low Frequency	Update data by exception	Update data by exception

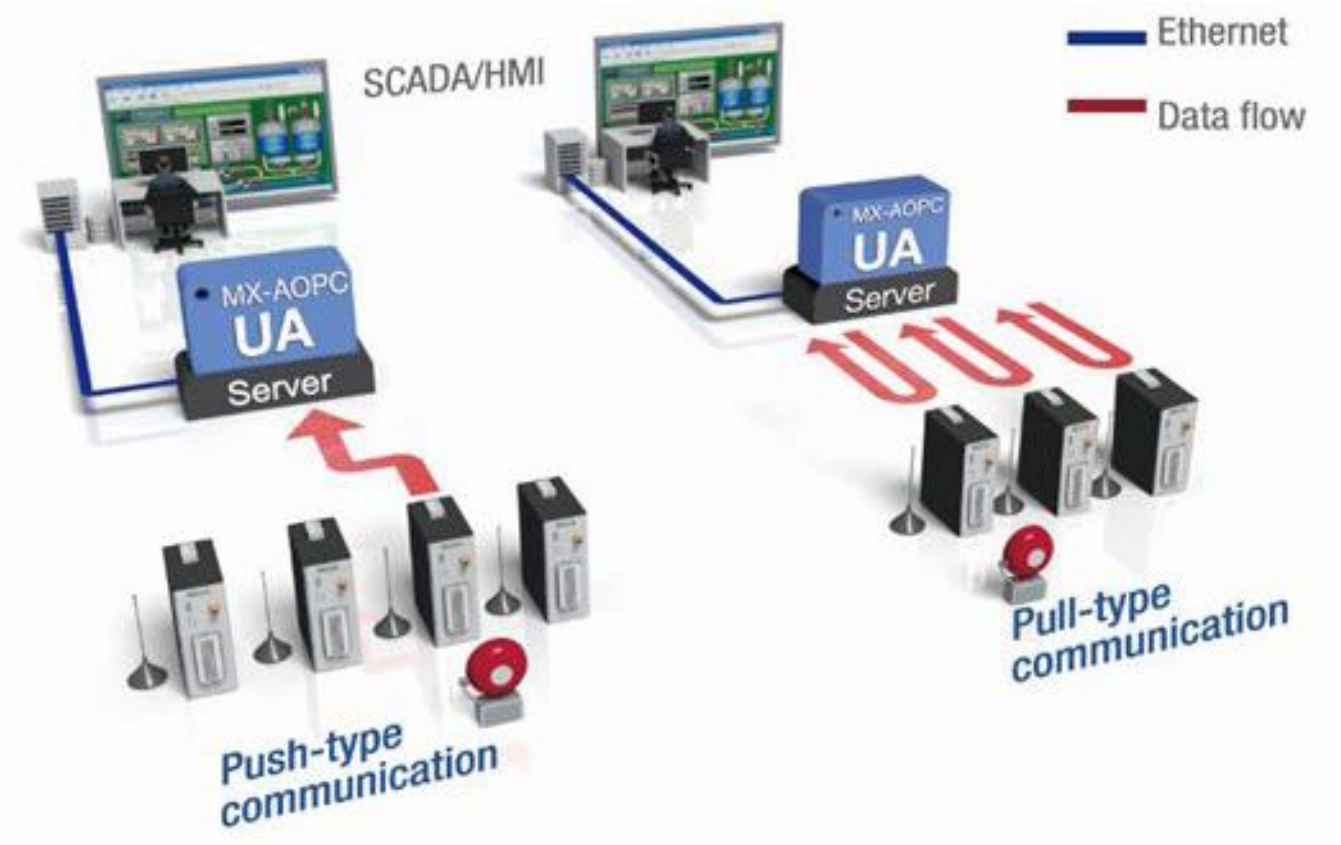
Selecting either polling or exception updates.

OPC UA simplifies connections

Configuring OPC to work between the server and the client on different computers was a real headache before the OPC unified architecture was available. For example, the user had to log in with the same account and password on both the server and client computers, which can be extremely inconvenient from a practical point of view. In addition, the user needed to follow detailed unintuitive step-by-step instructions to configure DCOM security.

In contrast, OPC UA uses an optimized TCP-based UA binary protocol for data exchange, in which communication transfers can be activated by opening up a single user-configurable port in the firewall. Users can create many TCP URLs for OPC server endpoints, with each endpoint mapping to a unique port. OPC UA clients only need the URL of the server endpoint to connect to the OPC UA server.

Integrated security mechanisms such as X509 certificates ensure secure communication on the Internet. Users can define security



SOURCE: MOXA

Report by exception uses a subscription and monitored item methodology. Readings that don't change aren't published, which forms the essence of the "report by exception" concept.

policies such as "Sign and Encrypt" between the OPC UA client and server.

Users only need to import the client's "Certificate Authority" file from the OPC UA client and export the server's "Certificate Authority" file to OPC UA clients to establish authority between the server and client.

Then, the "Discover Servers" function can be used in the OPC UA client to discover OPC UA servers accessible over the network.

Finally, users can select the TCP URL to connect to the OPC UA server.

OPC UA server solution

OPC UA servers that use Active OPC monitoring technology incorporate support for the Modbus protocol, and provide a secure and reliable gateway between local devices and a remote SCADA system. This technology pioneered "push type" I/O processing (versus "pull type" or "polling") to the automation industry. These servers offer both a polling and non-polling architecture alongside the standard OPC UA protocol, giving users the choice of pull or push-based communication with devices.

The OPC UA server's design logic is user-application oriented. Users can create device groups such as "SiteA" and "SiteB", for example, based on their application. In the example shown here, each site uses the same ioLogik E1210 remote I/O unit to monitor pump status. Tag names are much clearer and more readable when it comes time to configure the SCADA system.

***Charles ZK Chen is** a Product Manager for Moxa.*

Directions in convergence: SCADA & IT management

New switch technology is balancing the advantages and costs of managed versus unmanaged switches. Lower cost, lower functionality Layer 2 technology is aiming to meet the degree of connectivity required by IoT applications, leveraging solutions that support both Modbus/TCP and SNMP to simplify network management.

SENSORS, CONTROL NODES, PLCS AND SCADA servers are connected in the industrial environment using switches and wireless APs to create complex networks. As the number of devices increase, management and issue diagnostics are a challenging job for both IT and automation professionals.

With the onset of Industrial IoT initiatives for plant management, the drive to make the industrial Ethernet robust and transparent becomes a bigger focus in 2015.

Resolving network issues will be a large concern. Switch visibility would be implemented to ensure an agile network, a role usually reserved for a topology of robust, managed switches. The drawback is that such switches can be costly and require a ramp-up time to implement.

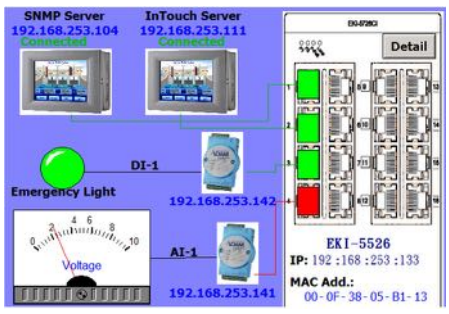
SOURCE: ADVANTECH

To allow automation and IT software to monitor status, the switch technology supports both Modbus/TCP and SNMP.

Industrial Ethernet infrastructure

IHS issued a new report on the market for industrial Ethernet infrastructure components in December 2014 in which John Morse predicts that "the introduction of lower-cost, lower-functionality layer-2 switches will economically serve the need of users as networks are expanded to meet the degree of connectivity required to join the industrial IoT revolution." Morse later added that, "this trend may, in the longer term, see the demise of the unmanaged switch as the prices converge, much in the way the hub has become all but extinct."

Advantech introduced new switch technology in 2014 aimed at enabling convergence management in support for Automation Engineers and IT staff. ProView technology combines the advantages of both managed and unmanaged switches at the price point of the latter, and introduces a simple solution that serves port information for all central network management on SCADA or SNMP systems.



SOURCE: ADVANTECH

Switch device information, switch port status and I/O device reading in one SCADA system. The red rectangle indicates that the port 4 has been disconnected.

In order to allow both automation software and IT software to monitor the switch status, the technology supports both Modbus/TCP and SNMP protocols. This allows SCADA software such as Wonderware InTouch, Advantech WebAccess, WinCC, iFix, and IT Network Management System (NMS) software such as SNMPc and OpenNMS to monitor device status in real time, and remotely. Such a benefit will be key in an Industry 4.0-aligned network, for quick port issue resolution via remote diagnostic that allows visibility for both Automation Engineers and IT staff.

In addition to real-time status monitoring, the devices come with Port-based QoS for deterministic data transmission that allows data from the VIP port to have a higher priority compared to data from a normal port.

Communication via Modbus/TCP

The Modbus/TCP protocol allows a majority of popular SCADA systems such as InTouch, InduSoft, WinCC and iFIX to obtain device status and information. This allows all devices, including ProView switches and I/O control devices, to be controlled and monitored through one HMI/SCADA system.

In the following SCADA software example, by using InTouch from Wonderware, the system is able to connect a SCADA server, one analog I/O Modbus TCP module and a digital I/O Modbus TCP module to a switch that uses ProView technology.

SCADA software is used to access the memory address through Modbus/TCP which makes it possible to obtain the device information such as the device name, FW version, MAC and IP address, and also the port status information such as port link up/down, link up counter and port speed.

This information further helps the engineer diagnose any issue. When a signal is lost by the end device, by having both the network information and the device information displayed on the SCADA, users are able to conclude that the signal loss is caused by either the network or the end device itself. For example, by reading the status of port 4 at the designated memory location through Modbus/TCP, the user is able to know that the port has been disconnected and combined with SCADA HMI, the status indicator of port 4 turns red. On-site engineers can then easily identify that the lost signal is caused by a disconnected network cable or by malfunction of the voltmeter or the Modbus TCP module. This helps to quickly narrow down the root cause of an issue.

As well as basic device information and the port link up/down status, the technology provides detailed statistical information on

each port including speed, linkup counter, count on the multicast packet, count on unicast packet and count on error. This allows engineers to observe the network status and statistic in detail from any HMI / SCADA software which supports Modbus/TCP.

In a HMI / SCADA system such as InTouch, address mapping and Modbus/TCP connection is the initial step in the InTouch setup.

Communication via SNMP

Support for SNMP (Simple Network Management Protocol) allows IT NMS (Network Management System/Station) software such as SNMPc, SUSIAccess NMS and OpenNMS to perform device management including status monitoring, configuration and even events notification.

This allows IT engineers to have better monitoring and control on the network and easier troubleshooting when something is incorrect on the network.

In an industrial environment such as manufacturing, nothing is more important than keeping the network, which is formed by thousands of sensor devices, running smoothly without any downtime. SNMP has been widely used by engineers to monitor the network device status and an NMS is able to provide an intuitive network topology with a real time device status. For information that is not supported by a standard SNMP MIB library, a private MIB file that allow NMS software have the method of obtaining this information.

As well as device monitoring, IT can also control or perform certain system configurations through SNMP. The setting of the device location, device IP mode, device IP, device netmask, default gateway and read/write community name can be configured directly through the NMS software.

For the statistical port information, the technology is able to provide statistical information including count on unicast, multicast and broadcast packet for each individual Ethernet port.

By supporting SNMP traps which automatically notify the SNMP server when there are events such as port link-down/up, cold start and warm start occurs, this information allows IT engineers to be notified of a network status change, not just on the switch, but also on the devices connected to it, imminently and act quickly.

QoS deterministic data transmission

A maximum of two VIP ports with high transmission priority can be used for deterministic data transmission. The priority ratio between the VIP port and the normal port is 1.5 to 1. For example, when there are two traffic flows on a switch at the same time.

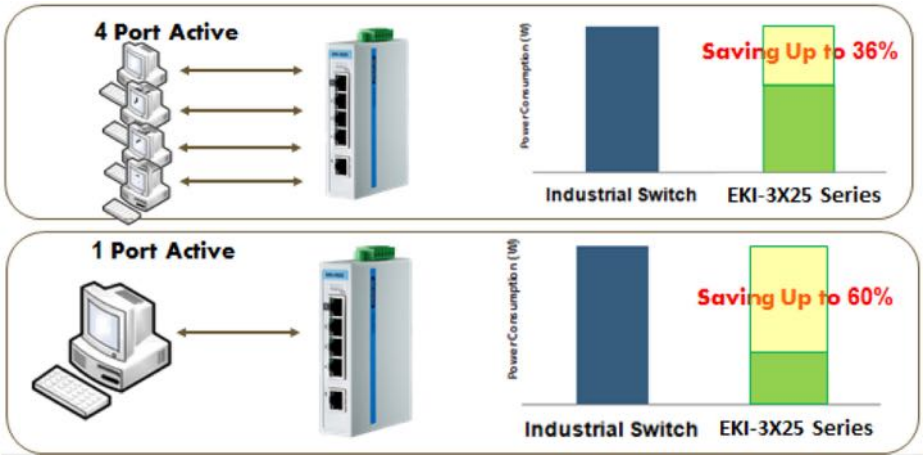
When traffic flow 1 is transmitting data from VIP port 1 to port 5 and also traffic flow 2 is forwarding data from port 3 to port 5, traffic flow 1 can have 50% more throughput than traffic flow 2. The port base QoS is useful to ensure high priority on important data to be transmitted in a busy network.

By supporting IEEE 802.3az standard, the technology provides a method for switching between higher power state (data mode) / lower power state (LPI mode) in response to whether data is flowing through them. This allows power saving up to 60%.

Managed vs. unmanaged switches

With the communication capability using both Modbus/TCP and SNMP protocol, the new classification of networking switches will provide management convergence between industrial control and IT networking management. ProView technology is positioned in between the two switch classes to introduce an option for increasingly complex industrial networking to bring plant engineers a robust and easily-diagnosed network with very little learning curve. In all, this means finding and resolving issues fast – practically as fast as Industry 4.0 nimbleness claims to be.

Technology report by ***Advantech.***



Use of IEEE802.3az provides a method for switching between higher power state (data mode) /lower power state (LPI mode) in response to whether data is flowing through them -- to reduce power consumption.

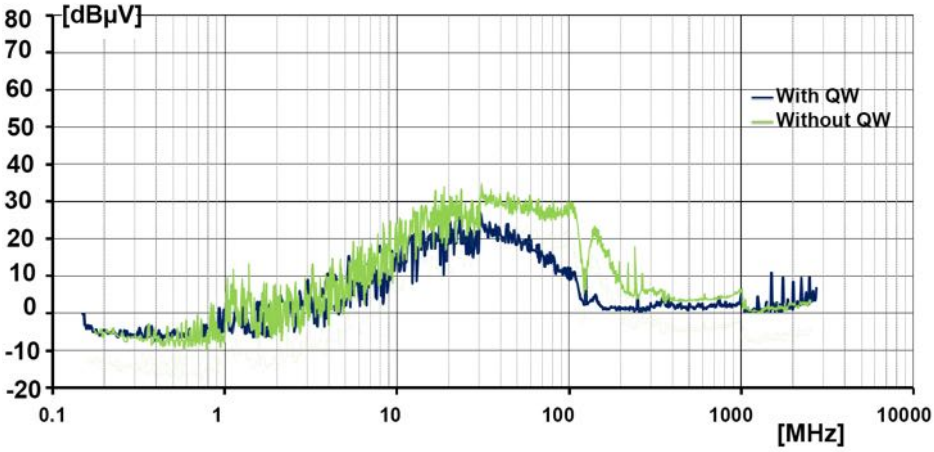
Ethernet device and sensor performance key for IoT

With Ethernet emerging as a replacement for device layer fieldbus technologies, the ability to remotely monitor, identify and control devices on the network is an enabling technology for the Internet of Things. But there is also an ongoing need for strong Ethernet PHY performance at the device and sensor levels.

ETHERNET IS ALREADY COMMONPLACE across industrial control and automation networking. Significantly, it is now emerging as the replacement for device-layer fieldbus technologies, enabling the advent of the Industrial Internet of Things (IIoT).

The ability to remotely identify, monitor and control every individual device on a network offers unparalleled benefits to the industry. Management efficiency is drastically improved, reducing operating costs, but more notably, risk of machine failure is significantly reduced or even eliminated.

Despite such key benefits Ethernet technology must evolve to meet the needs of the industry. This trend is continuing with the technology in the latest 10/100BASE-TX Ethernet PHY transceivers that combine robust performance coupled with a series of unique attributes designed to enhance Ethernet's ability to perform at device and sensor layers.



SOURCE: MICREL

Transceiver line RF emissions between typical Ethernet and a PHY utilizing Quiet-WIRE technology.

Enhanced EMC/reduced cable cost

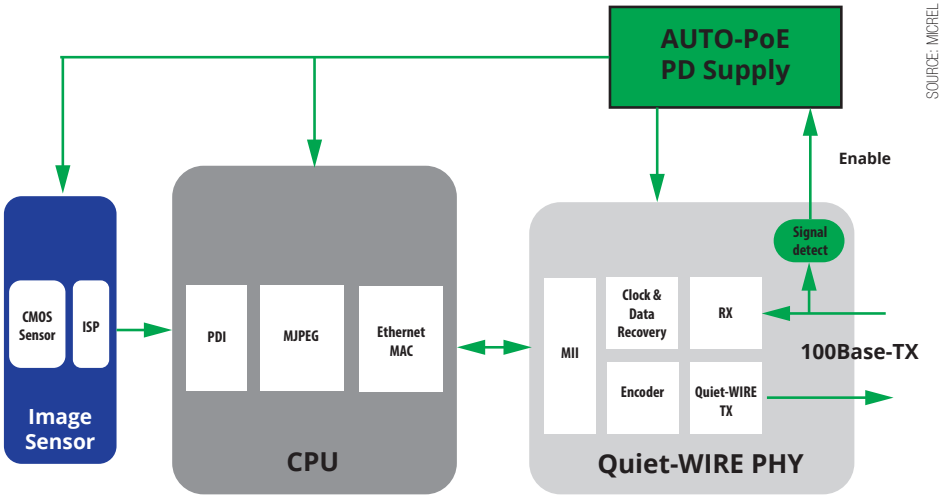
Quiet-WIRE is a technology that provides fully programmable, integrated noise filtering to reduce emissions and enhance immunity. This enables designers to meet automotive and industrial EMC standards, for example, while operating over low cost unshielded twisted pair cable.

Comparing transceiver line RF emissions based on the IEC61967 standard between a typical Ethernet and PHY utilizing this new technology, the result is up to 20dB reduction at frequency range 30MHz and above; this is without compromising on cable reach of 130m or more. The result is enhanced receiver immunity that delivers error-free performance in the most stringent noise environments, even over low cost unshielded cable.

With a typical Ethernet PHY using the IEC62132 DPI (Direct Power Injection) Immunity method, one can observe errors occurring in the frequency band 10MHz to 250MHz, reducing receiver immunity tolerance by up to 10dBm. In contrast the KSZ8061 PHY delivers error-free performance in the presence of maximum 39dBm noise injection, across the full frequency range.

Analogies can be made to the automotive industry where Ethernet is being adopted as the physical bus of choice for camera and sensors in advanced driver assistance systems (ADAS).

Here although digital processing cost in camera and ECU is somewhat higher than traditional analog or LVDS methods, cable costs are considerably reduced with the ability of using unshielded cabling. In addition Ethernet removes the need for an additional power cable, offered by Power-over-Ethernet (PoE). However, the ultimate goal is to deliver a single ubiquitous network seamlessly providing cross-domain communications down to devices and sensor layers.



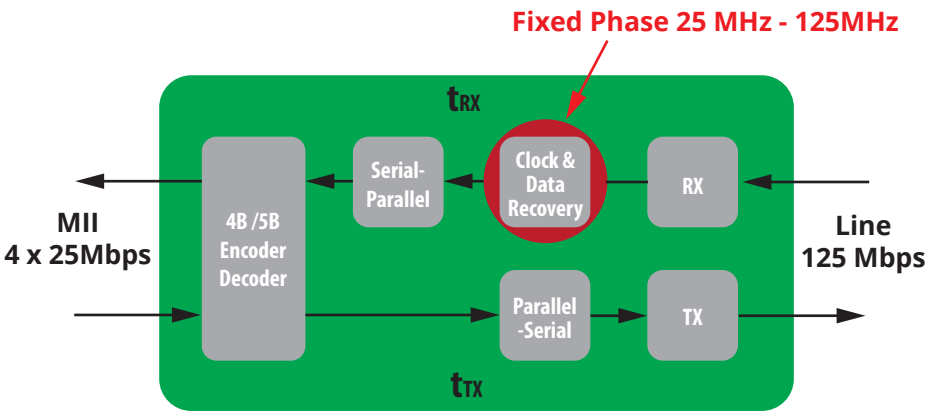
SOURCE: MICREL

DPI (Direct Power Injection) immunity method.

Low power, energy efficiency

Support of IEEE 802.3az Energy Efficient Ethernet (EEE) standards is becoming more common on Ethernet PHY devices. During idle periods (i.e., when no traffic is sent) the PHY can transition into a low power sleep mode, which reduces power consumption by over 50 percent.

However, such approaches, in addition to full power down modes, still consume an order of mA of current, unsuitable for any battery or battery back-up application. The KSZ8061 Ethernet PHY bucks this trend and provides a



SOURCE: MICREL

Basic building blocks of the Ethernet PHY architecture and Fixed Latency PHY Layer technology.

boost in performance, and standby current of less than 1uA with the introduction of Ultra Deep Sleep.

In addition the KSZ8061 PHY exhibits a Signal Detect output pin, to signify the presence of an active link partner, as shown in the figure on the bottom of page 22 with the example of a sensor module. PHY standby (Ultra Deep Sleep) mode can be activated and woken up automatically by the signal detection circuitry. Furthermore this output signal can then be employed by the power management to power down the processor and sensors, providing remote sub 1uA standby and wakeup of any remote module.

Using a physical layer signal detect remote power down scheme offers key advantages over other proposed methods using special waveforms or pattern sequences:

Totally interoperable with any Ethernet vendor link partner PHY (at ECU). The use of special waveforms / sequences tends to require proprietary implementation, restricting the practical use. A good example of this in the consumer world is the vendor driven Wake-on-LAN (WoL) method, which in reality is rarely utilised the field.

Reduced standby power. Implementing a detection circuit at the physical layer requires less signal processing and thus, consumes less power. In the above example, WoL still requires the PHY and partial MAC layers to always be powered, resulting in a standby consumption in the order of thousand fold greater.

Real-time and deterministic

Ethernet PHY transceiver latencies must be considered very carefully when designing real time, deterministic control networks. Reduced latencies are desirable but more critical is fixed latency as variable delays cannot be compensated in a network, resulting in synchronization jitter.

The figure at the top of this page shows the basic blocks of the Ethernet PHY architecture. In the transmit direction, data is synchronised to the local 25MHz oscillator and typically provides a fixed delay t_{TX}. However, in the receive direction a variable delay is typically exhibited by the locking mechanism of the clock recovery circuitry. This variable delay is due to the alignment, in one of the 5 possible phases: 0ns, 8ns, 16ns, 24ns or 32ns of the generated 25MHz MII RXC clock, with respect to the recovered 125MHz Line Clock. As a result a shift in the receive direction delay occurs every time the link is re-established. This common effect has been recognised by Micrel and corrected with fixed phase recovered clock mechanism PHY technology.

Safety-critical and real time control applications are also benefited by the PHY's ability to power up and link in less than 20ms, without the need for processor intervention.

Reliability and fault tolerance

Current common Ethernet fault detection mechanisms, such as error detection, link down and cable open/short diagnostics provide network management with the ability to identify and locate major faults.

This methodology reduces downtime but does little to prevent the actual occurrence of network faults. Micrel's Signal Quality Indicator (SQI) addresses this limitation by providing a unique simple 4-bit reading to reflect the receiver signal margin or probability of error. The benefits are two-fold:

1. Determine infrastructure cable link quality at installation
2. Real-time Link Quality Monitoring: Identifying potential problems prior to errors. The latter ensures any potential link issue conditions can be detected and dealt with prior to any catastrophic fault, hence, avoiding network downtime.

Reliability is also boosted by Quiet-WIRE technology enhanced receiver immunity, facilitating error free traffic over low cost unshielded cables in the harshest environments.

***Mike Jones** is Micrel's Marketing Director – LAN Solutions.*

EMC regulations and integration with Industrial Ethernet

The complexity of electromagnetic interference can affect the total performance of a wide range of systems that utilize Industrial Ethernet. Both electromagnetic interference (EMI) and electromagnetic sensitivity (EMS) need to be effectively addressed, and there is a wide range of considerations in EMC system design.

A COMPLETE VIDEO SURVEILLANCE SYSTEM may require a tremendous amount of network devices, together with the complicated cabling networks that connect all the equipment. This may cause the complexity of electromagnetic interference and affect the total performance of the system. Therefore, electromagnetic compatibility of electronic equipment should not be negligible when the video surveillance system is applied to environments with high-voltage current such as power plants, factories, transportation and infrastructure projects.

EMC regulations and certifications apply to a wide range of markets.

EMC compatibility

EMC stands for electromagnetic compatibility. This means electromagnetic energy generated by the equipment is neither interfering with other equipment, nor accepting the electromagnetic energy interference of other systems.

EMC includes two aspects, the first of which is electromagnetic interference (EMI). This refers to equipment in normal operation or where the process or environment cannot exceed a certain levels of electromagnetic interference. A second area is electromagnetic sensitivity (EMS) which refers to equipment in environments where electromagnetic interference immunity is present.

Designing in compliance with high EMC standards is a key index of quality and performance of excellent networking product. But along with that, EMC design of the components and PCBs also needs to be taken into consideration. With substations for example, when the high-voltage convertor, circuit breaker and relays are operating, they will step up the voltage to several hundred thousand volts, which may generate huge electromagnetic interference to the equipment in the substation, and cause unpredictable damages.

Transportation systems such as train and subway are operated by electric power. The electromagnetic interference can be sorted by environments into outside the cabin, the electronic equipment in the cabin, the main transformer substation and the backup transformer substations along the rail and other electrical substations.

The main electrical system provides the power for the cars to operate on. The auxiliary power system processes the electrical power and distributes it to electronic equipment on the cars. Due to the fact that the onboard units on the trains have higher voltage inputs, besides resisting the EMI of other equipment it is also crucial to withstand the huge electromagnetic radiation generated by the train itself. When communication equipment is installed in such complicated environments, the testing of the electronic equipment will become more demanding.

Considerations in EMC design

Selection of components: In high EMI environments like a substation or railway system, heat and electromagnetic interference are two crucial factors that can cause failure of communication products. Excessive heat coming from the electronic components in enclosed environment will increase the temperature inside the cabinet. Electromagnetic interference can result in communication noise, or even signal loss.

EtherWAN selects parts including active and passive components (resistors and capacitors) with high MTBF and wide temperature endurance ranges to ensure products work normally in high temperature environment.

Professional Circuit Design: Aiming at special EMS environments such as power plants and railways, the design of the circuit and PCB boards focuses on resistance of surge current, which requires experience in designing safe spacing and circuits.

Standards: Test levels and strict manufacturing standards for industrial and commercial grade products is also an important consideration. EtherWAN insists that in the stage of design verification, regardless of commercial grade or industrial grade, all products will be tested in an environmental simulation laboratory for temperature and EMC performance. Before the shipment, the product will go through a long period burn-in testing to ensure products work in high work load environments.

Third Party Test Reports: products should pass and obtain multiple third party certifications according to different requirements in different markets:

- EN61000-6-2/EN61000-6-4: Immunity requirements for electrical and electronic apparatus used in industrial environments.
- EN55022/EN55024: European limits and methods of measurement of radio disturbance characteristics of information technology equipment.
- IEC61850-3/IEEE1613: For power substations.
- EN50121-4: Railway applications - Electromagnetic compatibility - Part 4: emission and immunity of the signaling and telecommunications apparatus.
- EN50155: Railway applications - Electronic equipment used on rolling stock.
- NEMA TS2: Environmental requirements for Trac control equipment.

Flexible Product Selection and Service: Ethernet switches can provide highly flexible port number combinations, according to different transmission speed and transmission interface to fulfill different requirements.

*Technology report by **EtherWAN**.*

Understanding the basics of functional safety systems

SafetyNET p is defined in the IEC standards for fieldbus systems as Type 22 and CP 18, and has emerged as a solution for Ethernet-based fieldbus communication. It enables horizontal and vertical integration, so automation and safety-related data is transmitted simultaneously in a single communication protocol.

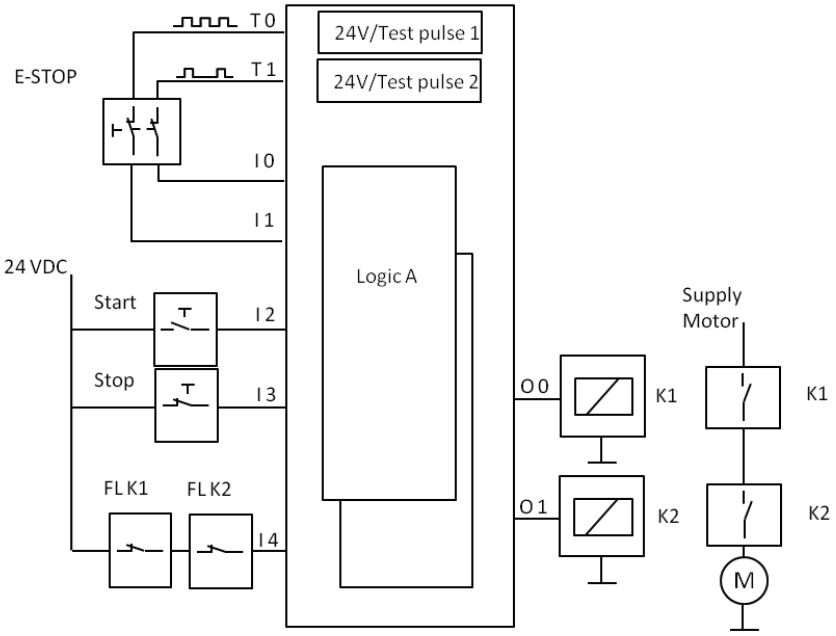
A PRIME OBJECTIVE OF FUNCTIONAL SAFETY is to protect people as much as possible from the hazards that can arise from a plant or machine during operation. This requires fixed safeguards such as fences or barriers, which make physical access to the plant or machine difficult.

Another possibility is to implement control technology solutions, which shut down one part or all parts of the machine or plant, should anyone approach a danger source, or use other means to bring the machine to a safe condition.

Connecting using parallel wiring

Generally speaking, safety relays perform pre-defined safety functions. They ensure that a movement is brought to a standstill in a controlled and therefore safe manner, for example.

Safe sensors such as emergency stop pushbuttons and contactors are connected in parallel. This means that each sensor and actuator is connected directly to the safety relay. Based on the hazards that can emanate from a plant or machine, the subsequent risk assessment and the resulting performance level, such systems usually have a dual channel structure.



SOURCE: SAFETY NETWORK INTL.

Fault-tolerant, dual-channel structure.

Potential data transfer faults

The figure on this page shows a fault-tolerant, dual-channel structure. In this case, a single fault will not lead to the loss of the safety function. In the event of a fault, the circuit will always shut down the motor. Let's take a closer look at the emergency stop pushbutton as a safety-related component and its connection to the safety relay. The emergency stop pushbutton is fitted with redundant contacts. If either of the two contacts should fail, a second is available to stop the motor if the pushbutton is operated. Emergency stop pushbuttons usually supply an unchanging signal over a long period of time. Any faults that occur in the pushbutton and connection cable may remain undetected and thereby lead to an accumulation of faults. To prevent this and to identify any shorts across the cable, the two contacts on the emergency stop pushbutton plus the cable are checked using two test pulses, which also have a different time characteristic.

On the output side, two independent outputs (O 0 and O 1) control two separate relays (K1 and K2). The motor can only run if both outputs and relays operate faultlessly, as the load contacts of both relays are connected in series. The feedback loops (FL 1 and FL 2) on the two positive-guided relays are also connected in series which ensures the motor cannot be started should either of the two load contacts stick. A sticking contact would also be a fault managed by the safety structure. In order to manage potential faults when processing safety-related signals, the logic in the safety relay also has a redundant structure.

Connecting safe sensors & actuators

Due to increasing demands on productivity and ever shorter cycle times, the demands on plant and machine control systems are also increasing. At the same time, the requirement for information regarding process and machine data is constantly growing. As a result, communication technologies from the office world are increasingly making their mark on plant and machinery. One consequence of this trend is the sharp increase in Ethernet-based networks such as SafetyNET p at field and process level.

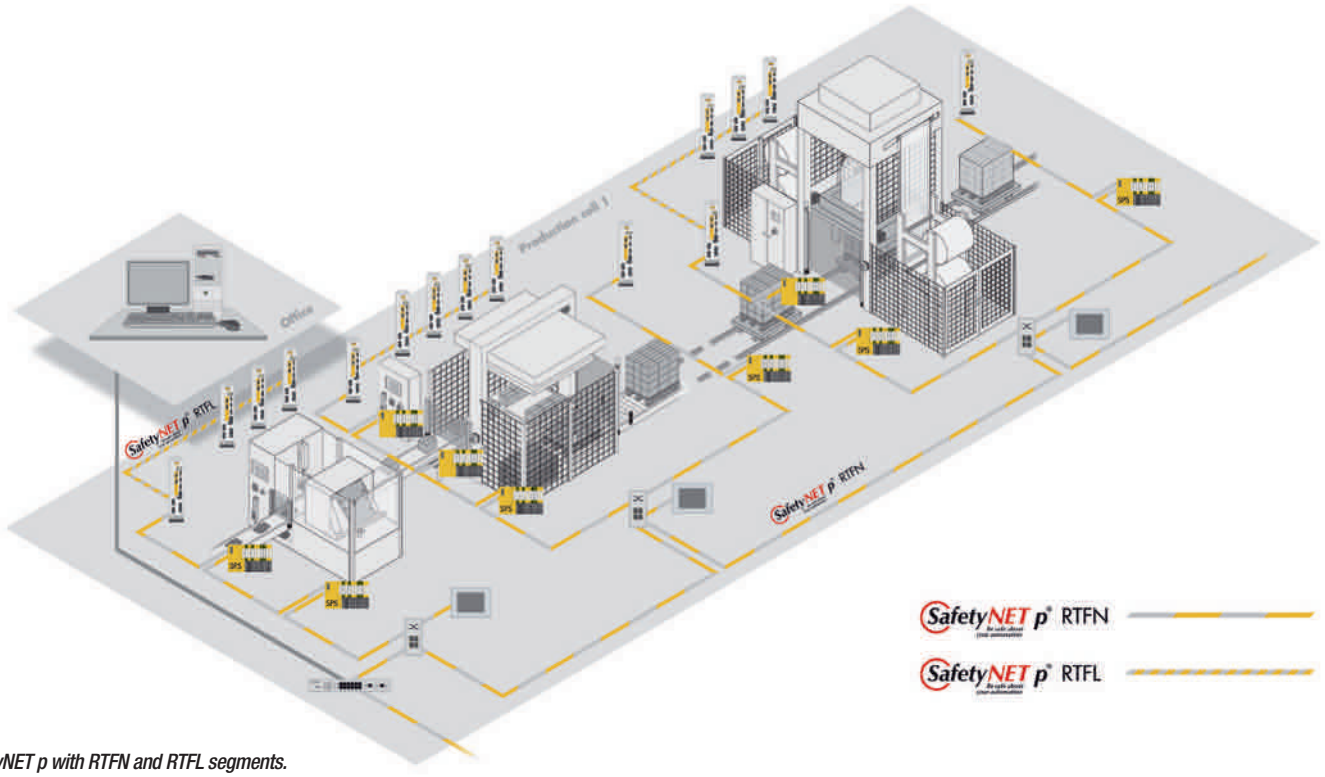
As is the case when connecting to safety relays, when functionally safe sensors such as emergency stop pushbuttons and contactors are connected directly to a safety control system, there is generally a dual channel structure. If such sensors or actuators are connected to decentralised I/O modules, which are connected to the safety control system via a network, data is transferred between the decentralised I/O modules and the safety control system in a serial, single channel structure. To detect any potential data transfer faults, additional measures must be implemented within the communication protocol.

Potential network transfer faults

Potential faults that can arise when communicating safety-related data via a network are:

- Message repetition
- Message loss
- Message insertion
- Incorrect message sequence
- Message corruption
- Message delay
- Combination of safety-related and non-safety-related messages

This overview alone illustrates that there is clearly more to consider when safety-related data is transferred via a network then when an emergency stop pushbutton is connected directly to a safety relay.



SOURCE: SAFETY NETWORK INTL

SafetyNET p with RTFN and RTFL segments.

Managing communication errors

From the very start, SafetyNET p was designed and developed as a network for the simultaneous transfer of safety-related and non-safety-related data. In the process, particular attention was naturally paid to detecting and managing potential faults during the serial transfer of messages.

Message repetition

Malfunctions within a network subscriber could lead to telegram repetition. Each message in a SafetyNET p system is given a sequential number so that repeated messages are detected. The receiver is "expecting" the sequential number, so it will detect repeated telegrams and initiate appropriate measures.

Message loss

Messages may be lost due to the communication channel being interrupted or due to a malfunction on a network subscriber. The receiver in a SafetyNET p network also uses a sequential number to detect the loss of data packets. A timeout on the receiver also monitors the latest time by which a new message must arrive. Once this timeout has elapsed, the receiver is able to bring the application to a safe condition.

Message insertion

Additional messages could creep in as the result of a malfunction on a network subscriber. As with message repetition, the sequential number in SafetyNET p telegrams can be used to detect this situation and manage it accordingly.

Incorrect message sequence

Network components that store telegrams, such as Ethernet Switches, or faults in a network subscriber can corrupt the telegram sequence. This will also be detected on the receiver side in a SafetyNET p device based on the sequential numbers.

Message corruption

Interference on the communication path, due to electromagnetic radiation (EMC) or the malfunction of a network subscriber for example, can corrupt messages. A data security mechanism (check sum) applied to the safety-related telegram on SafetyNET p detects corrupted messages by comparing the supplied check sum with the self-calculated check sum in the receiver. If the check sums do not match, the receiver is able to bring the application to a safe condition.

Message delay

An incalculable data volume in the network or a malfunction on the network subscriber can lead to a delay in the transfer of messages. A timeout on a SafetyNET p receiver will detect the delays and initiate appropriate measures.

Safety/non-safety-related messages

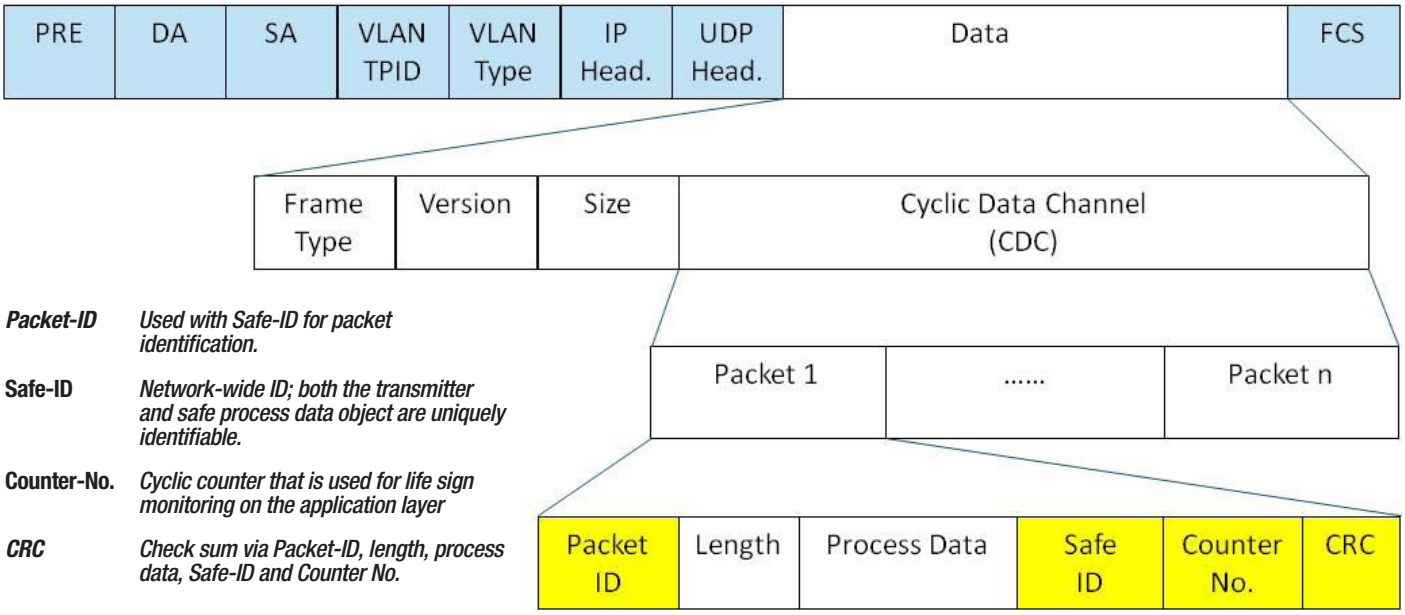
In mixed systems containing safety-related and non-safety-related subscribers, receivers will sometimes interpret a telegram from a standard subscriber as a safety-related telegram. Such mistakes on the part of the receiver can be avoided on SafetyNET p using measures such as unique IDs across the network and varied data security features for safety-related and non-safety-related messages.

SafetyNET p system description

SafetyNET p is a multi-master system. This means that all devices in the network have equal rights. The protocol contains a safe data channel, which is certified for data transfer in accordance with SIL 3 (IEC 61508). Both safety-related and non-safety-related data are transferred via an Ethernet cable. Non-safety-related subscribers can access safety-related data directly and can use this data for further non-safety-related processing tasks. The bus cycle time can be adjusted to suit the application's requirements. SafetyNET p is flexible, not just when it comes to selecting a suitable bus cycle, but also with regard to appropriate topology: SafetyNET p supports linear, star, tree and ring topologies.

On SafetyNET p, a distinction is made between communication within a cell and at higher levels. The RTFL communication principle (Real Time Frame Line) is suitable for intra-cell communication, as it allows the fastest cycle times. At higher levels, where the real-time requirements are lower, the RTFN communication principle (Real Time Frame Network) is generally used.

SOURCE: SAFETY NETWORK INTL.



Ethernet telegram with safe SafetyNET p – process data in an RTFN segment.

With RTFL, the devices are typically networked in a linear structure, in which all SafetyNET p subscribers have equal rights. Data is exchanged in accordance with the producer/consumer principle. As producer, each device can supply data to the other devices. The other subscribers (consumers) can read the published data from individual subscribers or all subscribers. This way it is possible to exchange data efficiently between all the subscribers.

The communication mechanism used by RTFL is a very fast cyclic data transfer in one or more Ethernet frames per cycle. Communication is initiated by a "root device" (RD). The Ethernet frame generated within the root device is transferred to the other devices, which successively fill the Ethernet frame with the data to be published and extract from the Ethernet frame the data to be read. Devices in an RFFL segment are addressed via their MAC address. RTFN is used to network the RTFL real-time cells and to connect Ethernet subscribers, such as visualisation devices or service PCs to a SafetyNET p network. The RTFN level typically has a tree topology, as used in office communication. Ethernet switches are used to connect the network subscribers via individual point-to-point connections. Alternatively, subscribers can be addressed via their MAC or IP address. If IP-based communication is used, RTFN frames can be routed from one network to another.

During communication via the network SafetyNET p also distinguishes between cyclic and acyclic data, because the communication requirements change based on the operating status of the network or individual devices. Phases for device programming, diagnostics and parameter settings are mainly phases in which the data transfer is not time-critical. The corresponding data packets are generally larger than during actual operation. When necessary, acyclic, non-time-critical data is transmitted via the message channel (MSC). In contrast, safety-related and non-safety-related process data is transmitted via the cyclic data channel (CDC).

The SafetyNET p application layer superimposed over RFTL/RTFN is largely based on the CANopen standard. Adjustments to CANopen have been made in the communication area and in the way safe application data is handled. A key element is the object directory, which acts as the interface between the device function (application) and the communication channel. Essentially it is a grouping of objects and functions, which the application can store and call up as application objects. SafetyNET p telegram in diagram above contains safe process data and is transmitted in an RTFN network segment. It also shows elements in the telegram that are used to detect and manage potential data transmission faults in a SafetyNET p network.

The real-time Ethernet SafetyNET p is designed for complete automation. With the open system, time-critical safety-related data and standard control data can be physically mixed but at the same time logically separate, so it is free from feedback.

Harald Wessels *is a technical spokesman for Safety Network International e.V.*

Implementing intelligent CNC machine tools with EtherCAT

Shenyang Machine Tool, the largest manufacturer of machine tools in China, is utilizing EtherCAT as its bus system for the control platform of its latest intelligent CNC machine tool, the i5. EtherCAT was implemented not only for the master controller, but also on the slave side in all servo drives and I/O devices.

SOURCE: ETG

THE SHANGHAI RESEARCH INSTITUTE, a subsidiary of Shenyang Machine Tool, has been engaged with innovative development in the fields of motion control and cloud-based manufacturing concepts since 2007. The Institute concentrates on the special motion and controller technologies of machine tools, product development, as well as the technical basis for cloud-based manufacturing technology, that offer concrete benefits and innovative capacity for machine tool customers and their respective industries.

The Shanghai Research Institute has developed a number of products especially for those business areas covered by machine tools such as CNC systems, servo drives and WIS (Workshop Information Systems).

The i5 intelligent CNC machine leverages EtherCAT for communication, and was publicly debuted in 2014 at the China CNC Machine Tools Fair (CCMT). The i5 machine boasts a variety of intelligent functions such as graphical diagnostics, real-time monitoring, remote diagnostics, 3D simulation and STEP programming. Due to the possibility of individualized solutions, it is the perfect fit for the demands of today's market.

The i5 name encompasses the five following features and terms that are embodied by the machine (all beginning with the letter I): industry, information, Internet, integrated management, and intelligence.

i5 control platform

The i5 control platform consists of three component types: NC controller, HSHA series servo drives, as well as I/O devices developed by the research institute itself. PC-based control technology including the open, real-time industrial Ethernet protocol, EtherCAT forms the foundation for the i5 control platform.

EtherCAT enabled Shenyang Machine Tool to create a CNC system with external servo drives which can also exchange data between I/O and control subsystems – at high-speed and in real-time. This offers all users of this CNC machine tool a high performing control solution at a reasonable price through the use of cost-effective industrial Ethernet technologies.

Why EtherCAT?

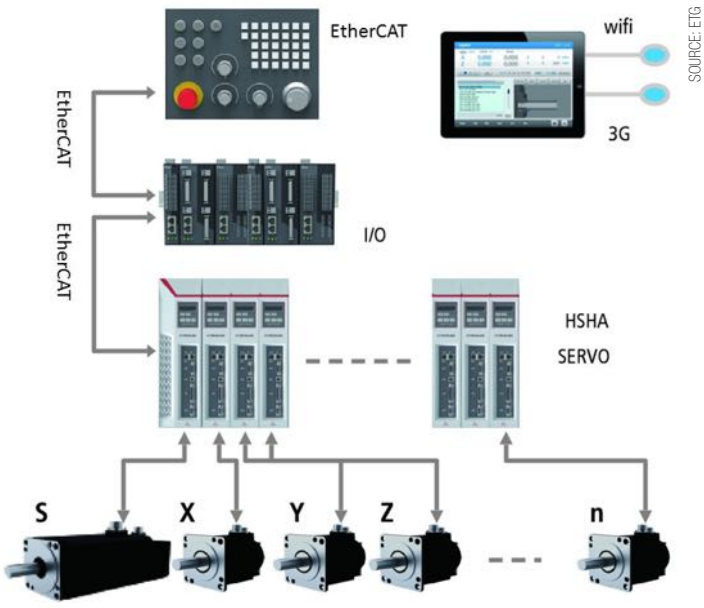
Prior to the implementation of the device functionalities, the Institute carried out an evaluation regarding the selection of a suitable bus system at the beginning of the i5 development process. The company decided on EtherCAT because, outside of performance, the i5 platform implements cloud connectivity via Ethernet. For consistency, it was determined that the control bus system should be Ethernet-based, so that Internet technologies could be integrated into the overall system seamlessly and made available at a reasonable price. In addition, the connection of a wide range of different devices is simplified.

The core technology of the i5 is the NC algorithm. Due to the necessary precision of the high-end drive technology, the requirements for the bus system are very demanding. Besides ultra-short communication cycles, highly precise synchronization is crucial. Additionally, achieving the smallest possible communication "dead time" regarding synchronization was very important for Shenyang Machine Tool, as the process data communication of machine tools requires a low deceleration to eliminate possible negative effects on NC characteristics by the bus performance.

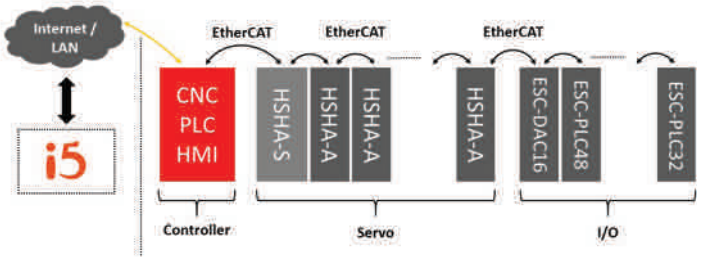
In addition to the high communication speed EtherCAT achieves with its "processing on-the-fly" principle, the mechanism of Distributed Clocks (DC) in EtherCAT enables the synchronization of all slaves with a jitter of just 50ns. As a result, EtherCAT enables the consistent movement of the feed axes during multi-axis contouring control which reduces contouring errors dramatically. The simultaneous nature found in setting the outputs, as guaranteed by the EtherCAT Slave Controllers, simplifies circuit design and the programming efforts for the real-time slave, leading to faster development and a shorter time to market.

EtherCAT's mailbox protocol accelerated the development process,

SOURCE: ETG



System architecture of the i5 control platform.



The CNC system of the i5 in detail.

SOURCE: ETG

particularly for complex applications and connections. Algorithms and parameters for function expansions, as well as firmware changes, could be integrated in the drives even during application development. IT applications can be tunneled through the mailbox via standard Internet technologies, simplifying integration of management software.

Similar to other modern industries, manufacturers of CNC systems strive to offer higher performance machine functionality, while saving development and production costs. EtherCAT does not need any switches, routers, or other active infrastructure components, and requires little in the way of complex IT knowledge. No special, cost-intensive communication card is necessary for the CNC system, and a standard Ethernet port is sufficient for data communication.

The slave devices only require cost-effective ESCs (EtherCAT Slave Controllers) that can be integrated as an ASIC or IP core for FPGAs. The Shenyang Machine Tool i5 uses ASIC chips from Beckhoff Automation for its servo drives and FPGA IP cores for its I/O panels to reduce costs effectively while simplifying the development process. With the decision to use EtherCAT, Shenyang Machine Tool did not need to invest in additional hardware and the performance of the i5 was enhanced enormously.

Especially in the field of complex CNC applications, user requirements for devices are very demanding. In these applications, high availability, high precision, flexibility in programming, high efficiency, and reliability are all very important. With EtherCAT, those requirements can be met right down the line. Using EtherCAT instead of traditional analog data lines eliminates problems with electromagnetic interference and signal attenuation, significantly enhancing the reliability of the CNC system.

HSHA series servo drives – EtherCAT slave.

SOURCE: ETG

Due to the environmental challenges in China, users require a high tolerance in their plants regarding temperature and humidity, especially in summer. EtherCAT removes the need for additional protection from electromagnetic influences in production facilities.

Conclusion

After viewing the benefits of EtherCAT, Shenyang Machine Tool decided to implement EtherCAT-enabled PC-based control in its i5 intelligent machine tool. The system has saved time by increasing performance. The interpolation cycle has been reduced from 4ms down to 0.5ms, increasing speed as well as the precision of the CNC system. The fast communication system reduces the response time of the PLC within the CNC system to one-tenth of the original time. This enhances the responsiveness of external devices and reduces processing time.

Production time and costs are also reduced. In a traditional analog control methodology, each servo drive has to transmit an analog control signal to the CNC system and react to encoder signals. This requires the installation of a bus terminal, as well as a special cable for each drive in the CNC system. Since those cables are non-standard, manufacturers incurred significant costs for material, installation and troubleshooting. In contrast, EtherCAT enables the use of standard Ethernet cables in all areas, which greatly reduces production time and costs.

CNC panel of the i5 – EtherCAT master.

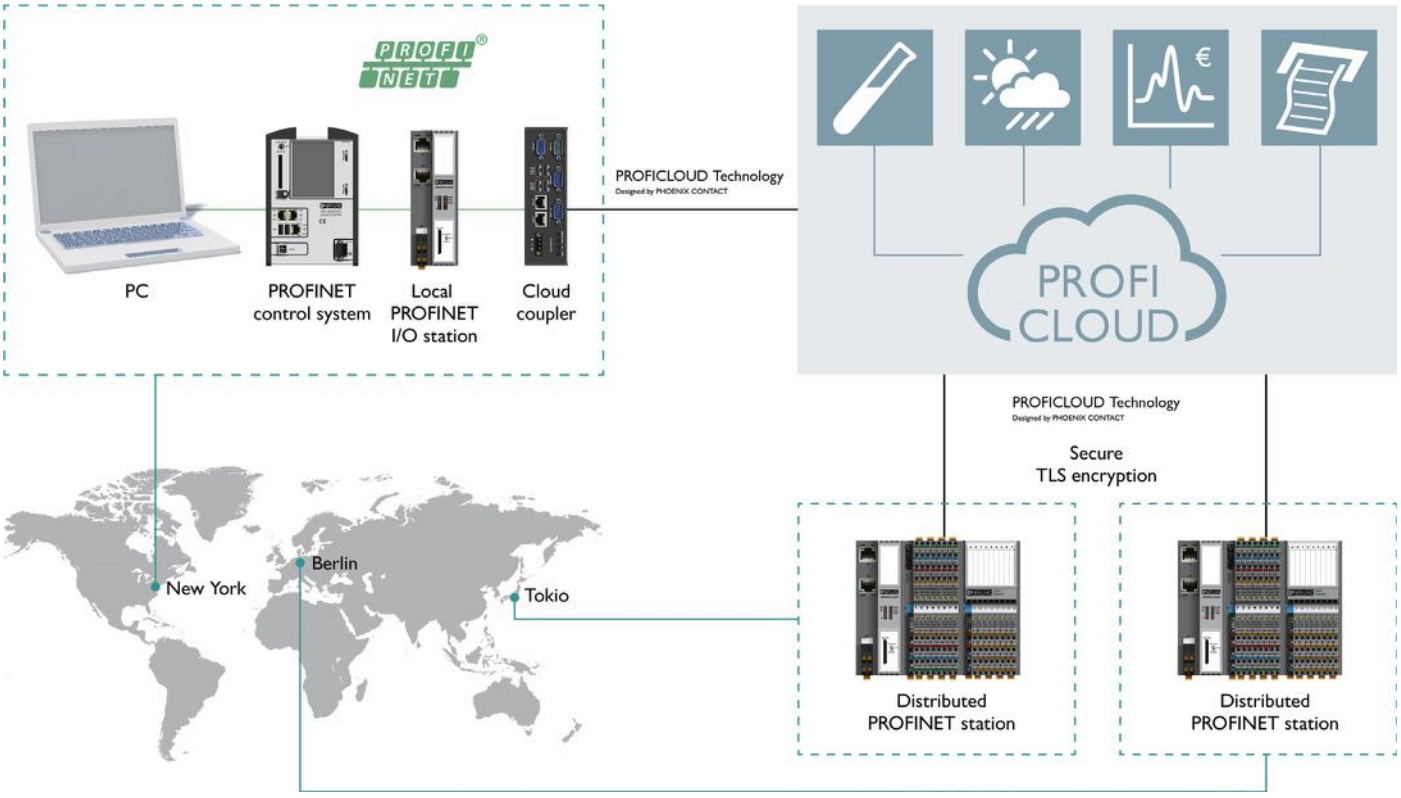
SOURCE: ETG

EtherCAT enables a flexible and appropriate network. In one network, up to 65,535 EtherCAT devices can be connected without any topological restrictions. Servo drives, I/O, operation panels, encoders and various sensors required for Shenyang Machine Tool's i5 CNC system are easily integrated into the machine control. Slave devices do not need an address switch for address configuration, and protocol diagnostics can locate erroneous devices and signals with high speed and precise localization.

Beryl Fan *is Manager of the EtherCAT Technology Group Office in China.*

Taking Profinet networks into the cloud

Proficloud technology makes it possible to add cloud functions to existing Profinet networks. Based on Profinet technology that is already in place, it allows users to draw on value-added cloud services without the need for difficult configurations, along with an ability to easily implement telecontrol applications.



SOURCE: PHOENIX CONTACT

Overview of the Proficloud technology.

A PROFICLOUD APPLICATION always consists of at least one cloud coupler and one cloud device. The coupler connects the local Profinet network with the cloud via two Ethernet interfaces. While one of the interfaces is used for linking to the local Profinet system, connection to the Internet is established via the second interface. Subsequently, the coupler automatically initiates a connection with the Proficloud and is ready for operation after a short period of time.

The same applies to Proficloud devices, which are also easily linked to the Internet and automatically connect to the Proficloud. All that is left for users to do before the system is ready for operation is to assign the devices to the respective coupler within the Proficloud .

VPN configuration difficulties

When a programmer views the local Profinet network where the coupler is located, the distributed Proficloud devices are displayed as local Profinet devices. The following simple telecontrol engineering example serves to explain the operating principle. The sample application includes a central control, which automates a waterworks that implements the local fieldbus system using Profinet. The waterworks includes two remotely installed pump stations, which can only be reached via public networks, such as the Internet, due to their geographical location and associated cost considerations.

VPN (Virtual Private Network) technology is frequently used in modern telecontrol solutions. The application engineer must first set up a VPN network and, for this purpose, create a certificate which ensures that transferred data is encrypted. In addition, there must be at least one VPN server in the application that can be contacted via a static IP address. This requirement can be implemented via DynDNS (Dynamic Domain Name System) services, which, however, still need to be configured.

The programmer must also set up the firewall such that the port necessary for the VPN server is communicated to the server. In addition, he must make sure that all devices are located in the same subnet so that communication can take place on the basis of TCP/IP. The final task is to configure a protocol for the connected devices. Modbus TCP or the IEC standard 60870-5-104 are usually used in telecontrol systems. Once these steps are completed, individual stations can finally exchange process data with each other.

Reduced hardware costs

In comparison to the procedure described above, the design of a Proficloud solution provides the same functionality but is very simple to implement. First, the programmer registers with the Proficloud by entering the ID delivered with each Proficloud-enabled device to personalize the corresponding device.

This applies both to couplers and other devices. Next, the programmer assigns the respective devices to each coupler via drag & drop. The devices are then linked to the

industrial ethernet book

Reader Service Card

IEB issue 86 - February 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

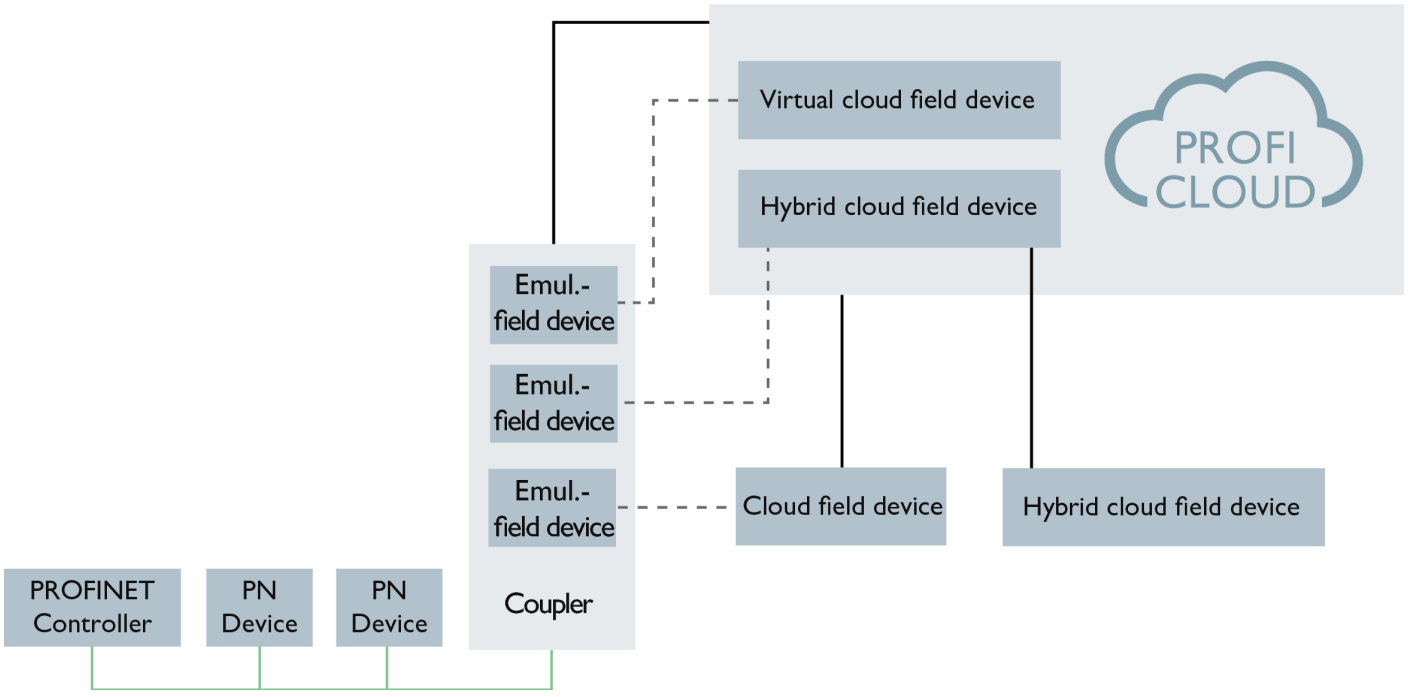
☐ Manager - Technical

☐ Manager - Commercial or Financial

☐ Manager - Plant & Process/Quality

☐ Scientific/Education/Market research

☐ Other: _____



SOURCE: PHOENIX CONTACT

Proficloud technology works with three different types of devices.

Internet on site. They obtain their network data automatically via DHCP (Dynamic Host Configuration Protocol) and integrate independently into the Proficloud solution where they initiate data exchange. No other settings are necessary in addition to the configuration within the Proficloud.

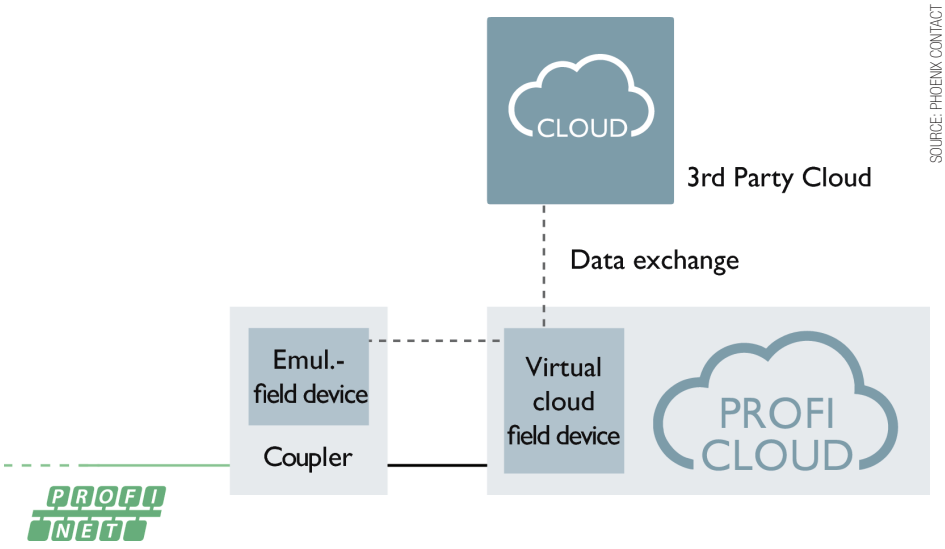
Finally, the programmer only needs to link the coupler with the local Profinet system and the Internet connection. Now the distributed devices can be added to the Profinet configuration in the familiar engineering environment. All distributed devices that have been assigned to the coupler via the Proficloud appear in the local Profinet system as if they were directly linked there. This allows the programmer to concentrate on processing the Profinet data without having to deal with the difficult configuration of VPN and telecontrol protocols. An additional advantage is the significant reduction of hardware costs, because no additional VPN clients or servers are needed in the distributed stations.

Integrate any Profinet network

Ease of use was the main priority when developing the Proficloud solution. For this reason, devices are delivered in a preconfigured state, which means they automatically connect with the cloud endpoint, which is also preset.

The coupler receives its configuration data after connecting with Proficloud. The data describes all devices that are connected to the coupler or linked logically with it in the cloud. Afterwards, the coupler starts to emulate local Profinet IO devices, so that components are represented externally exactly like normal Profinet devices. Because of this procedure, the Proficloud solution can be integrated into any existing Profinet network irrespective of the manufacturer.

Data is transmitted via TLS (Transport Layer Security) encoding, a procedure also used, for example, in online banking solutions. WebSockets, which are often used in current web applications, act as data transfer points. Given that the WebSockets are based on standardized web mechanisms and use corresponding web ports (port 443, port 80), they are firewall friendly due to the fact that ports 80 and/or 443 are open to the TSL protocol in the case of most firewalls, as it is needed for normal surfing on the Internet. As a result, the Proficloud solution avoids difficult firewall configurations.



SOURCE: PHOENIX CONTACT

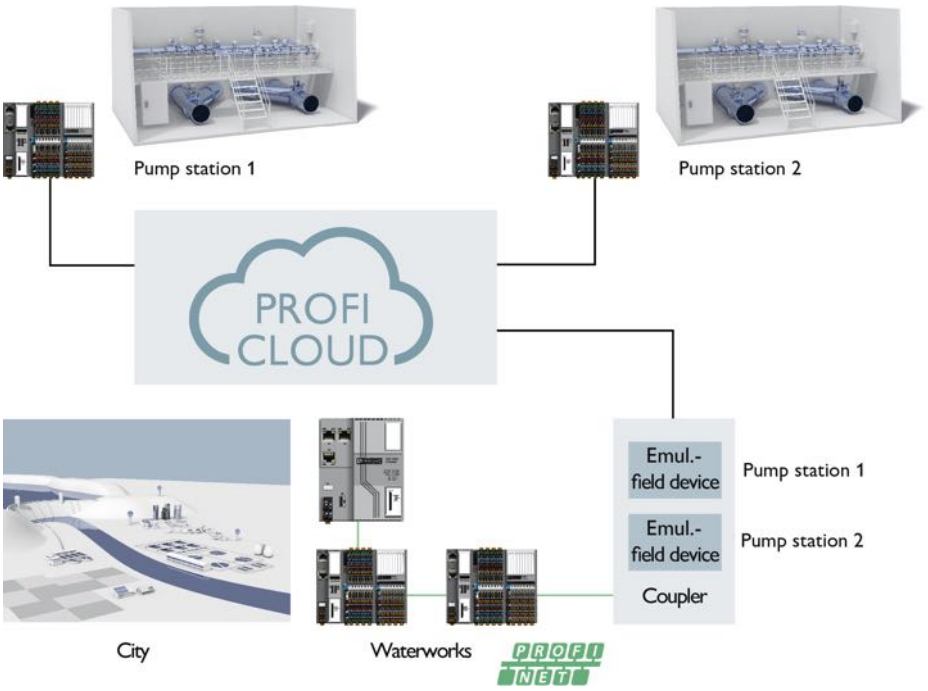
Possible expansions of the Proficloud solution.

Comprehensive access security

In order to further increase access security, Proficloud devices exclusively use an outbound connection. This means that a connection from the Internet to the local network can never be established. In addition, Proficloud components do not have open ports and thus cannot be reached from the outside.

This means that potential attackers are denied a basis for unauthorized access. An additional security aspect concerns the coupler, which appears to connect the production network with the Internet. However, this is actually not the case.

Instead, the coupler contains two separate network cards. One card is for the local production network, the other for connecting to the Internet. Both cards are not linked via TCP/IP, so that communication takes place exclusively in the application layer and is limited to exchange of Profinet-relevant data.



SOURCE: PHOENIX CONTACT

Explanation of the Proficloud technology's operating principle based on the example of a waterworks.

Smart forecasting

There are three different types of Proficloud devices. Standard devices as exist in a normal Profinet environment include distributed I/O devices or control systems that serve as devices. They are mainly used in the previously mentioned telecontrol applications.

So-called virtual devices represent a new type of device. With their help, the advantages of the Proficloud can be harnessed within the Profinet network. Virtual devices have no physical counterpart – they only exist within the cloud, where they function exactly like a real IO device. Unlike real devices, however, their IO data does not originate from sensors and control actuators; instead, it represents information from the Proficloud.

Given this system design, it is possible, for example, to obtain weather information from the Internet and make it available to the control system via the virtual device. Such a device could, for instance, have latitude and longitude as input data and return to the control system the current temperature, air pressure, and chance of rain or weather forecast – thus making it possible to feed information into the system that may not be offered by the local weather station. Such a function can generate added value in wind and solar farms, because it allows for precise yield forecasts, among other things.

Computationally intensive tasks

The third type of device is a mix of standard and virtual device. It is called a hybrid device as it connects the virtual world of the cloud with the physical world of the production network. The hybrid device, which receives input from real sensors and actuators, is additionally supported by cloud applications.

This allows for preprocessing sensor data within the cloud, which is then transmitted in processed form to the local Profinet system. Computationally intensive tasks, which would require a lot of time in the control system or the local IO device, can thus be executed in a short period of time inside the cloud. Operators can thus save hardware costs in the field and are able to perform complex calculations that were previously not feasible at all.

As another example, consider a complex controller based on complex algorithms. Of course, users must account for Internet-related delays in the calculation. However, with a good Internet connection, these delays are significantly below one second.

Broad range of applications

The Proficloud solution also provides multiple advantages in the context of Industry 4.0 by providing a technology for comprehensive networking. With the help of virtual devices, almost any information delivered by the cloud can be broken down to the Profinet protocol and thus made available to the lowest level in the automation hierarchy. In this way, ERP order data can be transferred from the ERP system directly to the shop floor without the need to prepare it in an intermediate IT system.

Given that fieldbus data can also be used and processed in the Proficloud via virtual devices, this opens up various new fields of application. Examples include alerting maintenance personnel via the cloud or gathering usage statistics for mechanical engineering companies. With the help of virtual devices, users can also control and supply data to additional cloud services or provide them in the Profinet system, as shown in the weather information sample application above. The visualization of data on a web portal or a smart phone app – or any other form of data processing – is also possible.

The current Big Data hype can also be addressed with the Proficloud. For instance, manufacturers can monitor the state of all their systems installed across the world. The evaluation of the obtained data provides early indications of possible failures (predictive maintenance). In addition, maintenance intervals can be executed according to need, which decreases costs for the end user. Missing information is frequently the root cause of imperfect product lifecycle management. The new Proficloud solution and the corresponding cloud applications allow for precise documentation and therefore an optimized development of new systems and components.

Given that Proficloud uses established standards such as Profinet, users can easily integrate the solution into their existing systems. A complex configuration of IT systems or VPN components is not necessary. With this new technology, it is extremely easy and secure for users to adopt the cloud, opening up the door to new technological approaches and forward-looking projects.

***Mathias Weßelmann**, Research & Development, Business Unit Control Systems, Phoenix Contact.*

SOURCE: PHOENIX CONTACT

Engineering design of the Proficloud solution.

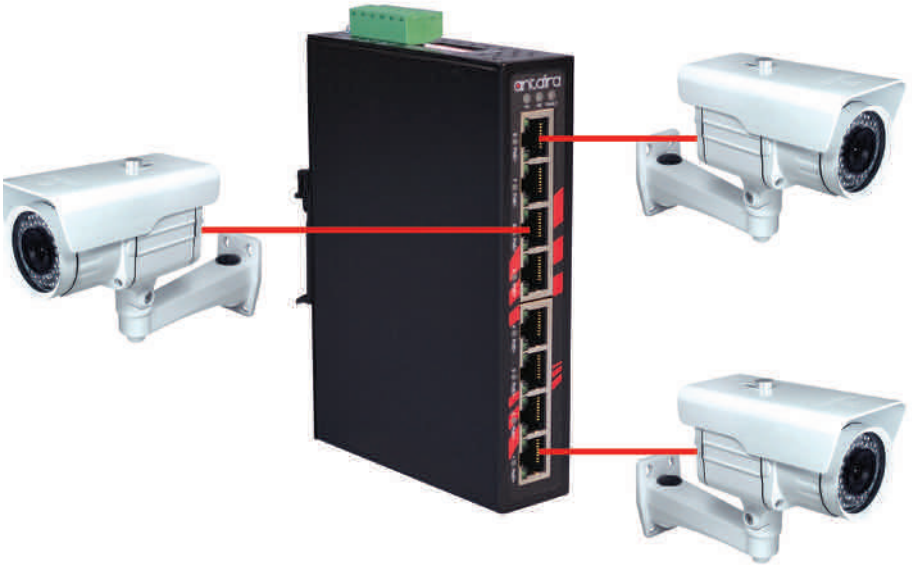
Advantages of PoE in industrial networking applications

Power over Ethernet (PoE) is a technology that takes advantage of high-speed networking to integrate cameras and other industrial devices. The ability to power devices often simplifies network installations and cabling. This report takes a look at the differences in PoE standards and advanced management features.

POWER OVER ETHERNET (PoE) has become a hot term that is frequently referenced but not completely understood. There are a lot of different acronyms and subtle differences used in the PoE arena that can quickly confuse and frustrate even advanced users.

Let's go over some of the more common differences such as multiple standards, varying power outputs and standard Ethernet restrictions as well as some more advanced management features available with respect to PoE.

Despite all of the naming rules and subtle confusion, PoE has been widely adopted in applications due to the challenges it has overcome and simplicity it has provided. PoE in its basic function is quite simple, plug in an Ethernet cord and it can receive both communication as well as power to the PoE capable device.



SOURCE: ANTAIRA

A key benefit of Power over Ethernet (PoE) technology can be traced back to the reduction in both the equipment needed and wired connections to the devices.

Power over Ethernet technology

A new technology, now referred to as PoE, was first developed in the year 2000 by Cisco to reduce noise issues in the emerging VoIP phone system. Power over Ethernet quickly took off; by the year 2003 the first PoE standardization was developed to create uniformity amongst all of the PoE device manufacturers.

PoE is beneficial over standard Ethernet network communication because of the reduction in both the equipment needed and wired connections to the devices. Why run both an Ethernet wire and a power cord to a unit when one Ethernet wire can work?

PoE Naming Rule

To start off, PoE is used as an all-encompassing term for all devices within the PoE market. When in actuality PoE can be split into two broad categories. The main unit is the Power Sourcing Equipment (PSE), This is the device that injects the power into and along the Ethernet cord.

The PSE is typically a switch or power injector. The other units are end devices and are classified as the Powered Device (PD); these are the units that require power through the Ethernet cable to turn on. A good example would be an IP camera, VoIP phone or a variety of outdoor industrial wireless access points.

Standardization

When looking to get either a PSE or a PD there are a couple important pieces of information to consider. First, there are two different standards of how the power is sent along the Ethernet wire. PoE mode A, which seems to include the majority of PoE devices, uses pins 1, 2, 3 and 6 to send power along the Ethernet cable. Whereas, mode B devices will use pins 4, 5, 7 and 8 for power transmission. Second, how much power is required? PoE PSE sourcing units have multiple different power output levels; mainly standard power and high power or what is referred to as PoE+ are used.

SOURCE: ANTAIRA

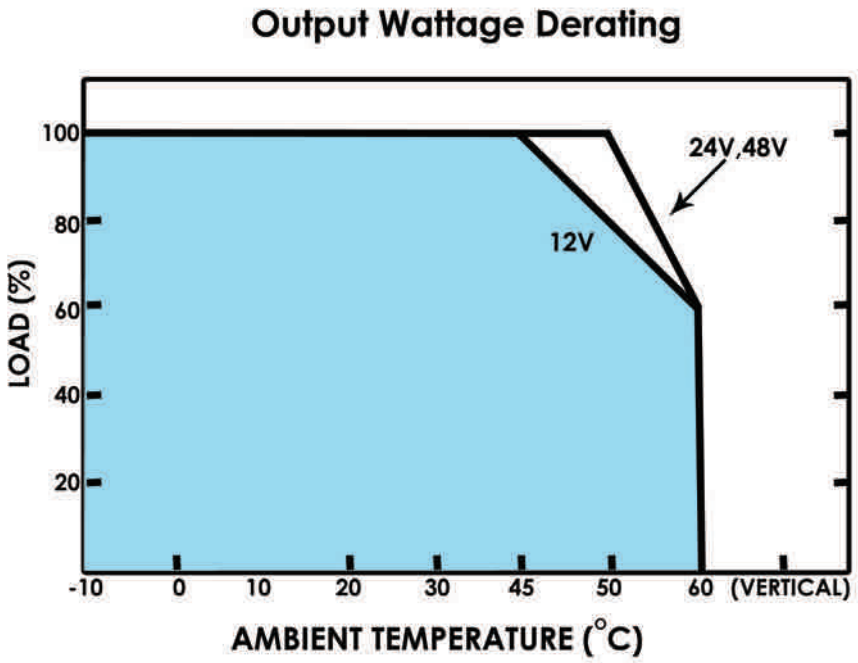
Cameras are an example of "powered devices" (PD) that required power through the Ethernet cable to turn on.

The Institute of Electrical and Electronics Engineers (IEEE) has two different official categories for the different power outputs of a PSE device. The IEEE 802.3af standard states that devices will not output more than 15.4 Watts of power out of each port. The PoE+ or IEEE 802.3at standard allows each port to provide an output power of up to 30 Watts per port.

Typically, if a manufacturer's PoE PSE switch supports IEEE 802.3at high power devices capable of up to 30 watts of power, the switch will also do power auto negotiation. This means that the high power PSE will detect how much power is required by the PD to operate and not provide excess power to a device that only requires 15 Watts or less.

Applications

A great benefit and use of PoE units is when a power source is not available at the end location, such as the side or top of a building for a security camera or Wi-Fi access point. Another benefit of implementing PoE is when installing multiple devices at a location, such as surveillance cameras, a PoE switch and all of the cameras can all use a single



SOURCE: ANTAIRA

An example of an output derating curve shows that, at the extreme end, the total power supplied by a power supply can be reduced by as much as 60% depending on the environment.

power supply. This can reduce the installation cost because there will be a reduction in the amount of equipment as well as a reduction in the amount of power cables needed to be installed.

One thing to remember is that it is the responsibility of the user to keep in mind the power budget for the power supply that will be used. For example, if the application requires connecting three IEEE 802.3af cameras (15 Watts per camera) to a PSE switch, the output wattage of the power supply will need to be able to supply 45 Watts of power for the cameras plus the additional wattage required to power the switch.

Environment

There is a wide variety of products to choose from when preparing for a project. An additional consideration needs to be made regarding the temperature of the environment the application will be used. In extreme environment conditions, industrial grade equipment is essential and extended temperature range equipment can prove beneficial.

This is especially true when selecting PSE switches or a power supply. Proper selection of industrial grade equipment is particularly important when using PSE units for PoE applications. A PSE unit will receive additional thermal activity over non PSE devices, because it will be generating additional heat through the power it is generating and providing to the PDs that are connected to it.

Additionally, power supplies have an optimal operating temperature range. In hot environments the power supply will be affected by an operational output derating curve, where the total output wattage of the unit will be reduced by a percentage depending on the ambient temperature of the environment. The ambient temperature can have a significant effect on the power budget that is being calculated for a specific application.

An example of an output derating curve is displayed in the power diagram (left) which shows that at the extreme end the total power supplied by a power supply can be reduced by as much as 60% depending on the environment. Due to the drop off in available power in hot environments, a higher wattage unit might be required to provide adequate power.

Managed switches

Managed switches are capable of providing users with a multitude of advanced features that can improve the management capabilities, performance, security and resilience of a network.

The capabilities that a managed switch provides have been proven time and time again why the managed switch is the workhorse of the network. All the standard features a managed switch can provide end users with to enhance network performance are still relevant when using and implementing PoE devices. In fact, PoE switches with management capabilities provide even more function features that can be critical in optimizing network performance.

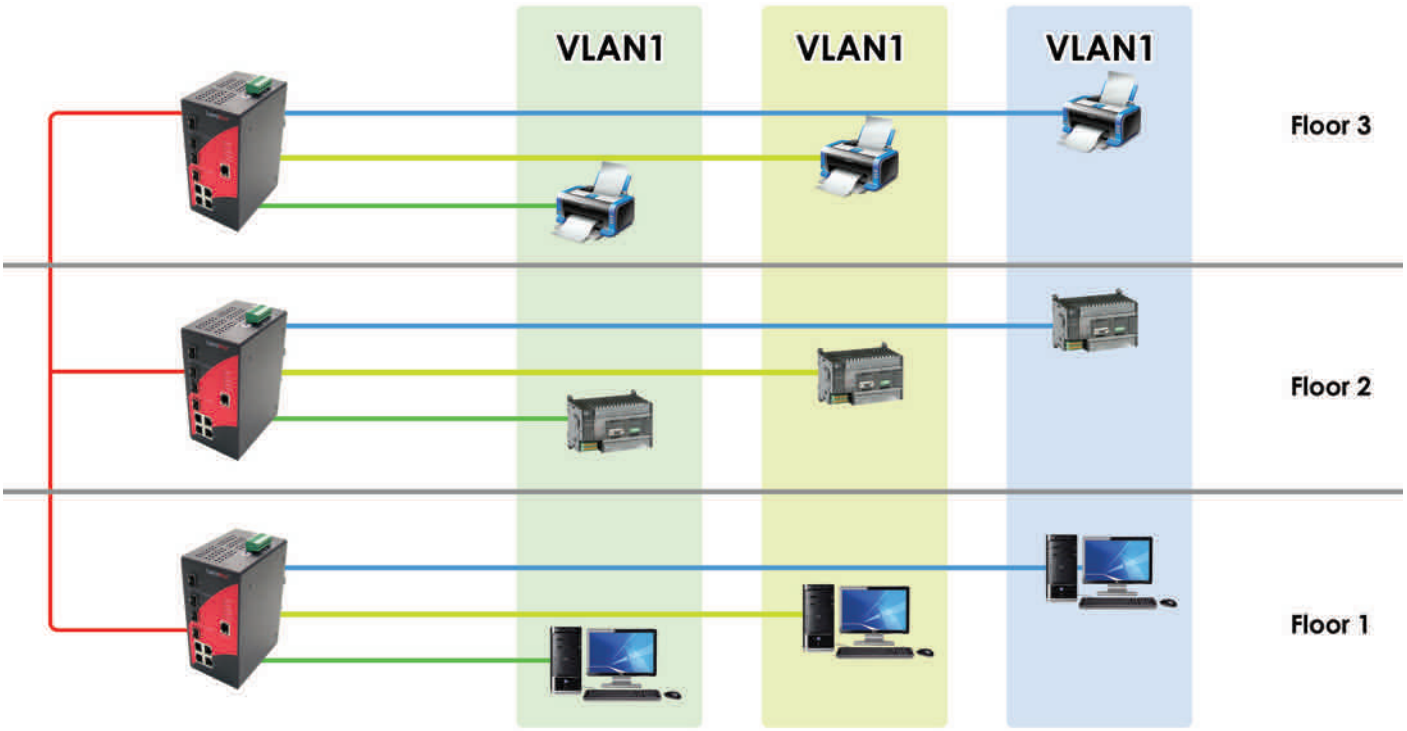
Management features such as Internet Group Management Protocol (IGMP) are very

No.	Time	Source	Destination
8554	16.218813	192.168.1.112	239.192.0.20
8555	16.219330	192.168.1.112	239.192.0.20
8556	16.219889	192.168.1.112	239.192.0.20
8557	16.220067	192.168.1.112	239.192.0.20
8558	16.244815	192.168.1.112	239.192.0.20
8559	16.245078	192.168.1.112	239.192.0.20
8560	16.245335	192.168.1.112	239.192.0.20
8561	16.246131	192.168.1.111	239.192.1.111
8562	16.246256	192.168.1.112	239.192.0.20
8563	16.246826	192.168.1.112	239.192.0.20
8564	16.247291	192.168.1.112	239.192.0.20
8565	16.247921	192.168.1.112	239.192.0.20
8566	16.248390	192.168.1.112	239.192.0.20
8567	16.248980	192.168.1.112	239.192.0.20
8568	16.249474	192.168.1.112	239.192.0.20
8569	16.249993	192.168.1.112	239.192.0.20
8570	16.250505	192.168.1.112	239.192.0.20
8571	16.250964	192.168.1.112	239.192.0.20
8572	16.278116	192.168.1.112	239.192.0.20
8573	16.278425	192.168.1.112	239.192.0.20
8574	16.278645	192.168.1.112	239.192.0.20
8575	16.279610	192.168.1.112	239.192.0.20
8576	16.279946	192.168.1.111	239.192.1.111

No.	Time	Source	Destination
40	9.657700	192.168.10.2	192.168.10.119
41	9.799580	192.168.10.119	192.168.10.2
42	9.800344	192.168.10.2	192.168.10.119
43	10.000764	192.168.10.119	192.168.10.2
44	11.183221	AaxeonTe_02:2d:83	LLDP_Multicast
45	11.856274	Dell_a4:50:34	Broadcast
46	11.887577	192.168.10.119	192.168.10.2
47	11.889764	192.168.10.2	192.168.10.119
48	12.012485	192.168.10.119	192.168.10.2
49	12.013360	192.168.10.2	192.168.10.119
50	12.213648	192.168.10.119	192.168.10.2
51	12.923640	192.168.10.119	192.168.10.2
52	12.925776	192.168.10.2	192.168.10.119
53	13.118956	192.168.10.119	192.168.10.2
54	13.119824	192.168.10.2	192.168.10.119
55	13.320111	192.168.10.119	192.168.10.2
56	13.547048	192.168.1.119	255.255.255.255
57	15.130791	192.168.10.119	192.168.10.2
58	15.133010	192.168.10.2	192.168.10.119
59	15.145724	Dell_a4:50:34	Broadcast
60	15.331825	192.168.10.119	192.168.10.2
61	15.332775	192.168.10.2	192.168.10.119
62	15.533009	192.168.10.119	192.168.10.2

SOURCE: ANTAIRA

Table on left shows the results of running the test without the Internet Group Management Protocol (IGMP) management feature enabled. The right table shows the results of the same test being performed but this time with IGMP enabled.



SOURCE: ANTAIRA

A flexible feature of a VLAN implementation is that devices can be located anywhere on the network, and be connected to any VLAN within the network.

efficient in handling multicast traffic, such as PoE security camera monitoring, within a network.

A typical unmanaged switch tries to send the camera data to all of the devices connected to it, creating unneeded broadcast traffic. Whereas a managed switch capable of IGMP with snooping is able to build a Group Destination Address (GDA) table.

The GDA table determines the most effective pathways to all of the devices on the network and thus will only send the data to the units that require the data. The improved flow of data to only devices that require the information reduces the amount of network traffic and improves bandwidth availability.

In the example below, two controlled tests were performed on the same network which consisted of two computers, a managed PSE switch and two PD IP cameras. Packet analyzing software was used to view the amount of data that was transmitted in a 10 second time frame.

The table on the bottom of page 33 shows the results of running the test without the IGMP management feature enabled. The right table shows the results of the same test being performed but this time with IGMP enabled.

From the results, there was a drastic amount of traffic reduction from 8500 packets when no management features were used down to 62 packets when IGMP management was enabled for the same 10 second time period. The benefits from implementing IGMP on managed switches only increases as a network size becomes larger.

VLAN management

Management features such as VLANs are used to create separate segments within the main network. By preventing access from one VLAN group to another, it is possible to keep different departments such as accounting, customer service and product development on the same main network without being able to access the others departments files. A flexible feature of VLAN implementation is that the devices can be located anywhere on the network and be connected to any VLAN within the network. There are no physical restrictions of units being too close to one another to be on the same VLAN as shown to the right.

Another useful VLAN application would be a PoE Wi-Fi unit that allows guests visiting an office to get an internet connection. For security reasons it would not be wise to allow guests to go through the main network to access the internet; although a private guest VLAN could be implemented to allow connectivity and ensure network security.

Managed PoE Features

Managed PoE switches also include some additional features that can provide information specifically for PoE devices. Within the management features, a user is capable of setting and viewing the exact power being supplied to each port as well as setting power priority levels. A very useful feature is the ability of the user to cycle power to specific ports.

PoE power cycling can be done either manually through the web console or automatically with an auto-ping tool. The auto-ping tool can be used to periodically ping an IP address associated to one of the ports of the managed switch.

If there is not a response from the IP address after a certain number of attempts, then the managed switch will cycle power to the port. Being able to cycle the power to a specific port can be used to re-establish communication to a device that might have become unresponsive in a remote or hard to reach location.

Conclusion

In summary, the major points that require attention when using PoE devices are: What mode of wiring (Mode A or B) is used for the power being sent along the Ethernet cable, what standard PD is being used (IEEE 802.3af or 802.3at), and how much wattage does the power supply need to provide? Knowing and avoiding the causes of potential issues can save time and money.

Being able to offer advanced management features that provide key solutions will demonstrate knowledge and increase reputation. Due to the cost saving benefits from utilizing PoE devices, and an increased organization with a reduction in the amount of wiring and devices used in the facility, PoE applications will only be increasing in quantity due to its ability to provide flexibility during installation, maintenance and expansion.

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

HART-IP solution communicates at Ethernet speed

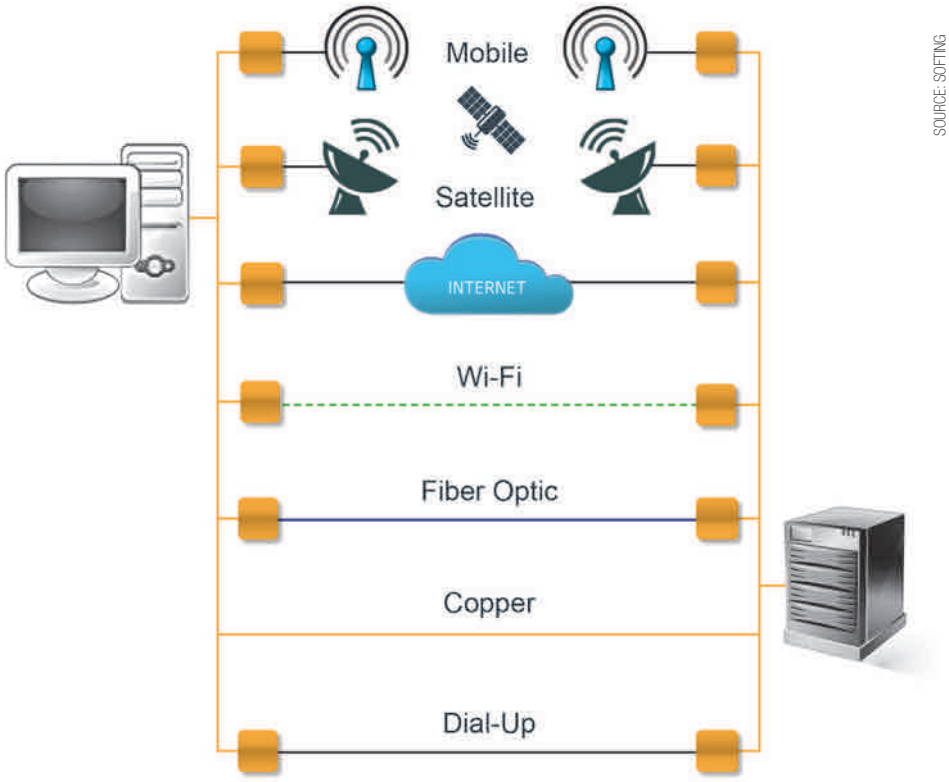
HART-IP can be run on Ethernet or WiFi, and enables vertical data integration for field devices all the way to the control room. Access to process variables allows support for device parameterization and advanced diagnostics. It will also play an important role in the Internet of Things for process plants in the future.

WITH THE DIGITIZATION OF FIELD DEVICES and the growing importance of predictive maintenance, and with the increasing possibilities of centralized field device configuration as well as modern asset management, the use of digital communication protocols like fieldbus and HART is on the rise.

At the same time, WirelessHART has established itself around the world as the leading wireless protocol for process applications. Some plants have up to 1,000 wireless transmitters which are distributed and managed over multiple gateways. When WirelessHART gateways need to be implemented or HART multiplexers need to be added to an existing infrastructure, HART-IP provides a new standard protocol ensuring tight, efficient integration.

Even though the process industry is renowned for being slow to adopt new technology, an IMS Research study from February 2013 reports that use of Industrial Ethernet in the process industry will almost double from 2011 to 2016. In response to this trend, the HART Communication Foundation (HCF) has released the HART-IP Ethernet protocol specification. HART-IP offers the possibility to tightly and efficiently integrate WirelessHART gateways and HART multiplexers into the control systems of legacy or new process plants.

The HART protocol can be run over Ethernet, Wi-Fi, or other network media without sacrificing the detailed device setup or diagnostics information of existing networks. HART-IP allows vertical data integration from the field device through to the control room. In addition to providing access to the process variables of a device, the protocol supports device parameterization and advanced diagnostics. WirelessHART and HART-IP will play an important role in enabling the Internet of Things in process plants in the future.



SOURCE: SOFTING

HART can be run over Ethernet, Wi-Fi, or other network media without sacrificing setup or diagnostics information.

The system integration challenge

System integration using traditional PLC protocols is increasingly reaching its limits. It is time consuming and not suitable for device data management. Hardwired transmitters often deliver only a single variable – the process value. Mapping a single variable per device from a PLC or RTU Modbus register to process visualization software is manageable.

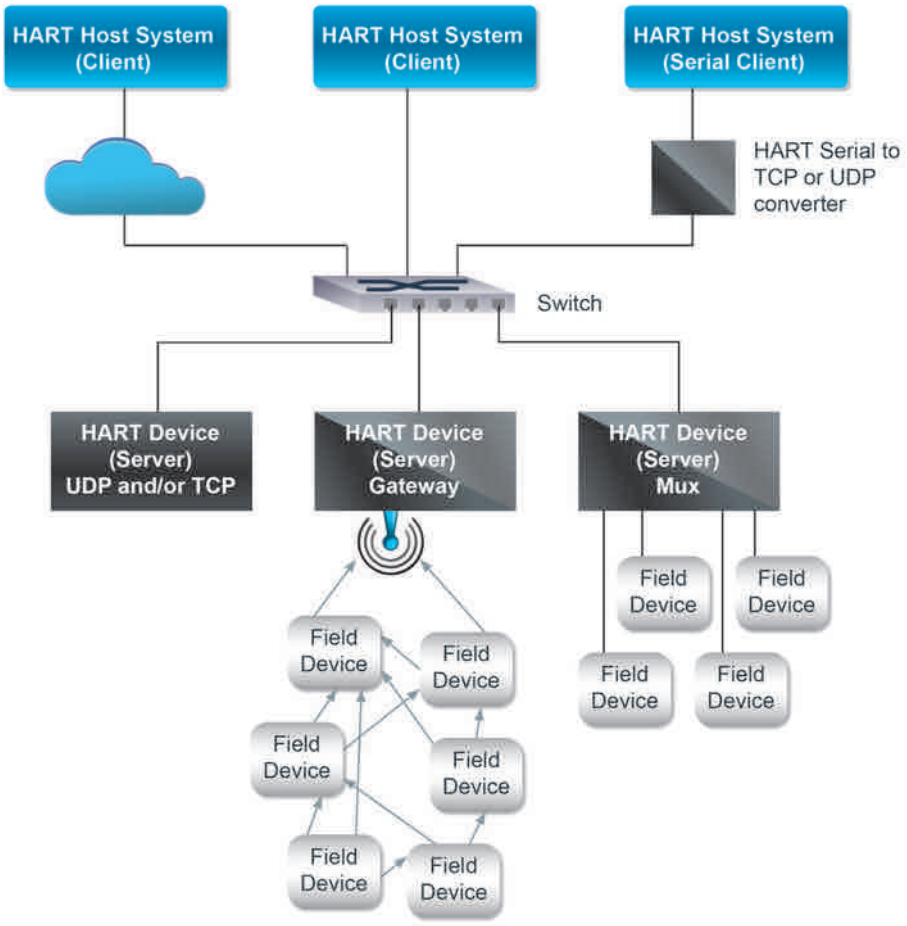
However, WirelessHART devices provide multiple measurements, control signals, and feedback; often two, three, or even four dynamic variables per device, each with an associated status. For instance, two or more sensors on a temperature transmitter, pressure and differential pressure from a pressure transmitter, noise and temperature from an acoustic transmitter, vibration, acceleration, and temperature from a vibration transmitter, etc. Mapping all the dynamic variables for these multi-variable devices in Modbus registers or OPC groups and items today would be time consuming and error prone.

In many plants, the number of WirelessHART devices in use exceeds the capacity of a single WirelessHART gateway. Plant-wide applications therefore require a WirelessHART gateway in each plant area or segment. These gateways then need to be integrated into the control system. Data also has to be available to applications beyond the control room.

HART and WirelessHART transmitters are intelligent devices that should support centralized configuration as well as diagnostics monitoring and battery power monitoring. A handheld field communicator can be used for device configuration and troubleshooting,

Features of HART-IP technology: At A Glance

- Easy implementation through use of existing Ethernet infrastructure
- Standardized use throughout the process plant
- Intelligent device management via Ethernet or Wi-Fi
- Company-wide access to device data and condition-based diagnostics information as well as process data with no mapping required
- Support of proactive maintenance strategy through fast access to diagnostics data
- Compatibility with standardized encryption protocols for data transport



HART-IP is a suitable backhaul network, in part because it eliminates error-prone data mapping (e.g. Modbus or OPC).

but is impractical for plant-wide deployment. Intelligent device management software is a better solution for plant-wide networks. Modbus registers and OPC items work for process variables, but are not suitable for intelligent device management (IDM) software as part of asset management systems.

The HART-IP solution

With the growing importance of WirelessHART and with increasing digitization at the field level in process plants, more users and system providers are moving their focus to HART-IP, which has been part of the HCF Network Management Specification since June 2012.

HART-IP enables plant-wide large-scale solutions and provides a high degree of interoperability between devices and applications. The protocol runs over IP networks such as Ethernet and Wi-Fi, and works over UDP and TCP using IPv4 or IPv6. The HART-IP application layer is based on the same application layer commands as 4-20 mA/HART and WirelessHART. Ethernet offers a wide range of benefits compared to serial data transmission. For instance, process data and IT data can be transmitted over a common medium. There is a large address space with an almost unlimited number of participants available and by cascading switches large network expansions are possible. Larger amounts of data can be transferred efficiently and the combination of different transmission media is possible (copper, optical fiber, radio).

HART-IP is a high-level application protocol independent of the underlying media and works over standard Ethernet (IEEE 802.3), both copper and fiber, as well as Wi-Fi (IEEE 802.11) equipment. It is suitable for use with standard infrastructure components like LAN switches, routers, access points, cables and connectors. HART-IP can utilize existing network structures with redundant Ethernet media, mesh or ring topologies, or Power over Ethernet (PoE). Various speeds like 10 Mbit/s, 100 Mbit/s and 1 Gbit/s are supported.

IP-based communication enables multiple protocols to share the same network, each protocol with a specific application. That is, HART-IP coexists with IT protocols and other industrial Ethernet protocols such as HTTP, Ethernet/IP or PROFINET. There is no need for dedicated infrastructure. The use of multiple clients and servers is also supported, enabling multiple controllers and software applications to access the data in one or more gateways or multiplexers over the same network.

HART-IP can be employed for devices using Ethernet and for HART-IP backhaul networks in WirelessHART gateways and HART multiplexers. HART-IP is used in Intelligent Device Management (IDM) software as part of asset management systems as well as in OPC servers to access data in WirelessHART and 4-20 mA/HART field devices. Specialized applications such as steam trap monitoring software and machinery health monitoring software etc. today already use HART-IP to get device data. In the future, control systems and automation solutions are expected to provide HART pass-through over HART-IP. HART-IP devices for seamless vertical integration in the plant are also conceivable. Some devices already supporting Ethernet today, such as flowmeters, may adopt HART-IP.Many plant devices do not have Ethernet connectivity, and will not in the foreseeable future. These will continue to use 4-20 mA/HART, fieldbus or WirelessHART. HART-IP is not anticipated to replace these protocols for many reasons:

- Distances reached by copper Ethernet are too short.
- Fiber optic Ethernet provides no power.
- Power over Ethernet (PoE) so far is not intrinsically safe.
- There are thousands of transmitters and valves in a plant so the number of LAN switches mounted in field junction boxes would be impractical.
- Fiber optic Ethernet makes device removal/connection for replacement and calibration etc. impractical.
- TCP/IP requires IT department involvement for cyber security.

HART-IP is expected to be predominantly used within the plant perimeter. If the protocol is used beyond the perimeter such as across the public Internet or if HART-IP "spills over the fence" such as using Wi-Fi, then security measures should be employed to protect the data during transport (firewalls, VPN tunneling, Secure Socket Layer (SSL), and remote authentication, etc.). Standard encryption protocols will evolve and HART-IP is designed to adapt to new versions.

Conclusion

HART-IP is a suitable backhaul network for WirelessHART gateways and infrastructure components since the application layer is the same, and time consuming and error-prone data mapping (e.g. for Modbus or OPC) is eliminated. HART-IP is easy to deploy because it uses the Ethernet infrastructure already available in most plants. Existing intelligent device management software can be upgraded to the latest version supporting HART-IP and the underlying WirelessHART gateways.

HART-IP might not revolutionize the entire process industry. But it will make a significant contribution to promoting and simplifying the exchange of data and information in process plants. It also fulfills the basic requirement for the implementation of Industry 4.0 – the vision of an "industrial Internet of Things".

*Technology report by **Softing**.*

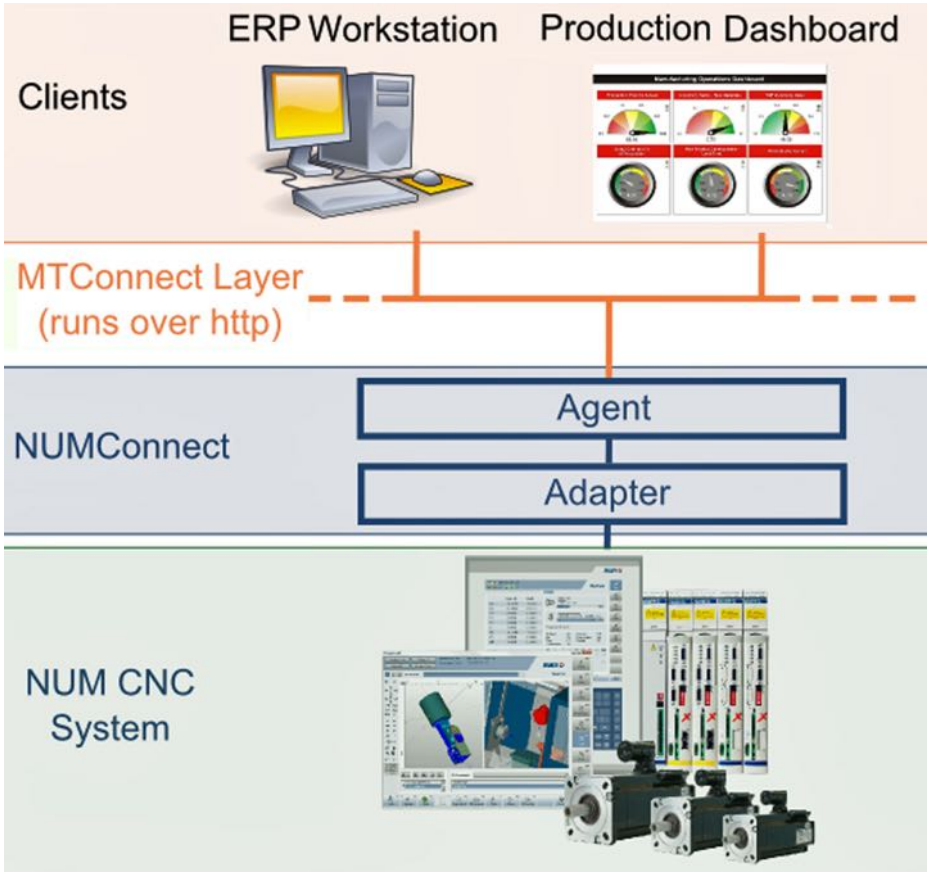
MTConnect offers machine tool interoperability

Open-source communications standard facilitates data-driven manufacturing by offering software-based interface option for new and existing CNC systems. The underlying technology is based on Extensible Markup Language (XML) for capturing data that is readable by both humans and machines.

A NEW COMMUNICATIONS INTERFACE OPTION for CNC systems fully complies with the open MTConnect interoperability standard. The interface can be fitted to new or existing systems and simplifies the integration of CNC machine tools with third party manufacturing management software. It enables users to implement powerful productivity-enhancing real-time data collection and retrieval facilities for production monitoring and analysis purposes.

NUMConnect technology allows CNC machine tool builders to add further value to their products very easily and cost-effectively, by providing uncompromised connectivity for manufacturing data. Manufacturers are increasingly making use of data retrieved from CNC machine tools on the shop floor to improve the efficiency of their production processes. However, until recently, the lack of a vendor-neutral data communications standard within the industry meant that CNC machine tool companies could only provide their customers with proprietary solutions for collecting and retrieving manufacturing data.

To compound the problem, most CNC systems have a closed architecture and only provide a data link via their PLC, limiting data collection to the PLC's scan rate. The inflexibility of this approach, which also demands custom client software for each machine type, drove an industry initiative to bring Internet style connectivity to manufacturing equipment.



SOURCE: NUM CORPORATION

The open MTConnect standard provides a method to seamlessly communicate between CNCs and business systems.

MTConnect Technology

MTConnect is an open, royalty-free communication standard that can be used by anyone and it is rapidly becoming a preferred choice for the machine tool industry. The standard is managed by the MTConnect Institute – a not-for-profit organisation that seeks to improve the use of real-data in manufacturing industries.

A growing number of machine tool manufacturers are adopting the standard, which is also now supported by many leading suppliers of enterprise resource planning (ERP), manufacturing operations management and production dashboard software.

XML for capturing data

The underlying technology of the MTConnect standard is the same as that used by the World Wide Web. It is based on Extensible Markup Language (XML) for capturing data that is readable by both humans and machines, with the format of all data transfers defined by hypertext transfer protocol (HTTP). Open architecture CNC systems already use similar software technology for their human-machine interface (HMI), which is based on HTML and JavaScript. It employs standardised server functions to facilitate the exchange of data between the CNC kernel, PLC, drives and motors.

As a result, NUMConnect can read anything that is capable of being displayed on the CNC system's HMI, regardless of whether it is in analog or digital format. Even detailed low level machine data, such as motor, drive or encoder error messages can be retrieved and used for monitoring machine performance, preventative maintenance or diagnostics.

The NUMConnect software interface essentially comprises two main components: an MTConnect Adapter and an MTConnect compliant information provider or lightweight webserver known as an 'Agent'. The Adapter collects data from the CNC system, associates it with defined MTConnect data items, filters out any duplicates and then pushes the data to the Agent, where it is held in a buffer store until overwritten by fresh information.

To help minimise response times, MTConnect does not require the establishment of a formal data transfer session, and under normal use there are no log-on or log-off sequences. When the Agent receives a request for information from any client application software, it transfers the appropriate data over the network, using HTTP. The system is inherently secure. MTConnect is a read-only standard designed to facilitate the retrieval of data from manufacturing equipment; it does not control or instruct a CNC machine tool to take action.

*Technology report by **NUM Corporation**.*

A technology perspective on the Internet of Things

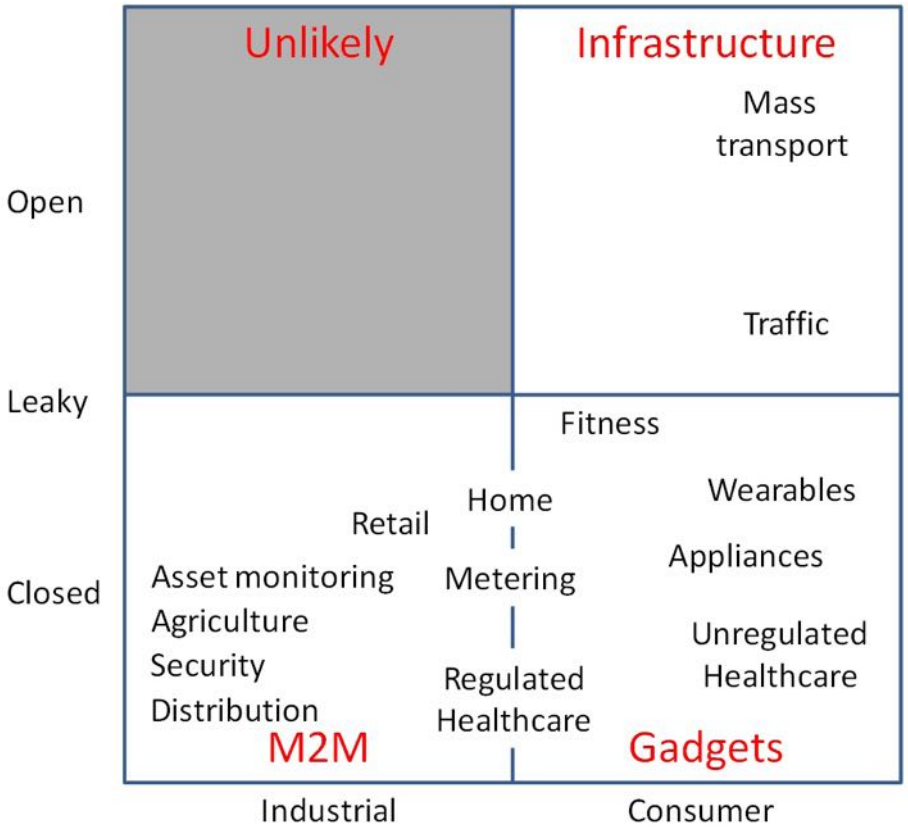
The Internet of Things is unfolding before us, but the exact direction of key technologies remains to be seen. This article offers a unique technological perspective on the IoT, analyses the nature of the Industrial Internet itself, and sets out some of the challenges and opportunities for the next phase of its deployment.

THE TERM INTERNET OF THINGS, or IoT, encompasses everything from existing developments in machine-to-machine communications to the newest wearable devices. The vision of the IoT world is that every Thing is connected and discoverable from its own IP address, sharing information freely. But will the future really be like this? There are good reasons to think that it won't. This article analyses the nature of the IoT and sets out some of the challenges and opportunities for the next phase of its deployment.

The web today is mostly horizontal – pages of open information, with revenues derived directly through purchasing or indirectly via advertising. The cost model in the Internet today is many-to-one – many consumers to one web server. This has driven revolutionary change in social media, search, file sharing, media distribution and more, enabled by the low cost of managing individual connections.

In the IoT, each Thing carries a finite cost; a hardware cost to establish the device and a maintenance cost to resolve and maintain its connection. For the IoT, the cost model is many-to-many and the issue of who pays makes a pivotal difference.

This article will show how industrial applications will be driven by cost of ownership of devices and cloud processing of their output. Devices from lower-cost economies will take value out of the consumer market and the most successful home and consumer products will derive value from information instead. Standards will remain important, but will never fully displace custom radio protocols. We will also show that strong opportunities also lie in cloud processing and truly low-power monitoring.



SOURCE: TTP

Many factors, technologies and diverse application areas must be put in focus to characterize the Internet of Things.

How open will the IoT really be?

Critical to understanding the IoT, is the spectrum of devices that will be open and those that will not. If an open Thing is defined as one that makes its data freely available on the Internet, and closed is defined as one where the information is tightly controlled, then a third definition is needed too; Leaky Things.

To implement a truly open Thing requires investment to be made that, by its own definition, cannot deliver an advantage to an individual or organisation. This in turn requires a force external to normal market economics. Smart cities and transportation are great examples of this – where investment in infrastructure by civil authorities allows improvement in the environment for many. There are, however, fewer other instances of this than are widely understood. The IoT may not be as open as much of the hyperbole suggests.

Leaky Things collect information that is private to the user, but which is then used anonymously and/or statistically to derive other benefits. Examples of this are traffic information, where the user of a satellite navigation device is at the same time uploading their own traffic speed. Sports applications use the cloud to create virtual competitors. Wired inhalers can indirectly report where air quality is causing problems for asthma sufferers. These represent innovative applications, where the product generates a secondary benefit and income.

Many of these applications are driven by new market entrants, keen to establish dominance in disruptive applications. Nest is a widely publicised example of this, where much of the value of the product and the company is outside of the product itself and in the relationships built with energy suppliers.

Characterising the IoT

In the consumer world, the Smartphone is the dominant communications and information hub for a range of new gadgets and wearables. However, barriers to entry for gadget makers are low, with semiconductor vendors creating sophisticated reference designs. This is encouraging a wide range of low-margin consumer devices from the East, making for a tough competitive environment. Products need to be highly differentiated, or gain secondary value from information to succeed.

In the closed industrial world, Things are

being used to derive hard economic value: resource optimisation, service delivery and efficiency. The value of the data is high to an organisation or individual where it's all about knowing the position and state of assets, to manage each one to maximum efficiency. This data is expensive to collect and differentiating to the organisation. This area will continue to evolve in a closed world, creating a steady evolution in industrial efficiency.

Overall, the next stage of the IoT will be characterised by a steady evolution in the industrial sector and more cheap gadgets in the consumer arena. Those looking to profit from enabling technologies need to look at lowering the cost of ownership of Things and by making maximum value from the information that is collected.

Future opportunity lies in driving the cost of monitoring down and the value of information up.

All Things Wireless

It's not the case that all Things will be wireless; just almost all of them. Some objects are very static and very close to the right kind of wire but vastly more devices are not. This is because of mobility, remoteness, convenience and, particularly in the home, because of aesthetics.

Utilising wireless technology invokes three very familiar issues:

- **Power:** If there's no wire then it's likely there's no convenient power source either. Solving this problem is critical to many applications. This isn't a single cost either; replacing or recharging a battery can cost as much as the original installation.
- **Cost:** A wireless transceiver has a finite cost in silicon. For this, it is important to understand the trends in the cost of wireless devices and what forces will be shaping the pricing of silicon in the future.
- **Standards:** Many devices re-use standard wireless technologies, such as WiFi, Bluetooth or GSM, but some of the critical issues of the IoT are creating an opposing force.

Powering the Internet of Things

Power is needed to measure, process and transmit data to the Internet. Devices also receive data and take action; but taking action often requires much more power than receiving data. Arguably it is in measurement that power is most critical.

Applications are highly variable, but many measurements are infrequent, particularly in tasks such as environmental monitoring or event detection.

It's not only the act of receiving data that uses power. Remaining in a conventional standby state can consume power too. Most short and long range wireless protocols require devices to listen continuously for a beacon and in those infrequent applications, it is often the case that the power consumed to remain in standby is the largest component of all power used in the device.

There are four mainstream ways to power the IoT :

- **Wired power:** Wired power is simple, reliable and predictable but is only suitable within a few metres of an outlet and where simple accessibility and/or ergonomic issues don't prevent its use.
- **Rechargeable cells:** Rechargeable cells work well in many consumer applications, providing that the time and patience exists for recharging. For fixed or remote applications, leakage will make the lifetime too short and recharging makes them impracticable.
- **Energy harvesting:** Energy harvesting has enabled some amazing applications including remote devices, in-body devices and near field devices for payment and communications. While it is possible to derive power from some unexpected places, the technology remains confined. In too many cases there is insufficient light, heat gradient, motion or physical space to generate the power needed.
- **Dry cell battery:** Dry cell batteries provide high capacity and low leakage. They represent a good choice for powering remote, inaccessible devices along with managing aesthetics and maintaining usability in the home. However, replacement can be expensive and periodic replacement creates a very undesirable operating expenditure.

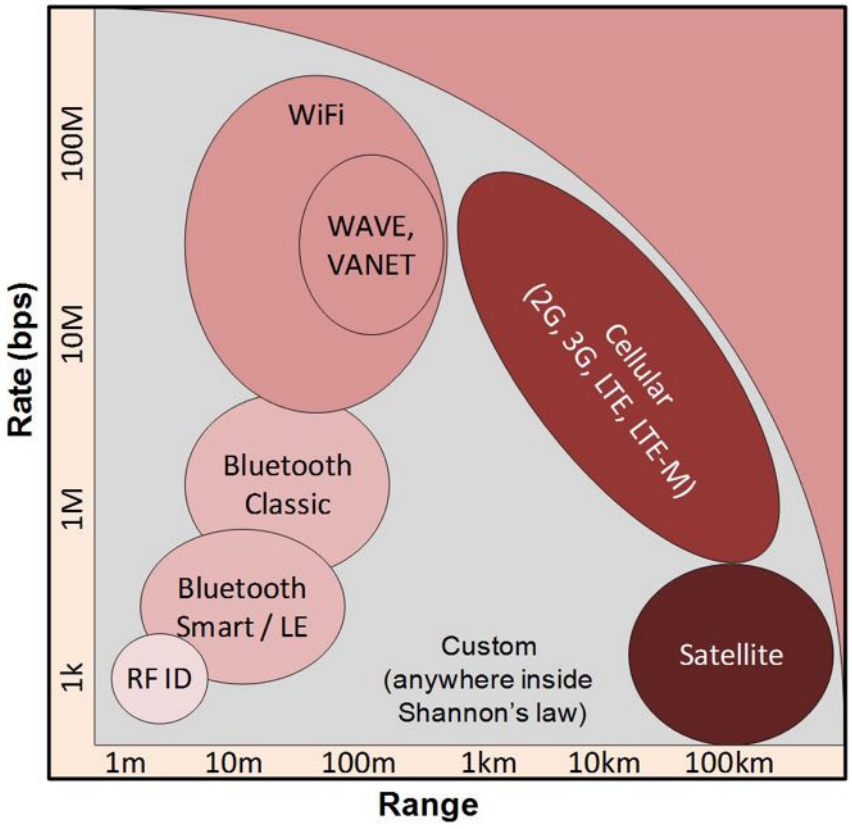
Power is critical to reducing the total cost of ownership of Things. To make new, differentiated applications, what's needed is fit-and-forget power – no recharging, no wires and multi-year battery life. Enabling that means either a big battery, or some truly low power technology.

Fit-and-forget power is critical to the next phase of the Internet of Things.

Are standards a problem..?

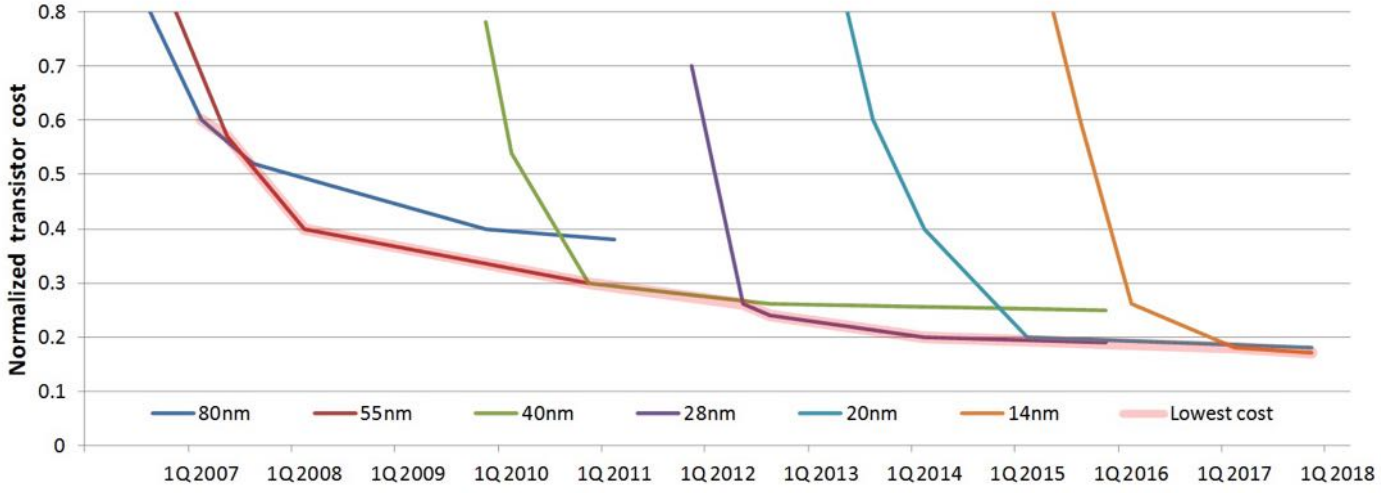
Standards have powered an incredible array of consumer electronics devices. Cellphones, wireless networks and short range personal devices have all been created as a result of the work of standards bodies and countless organisations that have sponsored them and developed technology based on them, including TTP.

At the physical layer, a wireless standard sits at a specific point in terms of spectrum, range and data rate. While most standards include options and/or fallbacks to mitigate interference, each standard is a compromise to meet the needs of a group of applications. Implementations make compromises too, selecting a set of functionality and interfaces to target a broad range of applications to maximise market share. These compromises



SOURCE: TTP

A Map of Wireless Standards for the Internet of Things.



SOURCE: TTP

Since Moore's law can no longer be relied upon to continue to reduce system cost and power, for those applications where cost and power are still too high, something more radical may still be needed to bring power consumption and cost down.

have a direct impact on all aspects of implementation – range, performance, silicon area, memory and power consumption.

A Map of Wireless Standards for the Internet of Things

In return, there are two advantages to the use of a standard: networks and scale. Using a standard means that you can piggy-back onto someone else's network and volumes derived elsewhere mean that silicon and module vendors have scale advantages. Higher volume drives increased integration and more investment in power-saving features. But is that enough?

Moore's law is exhausted

In 1965, Gordon E Moore first predicted the logarithmic progress of silicon integration. This evolved into Moore's law, which has proven to be one of the most accurate predictions of technological progress ever made. After nearly 40 years, the complexity of silicon devices continues to increase, but the costs of implementing each increment are becoming more and more prohibitive.

Moore's law is no longer able to predict a similar reduction in cost. Nvidia published its analysis in 2012 – while available silicon area roughly doubles with each shift in geometry, the incremental cost of implementing the same functionality through smaller processes has diminished to almost zero.

Diminishing returns for integration

Moore's law has had a further unintended consequence. While incremental improvements in efficiency of active power are still being achieved, static power consumption is becoming a serious problem.

With smaller and smaller physical features, electrons can much more easily leak past barriers and across the boundary of transistors. This directly impacts designers, who now have to constantly manage leakage and make tough implementation choices between high performance and lower leakage logic.

Since Moore's law can no longer be relied upon to continue to reduce system cost and power, then for those applications where cost and power are still too high, something more radical may still be needed to bring power consumption and cost down.

How to call a tractor a tractor

The focus of standards is to define how devices connect and exchange data over a common interface. A standard defines how to connect a Thing to a network, but then what? The data still needs to be put in context, to say what its data means and to define other parameters, such as how often it should be updated and where it should send its data too. Only when all these data types and parameters are defined, agreed and standardised, from tractor to washing machine, from engine temperature to cycle-complete, is it possible to interact with a Thing in a standard way.

Bluetooth encountered this problem very early in its development and approached it through the development of profiles – standardised behaviours and instructions for all parts of a user scenario. Profiles were defined for hands-free calling, video & audio distribution, synchronisation of personal information and many more. Each profile defines the format of information, protocol sequences and the usage of physical channels. The creation of each profile takes careful discussion, development, agreement and testing.

It's a lot of work. How then will the profiles develop for the IoT, across different physical media, different standards and a myriad of devices and applications?

Industry bodies and initiatives are already emerging to work on the problem. Today, the Open Interconnect Consortium, Google's Thread, the Allseen Alliance and Apple with its Homekit and Healthkit, are all working on different aspects of the IoT.

The focus of this work is on devices and the data that they submit to the Internet. As long as the focus is on standardising communications then this is the right approach: standardised formats for information that's sent over standardised links. However, the implication of this is that data needs to be formatted, conditioned and standardised at source. We are not sure this is the optimal approach for many cases because it forces resolution of the problem to the device.

There is a vision of intelligent, IP-addressable devices presenting correctly formatted information to the right place at the right time. For many devices, this is the right approach, but for others, it pushes an additional layer of formatting, configuration and options to the furthest and weakest part of the network.

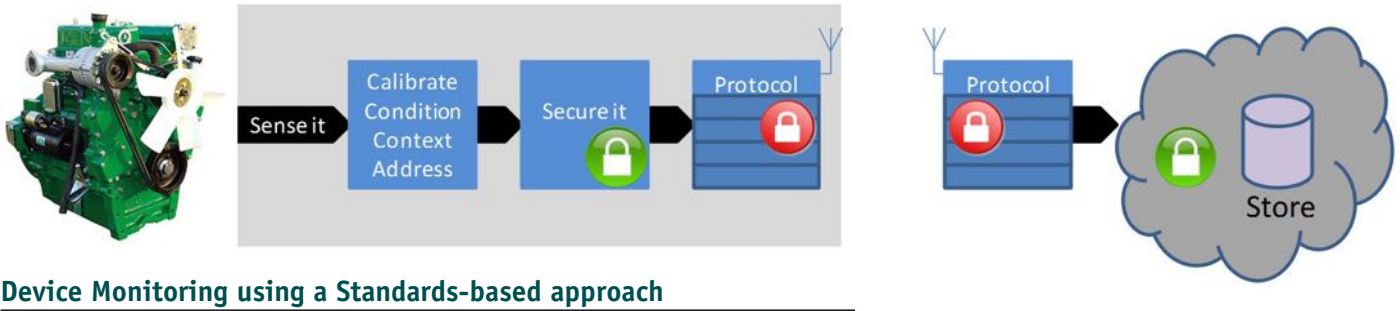
Standardising data at source can mean a missed opportunity to simplify the device.

The Cloud

The cloud is an essential component of the IoT; to collect, analyse and process information. However, it is possible to take cloud processing much further than that.

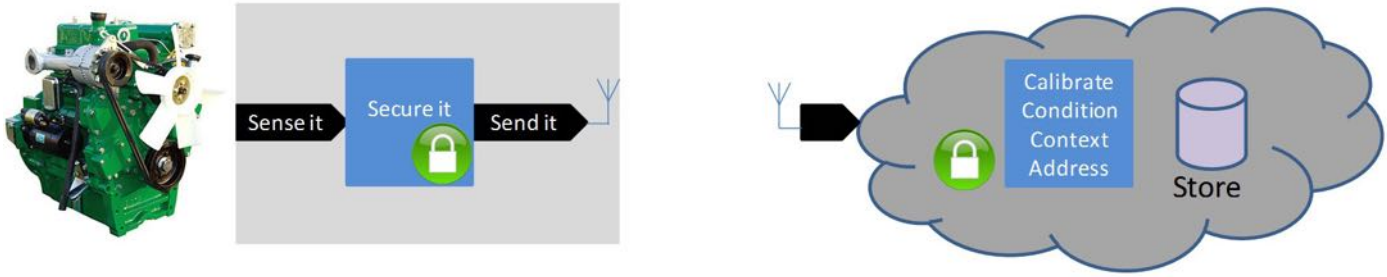
TTP is now integrating the cloud into wireless systems design from the start – developing the complete system together to minimise cost, simplify installation and enable new classes of application. The methodology is very simple; by making more intelligent use of data in the cloud it is possible to further reduce the complexity at each monitoring node or Thing. At each stage of processing, innovative algorithms can be applied to reduce per-node cost and power.

The cloud can receive and store data sent



SOURCE: TTP

Device Monitoring using a Standards-based approach



Device Monitoring using a novel low-cost approach

intermittently, process it to remove outliers and make it available to users and other cloud services. The rationale for this remains the same – to keep the device as simple and as low power as possible. Some ways the cloud can be used to simplify Things are:

- Allowing Things to provide raw data, with context and storage resolved in the cloud.
- Resolving IP addressing in the cloud, so the device is never directly polled.
- Resolving missed/duplicated transmissions in the cloud to reduce protocol overheads.
- Using data itself to relate to where in a system a specific node is installed.
- Performing storage, translation, calibration, context, signal conditioning and presentation in the cloud to reduce processing on the device.

The cloud can play a pivotal role in keeping Things simple.

Security

Security remains critical, but the trust relationships for Things are different to that applied by most standards today. Standards-based security, such as that applied over Bluetooth or 802.11, creates a secure and trusted relationship between device and base-station or from device-to-device.

For many Things however, the trust relationship is needed between the Thing and the cloud; and for standards based implementation, this often means a second layer of security.

The security requirements can be different too. Standards-based security is primarily concerned with privacy. Depending on the application, integrity of data from Things can be much more critical: knowing that the data has not been interfered with at any point on its journey from the Thing to its recipient. It's unclear how an attacker can benefit from knowing the oil level of a combine harvester, but if the data is falsified and the oil ran out, it could cause severe impact.

A single layer of end-to-end security is much simpler and can be just as effective for Things.

Custom Radio

Using a standard is always a compromise. In return there are economies of scale and network-side benefits that can simplify the connection. So, is there a place then for a proprietary radio solution?

Each application will have its own parameters of range, power and cost. If these map efficiently onto a standard, then a standards-based implementation can provide quick market access. It is important to recognise however, that there are also options available outside of this envelope and in many cases, these can lead to strongly differentiated solutions.

It is possible to combine a sweet-spot of spectrum, commodity silicon and cloud-based processing to enable exceptionally low-cost, low power and secure wireless devices.

By careful selection of radio technologies and by avoiding a complex protocol stack, it is possible to significantly reduce memory, processing requirements and signal processing in the radio link. The 2.4GHz ISM band is already over-used by WiFi, Bluetooth, Zigbee and your microwave oven and requires complex and careful avoidance of other users that adds complexity and power. There are better choices here too. Combining all these technologies can enable a radio bill of materials of less than a dollar and multi-year battery life for many simple monitoring devices.

It is often the case in vertical applications that both end-points of the wireless link are owned by one vendor, but simplifying the radio link means that the cost of implementing both ends can still be lower than a single standards-based end-point. Combined with diminishing returns for increased silicon integration and fit-and-forget power, custom implementations, if correctly done can drive some truly disruptive opportunities.

Moving forward, one Thing at a time

At TTP we have been quietly building the Internet of real Things and solving big challenges such as developing robust sensors to collect data, reliable and cost effective wireless technologies to deliver it and innovative cloud processing to make sense of it.

The Internet of Things represents a wide-ranging opportunity. There are a lot of suppliers, standards and technologies in a complicated market, but we believe there are still some big opportunities for companies to take on unresolved challenges in collecting measurements from Things and drive broad innovation in cloud processing.

Michael Barkway *is a consultant at The Technology Partnership plc.*

Integrated production control

Yokogawa: CENTUM VP R6.01, an enhanced version of the company's integrated production control system, will be released in February 2015. This marks the first step in the development of an all-new CENTUM VP that will play a central role in Yokogawa's VigilantPlant strategy for its industrial automation business.

This first R6-level release of the CENTUM VP system represents more than conventional functional improvements. R6 brings together engineering, advanced operation, system agility and sustainable plant. With R6, plant operators can be assured of an optimum engineering environment that spans the entire plant lifecycle, from plant design and the engineering and installation of systems and devices to the start-up of production, maintenance, and renovation.

R6.01 features an expansion of Yokogawa's lineup of I/O devices and introduces crucial new control system components. It is designed to reduce the time required to configure and install a control system.

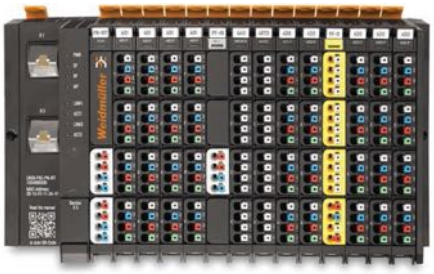
Industrial 3G routers

Westermo: The MRD-315 and MRD-355 3G routers are designed to provide resilient, high-speed remote access across mobile networks. These two mobile broadband routers offer a dedicated GPS antenna port, a faster downlink transfer rate and an improved CPU. A next generation 3G module is an important addition that characterizes the new arrivals.

The new routers offer a high level of connectivity, and support mobile standards including GSM, GPRS, EDGE, 3G UMTS, HSDPA and HSUPA allowing uplink transfer rates of up to 21.0 Mbit/s. Together with the compact enclosure, DIN-rail mounting, a wide operating temperature specification, they are designed for industrial applications in harsh environments.

Both MRD-315 and MRD-355 provide a built-in two-port 10/100 Ethernet switch and an RS-232 D-Sub which easily allows any type of devices to seamlessly connect over a vast geographical distance.

u-remote Remote I/O



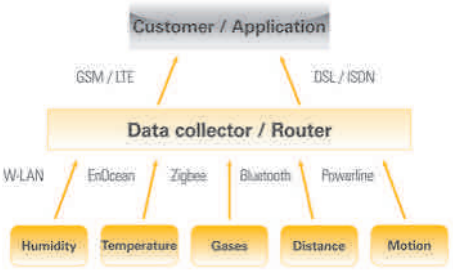
Weidmuller: The "u-remote" distributed I/O platform delivers a streamlined design while providing features such as hot-swappable slices, an integrated self-configuring web server interface and simple plug-in connections.

The new unit is an advanced IP20 platform that is built to ensure fast installation and setup, and designed to improve machine performance and productivity. At 11.5mm wide per I/O slice, its slim design with high-channel density makes it a viable distributed I/O platform. Using Push-In wire technology, each point is clearly visible with LED status indication. Card slices are hot-swappable and can be installed, updated and removed without the need for any tools.

750 series programmable controllers

WAGO: The PFC200 line provides advanced programmable controllers programming options in accordance with IEC 61131-3, using the WAGO-I/O-PRO development environment. It offers an easy to use environment for both PLC programming and process visualization.

Multiple fieldbus ports are available including Ethernet, MODBUS, TCP/UD/RTU, CAN port, PROFIBUS Slave, Smart Grid and Serial RS-232/RS-485. Built in web visualizations and support of mobile devices via Web Visu mobile application are also provided. Flexible I/O configurations can connect to 400 of the 750 series I/O and specialty modules.



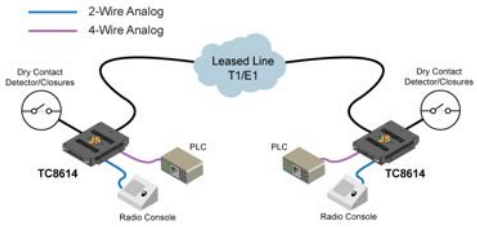
Industry 4.0 solutions

Unitronic: Complete Industry 4.0 solutions for typical smart home and industrial applications comprise an indoor climate control system for home automation and sensor-aided analysis and monitoring of an industrial process.

Unitronic has specialized in the areas of sensor technology and communication for years, and can demonstrate the necessary process steps starting from the selection of sensors to store measurement data onto an optimized IT structure for each individual application case including the necessary hardware.

Data collected by various sensors is sent to data collectors and gateways by different short-distance communication networks such as EnOcean, XBee (Zigbee/802.15.4/Digimesh), Bluetooth Low Energy or Wifi. They communicate with a server backbone which processes the sensor data provided to the exhibition booth and transmits the values live into the Internet.

Mux leverages T1/E1 circuits



TC Communications: The new Model TC8614 four-Channel 600Ω analog and dry contact-over-T1/E1 multiplexer links or extends various 600Ω analog, audio and intercom devices (FSK modems, E&M, teleprotection relay controllers) and dry contacts over existing T1/E1 links.

It can also be used as a backup network to ensure business continuity, to improve voice quality, to increase system reliability in harsh environments, to replace aging unreliable copper wire phone line circuits and to stabilize voice level settings for 600Ω audio channels.

It is available in two configurations: four-channel, two-wire analog with four-channel dry contact and four-channel, four-wire Analog with four-channel dry contact.

Physical security of field cabinets

SEL: Integrated physical security capabilities in the SEL-3622 security gateway enhance

operator awareness of physical tampering to field control cabinets in addition to cybersecurity threats.

The new technology provides added visibility and faster response times for potential physical security breaches in recloser and voltage regulator control cabinets. SEL designed and built the physical awareness sensor technology as part of the Padlock cooperative project with the U.S. Department of Energy (DOE), Tennessee Valley Authority (TVA), and Sandia National Laboratories (SNL).

With its enabled physical sensor components, the SEL-3622 will now be able to alert on possible malicious physical activity. The SEL-3622 detects sudden movement (through an embedded accelerometer), sudden changes in visible light (through an embedded light sensor), the opening of cabinet doors (through an input sensor), and the connection and disconnection of Ethernet cables to warn owner-operators of potential tampering. Physical awareness data can be sent through a variety of mechanisms, including Simple Network Management Protocol (SNMP), Syslog messages, and toggling of an alarm contact output.

Layer 3 industrial Ethernet switches

ORing: New Layer 3 industrial Ethernet switches offer high gigabit port density . New models include the IGPS-R9084GP, IGS-R9812GP and the DGS-R9812GP_AIO_S. With the provision of a total of 12 to 20 Gigabit ports, the switches are equipped with 100/1000Base-X SFP modules to offer more versatile and longer-distance connection options.

The Ethernet ports of the IGPS-R9084GP are compatible with the IEEE802.3af / IEEE 802.3at PoE standards, allowing each port to provide up to 30Watt power to a PD device.

Apart from static routing, these models will automatically forward packets to the destination device even if it is not on the same network and then update their MAC tables through the learning ability. Since the Layer 3 function can communicate with different network segments, each LAN will remain separated when no cross-network transmission is required, hence higher security and bandwidth usage efficiency. With the ability to connect different LANs together when necessary, the devices can provide excellent network scalability.

Industrial network connectivity

IXXAT: The Econ 100 is an ARM-based embedded PC platform for top-hat rail mounting incorporating a Linux operating system and unique multi-protocol support. Customer-specific gateway and control solutions can be swiftly and simply implemented for a variety of different fieldbus and industrial Ethernet standards.

A new expansion board combines a multi-protocol approach with local I/Os for enhanced data security. In addition to on-board communication interfaces (two Ethernet, two CAN and two USB interfaces), the unit can be expanded by means of a new expansion board. Alongside analog and digital I/Os, the expansion card offers a slot for HMS Anybus CompactCom modules, a serial interface and 512 kB NVRAM.

CompactCom modules are available for all popular fieldbus and Industrial Ethernet networks, and can be easily interfaced from the application software by means of the common Anybus programming interface.

Connect Modbus/TCP devices

Opto 22: An update has added Modbus/TCP communication to the company's groov web-based mobile interface software.

Acting as a Modbus/TCP master, groov communicates directly with Modbus/TCP slave devices over standard, non-proprietary Ethernet networks. No intermediary servers, protocol converters or communications interfaces are required. This simplifies hardware planning, reduces initial hardware cost and ongoing maintenance, and streamlines device setup and configuration.

Automation end-users, integrators, machine OEMs or any authorized person can quickly and securely monitor and control these devices, as well as automation, building and other control systems, all from a mobile device.

For mobile devices like iPhones, iPads, and Android-based smartphones and tablets, a groov View app for iOS and Android is available free of charge on the iOS App Store and Google Play Store.

Sercos IP core for Cyclone V FPGAs

Altera: Sercos International has announced the availability of a Sercos III IP Core for Altera's low-power Cyclone V devices.

The IP core is available for Sercos III master and slave controllers (SERCON100M/S). It includes all hardware functions, such as timing, synchronization and processing of cyclic and non-cyclic data on the basis of two integrated Ethernet MACs. Sercos III master and slave devices can be implemented as a single chip solution using either Cyclone V FPGAs or Cyclone V SoCs, which integrate an ARM dual-core Cortex-A9 processor.

Detailed documentation on the IP core, reference designs and example Ethernet interface diagrams are available.

VeriSens vision sensors

Baumer: The VeriSens XC series vision sensor portfolio now includes models with color identification and inspection. With the Color FEX assistant, setup is simplified and reliable. Available resolutions are VGA and 1.2 megapixel.

Previously the RGB color space offered a challenge during setup of a color inspection task. Color FEX is a new, intelligent assistant

for intuitive and quick setup of 3D color identification and definition. Object colors and their shades are automatically identified and visualized in 3D as color spheres. The resulting absence of sphere collisions ensures reliable color inspection can be achieved.

The new models with color identification enable applications in packaging, pick and pack, assembly and quality assurance.

Wireless gateway flexible antenna

Emerson Process Management: The compact 1410D smart wireless gateway for wireless network applications provides a solution where gateway installation locations are limited, and in difficult safe areas that must connect to distant wireless application networks.

Wireless gateway installations can be difficult when antenna distances are limited and there are few safe locations. The 1410D gateway uses the Smart Wireless 781 Field Link to enable flexible remote antenna location up to 200 metres, and the separate possibility of connection to hazardous areas with intrinsic safety protection.

A smaller size and DIN-Rail mount capability makes the 1410D a choice for limited cabinet space requirements. Built-in layered security functions ensure that the network stays protected at all times. The gateway manages the wireless network automatically and delivers greater than 99.9% data reliability.

Open source firewall alternative

Deciso: By releasing the potential of the AMD G-Series SOC for wire speed gigabit network security, it is now possible to protect networks with affordable and turnkey open source firewall appliances.

The new OPNsense firewall appliances provide an easy-to-use, powerful platform for users and developers. Its source code is open and verifiable for all. The G-Series SOC made it possible to design a product without bottlenecks that is stable, cost effective and durable.

The embedded low-power design eliminates high cooling requirements that current high performing server-like designs demand, as demonstrated by a typical power usage of only 20W for the quad-core version.

Optical network securitv

MICROSENS: Providing protection against manipulation, new management modules (NM3 and NM3+) make optical networks setup with the company's WDM platform MSP 1000 in an even more secure mode.

If transfer of sensitive data is a concern and it's important to protect the network configuration against unauthorised and unwanted access attempts, the two new modules offer several options. All access attempts to the configuration are made over secure, encrypted protocols such as SSH, HTTPS, or SNMPv3. Each access attempt requires the login to the system with valid user authorisation. The user model permits the assignment of permissions on several authorisation levels, in analogy to SNMPv3. In addition, the integrated RADIUS client allows centralised user authentication. MICROSENS also supports TACACS+ and the use of access control lists.

X20 controllers and modules

B&R Industrial Automation: With the X20c

series, B&R is adding protection against harsh environmental conditions. The "coated" variants of the compact controller and I/O modules are protected against condensation and corrosive gases by a special coating on the electronics module. This makes these modules suitable for use in corrosive environmental conditions.

The coating on the electronics module protects the components and circuit board from the effects of condensation and corrosive gases. The protection against condensation is checked using the test specified in BMW GS 95011-4, and protection against corrosive gases using the 4-part corrosive gas tests specified in EN 60068-2-6, test method 4.

5-port PoE+ managed switches

Antaira Technologies: The OLMP-0501 and LMP-0501-24 series is a 5-port industrial PoE+ managed Ethernet switch, with 48-55VDC high voltage power input (LMP-0501) and 12-36VDC low voltage power input with a built-in voltage booster (LMP-0501-24).

Each unit is designed with four 10/100Tx Fast Ethernet ports that are IEEE 8023.at/af compliant (PoE+/PoE) with data and PoE up to a maximum power output of 30W per port. There is one additional 100Fx Fiber port that supports either an SC or ST type connection, and has either a multi-mode 2Km or single-mode 30Km option.

This CE compliant product features eight temperature input channels and supports thermocouple types J, K, T, E,R,S,B,N, RTDs, thermistors and semiconductor temperature sensors. The OM-WLS-TEMP can be operated as a standalone plug-and-play USB device or as a remote wireless device with a range of up to 46 M (150 ft) indoors and 732 m (2400 ft) outdoors. It is designed to monitor process temperature in industrial or laboratory settings.

UNIGATE CL protocol converters

Deutschmann Automation: New UNIGATE CL protocol converter models can be fitted with eight integrated, freely configurable I/O interfaces. The housing size stays the same. The I/Os are provided as plug-in connections on top of the housing.

The converters for DIN rail installation enable the integration of existing devices in diverse fieldbus and Ethernet environments. The new models support direct and application-

specific control of actuators, sensors, and signaling devices – external I/Os from other manufacturers are no longer required. The integrated I/Os are configured via the same script that is the basis of all Deutschmann gateways, handling the conversion of the terminal device protocol to the respective fieldbus or Ethernet protocol. Users are free to define each I/O as an input or output, and to apply their individual switching logic in associating I/Os with each other.

EyeSens vision with Profinet

EVT Eye Vision: In addition to EtherNet/IP, the EyeSens vision sensors by now also support Profinet IO and can communicate with both of the most common communication standards of industrial Ethernet.

With Profinet, it is possible to create solutions for product engineering, process automation and building automation as well as for the whole spectrum of the drive and control technology or synchronous motion control applications.

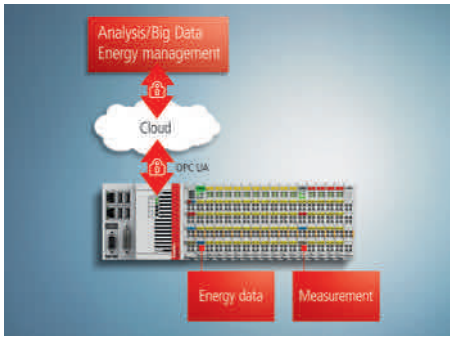
The EyeSens vision sensors provide conformity with class A (CC-A). This class makes fast, real time communication with superordinated control possible. All functions of the discrete inputs and outputs (Trigger, handshake as well as all results) can be communicated via Profinet.

PC control and smart metering

Beckhoff: Consumption data on the use of electricity, water, heat or gas in networked buildings, properties, towns or plants can be made available via the Cloud.

A new platform for Smart Metering uses PC-based control, so consumption data can be effectively acquired via modular I/O terminals. These flexible devices can be used either by the direct connection of a sensor, by distributed I/Os on a fieldbus (e.g. EtherCAT, PROFINET or BACnet/IP) or via lower-level buses such as M-Bus.

Control, regulation, and data pre-processing are performed by an Embedded PC, which is easily scalable with different performance classes. The programming of PLC functions, the integration of program codes as required (such as for C++), and the configuration of



I/O points, database interfaces, and the OPC UA (Unified Architecture) communication protocol, all take place in the universal TwinCAT engineering environment. A modern, Cloud-connected system interface can be realised via the TwinCAT database server. Optionally, the data can also be buffered and analysed locally in an Embedded PC.

Smart remote I/O

Moxa: A new remote I/O controller combines networking, automation and operational intelligence in one single, compact device. This concept not only saves additional costly cabinet equipment; it even allows the I/O controller to manage communication by itself and take appropriate action based on the controller's key task, data acquisition and control, without endangering the operational intelligence.

The ioLogik 2500 unit is designed for for distributed and remote I/O applications. Unlike traditional passive I/Os that have to poll for data, when used with Moxa's MX-AOPC UA Server, the ioLogik 2500 series will communicate with SCADA systems using active messaging that is pushed to the central server only when state changes or configured events occur. This event-based messaging technology immediately conveys alarms to the relevant decision makers. In addition, it saves costs for data traffic by sending required data packets only and it reduces both large amounts of (public) IP addresses and the amount of wasteful data.

The controller can be integrated into the Ethernet infrastructure via 802.11 a/b/g/i Wi-Fi, Five-Band UMTS/HSPA+ or Quad-Band GSM/GPRS/EDGE mobile networking with two SIM card slots or simply via LAN. Furthermore, it hosts a 4-port unmanaged switch; one of whose ports can be used to expand the available onboard mixed I/O combination with additional or different types of I/O, as required. In this way, up to eight additional ioLogik E1200 modules can be attached in a daisy-chain under the controller's (public) IP address. Two built-in 3-in-1 serial RJ45 ports can either act as serial gateways, Modbus/RTU masters or serial tags controllers.

Rugged cellular wireless router

Siemens: The Ruggedcom RX1400 is a multiprotocol intelligent node which combines Ethernet switching, routing and firewall functionality with various WAN connectivity options.

The device is IP40 rated, does not use fans for cooling, operates continuously within a -40° C to +85° C temperature range and comes with a rugged metal housing that supports DIN rail, panel, or rack mounting. The Ruggedcom RX1400 provides a high level of immunity to electromagnetic interference, heavy electrical surges, extreme temperature and humidity for reliable operation in harsh environments. Integrated GNSS (GPS/GLONASS) functionality allows the device to report its location as necessary for asset tracking purposes in large scale deployments.

The router is designed to support primary communications over commercial LTE networks and leverage LTE's enhanced capabilities for QoS (Quality of Service) management. For reliability purposes the device is able to rollback to 2G and 3G wireless connectivity. In addition the cellular router is equipped with a Dual SIM card slot which enables automatic failover in case of interruption in the communication.

IO-Link master modules

Balluff: New push-pull variants of its PROFINET IO-Link master modules are available with the choice of a fiber-optic cable or copper cable connection.

All of the modules have the push-pull connection technology for fieldbus and power cables that is specified in the AIDA (Automation Initiative of German Automobile Manufacturers). A special, third variant combines both worlds and provides both a fiber-optic (SCRJ) and a copper (RJ45) push-pull connection. The particular attraction is that this module can be used for converting from a copper to a fiber-optic cable right in the I/O module, without needing a additional, external converter module.

Like all Ethernet-based IO-Link master modules from Balluff, the push-pull modules also have an integrated display for information and additional diagnostics as well as an integrated switch for setting up a PROFINET line structure. All functions based on IO-Link specification 1.1 are made available by the 8 integrated IO-Link ports. The user is provided with a real-time display of the module with all current statuses for extended diagnostics through an integrated web server.

Industrial Ethernet switches

Delta Electronics: Two new rugged Ethernet switches offer an array of management functions, and allow multi-network connection, immediate self-recovery along with bringing high-efficiency and reliability to systems.

Delta's proprietary self-healing redundant ring technology is called ONE RING and ONE CHAIN. It can enable redundant paths and provide self-healing recovery time of less than 20 milliseconds to ensure smooth data transmission with minimum loss. In addition, this approach offers customers the selection of Trunking Ring, Multi-Ring, Ring Coupling, and Dual-Homing modes to satisfy their specific needs. With strong ring network functions, ONE RING and ONE CHAIN provide highly-flexible and highly-reliable network structures, which greatly save on wiring costs.

The DVS Series feature numerous management functions in order to ease configuration and to ensure a safe operation. IPv6 address is suitable for larger network and neighbor discovery. They support EtherNet/IP and MODBUS TCP protocols that facilitate the remote management by SCADA and other industrial devices. QoS (IEEE 802.1p) allows real-time traffic classification and prioritization and TOS/DSCP enable mission-critical applications.

Remote access routers

eWON: The new Cosy 131 is a family of industrial VPN remote access routers that offer LAN, WiFi and 3G+ connection options.

With the routers, machine builders and OEMs can access machine PLCs and HMIs, and troubleshoot them from the office. The Cosy 131 complements the existing Cosy 141 with new features such as WiFi and 3G (no need to use the LAN anymore), a USB port for additional serial devices connectivity, a SD card reader for an easier on-site configuration and a configurable LAN/WAN 4 port switch.

The complexity of connecting remote equipment has increased while the technology has evolved from traditional modems to the Internet. The Cosy lets maintenance engineers establish a secure VPN connection from the machine to anywhere via Talk2M, eWON's cloud-based remote connectivity solution. The router seamlessly communicates on the local area network with the PLC and the HMI, and allows remote connection from anywhere with a simple laptop, tablet or smartphone.

DIN-Rail PoE switch

EtherWAN: The EX42300 Series is a hardened-grade, 802.3at unmanaged PoE switch designed for integration of mission-critical

PoE devices in IP security, access control and intelligent transportation systems.

The EX42300 features four fast Ethernet PoE copper ports, one Gigabit copper port, and a 1000BASE-X fiber port. The IEEE802.at compliant PoE/PSE ports provide up to 30W per port with a full 120W power budget for maximizing power delivery to powered devices such as PTZ cameras. Two Gigabit uplink ports are also available on the EX42300 with copper, fixed fiber or SFP options to provide full non-blocking switching performance to meet the expectations of critical applications such as, wireless AP connections, multicast traffic of machine control messages, or video surveillance systems.

The EX42300's built-in DC/DC power converter circuit enables 24/48VDC redundant power inputs for industrial applications, plus relay alarm support which notifies the network administrator immediately when port fault occurs. Additionally, the QoS support carries up to four VLAN priority markings, allowing users to direct existing network more efficiently. The EX42300 is also compliant with energy efficient Ethernet standard allowing less power consumption during periods of low-data transmission.

Connecting devices wirelessly

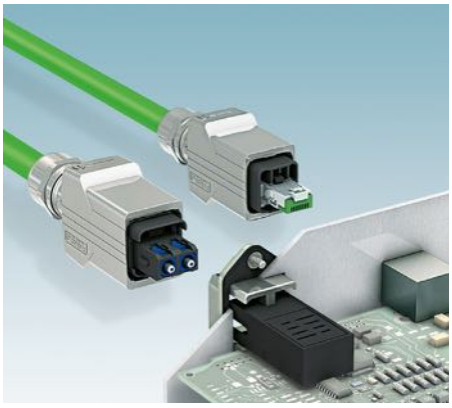
HMS Industrial Networks: After the acquisition of the wireless gateways from u-blox/connectBlue, Anybus wireless bridge has expanded its suite of wireless bridge products for connecting industrial devices wirelessly.

The new offerings include: Industrial Ethernet over WLAN (point-to-point), 2.4 or 5 GHz; Industrial Ethernet over Bluetooth (point-to-point or multi-point); and Serial over Bluetooth (point-to-point or multi-point).

These new solutions solve network problems for system integrators as industrial Ethernet and serial links go wireless. By connecting industrial devices and networks over a wireless link, a wireless bridge makes it easier for system integrators and automation engineers needing to create connections through hazardous areas, hard-to-reach locations or moving installations where cables are not desirable.

The wireless bridge is also a solution for bridging popular industrial Ethernet standards such as PROFINET, EtherNet/IP, BACnet/IP and Modbus TCP, as well as serial networks, and provides users with a robust and maintenance-free wireless connection.

Safe data transmission in the field



Phoenix Contact: New push-pull Advance data connectors bring future-proof high-speed cabling directly to the field. Designed for data rates of up to ten Gbps, the connectors are protected against dirt, dust or humidity by means of IP65/IP67 protection. Due to their 360° shielding, they are also immune to electromagnetic interference.

The push-pull technology means that users can insert and remove the connectors easily. But a mechanical locking mechanism reliably also prevents unintentional release of the connection. The series includes versions for Profinet and Ethernet as well as fiber optic versions for POF, GOF, and PCF fibers. All connectors are designed for conductor cross sections from 26 to 22 AWG. Both the straight and 45° angled versions are suitable for cable diameters up to 9.5 mm.

Crimson 3.0 supports 300 protocols

Red Lion Controls: Crimson 3.0 software now offers communication support for more than 300 industrial protocols. Protocol conversion is a key element needed to make the connected factory a reality, empowering plant managers to adapt existing equipment including drives, PLCs and HMIs to drive efficiency while reducing total cost of ownership in industrial environments.

One of the challenges faced by end users, OEMs and system integrators is software tools that enable communications between disparate

devices and protocols in a cost effective and time effective manner.

Providing a user-friendly interface, Crimson converts protocols for disparate industrial devices, allowing them to share work-in-process, machine status and other information. Deployed on Red Lion's HMI panels (ProducTVity Station, Data Station Plus or other industrial automation HMI offerings), Crimson gives organizations the ability to boost productivity, optimize material usage and troubleshoot systems in real time.

Supporting simultaneous conversion of multiple protocols, the use of Crimson-enabled products allow companies to easily integrate PLCs, PCs or SCADA systems for data collection, monitoring and control of factory floor equipment from different manufacturers.

Entry-level Ethernet switches

Belden: A new Gigabit Ethernet switch from Hirschmann, the GREYHOUND switch, is designed for industrial environments that need cost-effective, entry-level devices with rugged features to handle demanding applications.

As network needs change, customers need flexibility and a way to keep pace with evolving requirements. These new switches have been built to easily adapt through its field-exchangeable ports, whether the customer needs copper, fiber or Gigabit port options.

The GREYHOUND switch is available in two basic versions, with configurable options: 16 fast Ethernet TX ports; eight fast Ethernet TX ports, plus eight fast Ethernet small form-factor pluggable ports; or four optional Gigabit Ethernet combination ports in either configuration

The ruggedized switches have been specially designed to handle demanding electrical power generation and distribution applications, including new installations and retrofits of existing substations. The device also performs well in transportation and industrial automation applications such as railroad optical networks and traffic surveillance on highways.

Sercos/EtherCAT-Bridge

CANNON-Automata: A new Sercos/EtherCAT-bridge connects a Sercos master with KUKA robots. Now it is possible to connect Sercos and EtherCAT masters, and to exchange bidirectional data in real-time within heterogeneous, real-time Ethernet communication structures.

Using this approach, a Sercos master in combination with the mxAutomation library for CODESYS, can directly communicate with KUKA robots. The Sercos master can send very fast motion commands to the robot and receive and handle feedback values in real-time. The IEC-61131 programming languages can be used, so special know-how in robot programming languages is not required.

The Sercos/EtherCAT-Bridge operates on both busses as an I/O device. The width of the real-time data is flexibly configurable in the range of 32 to 2048 bytes and can be adapted to the needs of various applications. The exchange of real-time data between the two busses is supported by hardware and is executed within one communication cycle. In addition to the application-specific I/O, data information communicating status and diagnostic data for either the Sercos or EtherCAT bus can be transferred to the other side. This allows the two masters to react very quickly to changes of the communication state, or on error events.

Beside the real-time data channel the device also supports a bidirectional channel for acyclic data exchange. On the Sercos side this mailbox mechanism is represented by IDNs which are readable and writeable over the service channel. From the EtherCAT side the mailboxes are accessible over CoE objects.

The device uses DIN-rail mounting and provides two RJ45 ports. An additional RJ45 connector at the front side serves as a standard Ethernet port. Over this interface, devices can communicate with other devices connected using the respective mechanisms (UC channel and EoE protocol).

Making air travel more fun: Gear for frequent flyers

It seems that we are constantly in motion today. We are travelling to conferences, business meetings, trade shows, or vacations, and spend a lot of time in airports and on airplanes. Whether you are a platinum-status first-class passenger or typically fly crammed into seat 37b, these accessories will greatly improve your travel experience.

Peace and quiet

FOR MANY YEARS THERE WAS only one way to get some peace and quiet on an airplane: Bose QuietComfort headphones.

PHOTO: BEATS ELECTRONICS LLC.

Now there is an option from beats by Dr. Dre. The Beats Studio offers dual-mode Adaptive Noise Canceling (ANC). It automatically strikes a balance between your music and the world outside. If you only want to use the headphone to cancel external sounds, the ANC only mode increases the level of noise cancellation, for a quieter world.

At US$ 300 the Beats are as expensive as the Bose, but they make you look younger.

www.beatsbydre.com

Peace of mind

If you're prone to losing things while travelling, Tile will make your life easier. Tile is a coin-sized, square device that uses Bluetooth LE to communicate with nearby smartphones.

You can attach it to your key ring, put it into your wallet, stick it to your headphones or any other item that you want to keep track of. With the corresponding app you can track your Tile up to a 100 feet radius.

PHOTO: TILE INC.

Once the Tile tag is outside this radius, the app will remember the last known position.

Great if you discover that your laptop is still in the Lufthansa lounge when you are on the way to the gate, but what if your flight has already taken off?

All is not lost, because Tile also uses a a feature called Community Find: Every smartphone running the Tile app can find any misplaced Tile and report the location anonymously to the owner.

www.thetileapp.com

Personal hotspot

Slow, unreliable public WiFi can be a real nuisance, so why not pack your own personal hotspot?

Win a power pack

Extra battery power for all your essential travel gear. Enter our reader contest to win a 6000 mAh Mophie Powerstation Duo with dual USB outputs.

www.iebmedia.com/quiz

The winner will be announced March 19.

Contest sponsored by:

CC-Link Partner Association
G2A.CCLinkAmerica.org
CC-Link-G2A.com

With the Verizon Jetpack 4G LTE Mobile Hotspot you can connect up to 10 WiFi-enabled devices in 4G LTE coverage areas.

You can expect speeds of around 6Mbps in a radius of up to 50 feet.

PHOTO: VERIZON

A nice feature of the Jetpack is the status indicator, which shows not only signal strength and battery life (up to 8 hours), but also real-time data usage. This helps you to stay within the limits of your plan.

For international travels Verizon also offers a global version (model 6620L), which works with 4G networks in over 200 countries.

www.verizonwireless.com

Pack extra power

It's great to travel with smartphone, tablet, noise cancelling headphones, and personal hotspot, but all these devices need to be recharged frequently. We all know that batteries typically die when there is no wall outlet in sight, so it's a good idea to take a battery pack with you.

The Mophie Powerstation Duo is the Hoover Dam of portable power stations. At 6000 mAh it offers more than twice the capacity of your iPhone 6 battery. The rugged design features a protective metal outer band, and is compact enough (2.5" x 4.5" x 1") to easily fit into your briefcase or backpack.

Thanks to two USB ports you can charge your phone and tablet simultaneously. Or you can share a port with someone in need. A great way to make new friends while travelling.

www.mophie.com

Leopold Ploner

Your Gateway to Asia

Access markets closed to your current network strategy

You've implemented the local open network technologies in your products. But now it's time to look further afield. Chances are these technologies leave a large part of the Asian market inaccessible. So how can you also capture that? CC-Link is a market leading technology for open automation networking in Asia. Adding this connectivity can lead to a significant business increase in critical markets such as China. Our Gateway to Asia (G2A) programme offers a comprehensive package of development and marketing benefits to capture this additional market share.

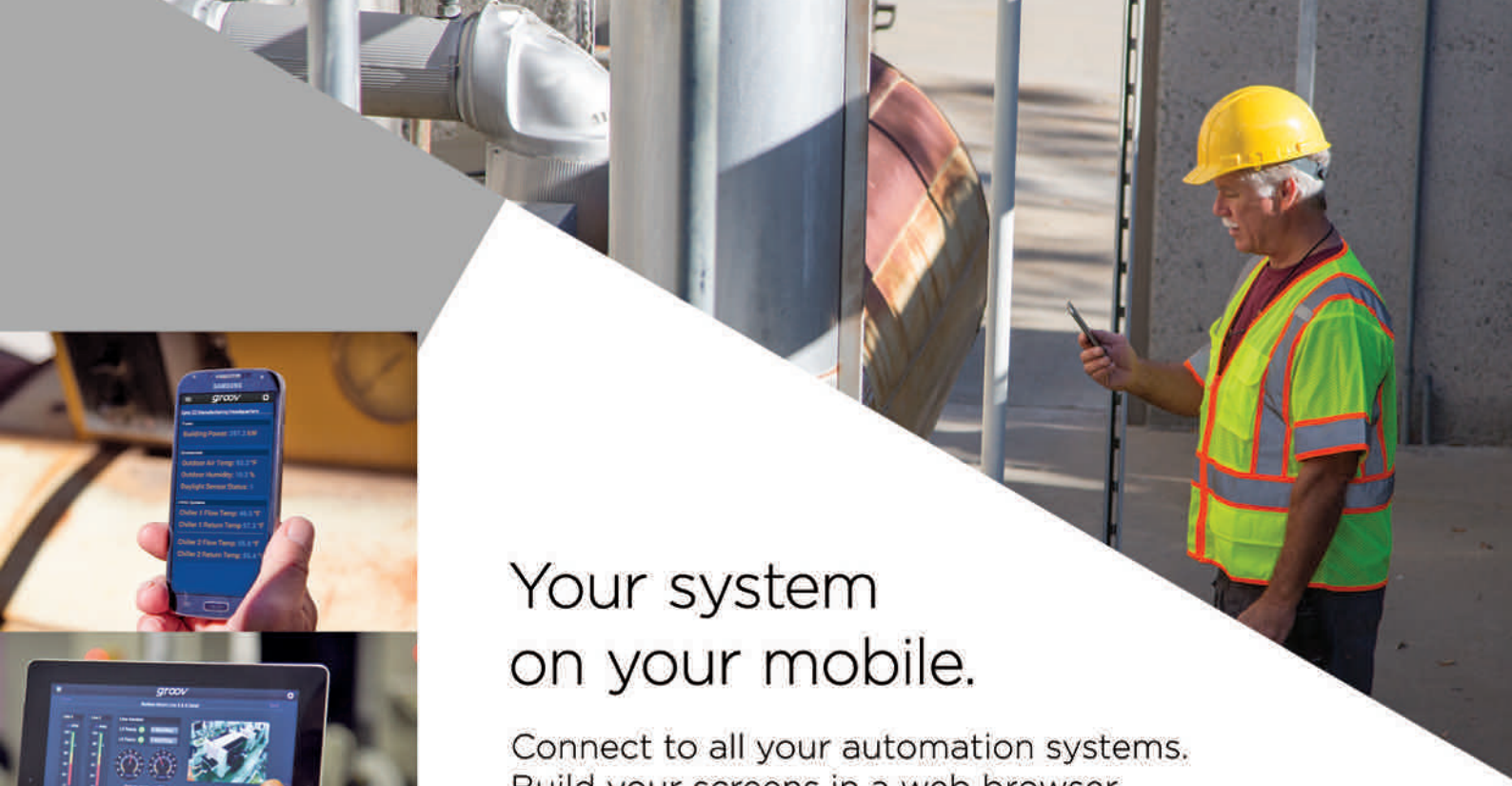
Interested?

Visit G2A.CC-LinkAmerica.org
Contact CLPA-Americas: info@CCLinkAmerica.org

Visit cc-link-g2a.com
Contact CLPA-Europe: G2A@CLPA-Europe.com

CC-Link CLPA PARTNER ASSOCIATION

CC-Link
CC-Link IE



Your system on your mobile.

Connect to all your automation systems.
Build your screens in a web browser.
View on your mobile devices.
groov on.

Compatible with:

OPC UNIFIED ARCHITECTURE

Modbus

See it now!
Visit op22.co/trial-demo
or scan this QR code.
Username: **trial** Password: **opto22**

Get the *groov* View app for free:

Available on the App Store

ANDROID APP ON Google play

MADE IN THE USA

Made and supported in the U.S.A.
Call us toll-free at **800-321-6786**
or visit **www.groov.com**.

groov from OPTO 22