7.2020 Issue 119
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking and IoT

Edge computing enables IoT technology solutions 7

FLEXEDGE™

GET EVERY LAST DROP FROM YOUR EXISTING EQUIPMENT.

Inefficient processes and wasteful operations can put a drain on the bottom line; but transforming your operation into a Smart Factory doesn't always mean costly capital investment.

FlexEdge™ Edge Automation Platform All-In-One:

- Protocol Converter : > 300 protocols for more than 1000 combinations
- Digitalisation of legacy equipment to current standards
- Easy edge programming with automation software Crimson®
- Modular network connection - cloud or on-premises, 5G ready

RED LION™
a spectris company

www.redlion.net

WWW.FLEXEDGE.NET OR EMAIL FLEXEDGE@REDLION.NET TO REQUEST A DEMONSTRATION

Importance of edge computing

Edge computing technology leverages the computer resources of the cloud—processing power, mass storage and networking technology—and brings it closer to the manufacturing floor, devices and users. It enables data to travel at high speeds without the requirement of travelling long distances to a cloud data center.

One debate about the viability of cloud computing in some applications is whether the data can be easily and cost effectively migrated to and operated in the cloud. Many have concluded that there is a need for alternative architectures to accommodate what can't easily be moved, and to simplify the integration process.

As a result, edge computing has found its own place alongside the rapidly expanding use of the cloud for all types of industrial computing and enterprise applications. The cloud is driving the profits of Amazon, Microsoft and even Google, to some extent, and we have only just begun to see its full impact.

According to a Cisco article on edge computing and 5G, edge computing and especially IoT devices will depend on network access to the cloud to receive machine learning and complex event processing models, for example. Likewise, these devices need network access to send sensor and status data back to the cloud. In an enterprise environment, many of these devices are already on SCADA networks and will continue to operate there.

"Many of these IoT devices will continue to use gateway and other aggregator devices to control the volume of data being sent to the cloud and the types of data. Many of these devices can be replaced without affecting existing IoT devices when 5G-ready versions become available."

On page 7 of this issue, Tom Kovanic of Panduit talks about the journey to the edge.

His conclusion is that edge computing may be a requirement in the wide deployment of IoT. The IoT requires responses in real-time, but deploying the compute and storage resources for IoT in the cloud may not support IoT because of network latency.

The solution to lowering latency is to move those resources closer to the IoT sensors that are providing the data, or expecting a real-time response.

If a company is thinking about deploying IoT, there is a need to think through the cloud and out to the edge.

The cloud itself is really the big story when it comes to the Internet of Things, and is an unbelievable success story already. But we've only just begun to gauge its impact, and edge computing will be an important factor for industry applications moving ahead.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2020**
Deadline for editorial: August 7, 2020 **Deadline for artwork:** August 28, 2020

Product & Sources Listing

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

Update your own products

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

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

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

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

First OPC UA companion specification for PROFINET

Standardized OPC UA object model for PROFINET enables devices from a wide variety of different manufacturers to transfer device data to asset management systems in a standardized way.

PROFIBUS & PROFINET INTERNATIONAL (PI) has published the first OPC UA companion specification for PROFINET. This specification describes a standardized OPC UA object model for PROFINET devices which enables PROFINET devices from a wide variety of different manufacturers to transfer device data to asset management systems in a standardized way, for example.

Standardization makes information collection significantly easier for tool manufacturers, regardless of the manufacturer, and is the beginning of PI's vertical integration strategy.

Many Industry 4.0 use cases are based on transferring data from the shop floor to IT systems or the cloud in the operating phase of a plant so it can be evaluated there. In the simplest case, this is device information like the serial number or firmware version of a device. It can go far beyond this, though, if it's possible to determine network or device diagnostic data, for example. In such cases, maintenance and diagnostic schedules can then be created or statements on availability derived. PI's goal is to define an open standard for PROFINET devices which specifies a very wide variety of information in standardized

SOURCE: PI

Companion specification can be downloaded from the PI and OPC Foundation websites.

object models so that they can easily be integrated by device manufacturers and used by plant operators and system integrators. Finally, it also reduces the effort and expenses involved in data collection.

When it comes to implementation, it doesn't matter whether the OPC UA server is located directly on the device or whether a higher-level edge gateway or controller is aggregating the data for multiple PROFINET devices. In each case, the user has a uniform picture of the information. Here, PROFINET benefits from the basic feature of additional TCP/IP channels being operable in parallel to the actual real-time traffic.

This initial specification represents the basis for subsequent, more far-reaching information models. The next goal taken on by the working group will be the modeling of energy management data in OPC UA based on PROFIenergy. Additional requirements are already being clarified now. The working groups are also working closely together on overarching OPC specifications like device integration and a base network information model.

The companion specification can be downloaded from the PI and OPC Foundation websites. More detailed information on vertical integration with PROFINET and OPC UA can be found on PI's newly redesigned web pages on Industry 4.

View website at: www.profibus.com/I40

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

OPC, ODVA & Sercos groups to develop OPC UA Motion

Cooperation to speed up Field Level Communications (FLC) initiative is backed by proven technologies from established organizations. The OPC Foundation, ODVA and Sercos International have announced a collaboration to develop a new generation of motion technology for industry. This new motion technology will be initially published as OPC UA Motion, with subsequent updates to the Sercos technology and the CIP Motion technology for EtherNet/IP.

This development will provide a flexible architecture for distributing motion control features between controllers and drives, based on a common information model for motion devices such as PLCs / motion controllers, standard drives / frequency converters, positioning drives, servo drives, motion encoders, motor starters, and power supplies.

To begin the work, a new OPC UA Motion Working Group (WG) was launched on May 18th. The new Motion WG is tasked with specifying the motion facet of FLC to enable inter-vendor operation for motion automation. Many well-known industrial automation manufacturers in the field of motion control are represented within this WG to ensure a uniform, worldwide, and coordinated standard for motion automation in discrete and process manufacturing. This new motion specification will use PubSub, with and without TSN network access, and can be combined with OPC UA Safety to support all relevant use cases for centralized and non-centralized motion solution concepts.

In order to provide end users with a best-in-class solution, the FLC Initiative selected motion solutions backed by proven technologies from established organizations: as a result, CIP Motion and Sercos specifications have been determined to be solutions on which to base OPC UA Motion. In turn, ODVA and Sercos International are committed to building upon their existing collaborations with the OPC Foundation and to providing end users of their technologies, EtherNet/IP and Sercos, with an expanded solution set as well as improved motion technology. The CIP Motion and Sercos specifications will be used and may be changed or extended for:

- Adaptation to OPC UA & FLC system architecture
- Innovation to cover Industrie 4.0 and digitalization use cases
- Modern concepts of data modelling and real time requirements

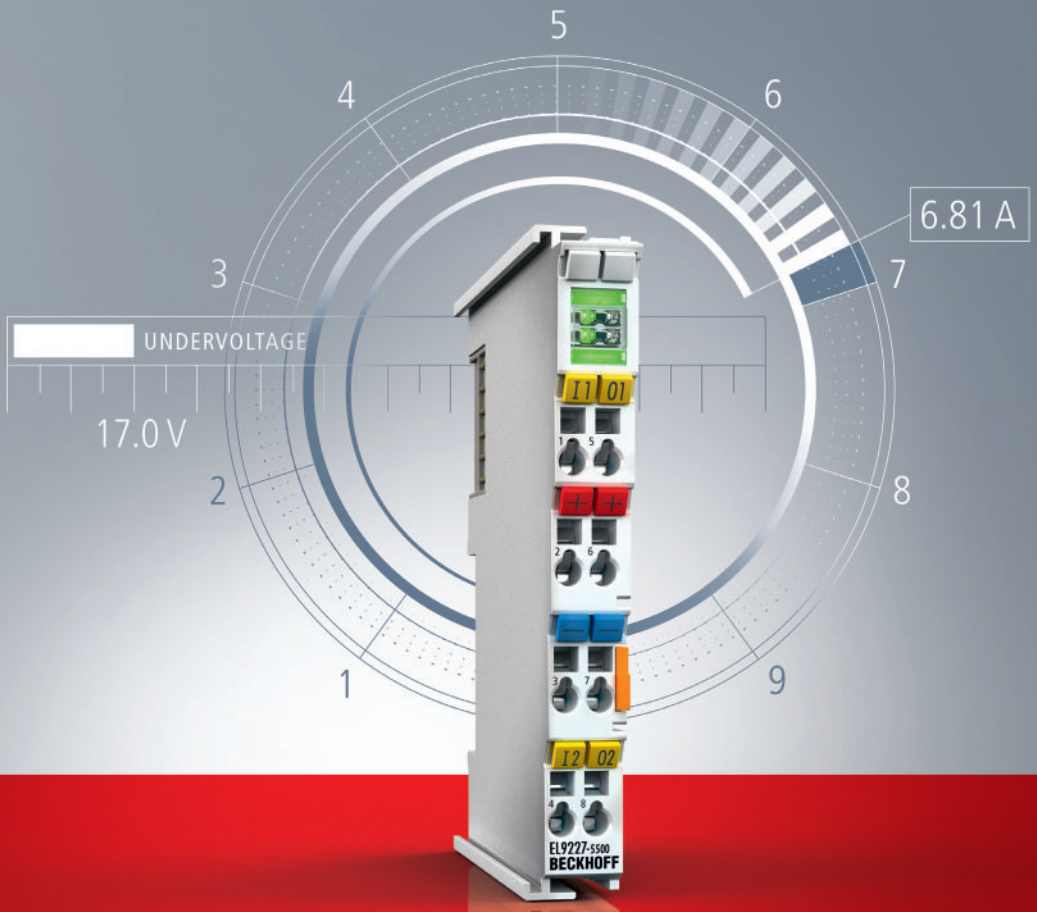
The FLC Initiative – with its Architecture & Infrastructure (A&I) and Safety Working Groups – aims to deliver a harmonized solution for motion automation applications including safe motion functionality. In addition, cooperation is planned with the existing VDMA/OPC Foundation joint WG for electrical power train systems.

News report by ***ODVA.***

[EK11-16E]

System-integrated overcurrent protection with EtherCAT interface

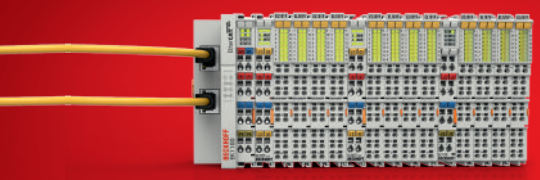
Extremely space-saving and flexibly usable



www.beckhoff.com/overcurrent-protection

In the EtherCAT Terminals from the EL922x series Beckhoff integrates the overcurrent protection for the fusing of 24 V DC systems – including EtherCAT interface – in a compact 12 mm. Transparent plant monitoring via EtherCAT is thus also directly integrated. The EL922x can supply both consumers outside the terminal network and further terminals inside it with a fused voltage – simply and conveniently. Virtually all typical requirements can be met through the individual settings. The range consists of a total of 19 different standard and high-line terminals with a particularly high number of analysis options.

EtherCAT



Direct overcurrent protection integration in the I/O system

HANNOVER MESSE

DIGITAL DAYS
14 – 15 July 2020
We're in!

New Automation Technology **BECKHOFF**

OPC joins Advanced Physical Layer (APL) project group

APL and its Field Level Communications (FLC) initiative is a critically important piece of technology in the strategy to expand OPC UA to all use cases and requirements in factory and process automation.

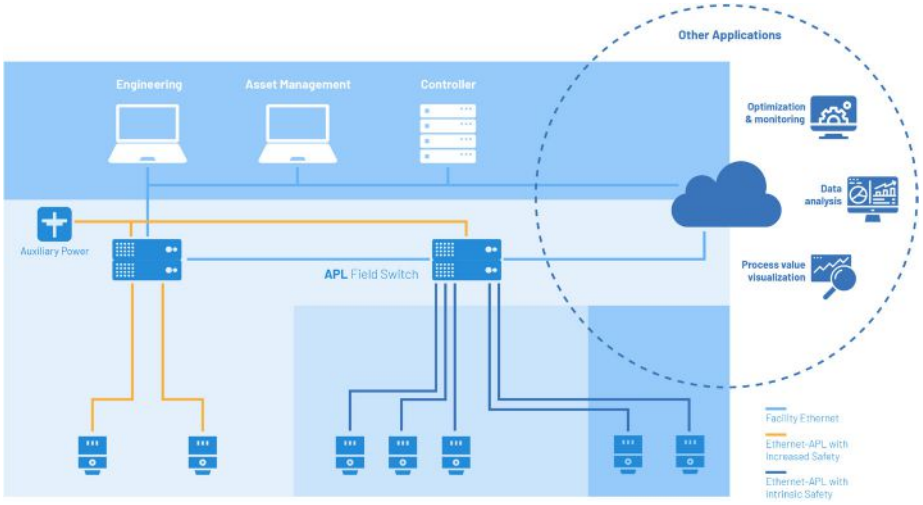
ETHERNET-APL, (ADVANCED PHYSICAL LAYER) has become critically important for the OPC UA field level strategy in process automation.

As a result, OPC Foundation announced that it has joined the APL project group in order to support the development and promotion of an advanced physical layer (APL) for Industrial Ethernet, suitable for use in demanding applications and hazardous locations in the process industry, named "Ethernet-APL". To date, the APL Project Group has consisted of 12 industry partners and the three leading fieldbus organizations in process automation: FieldComm Group (FCG), ODVA, and Profibus & Profinet International (PI).

Jörg Hähniche, Endress+Hauser and Chairperson of APL project group said: "We welcome the OPC Foundation. While the APL project is well advanced, we are even more pleased that OPC Foundation has joined the project. Their membership completes the cooperation, as all leading organizations are now working on one Ethernet Advanced Physical Layer solution which will be integrated into their respective specifications. This has an enormous customer benefit, especially since one Ethernet Advanced Physical Layer solution now fits many applications. By jointly cooperating, we hope to benefit from the many years of experience of OPC Foundation thus benefiting a wide range of customers."

The decision of the OPC Foundation to join the APL project group is closely related to their strategy to extend OPC UA to the field level in discrete and continuous manufacturing. For this, the OPC Foundation launched the Field Level Communications (FLC) initiative in November 2018, supported by an impressive list of major automation suppliers.

Stefan Hoppe, President OPC Foundation: "It is because of the broad acceptance, high flexibility, and vendor independence of OPC UA that various initiatives in the process industry, including NAMUR Open Architecture (NOA), the Open Process Automation Forum (OPAF), Module Type Package (MTP), and MDIS (Oil&Gas), rely heavily on OPC UA as the core technology to model devices from different vendors and exchange information between them. The extension to utilize APL as a transport layer is a logical progression – the combination of OPC UA with Ethernet-APL will be the future standard for many users in the process industry."



SOURCE: OPC FOUNDATION

A primary goal of Ethernet-APL is networking the entire automation pyramid.

Because of its versatility and manufacturer independence, OPC UA is already used today in many different industrial applications. However, OPC UA is much more than just a transport protocol in its traditional sense. Instead, OPC UA is an industrial, protocol-agnostic framework for the Industrial Internet of Things and Industrie 4.0 that contains mechanisms for secure, reliable, manufacturer and platform-independent information exchange, as well as options for semantic information modeling and self-description of devices. OPC UA scales from the sensor across all levels to MES / ERP and also into the cloud including cyber security mechanisms built from the start.

In order to meet all requirements for use cases from end users, suppliers, and integrators from process automation to factory automation, the FLC-related technical work includes the following topics:

- definition of an "Automation Component" with functions, interfaces and behaviors that are common to the different FLC-conformant devices used in various applications in process and factory automation
- definition of system behaviors and sequences for common functionalities e.g. bootstrapping, connection establishment, etc.
- harmonization and standardization of application profiles like IO, motion control, functional safety, system redundancy
- standardization of OPC UA information models for field level devices in online and offline scenarios e.g. device description and diagnostics
- mapping to subordinate communication protocols and transmission physics, such as TCP, UDP, Ethernet APL / SPE, deterministic Ethernet (TSN) with future mapping to 5G and Wi-Fi 6
- guarantee the best integration of OPC UA companion specifications like FDI, FDT, PA-DIM, ADI (Analyzer Device Integration), Module Type Package (MTP), and MDIS (Oil&Gas), VDMA pumps, UMATI, Spectaris, and so forth

Peter Lutz, Director OPC Foundation FLC Initiative said: "APL is recognized by the OPC Foundation and particularly its Field Level Communications (FLC) initiative to be a critical important piece in the strategy to expand OPC UA to all use cases and requirements in Factory and Process Automation, supporting the vision of a fully scalable, industrial interoperability solution, from sensor to cloud."

About Advanced Physical Layer

Ethernet-APL describes a physical layer for Ethernet communication technology developed for the requirements of process industries. The development of Ethernet-APL was determined by the need for communication at high speeds over long distances; the supply of power and communication signals via common single, twisted-pair (2-wire) cable; and protective measures for the safe use within hazardous areas.

www.opcfoundation.org/apl

Edge computing key driver for wider IoT deployment

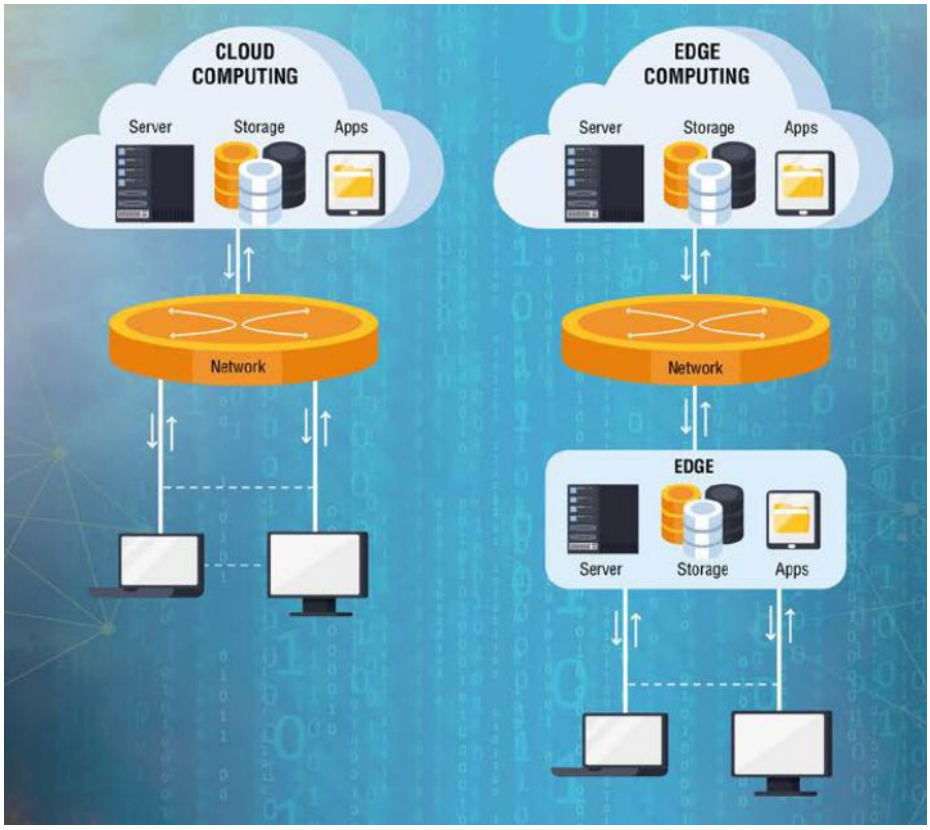
IoT applications require real-time response, but deploying the compute and storage resources for IoT in the cloud may not support IoT because of network latency. The solution to lowering latency is to move those resources closer to the IoT sensors that are providing the data, or expecting a real-time response.

THE INDUSTRIAL INTERNET OF THINGS HAS changed how industrial companies generate, collect, and analyze data, as new architectures extend the edge of the network to industrial devices, machines, controllers, and sensors. The end result is the edge computing and analytics are increasingly being located closer to machines and data sources, and the ability for data to be generated faster and in greater volume than ever before.

The cloud has taken a strong foothold in the IT world, and why not? You can add or remove computing and storage resources as needed and there is no need to worry where those resources are located. The cloud has its place. However, there is a downside: with the cloud you do not know where the compute and storage resources are located.

When it comes to the IoT, responding in real time to events is critical. With real-time applications, the amount of network latency in the system is critical; less is more.

You cannot manage latency if you do not know where the compute and storage resources are located. Not only do you not know where those resources are located, the location may change as the cloud provider balances its load among the servers within a data center. Even worse, the latency can change as the cloud provider moves those resources across its data centers. Edge computing can rescue network from too much latency.



SOURCE: PANDUIT

Edge computing offers the opportunity to provide a more secure environment regardless of how one would deploy.

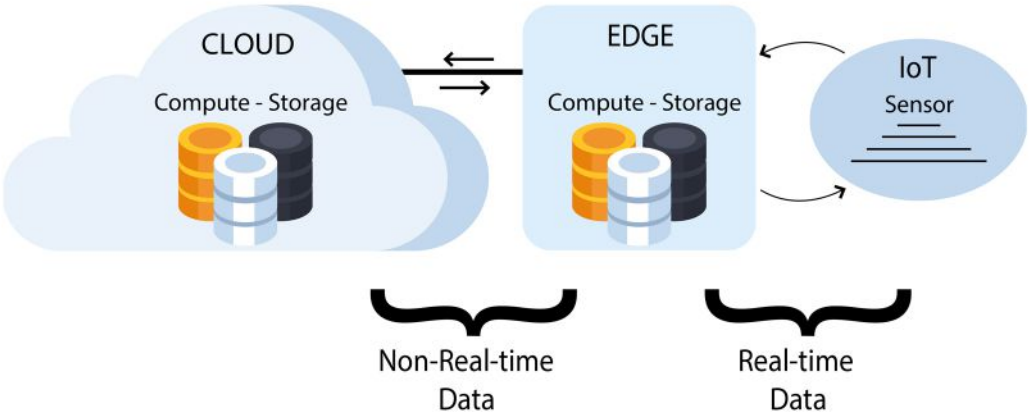
Edge computing

Edge computing is the opposite of cloud computing. With edge computing, the compute, storage, and application resources are located close to the user of the data, or the source of the data. This is in contrast to a cloud deployment where those resources are in some distant data center owned by the cloud provider.

Although edge computing may appear to be a new concept, it is just the computing pendulum swinging to one side of the computing continuum.

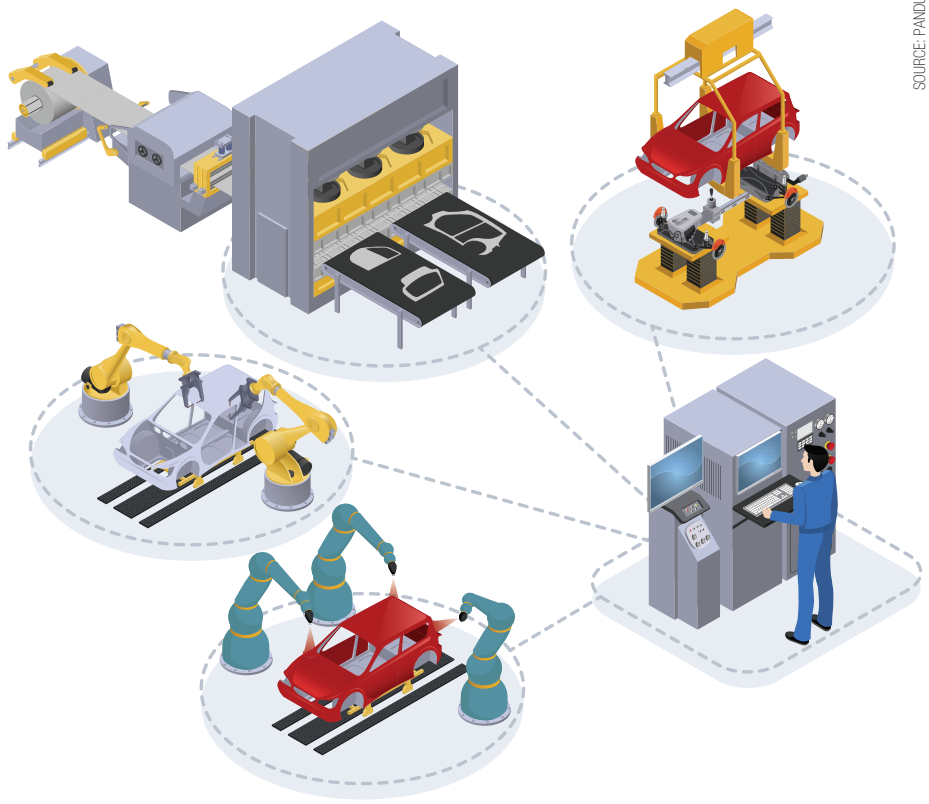
Computing started with the advent of mainframes in the late 1950s. Mainframes are an example of centralized computing; they were too large and expensive for one to be on every user's desk. In the late 1960s, minicomputers appeared, which moved compute power away from centralized control and into research labs where they controlled experiments, the factory floor for process control, and many other use cases.

The pendulum moved all the way to the distributed side with the arrival of the PC in the mid-1980s. With the PC, individuals had computing power at their fingertips.



SOURCE: PANDUIT

A first step toward implementing effective edge computing solutions is to identify the IoT applications that require a real-time response.



SOURCE: PANDUIT

The latency in an IoT deployment is the amount of time between when an IoT sensor starts sending data and when an action is taken on the data.

The computing pendulum swings back and forth, and today, it is swinging towards edge computing, which puts the processing and storage resources closer to where they are used and needed.

IoT deployments can benefit from edge computing in three ways.

Reduced network latency

The latency in an IoT deployment is the amount of time between when an IoT sensor starts sending data and when an action is taken on the data. Several factors impact network latency: the propagation delay through the physical media of the network; the amount of time it takes to route data through the networking equipment (switches, routers, servers, etc.); and the amount of time it takes to process the data.

Let's say that the distance between an IoT sensor and the data center that needs to process that data is 2,300 miles (3,700 km) apart. That is roughly the distance between Cleveland and Lake Tahoe. The speed of light in a typical single mode optical fiber is approximately 4.9 µs/km, therefore, the round-trip delay would then be 36mS. Adopting edge computing and locating the processing and storage resources in Cleveland would make the round-trip delay almost negligible. Additionally, the data would travel through fewer routers since it would not have to make a cross-country trip, and the possibility of the data packets being corrupted would be far less.

Reduced network jitter

The jitter in a network is the variation of latency over time. Some real-time IoT applications may not be tolerant of network jitter if that jitter causes the latency to lengthen such that it prevents the system to act in the required time frame.

Cloud-based applications are inherently jittery. At the data center level, the required resources for an IoT application can be moved from one server to the other, changing the latency. In addition, while the applications are being moved they will be unavailable. At the macro level, the applications could be moved among the cloud provider's data centers, which would have an impact on latency and, therefore, jitter.

Edge computing provides reduced jitter because the computing resources and storage are in a fixed location that does not move, or if they are moved, it is to a platform near the original location. Additionally, the network is generally a fixed path, which means repeatable latency. Another issue with the cloud is that one most likely accesses the application using the Internet, which is inherently jittery. The Internet was designed to be resilient.

It will automatically route packets around downed network links and unavailable routers. One can send two consecutive packets out onto the Internet, and they could take two different paths to the destination and, therefore, be subject to two different time delays. In fact, the second packet that is sent could be the first one that arrives.

SOURCE: PANDUIT

When deploying edge computing applications, there is a need to decouple the real-time performance requirements of the system from the cloud.

SOURCE: PANDUIT

As digitization moves ahead, so does analysis, decision-making, and control being physically distributed among edge devices, the network, the cloud, and connected systems.

Enhanced security

Edge computing offers the opportunity to provide a more secure environment regardless of how one would deploy: co-location or directly owning the equipment. Co-location facilities are physically secure locations. If one owns the edge computing equipment, it can be in the factory where the IoT sensors are located or in another company-owned facility.

"The IoT is changing the way industrial organizations generate, collect, and analyze data, as IoT extends the edge to industrial devices, machines, controllers, and sensors. Edge computing and analytics are increasingly being located close to the machines and data sources, enabling data to be generated faster and in greater volume than ever before," according to Craig Resnick, vice president, ARC Advisory Group.

"Besides providing control, these edge devices will securely collect, aggregate, filter, and relay data, leveraging their proximity to industrial processes or production assets. This data will be analyzed by powerful analytics tools, which will detect anomalies in real time, and raise alarms so that operators can take appropriate actions. As IoT and the digitization of industrial systems proceeds, so does analysis, decision-making, and control being physically distributed among edge devices, the network, the cloud, and connected systems, as appropriate."

What to consider?

When deploying edge computing, there is a need to decouple the real-time requirements from the cloud.

The first step toward implementing an effective edge computing solution is to identify the IoT applications that require a real-time response. These are the applications to consider when deploying on the edge. The remaining applications can run in the on-premises data centers or in the cloud.

This turns the cloud into a type of historian for the IoT-gathered data. It receives non-real-time data that can be processed, analyzed, and stored in a time frame that meets the business's needs.

Harsh environment

The ideal location for the shortest network latency may not be the ideal choice for environmentally delicate equipment and cabling. It may be that the best place to locate the edge computing resources is on a harsh factory floor.

This might necessitate ruggedized compute and storage equipment, but may impact the networking infrastructure as well. Electromagnetic interference (EMI) may also be a part of a harsh environment. This might require using shielded copper cabling which has improved immunity to EMI, or using fiber optic cabling which is completely immune.

One thing to consider would be deploying environmental sensors to monitor the environment in proximity of the edge computing equipment.

Space constraints

The edge computing solution may need to be deployed in a location that is space constrained. This would lead one to deploy a high-density network infrastructure, such as a fiber enclosure that can accommodate 72 duplex LC ports in 1 RU of rack space.

Depending on the mix of copper connections versus fiber optic connections, one may opt for a lower density enclosure as it can support both copper and fiber connections within the same space.

Security

The ideal location for the edge may not be secure. It may be in a remote location where there is no surveillance or on the factory floor where there might be opportunities for unauthorized entry. In both cases, and in others, consideration should be given to how to manage access. There are a range of choices from key card entry readers, numerical keypads, and remote access control.

The journey to the edge

Edge computing may be a requirement in the wide deployment of IoT. The IoT requires responses in real time, but deploying the compute and storage resources for IoT in the cloud may not support IoT because of network latency.

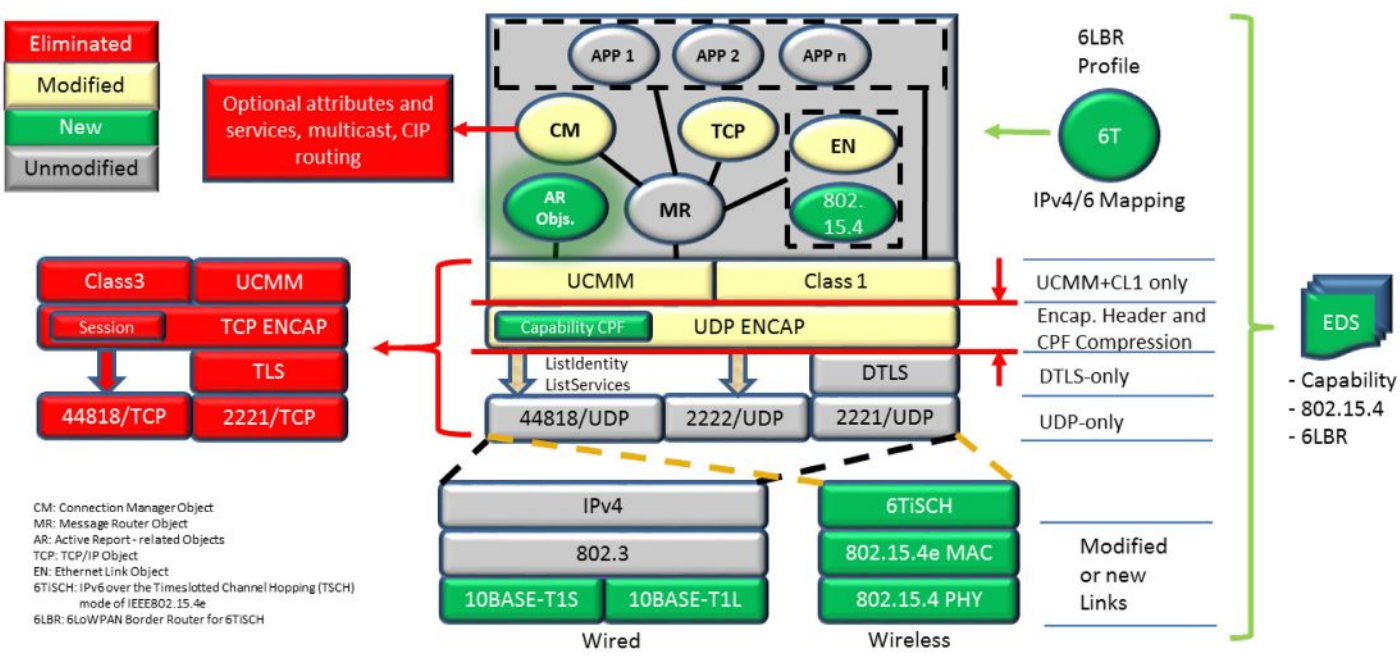
The solution to lowering latency is to move those resources closer to the IoT sensors that are providing the data, or expecting a real-time response.

If a company is thinking about deploying IoT, there is a need to think through the cloud and out to the edge.

Tom Kovanic, Business Development Manager, R&D – Strategic Growth, ***Panduit.***

Single-Pair Ethernet for constrained devices

Single Pair Ethernet offers reduction in wiring, node cost, size and power consumption, delivering communication and power over a single pair. New operational concepts are being developed to drive EtherNet/IP deployment to low-end constrained, in-cabinet devices such as contactors and push buttons.



SOURCE: ODVA

Figure summarizes the constrained EtherNet/IP proposal. Features in red are eliminated. Features in green are new additions. Features in yellow are modified (reduced).

A NEW SET OF OPERATIONAL CONCEPTS and technologies are being developed to drive successful EtherNet/IP deployment to many low end constrained devices or "Things" such as contactors and push buttons. This development could help enable a single-network vision where all devices in an industrial plant can communicate with the same set of protocols, while balancing node cost, node size, and ease of commissioning the smart system.

Industrial Ethernet has exhibited rapid growth, with EtherNet/IP emerging as a leader. The reality is that fieldbuses and sensor networks still retain a large position and many potential network nodes remain hardwired. End users understand and seek the advantages of a harmonized network based on EtherNet/IP, and the related open ecosystem. Benefits include reduced complexity and cost by minimization of gateways and elimination of hardwiring, expansion of the qualified labor pool, and improved optimization and maintenance opportunities via Cloud connectivity and analytics.

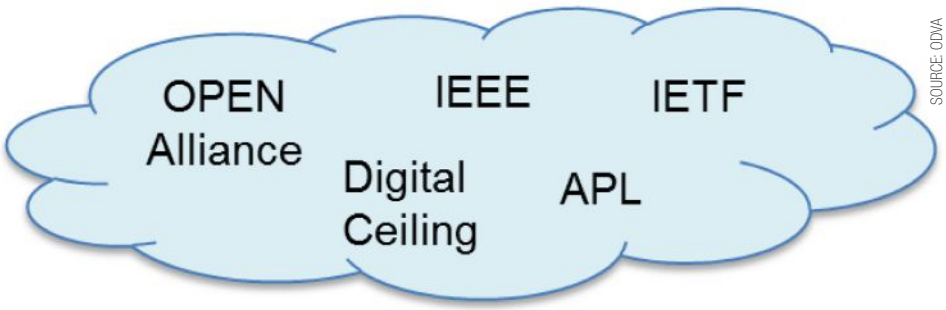
With these benefits numerous industries have flooded into IEEE to develop enhancements for enabling Ethernet to displace other networks at the edge. The resulting Single Pair Ethernet suite offers reduction in wiring, node cost, size, and power consumption, delivering communication and power over a single pair.

A deterministic Ethernet bus variant targets very constrained devices, such as in-cabinet components. In prior years, we proposed a set of enhancements, adopted from or inspired by IETF and IEEE, to extend EtherNet/IP into constrained applications, further enabling the single network vision.

With an operational concept and IEEE P802.3cg, the current standard and probable follow-on for T1S PHY specification upgrades will expand the market for PHYs, SIG work in the EtherNet/IP System Architecture Special Interest Group and EtherNet/IP Physical Layer Special Interest Group covering UDP-only, capability discovery, profile concepts and modular additions of PHYs, cables, connector, and profile concepts.

The single network vision

Many end users understand and are seeking the advantages of a harmonized network based on Ethernet, Internet Protocol (IP), and the related open ecosystem. This desire



SOURCE: ODVA

Organizations promoting expansion of Ethernet and/or IP at the edge.

is expressed within organizations across many industries.

The Automotive industry has been working toward an all-Ethernet vehicle. The industry formed the OPEN (One Pair EtherNet) Alliance to promote a variety of Single Pair Ethernet (SPE) solutions. Ethernet now pushes to the edge to displace other networks in the vehicle.

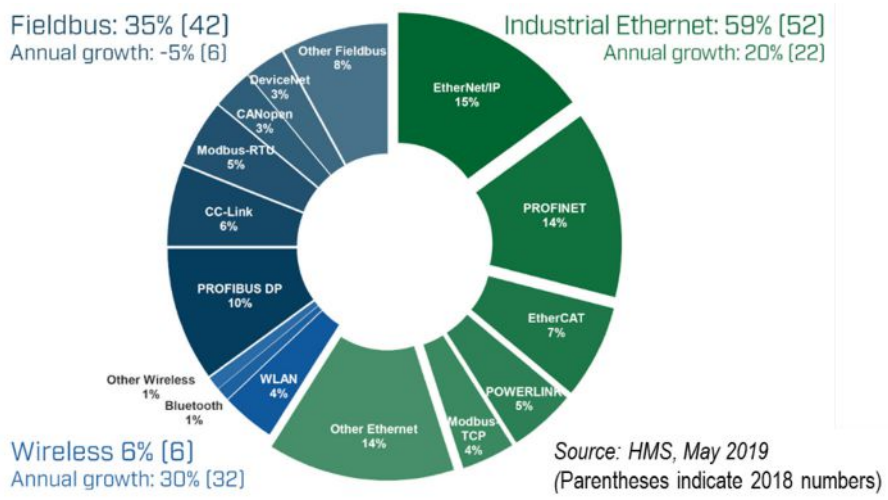
The Digital Ceiling partner ecosystem is promoting Ethernet-based smart LED lighting and associated sensors for occupancy, security, etc.

Process Automation end users (NAMUR) demanded Ethernet and IP-based automation protocols for instruments and related devices. The Advanced Physical Layer (APL) organization, including ODVA and their peer organizations are responding with solutions.

IEEE continues to extend the standards for Single Pair Ethernet (SPE) to meet the specialized needs at the edge.

These initiatives exist due to compelling advantages of a single network:

- Higher performance for a similar cost (compared to the displaced networks)
- Elimination of application-level gateways
- Leverage of a large existing ecosystem (protocols, security, network switches, etc.)
- Reduced installation, maintenance, and management complexity



SOURCE: ODVA

Industrial Ethernet solutions have been growing. Fieldbus and sensor networks form a shrinking portion.

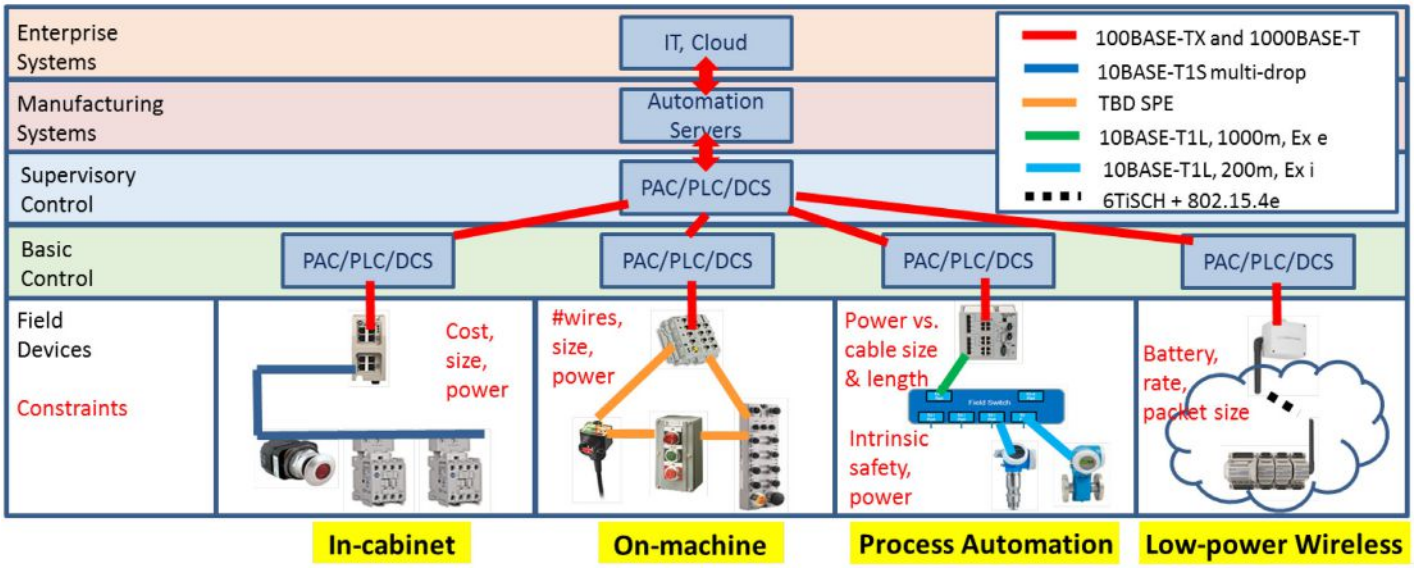
- Simplified integration with cloud applications
- Reduced interoperability issues

IEEE contributions

Within IEEE, a family of Single Pair Ethernet (SPE) standards has been developed. These enable communication and optional power over a single pair, facilitating reduction in wiring, node cost, size, and power consumption.

Early SPE standards included 100BASE-T1 (100 Mb/s), 1000BASE-T1 (1000 Mb/s), and optional power known as PoDL. In February of 2020, another family member was released: IEEE Std 802.3cg-2019. The new standard introduces a pair of 10 Mbit/s SPE PHYs that are targeted for constrained applications. Numerous industries sought Ethernet enhancements to displace edge networks and contributed to the standard.

IEEE Std 802.3cg-2019 includes the following 2 PHYs.



SOURCE: ODVA

Candidate constrained application areas for EtherNet/IP.

10BASE-T1L:

- Addresses long distance
- Targeted at process instruments
- 1000 m, intrinsic safety compatible, legacy wiring

10BASE-T1S:

- Addresses low cost control
- Targeted at replacing: CAN, CAN FD, MOST, and FlexRay protocols in automotive; Hardwired components for in-cabinet industrial automation; I2C and SPI in data centers
- 25 m multidrop option
- Determinism by PHY-level Collision Avoidance (PLCA) protocol

Constrained EtherNet/IP applications

Several new application areas are being targeted for EtherNet/IP at the network edge. These are constrained applications for field devices. From basic control, up through the enterprise, 100BASE-TX Ethernet and emerging 1000BASE-T Ethernet is suitable and likely to remain in place. At the field level, these are not well suited to meet the listed constraints.

Constrained EtherNet/IP application areas include Process Automation and the related application area of Low-power Wireless. They also include On-machine components. Each has unique constraints.

Another important application is In-cabinet components. Here the transition is primarily from hardwiring to networked devices. Very strict constraints exist for low cost, small size, and low power.

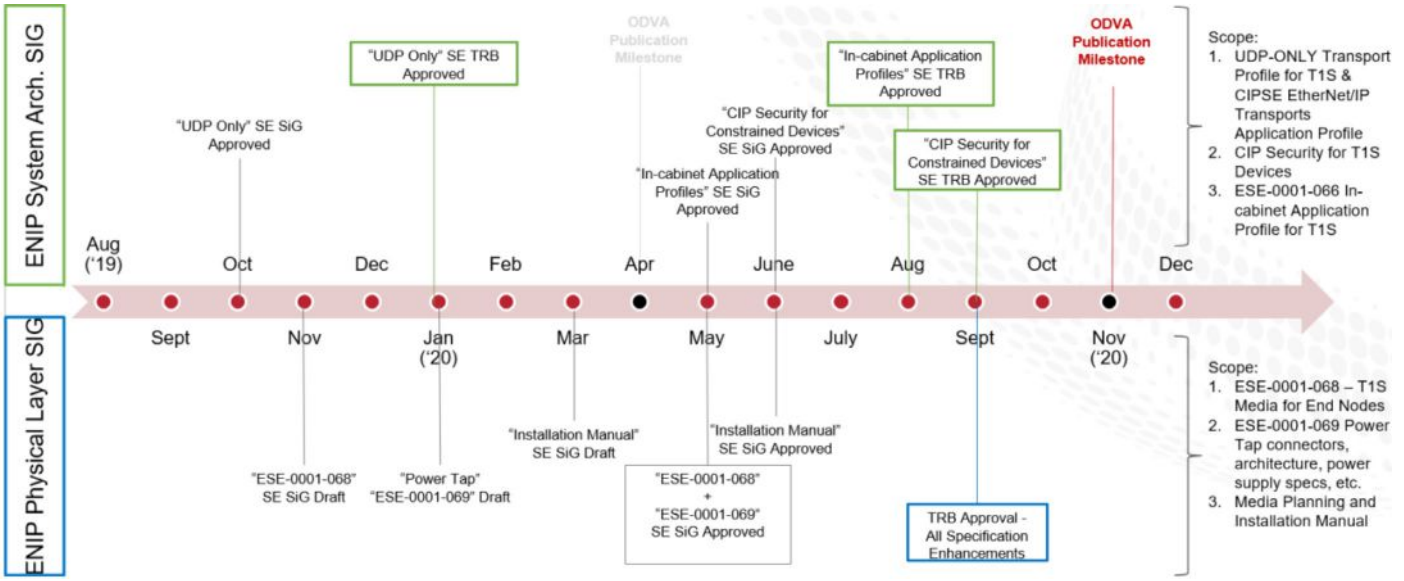
Constrained in-cabinet devices

The following section covers the Constrained In-Cabinet Device viewpoint and describes how the Single Pair Ethernet technology can be applied in this space.

The amount of control power (24VDC) wiring required to control pilot devices (such as push buttons, indicator buttons, contactors, etc.) is substantial. The wired connections, typically referred to as "hard wired connections", supply control power to the pilot devices for operation.

The number of wires for a simple in-cabinet application would require numerous hours for commissioning and is error prone if needed to be replicated.

Once commissioned, "hard-wired" systems for industrial applications create a high overhead for maintenance including, component updates or troubleshooting errors during operation or commissioning process while providing little to no intelligent data for analytics.



SOURCE: ODVA

ODVA SIG technical development group proposed timeline.

Constrained in-cabinet requirements

Based on the constrained in-cabinet device problem space, following are extracted key customer requirements based on extensive customer listening sessions:

Economical

- Low cost media
- Allow for a reduction in price and size of typical products
- Allow the use of commercial off-the-shelf power supplies
- Result in a lower "total cost of ownership" than hard-wired solutions

Simple to use

- Single easy to use media connector
- Simple (or no) network commissioning methodology
- Eliminate the need for media trunk and drop distance calculations

Just Enough Functionality

- Must simplify In-Cabinet wiring for panel builders
- Must deliver both Network Power to power device electronics and Switched (Control) Power to facilitate the actuation of Contactors and Relays
- Must support Non-Safety and Safety devices on the same wire

SPE for in-cabinet devices

Single Pair Ethernet consists of multiple technical speeds and topologies, reference Constrained EtherNet/IP application areas. To match customer needs of just enough functionality, ease of use and low cost, 10BASE technologies would suffice, namely 10BASE-T1S.

Following are key technical characteristics of 10BASE-T1S that could be leveraged in the development of in-cabinet applications:

- Low Power ~250mW, with in-cabinet applications, the thermal dissipation of devices is constrained.
- Lower Cost, as most of the target pilot devices are low cost, the communication interfaces to such devices would need to be low cost to maintain commercial acceptance of this solution.
- Constrained Ethernet (UDP only), with a small physical footprint of pilot devices, typically there are physical constraints to the package size of the electronics deployable in this solution, hence, a constrained Ethernet stack to reduce the memory requirements.
- 10Mbps ½ duplex, since the end nodes are typically are pilot devices, system performance measures, such as communication speed, can be a chosen to be minimum, following the IEEE 802.3cg 10BASE-T1S Specifications.
- Media to be a Multi-conductor cable, 25-meter cable length, Multi-Drop topology to help the Constrained In-Cabinet problem space to reduce the total commissioning time, providing a level of ease of use in adopting this solution.

Technical architecture

1. A Multi-conductor flat cable connecting multiple devices delivers power (switched power and network power) in a multi-drop topology which enables 10BASE-T1S communication.
2. 4-wire Ethernet connection to a controller.
3. The overall system is powered by a 24VDC power supply. There are two power channels defined: NP (Network Power) and SP (Switched Power). NP power is used to power the communication circuit of the whole network. SP power is utilized for all the output loads (contactor control coil, sounder, etc.)
4. Gateway provides power for both NP and SP channels.
5. SP Tap is required to inject new SP power to the system when Gateway is not capable of providing SP power for all the loads.

Proposed timeframe

ODVA SIG Proposed Timeline highlights a timeframe of activities to publishing a complete specification for Single-pair Ethernet for Constrained In-Cabinet devices.

Definition of the communication protocol and related specification is being defined by the ODVA ENIP System Architecture Special Interest Group, focused on delivering 3 ESEs pronouncing the UDP only Transport profile for T1S (currently to be published April '20), CIP Security for Constraint In-Cabinet Devices and Constrained In-Cabinet Application profile for T1S.

Definition of the media is conducted in the ENIP Physical Layer SIG, which is focused on delivering 3 ESEs, pronouncing the cable and connector specifications, the SP Tap connectors and grounding specifications and the Media Planning and Installation Manual.

EtherNet/IP media

The proposal is for a mixed gauge 7 conductor cable:

- Two conductors for Switched (Control) Power to actuate contactor coils
- Two conductors for Network Power to power device electronics
- Two conductors for SPE Signal Pair for T1S based PLCA Multidrop Ethernet Communication
- One conductor for Select Line for simple sequential network service delivery to discover linear nodal topology.

Wire gauge:

- 20AWG wires (19 strands) for NP-, NP+, SP+, SP-
- 24AWG wires (7 strands) for SPE+, SPE-, Select Line

Keying feature:

- SPE data pair and Select line conductors will be used as keying feature to minimize chance of wrong connector orientation.

Data pair Impedance:

- 100ohm, insulation voltage: 600V.

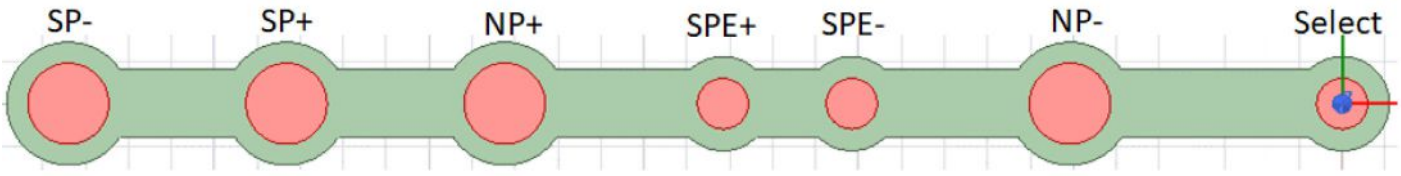
Media interface

A node connector with 8-pin receptacle interfaces with headers of the constrained devices. The pin header has standard 2.54mm pitch, 0.635mm X 0.635mm square pin.

- 8 pin single row header, 8 pins populated, each pin can carry current greater than 2 Amps
- Connector shall be connected to and make an electrical connection with the media using standard or no tools
- Connector shall break Select line and then establish connections to Select_A and Select_B pins
- Connector may break both SPE+ and SPE- lines and add inline inductors for improved signal integrity.

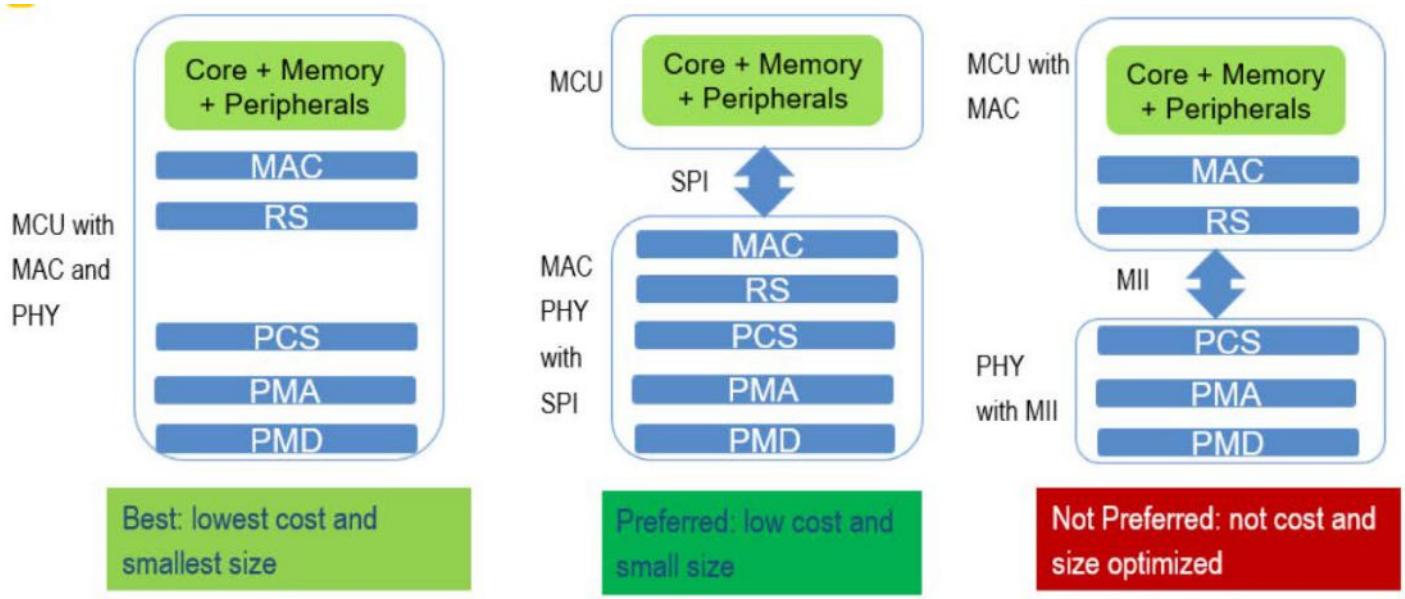
SPE 10BASE-T1S PHY Requirements

Working with different semiconductor vendors for early 10BASE-T1S PHYs, there are three options.



SOURCE: ODVA

Design of conductor cable.



SOURCE: ODVA

Data transmission communicates from an automation system to a cloud system for further analysis.

Option 1 is PHY with MII interface, which will require MCU with MAC and RS built in. This is not a preferred option since MCU with MII interface tend to be a lot more expensive than what the constrained in-cabinet device can afford. More than 16 signals need to be routed between PHY and MCU, therefore requires more board space.

Option 2 is PHY with SPI interface with integrated MAC and RS. This will only require a MCU with SPI interface. This is a preferred option since MCU with SPI interface tend to be a lot less expensive and is the target MCU for constrained in-cabinet devices.

Standard organizations are working on standardizing SPI interface for 10BASE-T1S PHY and we have learned from semiconductor vendors that the SPI PHY will be available in 2020.

Option 3 is PHY and MCU integrated on a single chip. This will greatly reduce the overall package size and could potentially offer the lowest cost option. The challenge is to come up with a part that has right mix of processor power, memory footprint and security features, which can be adopted by the mass market.

SPE 10BASE-T1S media/hardware

Cable Sample: Impedance at 104ohm, Insertion loss of 6.7dB @40MHz for 25meter

Connector Sample: Insertion loss of 0.1dB@40MHZ return loss of 33dB@40MHz, breaking both SPE+ and SPE-lines, 36nH in-line inductors are built-in.

T1S hardware: Evaluation boards with T1S PHY compliant to IEEE 802.3CG draft 2.1, MII Interface Integrated PLCA functions

System Evaluation Results

- Multiple setups were evaluated to determine the number of nodes that can be supported with T1S hardware, cable and connectors.
- 40 total nodes; master node 0 at the beginning of 25meter cable, node 1 in the middle of the cable, 38 nodes lumped at the end of the 25meter cable
- Conducted BER test with no bit errors.
- Measured eye height at nodes and matched simulation results.

Communication profile & stack

Current EtherNet/IP communication does not support constrained device and network requirements.

It is proposed to develop a constrained EtherNet/IP communication profile. Note that this differs from the concept of a device profile.

The minimum device object model uses the same base objects for constrained EtherNet/IP but minimizes the implementation of the base objects. There are minimized CIP transports over UDP, supporting only UCMM + Class 1.

As part of reducing the overhead in a device, the objects are minimized by limiting the optional features. The Connection Manager is an example. Attributes and services are minimized. The communication methods are minimized. The simplifications still retain the required interoperability.

The application profiles that a device supports are reported via the Application Profiles attribute 25 of the Identity object. Chapter 11 has been proposed for Volume 2, EtherNet/IP Adaptation of CIP to define the EtherNet/IP Transports Application Profile. The new EtherNet/IP Transports Application Profile defines the "Full" and "UDP-Only" transport profiles.

The Full EtherNet/IP transport profile specifies the use of TCP and EtherNet/IP encapsulation sessions for CIP connection management and connected explicit messaging, and UDP transport protocols for implicit message transmission.

The UDP-Only EtherNet/IP transport profile specifies the exclusive use of UDP for the transmission of all CIP messages. This profile, since TCP is no longer required, results in a simplified EtherNet/IP stack.

A new "EtherNet/IP Capability" CPF item is propose, this new CPF item will use the EtherNet/IP Transports application profile data. The EtherNet/IP Capability" CPF item has been added as a valid item to the ListIdentity response. This allows discovery of a constrained device's EtherNet/IP capability using ListIdentity.

Paired with this is a new EDS entry to describe constrained device's EtherNet/IP Capability. The following is the define on the new EtherNet/IP Capability" CPF item:

The new EtherNet/IP Transports Application Profile definition allows the combinations of supported features.

The simplification of the communication of an UDP-only device eliminates the TCP connections and the encapsulation sessions and this will reduce the complexity of the communication stack.

Since CIP Security requires both TLS and DTLS, we also propose to add optional support for into the EtherNet/IP adaptation for DTLS-only. Proposed additions to Volume 8 CIP Security will allow devices implementing the UDP-only EtherNet/IP transport application profile, DTLS is used for all CIP communications sent in a CIP Security context.

David Brandt, Engineering Fellow, Advanced Technology, Chirag Malkan, Senior Manager, Advanced Engineering, Tony Wang, Senior Project Engineer, Electrical Engineering and Jeff Martin, Project Engineer, Firmware Engineering, ***Rockwell Automation.***

Supporting a sustainable mode of transportation

A modern radiolocation solution helps the operator of the subways in Oslo, Norway to provide a high-performance and attractive offering. In recognition of the city's efforts towards a sustainable way of life. public transport and the subway as an alternative to a car, represents an important pillar of the concept.

SOURCE: SIEMENS

Public transport systems form the backbone of individual transport in Oslo – and the T-Bane has a substantial part in it.

THE "T-BANE" TUNNEL RAILWAY IS WHAT the people of Oslo call their subway, although just 17 out of the 101 stations are actually underground. The 115 trains operated at present carry almost 350,000 passengers daily on a rail network spanning 86 km.

In order to achieve the ambitious climate goals of the city of Oslo – reduce CO2 emissions by 95% by 2030 and in doing so becoming a car-free city – the subway network makes a significant contribution. Notwithstanding the achievements made so far, Sporveien, the subway operator, cannot rest on its laurels: Because if the residents of the Norwegian capital are to do without the car, they need an attractive and increasingly powerful alternative – like the T-Bane.

For years, the city, transport association, and operator have been investing in the climate-friendly expansion of the subway network. The train fleet has been undergoing modernization since 2007 and today is entirely equipped with white, energy-efficient trains of the MX3000 series from Siemens. New lines and stations are planned and being implemented, such as the new Løren station on Line 4, which was opened to traffic in 2015. Sporveien is currently working on increasing train frequency through the central inner-city tunnel, which is shared by all lines: In the future, 9–10 trains per 15 minutes are to be able to pass through the bottleneck, which means a capacity increase of up to 25%.

Digitalization in the workshops

Behind the scenes, too, the modernization of the subway system is being spurred on. Digitalization is the motto here to automate planning processes, reduce failures, improve flexibility, gain higher efficiency and decrease response time.

Numerous digital systems are already in use at Sporveien – e.g. digital timetable and digital maintenance records for the trains. However, digital systems can only process the information that is fed to them. Posing a potential problem here, were the depots and the manual processes around parking-lot planning and physical parking of trains. Previously, there used to be more manual work-processes in the depots – much due the position of the trains could not be automatically synchronized with the digital workshop system.

Manual effort, hectic phone calls, and unnecessary searches were part of the daily routine of the employees, which caused some process-inefficiency getting the rolling stock ready. In particular, the manual search processes, picking out the specific train at the correct time, did cost time. Valuable service-time elapsed quickly if an employee in the depot had to walk around in the yard searching for a specific train.

A real-time locating system Simatic RTLS from Siemens now helps to put things right. In order to do so, all trains were equipped with transponders and antennas, which can continuously and fully automatically be located via so-called RTLS gateways. To this end, the transit time of the radio signals to the transponders is determined and compared between different gateways – within fractions of a second.

All information is fed into the visualization in the workshops of Sporveien via the Simatic Locating Manager and combined with other systems, for example, the maintenance planning for the trains. Employees can now see the positions of each train in each depot on large displays and retrieve all other necessary information (What is to be done? When must the train be back on the line? When is the next service due?).

Locating supplies with real-time data

This transparency is already an important advantage of the locating system for Christian Grønnerød, RTLS product manager at Sporveien. "Just the visualization of the train movements in the depots and the combination with all other systems make the work considerably easier. Instead of through a variety of programs, paper documentation, and phone calls, employees now have everything at their fingertips and with just a few mouse clicks get what they need to perform their job!" said Grønnerød.

But that is not all. The improved and accurate planning and provision of the trains means that the service intervals can be maximized – which improves fleet utilization and reduces costs. Also, solving any breakdowns is greatly simplified, because it can be seen at a glance which train is present in which depot. And the project team is already thinking about more ideas – as you know, appetite comes with eating.

The first ideas for the introduction of RTLS go back to 2017. Initial proof-of-concept tests showed early on that the Siemens solution is particularly well-suited to the requirements of Sporveien. First of all, the possibility to operate Simatic RTLS from Siemens both indoors and outdoors spoke in favor of the system. The system scalability, too, is an important advantage: Thus, the implementation in the project can be carried out step by step, while still gaining experience early on in actual operations.

Last but not least, the special industrial suitability of the components is a decisive argument: Antennas and transponders are sufficiently robust for daily use in trains subject to temperature fluctuations and vibrations, and the interfaces of the transponder allows feeding of signals from the trains (direction of travel, coupling status). There are now approximately 250 gateways in use, and each train is equipped with two transponders and antennas (at each driver's cab).

Optimal project progression

As project manager of Norwegian consultancy company Bouvet, Bjørn Stokkeland was responsible for the introduction of Simatic RTLS. In addition to selecting the technology supplier, numerous other aspects had to be clarified – ranging from the conversion of the trains to the IT interfaces.

Thanks to a clear expectation of results and an agile approach with defined project sprints, the actual implementation could be completed in just a few months. And that even though several partners were involved in the project: Siemens supplied the RTLS technology and equipped the trains with transponders and antennas, and a local company installed the infrastructure in the depots. In addition, Bouvet took the role of a software system development partner of Sporveien, developing the tool that handled the visualization and system integration.

SOURCE: SIEMENS

On large displays, employees can retrieve all the data for each vehicle – including the current location in the sprawling depots.

In addition, RTLS specialists from Siemens provided live support from Chemnitz (Germany). According to Stokkeland: "In my long career, I have not experienced a project that was as easily implemented. The agile development process involved a lot of stakeholders, and the end users were some of the key group. That was a great achievement for everyone involved!" Christian Grønnerød added: "We are really very satisfied with both the technology and the management of the implementation project on Siemens side. This has become a great benefit for us."

SOURCE: SIEMENS

The RTLS transponders also transmit other information from the vehicles (direction of travel, coupling status).

Proven from the first day

In practice, SIMATIC RTLS has proven itself from the very first day. On the one hand, Sporveien employees were impressed by the high locating precision. "We are accurate to about 20cm," reports RTLS product manager Grønnerød: "Of course that is not needed for the trains, which are significantly larger."

However, this accuracy of SIMATIC RTLS creates the prerequisite for possibly adapting other workshop processes to real-time locating – after all, the installed gateway infrastructure can locate much more than just a few trains. The availability of the system also far exceeds Sporveien's expectations, aided by the status monitoring of the RTLS infrastructure integrated into the visualization.

The users in the workshops, too, became fast enthusiasts of the new technology. "Such projects often require a lot of coordination effort and come with many change requests," stated project manager Stokkeland. "But in the case of RTLS, all colleagues were immediately convinced of the advantages." The new systems ultimately enable employees to concentrate on their actual tasks without wasting time on searches, phone calls, or unnecessary detours. "The acceptance is really enormous," said Stokkeland.

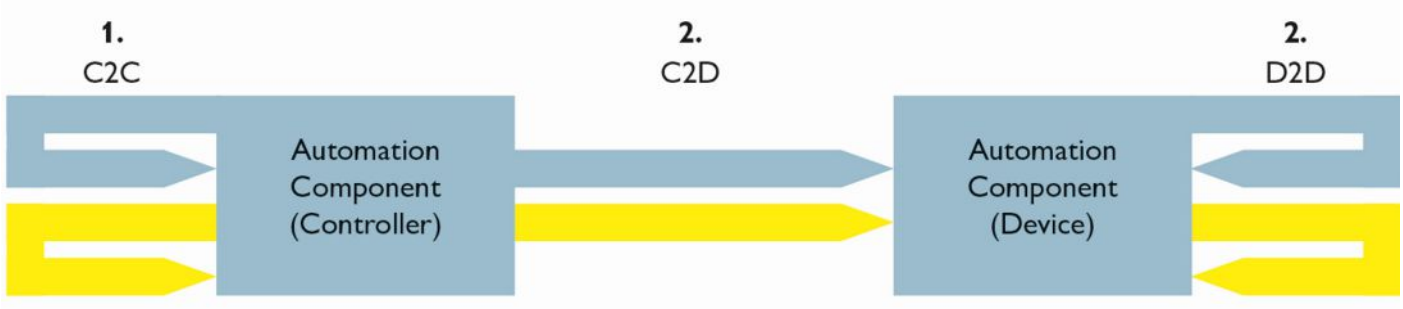
Improving public transport services

Punctual provision of trains, reduction of running costs for service and maintenance, and increase of capacities in depots: For Sporveien, Simatic RTLS is another important component for the continuous improvement of public transport services. So that the people of Oslo have one more reason to exchange the car with the subway.

Markus Weinländer, Head of Product Management SIMATIC Net, ***Siemens.***

Initial FLC initiative results: OPC UA into the field

Field level communications (FLC) activities focusing on making OPC UA suitable for the field are in full swing. A step forward will be made if devices developed for OT can communicate in one language with OPC UA, and at the same time be based on real-time capable Ethernet hardware with TSN in the future.



SOURCE: PHOENIX CONTACT

The first stage involved defining controller-to-controller (C2C) communication for standard and safety data which can then be extended to controller-to-device (C2D) and device-to-device (D2D) communication.

DEVELOPMENT WORK FOR USING OPC technology on the field level began with the standardization of TSN (Time-Sensitive Networking). A large number of single- and multi-vendor demonstrators were illustrating the possibilities of TSN technology in terms of synchronicity and real-time capabilities at an early stage. However, if every company or user organization were to upgrade their own existing system to TSN, there would be no benefits for the automation world.

Against this backdrop, a TSN standardization project (IEC/IEEE 60802-IA) was started at the IEEE/IEC standardization level early on, aimed at standardizing TSN use in industrial automation technology. Upon completion of a uniform TSN profile, automation and IT protocols should be able to share a TSN network with corresponding guarantees. At the same time, the resulting new communication level – the "converged network" – should not interfere with existing communications. To be able to communicate in a common language at the application level, however, the two technologies TSN and OPC UA Pub/Sub (Publisher/Subscriber) had to be combined with each other.

To this end, a group of automation service providers, technology providers, and component and switch manufacturers within the OPC user organization came together at the 2018 SPS trade fair in Nuremberg to establish the Field Level Communication (FLC) initiative. There are currently 26 companies involved. They have committed to actively supporting the FLC initiative to develop a comprehensive FLC communication standard for automation technology based on OPC UA and TSN. Although these 26 companies are steering the initiative, the actual specification work carried out in working groups is open to every member of the OPC Foundation. And now, after around one and a half years, the initial results can be seen.

Controller-to-controller

Developing a completely new ecosystem for automation which is also capable of integrating technological developments that will be made in the coming 20 years is proving to be a great challenge. The specification will have to cover a range of requirements, from those of process technology all the way to synchronous motion control applications. Therefore, the FLC initiative members decided to realize a successive concept.

The first stage focused on exchanging data between controllers. The initial work addressed application scenarios in which two controllers are configured from both sides to coordinate with each other. The IP addresses have already been assigned and there is no need to configure the communication parameters.

Along with online communication, mechanisms were also defined for the offline engineering phase. In addition, the controllers are supposed to transmit standard and safety data securely. This step alone will create significant added value compared to current solution approaches.

Offline engineering with FLC

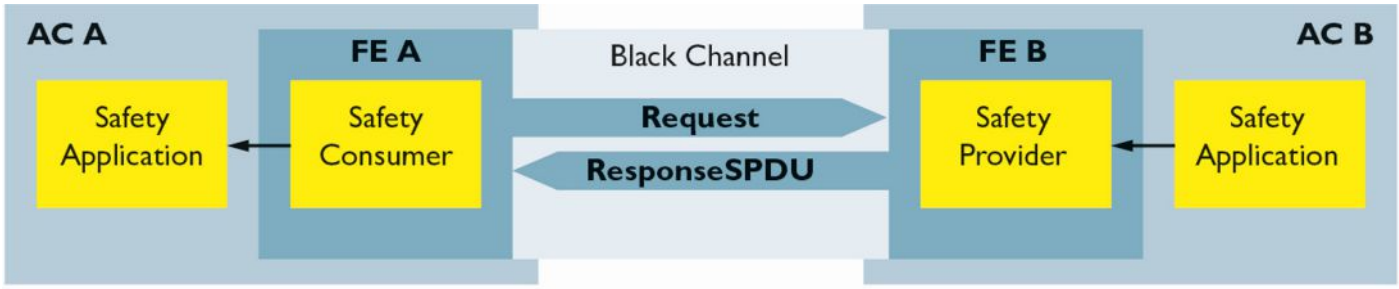
The device description solutions available today focus on integrating a specific sensor or actuator device type into a system provider's engineering concept. Often, the file is no longer actively used once the device has been instantiated. This is not the case with FLC; the file can only contain type information (product descriptor), but it can also be extended with instance information. With this procedure, the file automatically becomes an instantiated solution descriptor.

If known, address information or specific configurations can therefore be defined in advance before then being integrated into the other engineering system. The device description file therefore automatically becomes the digital twin of the communication partner. Each user can add the information that they already know as a part of their engineering tasks. Consequently, the file content grows as the project develops. This is resolved using an approach based on the AML (Automation Markup Language) programming language, which combines both FLC-specific and other information in one packet.

Data receiver communications

In the first stage, the FLC initiative is favoring a simplified model for establishing a connection. Here, establishing communication is initiated by the data receiver, and the sender then transmits the data cyclically in the respective quality and cycle time in accordance with the receiver requirements. The idea behind this model is that where there are two communication participants, the receiver knows best when its application needs the data. If bidirectional data exchange is to be established, then both sides must be able to initiate data transmission. This approach has therefore been specified such that it can also be extended to bidirectional communication models.

A similar communication model has been created for forwarding safety-related data



Automation component B supplies safety-related data to automation component A through a black channel between two functional entities (FEs).

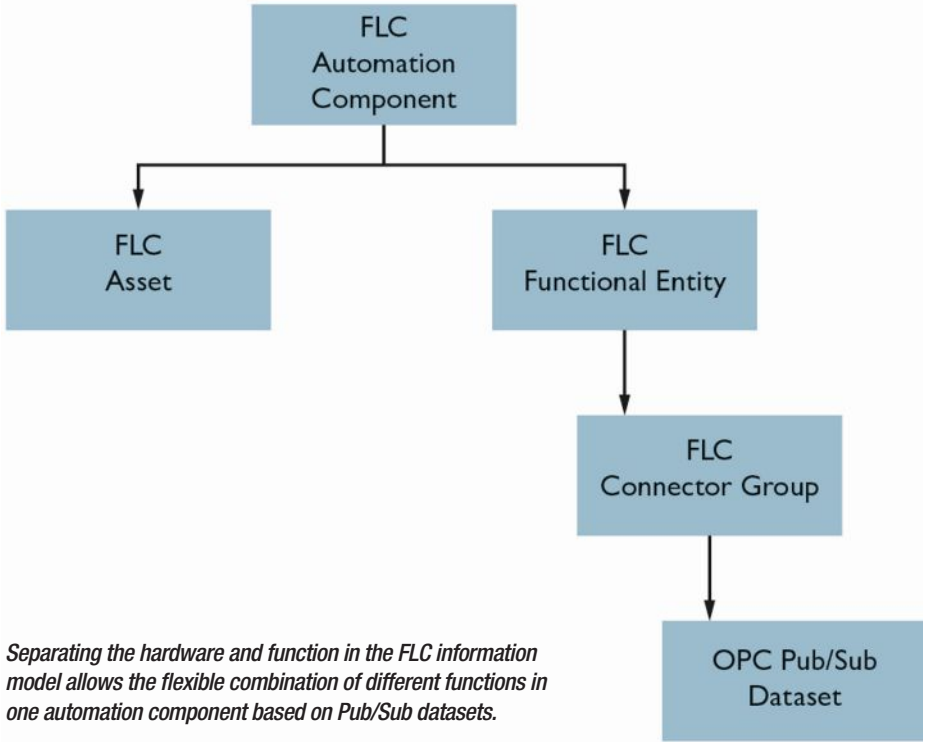
in OPC UA Safety applications: The safety consumer starts a cyclical request for the safety provider to send data to the consumer. If the consumer does not request any data, the provider does not send any. This means that the provider-side protocol is simple, because time and control mechanisms are not required. On the consumer side, safety-related control is based on timeouts or CRC and address errors. Therefore, any safety information can be transmitted securely, even in dynamically changing application scenarios. The safety specification through OPC UA through the client server has already been completed and will now be converted for FLC integration to Pub/Sub mechanisms, among other things.

Separating assets and functions

The FLC device model for the communication participants has also been redesigned. The participants are now called automation components (ACs). All devices have the same fundamental structure, regardless of whether they are controllers or sensors. Here, the asset and the function have been strictly separated. This separation means that functionalities can be viewed independently of the hardware in the future and, for example, can be easily combined in new products. Such a unit will be described as a functional entity (FE). The standardized FE will not know whether it is being operated in a modular or rigid structure, in a controller, or on a drive. On the other hand, the asset contains all hardware-related information, the device structure, Ethernet interfaces, and the firmware versions for the device or the device part.

The security mechanisms are based entirely on the mechanisms already defined in OPC UA. The few aspects that have not yet been implemented in OPC Security must become part of the OPC Security specification. The actual connection between the devices – the FLC connection – will therefore be established between functional entities that use existing OPC-specification Pub/Sub mechanisms. Connections to a participant will be managed in a connector group, which in turn comprises one or more datasets.

With this approach, different data, update rates, and communication participants can be mapped using one model. At the same time, the focus is currently placed on establishing a secure, multi-level connection. Both the asset and the functional entity can be checked for compatibility; there is a clear configuration phase, and then the switchover can be made to cyclic data exchange. Moreover, a corresponding status machine has been defined for both communication participants.



Separating the hardware and function in the FLC information model allows the flexible combination of different functions in one automation component based on Pub/Sub datasets.

Function-specific integration models

In this first stage, the FLC initiative members have defined a reduced range of functions that are sufficient for transmitting standard and safety data between two controllers securely. The functions will be published in summer 2020. The second stage will focus on describing the functions not yet available that are necessary for transmitting data between controllers and devices, such as addressing, configuring, and extended diagnostics. Moreover, working groups are being established to develop function-specific information models for the first time, for example for motion applications, based on this model.

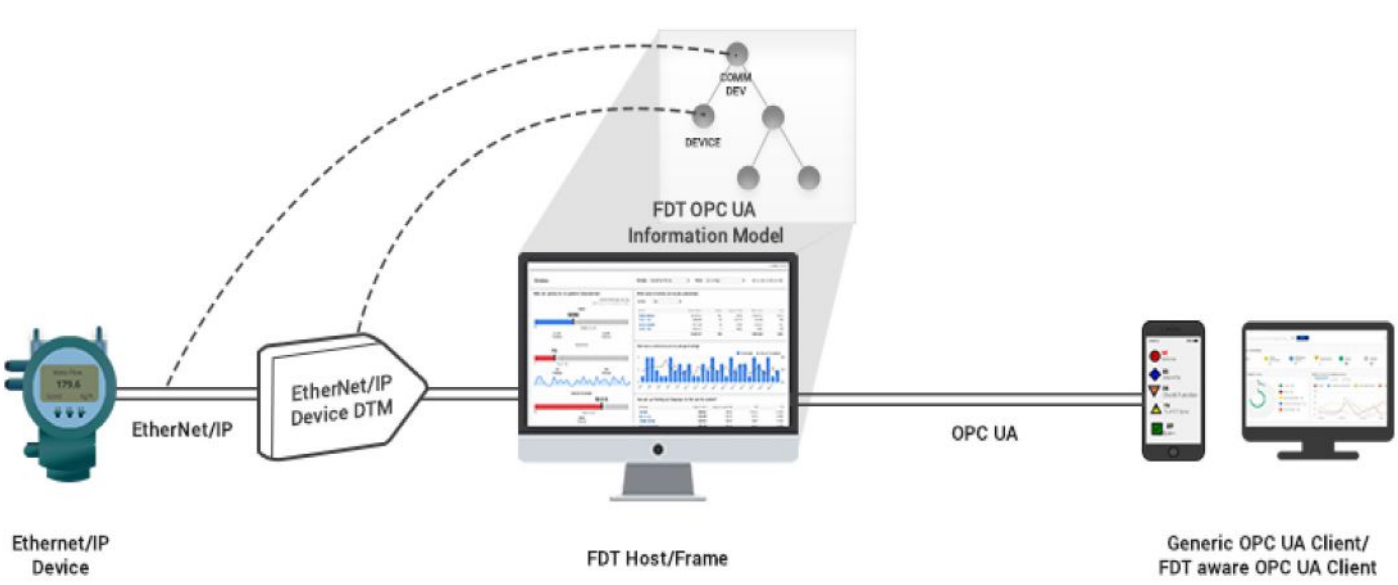
Here, the subject of TSN will always be addressed in parallel. It will be based on mechanisms that have long been defined in an OPC Foundation working group on TSN integration into the Pub/Sub model. Whether or not TSN, with its time guarantees, is ultimately used in a convergent network with numerous different communication systems will depend on the respective application. If the application has an unknown network load and short cycle times and yet demands low and guaranteed latency times, data exchange within the network must be switched over to TSN streams.

The FLC-initiative activities focusing on making OPC UA suitable for the field are in full swing and are beginning to bear fruit. A huge step forward will be made in field-related communication providing a great deal of innovation if the devices developed for OT can communicate in one language with OPC UA and at the same time be based on real-time capable Ethernet hardware with TSN in the future.

Robert Wilmes, System Management PLCnext, ***Phoenix Contact Electronics GmbH.***

Mapping EtherNet/IP CIP object to OPC UA information model

Exposing EtherNet/IP object via OPC UA Information model provides new technology for EtherNet/IP devices in the process automation. Mapping of CIP objects like Identity, Assembly to OPC UA Information Model will enable standard OPC UA Services to access the objects defining devices in a vendor-neutral way.



SOURCE: ODVA

EtherNet/IP field device connected to FDT Host.

OPC IS A WIDELY ADOPTED INTEROPERABILITY standard for secure, reliable and platform-independent information exchange in the industrial automation space and other industries like automotive and building automation.

Mapping of EtherNet/IP (CIP) objects like Identity, Assembly to OPC UA Information Model will enable standard OPC UA Services to access the objects of EtherNet/IP devices in a vendor-neutral way.

This article focuses on various ways of supporting OPC UA standard for EtherNet/IP devices - Deployment Scenarios, some specific use cases relevant for Process Automation Industries, and mapping and comparing use cases with various OPC UA Information models.

Supporting OPC UA standard

The access of EtherNet/IP object via OPC UA Service is possible in three different scenarios

- Scenario 1: OPC supported Host/DCS system (FDT/FDI/PA-DIM)
- Scenario 2: EtherNet/IP OPC UA Server using EDS file embedded in Industrial Gateway or in any HMI/Industrial Software application
- Scenario 3: OPC UA Server directly embedded in EtherNet/IP device

Process automation use cases

Some of the process automation industry specific use cases relevant for EtherNet/IP device listed below.

- Use Case 1: Device Identification
- Use Case 2: Device Health Status (NAMUR NE107)
- Use Case 3: Monitoring Process Variable
- Use Case 4: Parameterization
- Use Case 5: Calibrating the field device

For Scenario 1: Map and compare the Process Automation Industry specific use cases listed above to:

- FDT OPC UA Information Model
- FDI Information Model
- PA-DIM

For Scenario 2: Possible mapping of EDS Information to OPC UA Information model for above listed use cases

For Scenario 3: High level understanding of supporting OPC UA in EtherNet/IP device

Mapping to OPC UA Model

This section covers the mapping of EtherNet/IP (CIP) object to the standard OPC UA Information model for above three scenarios and process automation industry specific use cases.

Scenario 1: OPC supported Host/DCS system (FDT/FDI/PA-DIM)

OPC UA supported FDT/FDI Host or DCS system can expose the EtherNet/ IP (CIP) object via any of the below three information model

- FDT OPC UA Information Model
- FDI Information Model
- Process Automation - Device Information Model (PA-DIM)

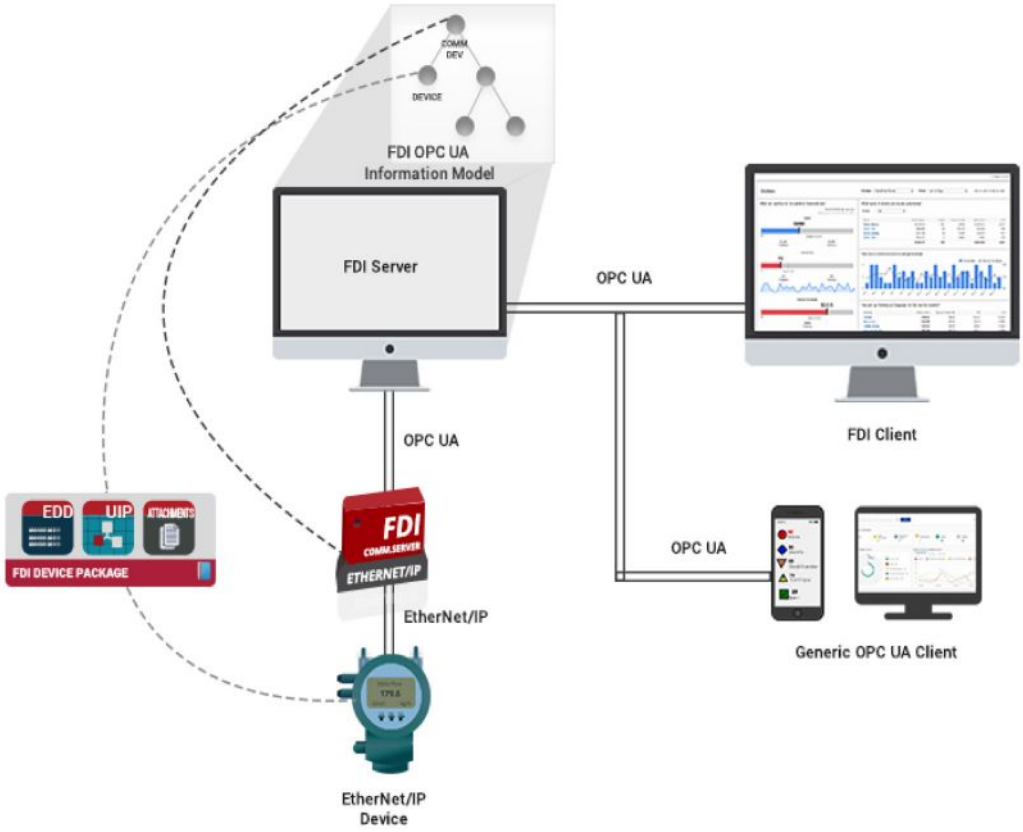
EtherNet/IP objects mapped to FDT OPC UA Information Model

As part of IIoT/Industrie 4.0 strategy, FDT Group and OPC Foundation have jointly worked on FDT OPC UA Information model specification document.EtherNet/IP devices connected to OPC enabled FDT Host/Frame allows access to the EtherNet/IP object via OPC UA Services. No additional implementation is necessary for exposing EtherNet/IP (CIP) via OPC UA services in FDT Host/Frame system.

Use Cases Supported by FDT OPC UA Information Model

Below are the set of use cases supported by FDT OPC UA Information Model:

- List Topology
- Device Identification
- Browse Parameters and its attributes



SOURCE: ODVA

EtherNet/IP device connected to FDI Host supporting generic protocol extension.

- Get Device Status
- Get Device Diagnostics
- Read Offline Parameters
- Read Online Data
- Write Device Parameters
- Audit Trail

EtherNet/IP field device is represented by EtherNet/IP Device DTM in the FDT Host/Frame application. FDT Host application exposes the FDT OPC UA Information model and enables the access to the EtherNet/IP device object via OPC UA Services. Any generic or FDT aware OPC UA Client can access the EtherNet/IP device by connecting to FDT OPC UA Server.

Components required for supporting EtherNet/IP field device in FDT OPC UA Information Model listed below:

- FDT Host supporting OPC UA Server
- EtherNet/IP Communication DTM
- FDT EtherNet/IP (CIP) Annex Specification Document
- FDT EtherNet/IP Device DTM

EtherNet/IP objects mapped to FDI (Field Device Integration) Information Model

FDI specification can support EtherNet/IP devices using FDI generic protocol extension specification. EtherNet/IP devices connected to FDI Host supporting FDI Information model allows access to the EtherNet/IP device object via OPC UA Services.

Use Cases Supported by FDI Information Model

- Asset Management
- Supporting all the methods defined in the EtherNet/IP FDI Device Package (For example: Calibration, Device Setup, and Echo Curve for Level Transmitter etc.).
- Supporting all functionalities defined in the EtherNet/IP Device Package like Configuration, Alarms, Diagnostics, Trends etc.
- UIP Hosting for supporting complex device functionalities
- Upload/Download for Offline Configuration
- Audit Trail

EtherNet/IP FDI Device Package represents the EtherNet/IP device in FDI host system. FDI Server communicates with EtherNet/IP device using EtherNet/IP FDI Communication Server. It exposes the EtherNet/IP device object in the FDI Information Model. Any generic OPC UA Client or FDI Client application can access the EtherNet/IP device by connecting to the FDI Server (OPC UA Server).

Components required for supporting EtherNet/IP field device in FDI Information Model listed below:

- FDI Server supporting generic protocol extension
- EtherNet/IP FDI Communication Server
- EtherNet/IP FDI PSD Annex specification document
- EtherNet/IP FDI Device Package

EtherNet/IP objects mapped to PA-DIM

Devices mainly used in the process industries like chemical, oil & gas, pharmaceutical, food & beverage, power generations, water and waste water are known as process automation devices. They include measurement devices like flow, density, level, temperature and controlling devices like valves, actuators and positioners.

It is necessary to access the common set of parameters and functions from these devices for effective commissioning, operation and maintenance of these devices. This may be necessary to have this information even during procurement stage of these devices.

IEC standards like Common Data Dictionary (CDD) – IEC 61987 and eCl@ass have a unique way to identify the device parameters using the standard unique identifier. However, it is necessary to have the Information Model to manage the entire life cycle of device independent of the communication protocol.

OPC Foundation and FieldComm Group is jointly working on PA-DIM specification document.

PA-DIM use cases

The first release of PA-DIM focus mainly on the NAMUR Device Core Parameter NE131 and NAMUR OPEN Architecture (NOA) use cases for Pressure, Temperature, Flow, Level, Density, Control Actuator/Positioner devices.

- Identification
- Diagnostics
- Process Values
- Configuration

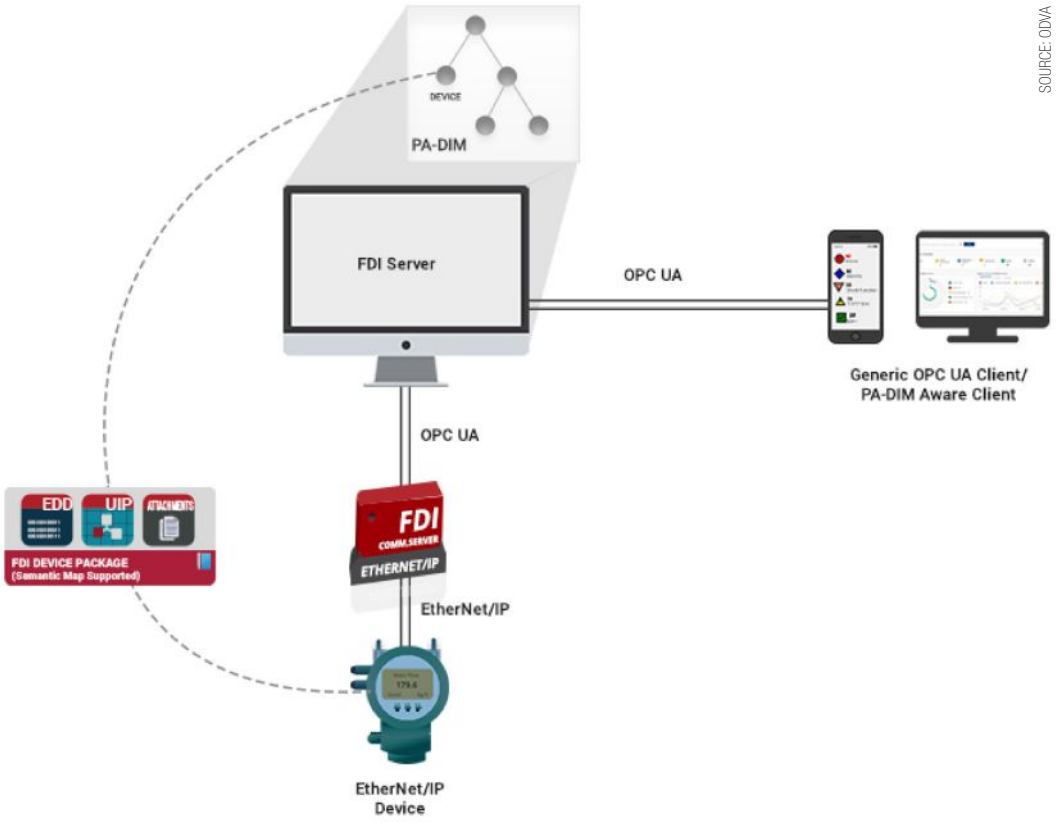
EtherNet/IP device connects to FDI Server using EtherNet/IP FDI Communication Server. FDI Server exposes the PA-DIM Server. EtherNet/IP FDI Device Package representing the EtherNet/IP field device supports the SEMANTIC_MAP information. PA-DIM Server exposes the EtherNet/IP device information. Any generic OPC UA client can access it by connecting to PA-DIM Server.

Components required for supporting EtherNet/IP field device in PA-DIM server listed below:

- FDI Server supporting generic protocol extension
- EtherNet/IP FDI Communication Server
- EtherNet/IP FDI PSD Annex specification document
- EtherNet/IP Device Package supporting the SEMANTIC_MAP

Use Case Mapping for FDT OPC UA, FDI Information Model and PA-DIM

Section maps below compare process specific use cases with the OPC UA Information model.



SOURCE: ODVA

EtherNet/IP Device connected to PA-DIM Server.

Use Case 1: Device Identification
Goal: Uniquely identify an EtherNet/IP field device in the network.

Use Case 2: Device Health Status (NAMUR NE107)
Goal: DeviceHealth indicates the status of a device as defined by NAMUR Recommendation NE107.

Use Case 3: Monitoring Process Variable
Goal: Remotely monitor the process variables read from the EtherNet/IP device using any OPC UA client application.

Use Case 4: Parameterization
Goal: Remotely configure the EtherNet/IP adapter device via OPC UA client application

Use Case 5: Calibrating the field Instruments
Goal: Calibrating the field instrument remotely via OPC UA Client

Scenario 2: EtherNet/IP OPC UA Server using EDS file embedded in Industrial Gateway or in any HMI/Industrial Software application

EDS File is a plain text file created and distributed by EtherNet/IP device vendors. The EDS file provides detailed information related to the device identification, configuration parameters, process variables, composition of assemblies etc. EtherNet/IP Configuration tool uses the EDS file to configure the device.

The EtherNet/IP OPC UA Server derives the information model from EDS file. EtherNet/IP OPC UA Server can be implemented in existing EtherNet/IP configuration tool or any Industrial IoT gateway supporting EtherNet/IP communication protocol.

'OPC UA for Devices - Part 100' specification is considered as base for mapping the EDS information to OPC UA.

Below section maps information derived from EDS file to the process industry specific use cases are listed.

Use Case 1: Device Identification
Goal: Uniquely identify an EtherNet/IP field device in the network.

Use Case 2: Device Health Status (NAMUR NE107)
Goal: Device Health indicates the status of a device as defined by NAMUR Recommendation NE107.

The EDS file does not have any standardized way to identify the device health. EtherNet/IP device health can be derived by reading the status attribute of Identity Object. However, values of Status attribute are not as per NAMUR Recommendation NE107.

As a future possibility/workaround, below are the options to map the Device Health Status to OPC UA DeviceHealth enumeration based on NAMUR Recommendation NE107.

Option #1: Process Device Diagnostic Object (Class Code 0x108) defined in CIP specification document follows the NAMUR Recommendation NE107. The EtherNet/IP device shall implement this object.

Note: It is not mandatory to implement the Process Device Diagnostic Object.

EDS file shall specify the details in the Public Object Class Sections to indicate the presence of Process Device Diagnostic Object.

Option #2: Standardization of a new Diagnostic Assembly as part of Predefined Diagnostics Assembly Instances of the EtherNet/IP spec as per NAMUR Recommendation NE107.

Note: As per the EtherNet/IP specification, for most of the objects it is not mandatory to specify the details in the Public Object Class Sections of EDS file.

Use Case 3: Monitoring Process Variable
Goal: Remotely monitoring the critical process variables read from the EtherNet/IP device using any OPC UA client application.

In the OPC UA for Device Information Model, the ParameterSet object of DeviceType instance can be mapped to device parameter information that is available from the EDS file as listed below for monitoring the process values.

Option #1: Parameters of EtherNet/IP devices are listed in the [Params] section of EDS file. Each parameter may contain the possible enumeration details associated with it. This parameter can be mapped to OPC UA Information Model.

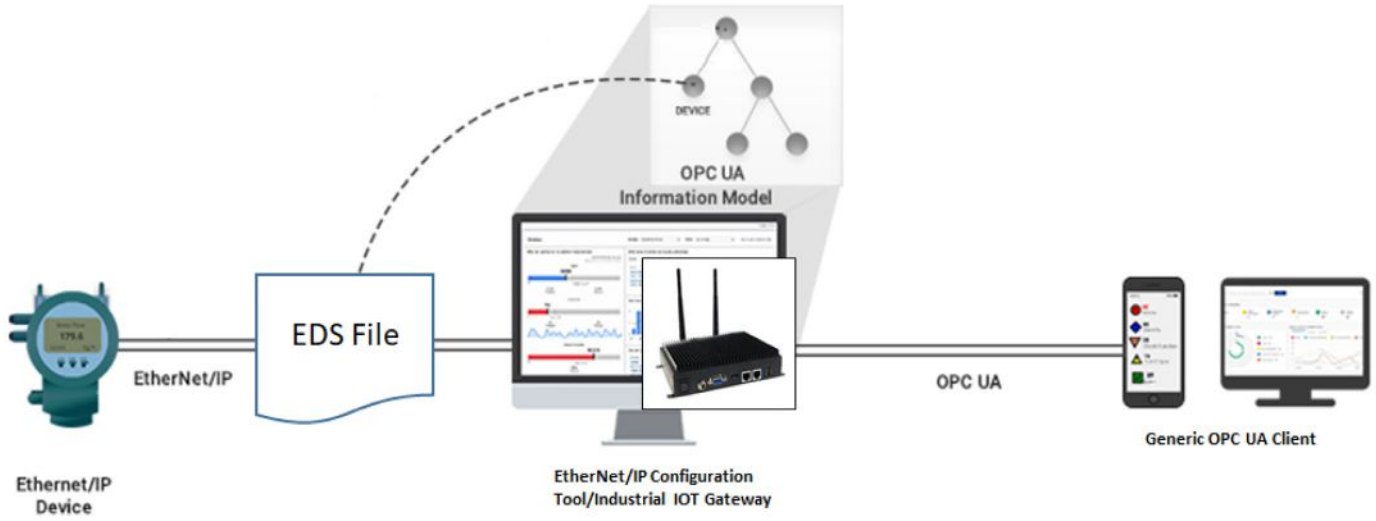
Link Path in the EDS file allows access to parameter. However, as per EDS specification Link Path is optional. Hence, OPC UA Information model mapping will not be possible for parameter without Link Path information.

Option #2: Another possibility to map the Parameter would be to use the [Assembly] section of the EDS file. Parameter Members of the each Assembly section can be mapped to OPC UA Information Model.

Note: Read/Subscription can be performed on ParameterSet in OPC UA Information Model for monitoring the process values.

Use Case 4: Parameterization
Goal: Remotely configuring EtherNet/IP adapter device parameters using OPC UA client. Parameterization use case is similar to Option #1 and Option #2 of Use Case 3.

Note: Write operation can be performed on ParameterSet in the OPC UA Information Model.



SOURCE: ODVA

EDS supported EtherNet/IP OPA UA Server.

Use Case 5: Calibration

Goal: Calibrating the field instrument remotely via OPC UA Client

Device profiles implementing S-Sensor Calibration Object can be calibrated from OPC UA Client. However, this requires the EDS file to specify the object details in the Public Object Class Sections. The instance services can be mapped to method call nodes of the OPC UA Information Model.

For Scenario 3: OPC UA Server directly embedded in EtherNet/IP device

Apart from fetching the information from OPC supported host system, it is possible to have the OPC UA embedded in EtherNet/IP adapter devices, drives, PLCs and Controllers.

EtherNet/IP Identity Object Response	Mapping to EDS File [Device] Section	Mapping to OPC UA Information Model
VendorID	VendCode	Manufacturer
DeviceType	ProdType	Model
Product Code	ProdCode	ProductCode
Revision (STRUCT of Major Revision, Minor Revision)	MajRev, MinRev	DeviceRevision
Serial Number	-	SerialNumber
Product Name	ProdName	-

This enables the vertical communication between the EtherNet/IP device and higher-level systems like MES, Visualization Tools for diagnostics, Asset monitoring, Configuration use cases.

Conclusion

Exposing EtherNet/IP object via OPC UA Information model will accelerate the adoption of EtherNet/IP devices in the process automation industry.

FDT OPC UA Information Model: EtherNet/IP Device DTM can take an advantage of FDT OPC UA Information model without any additional implementation. However, FDT2 CIP Annex specification document is necessary. FDT OPC UA Information model supports the network topology and other use cases listed in this document.

Even though EtherNet/IP DTM supports Complex methods/functionalities, it cannot executed from OPC UA client via FDT OPC UA Information model. For example, calibration methods which require user feedback during method execution using this approach are not supported.

FDI Information Model: FDI Information Model is very elaborate and it allows the distributed deployment of FDI Client and Server module. It is possible to support any complex methods remotely using FDI Client.

Some sections of FDI Information Model has been validated with the tools (reference FDI Host). FDI Client application is thick client application and requires complex UI Engine module. EtherNet/IP FDI PSD specification document is necessary to support FDI Information model for EtherNet/IP device.

PA-DIM: PA-DIM is limited, but highly focused on NAMUR use cases applicable for process automation industry. Using the Semantic ID, PA-DIM can fetch information from the field device without knowledge of the device or parameter specific details. PA-DIM supported Industrial IoT gateway can push the data to the cloud.

Semantic Map of the parameter is necessary to support PA-DIM Server. PA-DIM may require additional update to the Common Data Dictionary (IEC document) to support more use cases. Supporting complex method is not in scope of PA-DIM yet.

Information model using EDS file

EDS file is mandatory for the EtherNet/IP device. Use Cases like Device Identification, Monitoring Process Values and Parameterization can be supported in EDS driven OPC UA Information model.

Due to the flexible nature of EDS file, OPC UA Information model may have interoperability issues. Supporting the complex methods, user interfaces, etc. is not possible using the EDS file.

EtherNet/IP OPC UA Companion Specification Document: This companion specification document provides the flexibility to map any EtherNet/IP object to OPC UA Information Model.

Apart from supporting the common use cases like Device Identification, Parameterization, Monitoring process Values; Companion Specification should focus on Industry focused use cases like Diagnostic Information and other applications.

An appropriate OPC UA information model should be chosen based on the specific business need.

GV Chatrapathi, Director – Embedded; G Sivansethu, Director – Technology; Bhanu Prakash Technical Lead; and Smitha Rao, Co-founder, Director, ***Utthunga Technologies Pvt. Ltd.***

industrial ethernet book

Reader Service Card

IEB issue 119 - July 2020

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

Return by mail to:
IEB Media
Bahnhofstr. 12
86938 Schondorf
Germany

Or use our online reader service at:
www.iebmedia.com/service

Please enter your contact details below:

Name: _____
Position: _____
Company: _____
Address: _____
_____
City: _____
State: _____
Zip Code: _____
Country: _____
Phone: _____
Email: _____

I want to:

☐ **Start** a new subscription
☐ **Update** my subscription
☐ **Digital** edition or ☐ **Print** edition
☐ **Change** my address
☐ **I do not want** to receive promotional emails from Industrial Ethernet Book
☐ I want to be **removed** from the subscription list

Signature: _____

Date: _____

Company Activity (select one)

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

Job Activity (select one)

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

Time synchronization to improve determinism and response time

Synchronizing I/O tasks with application execution can result in improved application response times. In an ever-changing world where vendors are striving to eke out every bit of performance from their PLC systems, time synchronization is a method to add to the list of potential future upgrades.

IN A MODERN PLC SYSTEM, ONE OF THE KEY performance factors is application response time (the time it takes a PLC system to set an output based upon a change in an input). The application response time can vary significantly due to the independent components and tasks present in a modern PLC system.

Remote I/O systems are ubiquitous and synchronizing these data exchanges with an application can have a dramatic effect on performance. Examples using remote I/O protocols like Modbus scanners and EtherNet/IP implicit messaging will be shown. Investigating the use of time synchronization like CIP Sync and IEEE 802.1AS-Rev to synchronize the relevant asynchronous tasks can improve the predictability of application response times.

Overview

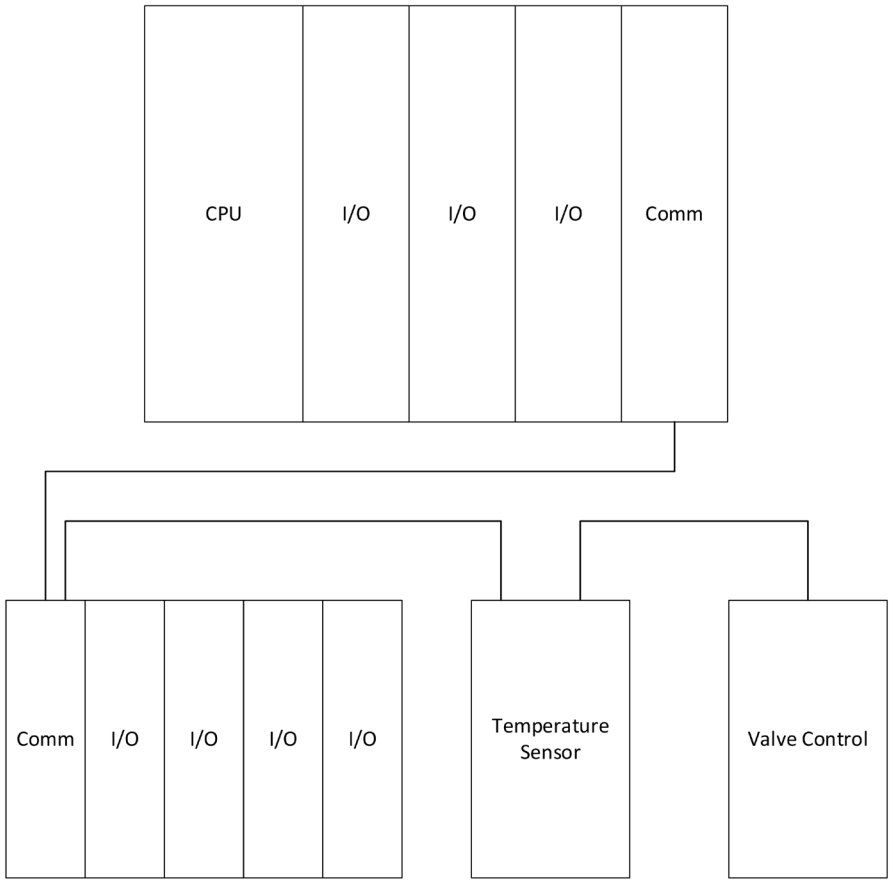
Today's modern Programmable Logic Controller (PLC) systems have come a long way since they were first introduced in the early 1970s. Microprocessor speeds and memory capacity have dramatically increased, and low-speed fieldbuses have been replaced with high-speed networks based on Ethernet. This has led to dramatic increases in overall system performance. However, with the exception of motion control systems, synchronization between I/O systems and PLC logic execution is not present. This article demonstrates the benefit of synchronizing these tasks.

Time synchronization

In order to synchronize tasks across multiple devices, they must all share the same time basis. This can be in the form of clock time (for example, date and time), sometimes called wall time, or simply an arbitrary counter value. This section describes some of the time synchronization methods available to synchronize time between network devices.

To send data at the appropriate time, all participating devices must have the same notion of time. Ethernet-based time synchronization protocols to choose include:

- Network Time Protocol (NTP)
- IEEE 1588 - Precision Time Protocol (PTP)
- IEEE 802.1AS-Rev
- CIP Sync



SOURCE: SCHNEIDER

Sample PLC System.

Network Time Protocol

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use.

NTP can usually maintain time to within tens of milliseconds over the public Internet and can achieve better than one millisecond accuracy in local area networks under ideal conditions.The current protocol is version 4 (NTPv4), which is a proposed standard as documented in RFC590 and compatible with version 3, specified in RFC1305.

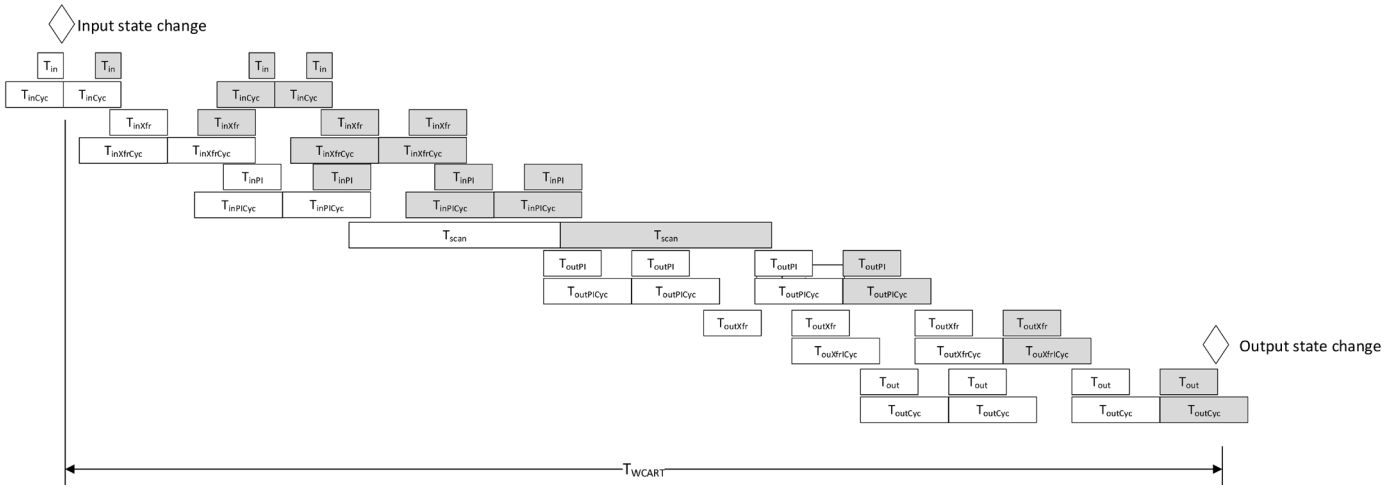
IEEE 1588 Precision Time Protocol

Precision Time Protocol (PTP) synchronizes clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" and published in 2002. In 2008, IEEE 1588-2008 was released as a revised standard; also known as PTP Version 2. It improves accuracy, precision, and robustness, but is not backward compatible with the original 2002 version.

IEEE 802.1AS-Rev

IEEE 802.1AS-Rev specifies the protocol and procedures used to ensure that the synchronization requirements are met for time-sensitive applications, such as audio,



SOURCE: SCHNEIDER

Worst-case Application Response Time.

video, and time-sensitive control, across networks (for example, IEEE 802 and similar media).

It specifies the use of IEEE Std 1588 specifications where applicable in the context of IEEE Std 802.1Q. Synchronization to an externally provided timing signal is not part of this standard but is not precluded.

This standard enables stations attached to bridged LANs to meet the respective jitter, wander, and time-synchronization requirements for time-sensitive applications. This includes applications that involve multiple streams delivered to multiple endpoints. This standard leverages the work of the IEEE 1588 Working Group by developing the additional specifications needed to address these requirements.

CIP Sync

CIP Sync provides increased control coordination needed for control applications where absolute time synchronization is vital to achieve real-time synchronization between distributed intelligent devices and systems. [3] CIP Sync is compliant with the IEEE-1588 standard and allows synchronization accuracy between two devices of fewer than 100 nanoseconds. Real-time synchronization can be achieved over conventional 100Mbps, Ethernet systems with a switch-based architecture.

PLC operation

This section describes the basic operation of a modern PLC system. The PLC used for the analysis is a rack-based device consisting of a CPU, a remote I/O communications module, and some local rack-based I/O. It is understood that many more peripherals exist in most installations, but this simple system should be sufficient to demonstrate the intended principles. Both rack-based and stand-alone I/O peripherals are shown.

PLCs perform many tasks in order to control a process. These include reading inputs and writing outputs from a network or local bus, executing user logic, updating I/O process images, and so on. Many of these tasks are performed cyclically but asynchronously, leading to wide variations in application response times.

Within a PLC, I/O data is typically contained in a block of memory called a Process Image (PI). This allows the user program to execute on a constant set of inputs for a cycle. As inputs are read, their contents are placed in the Input PI. The content of the Output PI is used to set output values. Copies of these tables are used during PLC program execution. This allows asynchronous I/O updates to occur during program execution without affecting I/O values operated upon during program execution.

PLC System program execution cycle

PLCs perform control by executing user-programmed logic on inputs and producing outputs. The typical operation is performed as described:

- Input data acquisition;
- Transfer inputs;
- Update PLC Input Process Image;
- Execute PLC application;
- Update output Process Image;
- Transfer outputs;
- Apply outputs.

The following sections describe the steps in more detail.

Input Data Acquisition

Typical input devices consist of physical inputs and some mechanism for transferring data that represents these inputs to a PLC via some communication mechanism (for example, network, fieldbus, backplane, and so on). In the case of an input device with multiple inputs, a task cyclically gathers the data from the physical inputs and places them into a local process image (PI), and then the communication task cyclically transfers this image over the communication mechanism.

In a stand-alone input module, the communication interface communicates the input process image directly with the PLC. In remote I/O racks, the input data can be transferred to a communications module (called a "head"), which gathers all the inputs from all input modules in the rack and provides an aggregated process image to be transferred to the PLC.

For future calculations, the time to acquire a device's inputs and place them into an input process image will be represented by the variable tin.

Transfer Inputs

This operation considers the time needed to transfer the input data from an input process image over a communication medium and to receive it at the PLC's communications interface. Generally, this is the time the data is on the communication medium. However, for high-speed networks or low-speed processors, the processing time may also need to be considered.

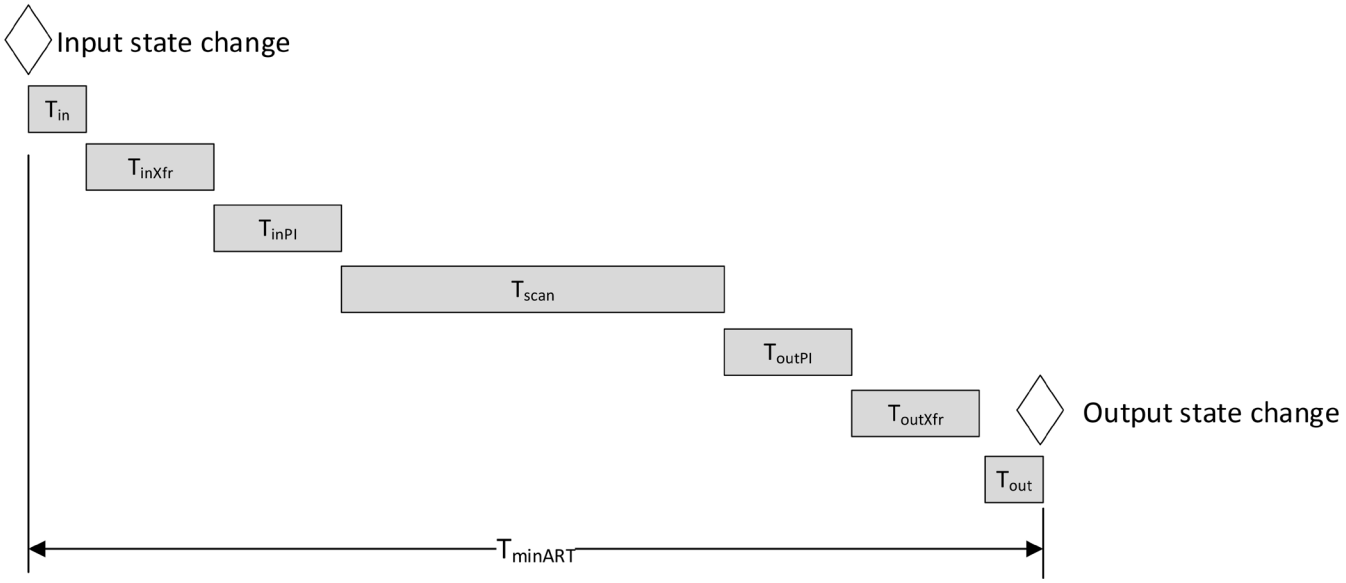
Transferring inputs can use a pull model, such as a read operation issued by the communications interface over a backplane or via a protocol like Modbus over a network. A push model can also be used, such as implicit messaging of EtherNet/IP.

For future calculations, the time to transfer a device's inputs to a PLC's communication interface will be represented by the variable tinXfr.

Update PLC Input Process Image

PLCs containing local I/O or a separate remote I/O communications module will need to transfer input data from these devices into the PLC. This cyclic task represents the time needed for a PLC to create a static representation of all the inputs that can be used by the user's program.

For future calculations, the time to update the PLC's input process image will be represented by the variable tinPI.



Minimum Application Response Time.

Execute PLC Application

This task represents the execution of the user's program. This is a cyclic activity, where each cycle is sometimes referred to as a scan. Each scan begins by making a copy of the input process built in the previous task for its inputs during the entire scan. It also maintains its own image of the outputs, which it copies to the output process image upon completion of each program scan.

While some PLCs provide multi-cycle capability, this article focuses on a PLC using a single thread of execution for user logic.

User programs typically contain conditional branches (for example, if an input is on, do X; if not, do Y or maybe nothing). Hence, the Execute Logic scan time can vary from cycle to cycle. Some PLC programming tools allow the user to set a constant scan time that is slightly larger than the time needed to execute the user's logic. This will be necessary if synchronization of I/O updates to user logic scan is desired.

For future calculations, the time to execute one scan of the user's program will be represented by the variable tscan.

Update output process image

This task represents the time needed for a PLC to transfer its output process image to the PLC's communication interface and/or local I/O modules.

For future calculations, the time to update the output process image will be represented by the variable toutPI.

Transfer outputs

This operation considers the time needed to transfer the output data from the PLC's communication interface and to receive it at the output device. Generally, this is the time the data is on the communication medium. However, for high-speed networks or low-speed processors, the processing time may also need to be considered. Transferring outputs from the PLC's communication interface typically uses a push model, such as a write operation issued by the PLC over a backplane or via a protocol like Modbus or EtherNet/IP over a network.

For future calculations, the time to transfer a PLC's outputs to an output device will be represented by the variable toutXfr.

Apply outputs

Typical output devices consist of physical outputs and some communication mechanism for transferring data that represents these outputs from a PLC via some communication mechanism (for example, network, fieldbus, backplane, and so on). In the case of an output device with multiple outputs, the communication task cyclically receives outputs and places them into a local output process image.

Another task takes data from the local output process image and writes it to the physical outputs.

In a stand-alone output module, the communication interface receives the output data directly from the PLC. In remote I/O racks, the output data can be transferred to a communications module (called a "head") that gathers all outputs from the PLC and transfers the appropriate outputs to the respective output modules in the rack.

For future calculations, the time to receive a PLC's outputs and write them to physical outputs is represented by the variable tout.

I/O Cycle

PLC I/O can be local or remote. Local I/O is present on the same bus or backplane as the PLC processor. Remote I/O is connected to a PLC using a network, such as a fieldbus or Ethernet protocol, like EtherNet/IP or Modbus TCP/IP. Local I/O typically has shorter update latencies, but as network speeds continue to improve, the differences in latencies continue to shrink.

Input and output values located on a network can be exchanged between a PLC and remote I/O devices using two methods.

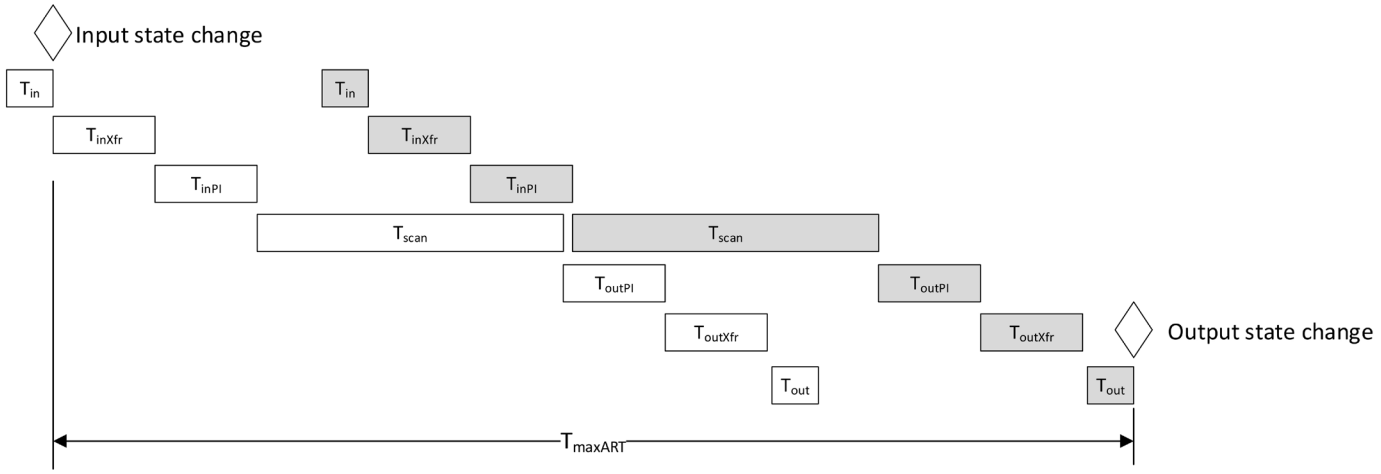
- Client / Server (CS), like Modbus TCP/IP
- Publish / Subscribe (PubSub), like implicit EtherNet/IP messaging

In the CS model, the PLC initiates a request for data and the input device responds with values. Synchronization of this task to PLC program execution is realizable by the PLC. In the PubSub model, the PLC cyclically sends outputs (which can be synchronized with program execution) while the input device continuously sends input data to the PLC at a predetermined interval (or upon change). In this case, the input data is sent asynchronous to a PLC scan cycle, causing variations in application response time.

Remote I/O cycle

A remote I/O device is responsible for receiving output values and applying them to outputs and taking input data and sending it to a remote device. As stated earlier, it can receive a request for inputs and subsequently send a response or it can periodically send its input values.

Whether the remote device is a single I/O device or a head device on a rack of I/O devices, it will take received output data and apply it to its outputs. It will also gather all its inputs and place them in input messages. Typically, a Remote I/O device will contain a PI and have asynchronous tasks processing input and output messages and a separate set of asynchronous tasks reading inputs and writing outputs. However, this implementation can add variances to application response time and can be improved using time synchronization.



Maximum Application Response Time.

Application response time

As stated earlier, application response time is defined as the time from when a physical input changes to when a physical output change occurs as a result of that input change.

With the exception of motion control applications, many PLC systems perform the tasks described in the previous sections asynchronously to each other and the application response time can vary greatly during execution of a user's program. The previously defined variables represented the times needed to complete a certain task.

These tasks are run cyclically, so some new variables are introduced to define the cycle times at which these tasks are executed. In most modern PLCs, these tasks are run at some repetitive rate. For example, on PLCs using the EtherNet/IP protocol, the transfer inputs and transfer output tasks are run at a Requested Packet Interval (RPI) that is loosely coordinated with the application scan time.

The worst-case application response time occurs when a task is preparing data for a dependent task but does not complete before the dependent task begins. Cascading this effect among all seven tasks creates the worst-case application response time. Calculating this worst-case time when the various tasks are unsynchronized is quite complicated. There are dependencies relative to the cyclic times of various tasks. These assumptions demonstrate the principle:

- Application scan time is longer than any other task's execution or cycle time.
- Task execution times are less than their respective cycle times.
- The amount of misalignment (overlap) that is needed for a subsequent task to miss the data provided by a dependent task is based upon task design. To demonstrate worst-case behavior, it is assumed that this value is negligible and is ignored.

Demonstrating worst-case timing for asynchronous cyclic task execution, then narrow rectangles represent cycle times while thicker rectangles represent task execution times. Shaded tasks show where the data that represents the changed input or output first appears in the task's data.

The equations for TminART and TmaxART, application response times can vary even when all tasks are ideally synchronized, because an input can change state at any given time.

Now, let's look at the various application response times using some typical values. Table 2denotes some typical values for these variables and the calculation results follow. All times are in milliseconds.

TminART = 52.4 ms TmaxART = 102.1 ms TWCART = 184.1 ms

One can see that the cycle times of the transfer input and output tasks and updating the input and output PIs has a large influence on the worst-case application response time. One might be tempted to simply increase the frequency of these tasks. However, this results in more load on CPUs and network bandwidth utilization. Conversely, decreasing the frequency of these tasks will lower CPU usage and network bandwidth utilization at the cost of a larger worst-case application response time.

Implementation considerations

So far, we have seen how synchronizing I/O tasks with application scanning can improve application response times but has offered no guidance on implementation. This section offers some implementation guidance. However, internal PLC architectures vary from vendor to vendor, so its applicability may require some interpretation.

Time ynchronization

Time synchronization is the first step needed to synchronize tasks across multiple devices. There are various choices, as shown earlier. The main factor for choosing a specific time synchronization protocol is the needed accuracy. Time synchronization provides each device on the network the same time reference so that they can trigger task executions at the appropriate times in order to complete their tasks just prior to a dependent task's start of execution.

Scheduling

Once all devices have the same time, tasks can be scheduled to complete just prior to a dependent task's start of execution. However, many of today's devices operating systems provide some sort of multi- tasking, so tasks can be interrupted. Scheduling needs to take this into account, either by padding start times or dynamically measuring and adjusting start time based upon data. Since execution times may vary by configuration, dynamic adjustment is preferred.

Similar situations exist on network traffic. I/O traffic could be interrupted by other traffic on the network. Again, padding start times to account for interruptions could be one solution. Another promising solution on the horizon is Time Sensitive Networking (TSN), which offers scheduling uninterruptable Ethernet traffic.

Conclusions

This article demonstrated the effects of synchronizing I/O tasks with application execution, resulting in improved application response times. Formulas were provided for calculating min and max times when fully synchronized as well as for a worst-case calculation when tasks are not synchronized. Implementation methods were also considered.

In an ever-changing world where vendors are striving to eke out every bit of performance from their PLC systems, this may be another method to add to the list of potential future upgrades.

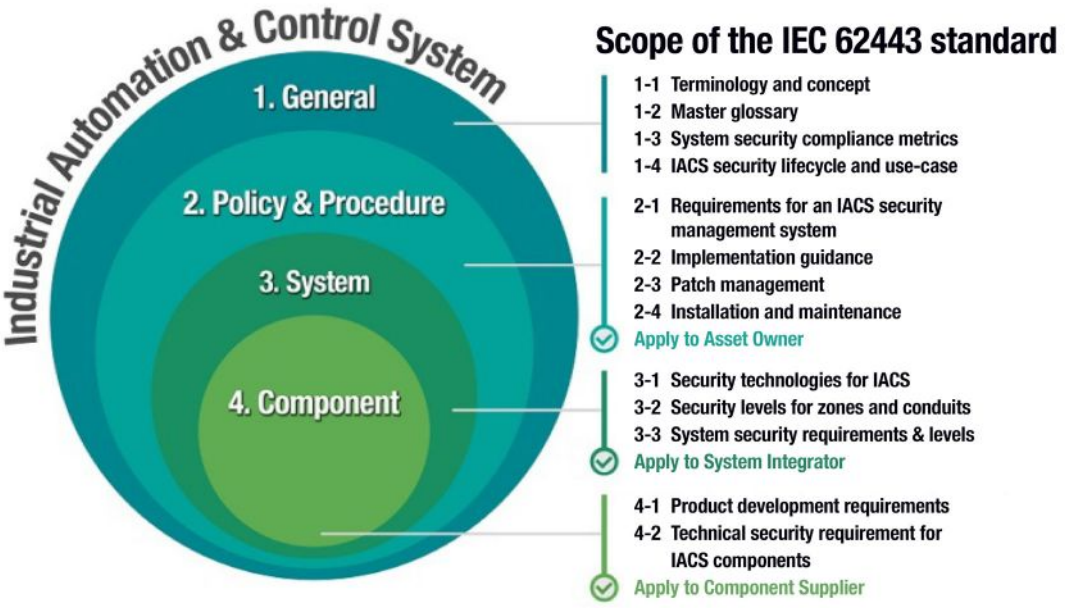
Rick Blair, Sr. Principal System Architect, ***Schneider Electric.***

Securing network devices with the IEC 62443-4-2 standard

As devices are being constantly added to networks, device security is of paramount concern to asset owners. Complete system-level security must be built upon the foundations that consist of each individual component's security functions, along with cybersecurity standards such as IEC 62443.

AS THE INDUSTRIAL IoT CONTINUES TO EXPAND, more and more devices are being connected to networks. This trend is seeing networks transitioning from closed networks to enterprise IT networks that are accessible over the public Internet. While this trend is enhancing operational efficiency, it is unfortunately causing asset owners to become increasingly concerned about the dangers posed by cybersecurity threats.

The asset owners' concerns are justified. A recent report released by the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) calculated that investigators responded to 392 incidents in 2016 in the U.S., compared to 295 the previous year regarding cyberattacks on infrastructure. The growth rate of product vulnerability incidents was 32.88% from 2015 to 2016. It is therefore unsurprising that asset owners are increasingly requiring cybersecurity solutions to allow them to build secure systems for industrial applications.



SOURCE: MOXA

IEC 62443 includes guidelines for different parts of a network and different responsibilities for those using the network.

Evolving cybersecurity standards

In 2002, the International Society for Automation (ISA) produced the ISA-99 document to advise businesses operating in the automation industries how to protect against cybersecurity threats. Fifteen years ago, cybersecurity wasn't the hot topic it is today.

The ISA documents have been aligned with those more frequently used by the International Electrotechnical Commission (IEC) as the concerns around cybersecurity have grown since the conception of the ISA standards. Currently, the IEC 62443 standard constitutes a series of standards, reports, and other relevant documentation that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). If the guidelines within the IEC 62443 standard are followed, it significantly reduces the chances of a cyber attack affecting the network.

IEC 62443 standard

The IEC 62443 standard includes guidelines for different parts of a network and those who perform different responsibilities on the network. In the past, asset owners relied on system integrators (SIs) such as Siemens, Honeywell, and ABB to provide the security solutions for the network. However, many SIs now demand that component suppliers comply with the subsection of the IEC 62443 standard that pertains to their devices. The diagram above provides a brief overview including the scope and the significance of each part for those who must ensure the secure operation of a network.

The IEC 62443 guidelines define four security threat levels. The security standard level 2 is the baseline requirement of the automation industry. It relates to cyber threats posed by hackers, which is the most common attack experienced by system integrators who secure industrial networks. Level 1 is to protect against accidental unauthenticated access and Levels 3 and 4 are against intentional access by hackers who utilize specific skills and tools.

IEC 62443-4-2 Level 2: Baseline

Automation industry requirements

Within the IEC 62443 standard are several subsections that relate to different parties. As SIs are demanding compliance with the IEC 62443-4-2 subsection, which issues guidelines for component suppliers, the subsection is becoming increasingly important. The component requirements are derived from foundational requirements, including identification and authentication control, use control, data integrity and confidentiality, as well as backup for resource availability.

Due to the increasingly important role that component suppliers are playing on IIoT networks, the remainder of this paper will focus on the details of the security requirements that component suppliers must meet when designing devices for deployment on IIoT networks.

Infrastructure

If a network component allows users to access devices or applications, the network component must be able to uniquely identify and authenticate all users, including humans, processes, and devices. This allows separation of duties and the principle of least privilege that ensures every user only has access to information and devices that are essential for the user to be able to perform their designated

role within the network. It is essential to avoid the unnecessary security risk of granting users greater access to the network than is necessary for them to perform their roles. Avoiding this unnecessary security risk will restrict users with malicious intent from being able to cause greater damage to the network. Following this guideline will help secure the infrastructure of a network and provide a solid foundation to develop networks so that the networks are ready to meet the security challenges of today and tomorrow.

Account management

The capability to support the management of accounts, including establishing, activating, modifying, disabling, and removing accounts, must be supported across the network. This ensures that no accounts are created, modified, or deleted unless permission has been granted, and forbids embedded devices from making any unauthenticated connections.

The management of accounts feature has several possible scenarios, which if not implemented could cause problems for asset owners. For example, a person who works on the network gets promoted, so they now require more access to devices and applications, and their privilege level must be adjusted accordingly. Another example that is frequently encountered is when an employee leaves the organization. As soon as they cease being an employee they must no longer be able to access the network and must have their network privileges revoked. It doesn't require a stretch of the imagination to envision the possibility of a disgruntled ex- employee who was recently dismissed accessing the network after his departure with malicious intent.

Identifier management

Any component of the network with a direct user interface must directly integrate into a system that identifies individuals by user, group, role, and/or system interface. This stops users from being able to access devices connected to the network that they haven't been granted access to. As those with different roles on a network have different privileges, a network administrator's account can often manage device configurations on a network, but someone who has guest level access can only view devices, but not alter configurations. In addition, there should be security procedures in place if an account hasn't been accessed for a certain period of time that allows the account to be deactivated. The identifier management feature controls each user's account on the network and ensures that users are confined to the roles assigned to them by network administrators so that users can't accidentally or on purpose access parts of the network that they don't need to access.

Authenticator management

All devices on a network must be able to confirm the validity of any requests for system/firmware upgrades, and verify that the source isn't trying to upload any viruses or malware. This is achieved by requiring the use of tokens, keys, certificates, or passwords. If no authenticator management system is in place, anyone wishing to attack the network could very easily upload malware, allowing them to change settings or take over control of the network.

Password-based authentication

For network components that utilize password-based authentication, the network component must integrate a password policy that enforces the following:

A) The password composition must state what type of characters are allowed, and the number of characters required before a password will be accepted as valid

B) The frequency that the password must be changed

The advantage of using a password is that it is a simple way for network administrators to protect their network without requiring any additional work from system engineer. Utilizing an effective password policy will keep out the majority of hackers who gain access to networks by using brute force to break weak passwords. A network that doesn't support a password policy or a network that allows weak passwords to be used is at a much greater risk of hackers gaining access to the network.

Public key authentication

Public key authentication should be used in order to build a secure connection between servers and devices, or device-to-device connections. In order to enable this function, each network component must be able to validate certificates by checking the authentication of the signature, as well as the revocation status of a certificate. In addition, it should construct a certification path to an accepted certification authority, or in the case of self-signed certificates deploy certificates to all hosts that communicate with the subject to which the certificate is issued.

Public key authentication is important because it stops information from being sent to the wrong place, and also stops confidential information that should remain within the network from being transferred to unverifiable sources outside.

Use control

All of the devices that appear on a network must support login authentication. To restrict unwanted users from gaining access to a device or the network, the application or device must limit the number of times a user can enter the password incorrectly before being locked out.

As the majority of attacks on industrial networks are performed by hackers using brute force attacks, login authentication is an extremely effective method of stopping hackers from gaining access to a network. In addition, the system or device must also be able to inform users whether their login attempt was successful or not. Informing users that they are logged into the network allows them to confirm their current status and proceed knowing that changes or alterations they make to network settings or devices have been authenticated.

Data integrity

Across all IIoT networks data integrity plays a vital role. It ensures that data is accurate, and that it can be processed and retrieved reliably. There are several security measures that can be utilized to protect the data, including SSL, which enables encryption between a web browser and a server. As data is constantly moving around a network, network operators need to be sure that the data is moving in a safe, reliable, and efficient manner. If the data is sent to unintended recipients, the network operators will not only lose control of their data, but also leave their networks vulnerable to hackers.

Backup for resource availability

All of the applications or devices that are found on a network must be able to back up data without interfering with network operations. The main advantage of performing regular backups is to ensure that no data is lost and that if the network experiences some problems the network can utilize the data that has been backed up to return the network to normal. In addition, the backup process must ensure that any private information that is on the network is stored in accordance with data protection policies and is not accessible by anyone who should not have access to that information. In some cases this means that data can't be stored outside the network. Any data breach containing users' personal information is extremely damaging to network operators as well as to those whose data has been accessed by those it shouldn't be accessed by.

Conclusion

As more devices are being added to networks, the security of these devices is of paramount concern to asset owners. It is acknowledged throughout the industry that adopting the best practice approach to security gives asset owners the best chance of protecting their network from those with malicious intent. The complete system-level security must be built upon the foundations that consist of each individual component's security functions.

Susan Lan, Product Manager, ***Moxa Corporation.***

Achieving successful IT/OT network convergence

The march toward converging IT and OT functions on a single Ethernet network is inevitable for companies to maximize the benefits of Ethernet connectivity while also optimizing the efficiency of networks. The process promises to be challenging but hopefully will also result in a smooth, mutually beneficial effort.

PLANT FLOOR OPERATIONAL TECHNOLOGY (OT) networks and office Information Technology (IT) networks have been wholly separate for years. On top of that, IT and OT personnel often have had little to do with one another. With the advent of industrial Ethernet replacing fieldbus protocols on the plant floor, they now share a common network, creating valuable opportunities to combine resources and collaborate on goals for overall organizational success.

However, this network convergence also sets the stage for interactions - some might say showdowns - between IT and OT network personnel with very different training, experiences and cultures. The extent to which these necessary collaborations become adversarial or collaborative is dependent upon the approach taken by the organizations and individuals involved.

There is a great deal of misunderstanding about what convergence is and what it entails—for example, one group within the organization might be working toward the creation of one single, flat network while the other is attempting to segregate through technologies such as VLANs. The chances of success in this environment are low due to the steep learning curve and the opportunity for costly missteps when combining these different perspectives.

Fortunately, these challenges have become less necessary to endure. As more and more organizations converge their networks, there is a growing body of resources and best practices being published. Assistance is available through third-party consultants, manufacturer representatives and resources such as this white paper. This is a collection of experiences from Belden and partners who have helped many organizations successfully establish their own converged network. These insights can help you reduce your learning curve and benefit from a converged IT/OT network quickly and efficiently at your location.

SOURCE: BELDEN

There is a great deal of misunderstanding about what IT/OT convergence is and what it entails.

What "One Network" means

With Ethernet now commonly running on both the office/enterprise/IT side and the industrial/Operational Technology (OT) plant floor, isolated networks are no longer advisable. Converged networks give us the ability to selectively share data. Thus, we are seeing the emergence of what has become known as the convergence of IT and OT—or the creation of a single network.

The properly converged IT/OT network is not one big flat network, but one network strategically protected, so only appropriate data flows. Selective sharing controls device connectivity and data access to ensure only authorized information and resources are accessed. Specific data might flow one way, from plant to office or office to plant; back and forth both ways; or not at all. This selective sharing is a key to an effective and secure network.

Benefits of a converged network

Economies of Scale: Moving to Ethernet in the Industrial/OT environment is both practical and cost-effective. Since Ethernet is prevalent and standards-based, it can be found in consumer appliances, IIoT devices and ruggedized industrial devices. By leveraging the availability of Ethernet products and associated standards, you can now choose the best solutions from different manufacturers and they should communicate with each other with little effort.

Interoperability: The flexibility of implementing Ethernet on a converged network provides exponential benefits to the individuals in both IT and OT. Historically, industrial devices communicated through fieldbus protocols. However, implementing a fieldbus protocol, such as PROFIBUS, limits device options to only those which speak PROFIBUS. Alternatively, Ethernet supports multiple protocols. For example, think of Ethernet as a highway. All different types and brands of vehicles can travel on a highway. Fieldbus, on the other hand, is like a train track, where only trains can travel.

Information: All machines are gathering data. However, data without context is useless. With the speed and immediacy of Ethernet communications, operators can, for

the first time, collect highly detailed, real-time production data that can be strategically deployed to make smarter, cheaper, more efficient business decisions. By converging your network, IT and OT can leverage the skillsets of both teams to interpret and analyze the information.

The value of data

The primary interest of many manufacturers is often data capture and analysis due to its powerful and quick rewards. They can raise the bar on production goals, then gather the appropriate data and determine how to get there.

Value is locked in OT production data nearly everywhere. For example, a past client who produces consumer goods lacked insight on the speed or functionality of their machines. When machine issues occurred, operators had difficulty communicating with maintenance staff. To combat this, an OT network was built that allowed their existing HMI to connect to a communication server and contact the appropriate maintenance personnel.

Through that data, they are able to monitor machines more effectively, measure response times and use real-time production data to proactively contact the appropriate person when a machine reaches certain milestones.

Many companies like these are also finding that having production and sourcing information down to each individual component is extremely valuable. They can use this information to track and trace issues with specific units and ensure that such issues are minimized. Further, many industrial companies are finding that collecting data and storing it is valuable, even if you don't have the right questions to ask yet. Manufacturers might want to investigate something later and having production data to analyze from previous months and years is very valuable in the pursuit of such knowledge.

In the pre-Ethernet days, if this type of information was collected at all, it might be hand captured on clipboards and all but lost. Even if it was later looked at, it was subject to illegibility, transposed digits, decimals in the wrong place and any other type of human error. Using Ethernet to capture and analyze information makes it potentially useful intelligence as opposed to pen scribbles. Nearly every industrial company can benefit from these possibilities, and with the technology so readily available, more and more are moving forward to put it to work.

Designing a converged network

Avoid quick fixes and short-sighted solutions, such as connecting existing IT and existing OT networks. A converged network should not be formed from two existing networks. The methodology "just plug them in" seldom works.

Network audit

The first step in designing this new network is identifying what is on the network currently. This process is known as a network audit and gives insight into what devices are where, and what each is currently talking to. This is also a good time to develop accurate documentation as to the network structure.

Odds are, if you've never audited and inventoried the network, you may be in for some surprises. Things tend to be added over the years without concern for the holistic nature of the network. This is your opportunity to start with a clean, streamlined, efficient slate. The concept of a handful of OT devices being joined with an IT network is not unusual and it is usually only discovered—and expensively so—when there is an IT-side incident or shut down.

Through a network audit, one factory discovered their capping machine was built with an unmonitored and unprotected cellular connection to the Internet. This device was unknown to the buyer of the equipment and they had no idea who had access to it or how it was connected. This is just one example of how network audits are essential to designing a converged network.

Assessment

Once you've inventoried everything, your next step is to assess the status of your current network. At this snapshot in time, what is the quality of your network? You will identify the purpose of each device and decide what should be talking to what. Then you can create the optimal data flows for each case. It's a very individual and technical discussion for the organization, and strategic planning should be done.

As a few general examples, production data might flow up to analysis software that may reside in the enterprise where it may be selectively reported to salespeople and non-technical managers. Other OT-generated data, such as real- time status reports or maintenance schedules, would likely stay in OT. By the same manner, IT data, such as personnel records and salary data, should not be accessible by the plant floor.

Structuring IT and OT

The inventory/audit will help you keep all OT machine functions out of the IT world and vice versa, ensuring that nothing is inappropriately tied to the wrong network, so the proper security protections, resources and connections can be applied. The often cited Purdue Architecture Model is a good, simplified illustration of a basic network architecture.

There are certainly some gray areas. Remember, it's not where the device is located, it's what it does. For example, there might be a device used to access e-mail on the plant floor and these would be connected to the IT network, not the OT network. Purposes should NOT be mixed; mixing capacity opens up serious vulnerabilities. The PC on the plant floor with browser and e-mail function should NOT also be used for production data. Each device should be strictly determined as an IT or OT device (think: what it does, not where it is located) and attached to the network accordingly.

SOURCE: B&R

Consider a DMZ

In between the IT and OT domains is what is known as the DMZ. This shared territory is where both worlds come together and what is shared with whom is determined.

Physically, this area is a collection of servers and PCs, with information flowing up from OT and down from IT, directionally protected by firewalls. Here it is appropriately processed and then directed back to the pre-determined location. The information flowing in and out is carefully controlled - selectively shared one way or two as appropriate.

One important function of the DMZ is to keep a wide buffer zone between the outside world accessed by IT—with its threat of hackers and viruses—and the bread and butter world of OT. Threats from the business side need to be isolated from the OT world and can be accomplished through compartmentalization such as ISA99 / IEC62443. This protects the manufacturing side from being impacted by IT threats and allows production to continue. Further, the DMZ helps ensure that production equipment would not be subject to IT necessities, such as virus scans or firmware updates.

Don't make security an afterthought

A plan needs to exist and be integrated as to how you will share data. Begin with determining security needs that should be built into your network. The National Institute of Standards and Technology (NIST) has made recommendations on cybersecurity for reference.

Don't wait for the perfect solution to solve every scenario. As part of this plan, document what simple actions you can take to increase your security and implement them immediately.

New organizational agreement

Even in an organization where IT and OT people work well together, inevitably, it will come up: Who is in charge in situation x? Does IT or OT have the final word on equipment and operations in the DMZ? Who specs network-wide Ethernet equipment?

When the converged organization is built, the purpose is to share information and support both the OT mission and the IT mission. Decisions need to be thoughtfully made to ensure there is not a "winner" and a "loser" and subsequent disgruntlement. A

SOURCE: BELDEN

IIoT edge gateways need to perform several different functions and process large amounts of data from a wide range of devices and systems.

better way may be to create a new dotted line organization, frontloading universal buy-in from both IT and OT, at all levels.

In most organizations, this starts with immediate and demonstrated support from the top. It's good practice to see leaders from both the business and production teams join together and express their support for all IT/OT convergence activities. It is vitally important that IT and OT collaborate and communicate, establishing clear responsibilities. Whether that is two individuals serving as representatives, a committee or a newly created role such as an Automation and Data Exchange Engineer (ADX).

Automation & data exchange engineer

We suggest the addition of a new individual, a professional who understands first-hand the functions and priorities of both the IT and the OT worlds and is capable of communicating with and relating to both departments. We call this individual the Automation & Data Exchange (ADX) Engineer. It is imperative that this person is cross-trained substantially in both OT and IT practices with their background of what discipline they came from originally being less important. They could, for example, be a networking engineer who has spent time working or training on the plant floor learning about automation operations, needs, and challenges. Or, they could be an automation engineer who has completed networking classes and earned certifications from educational organizations or vendors.

Led by the ADX Engineer, there should be governance responsibilities for all things related to the converged network, answering directly to upper management. One of their early duties might be to develop proper procedures for management and operation of the converged network. They can create a Standard Operating Procedures (SOP) guide for everyone to be aware of the new road ahead. The valid concerns of both IT and OT disciplines will be accounted for, with potential SOPs including directives such as "Patches will always be tested in an isolated sandbox before being applied to any OT equipment," or "Internet-connected devices shall not be placed directly on the OT network."

The committee or ADX Engineer should also lead all convergence establishment and maintenance activities. If it is a multi-location organization, they can start with a "pilot project" at a smaller location and take key learnings on to additional locations. After assessing the extent of the convergence challenge at each location, they can also decide, case by case, whether internal resources possess the expertise—and the extra time—to tackle each project. They can work together to identify and select a turnkey third-party expert, identify local resources to handle the job, or some combination of both as the team sees fit.

Often, an outside third-party is beneficial as they can provide insight from a different perspective, share best-practices and provide instant, on-demand man power.

Encouraging Cooperation

In the drive for successful IT/OT convergence, we have seen situations where one group or the other, resisting change, stuck their head in the sand and refused to cooperate, causing very difficult roadblocks. We have seen situations where one group or the other called in outside help and, literally, said "don't let the (other department) know that you're here." Fortunately, this is not the norm; most organizations are made up of professionals who will work together for the common good and it is assumed that your organization will not experience anything like this. But, theoretically, what if it does?

The visible involvement of C-Level executives will help in this regard. If it's holding up progress, they will hash it out. Petty squabbles like "I'm not working with that guy, he messed up (fill in the blank) last year" will presumably dissolve if cooperation is expected.

Another effective strategy is to involve a third party, at least at first. It's often amazing, humbly speaking, how an idea repeatedly expressed by an insider is ignored, but that same idea expressed by an outside expert is considered genius. That's reality and it's helpful to understand. Of course, a well-chosen IT/OT consultant who has "been there/done that" provides both technological and psychological mediator-type assistance and will deliver much more than inside people ever could, drawing upon the experience of driving convergence in other organizations and helping to flatten the learning curve.

It is important that the consultant understands, has experience in and speaks the language of both IT and OT. They should be without loyalty to one side and have knowledge of both so they are not seen as "the IT consultant" or "the OT consultant" but as the "Convergence Consultant." Otherwise, the internal disconnect can be worsened and frustrations compounded. Bringing in someone with a proven track record of understanding the needs of both IT and OT immediately bridges the gap, and sets the organization up for IT/OT convergence success.

Conclusion

The march towards the convergence of IT and OT functions on a single Ethernet network is inevitable for companies that wish to maximize the benefits of Ethernet connectivity while also optimizing the efficiency of the network. This will not come without challenges and growing pains which vary from costly, multi-year processes, to being accomplished by a smooth, mutually beneficial effort. Using information in resources such as this article can help move your organization decisively into the latter.

Technology report by ***Belden Corporation.***

Numerous tools on one platform save time and money

A manufacturer of precision machined aluminum die castings and subassemblies reduced costs and raised efficiency by implementing an industrial application platform. New tools enabled building solutions in human-machine interfaces, SCADA and the Industrial Internet of Things (IIoT).

MADISON-KIPP CORPORATION (MKC), BASED IN Madison, Wisconsin, makes precision machined aluminum die castings and subassemblies for the transportation, lawn & garden, and industrial markets. When it wanted to bring down costs and raise efficiency, MKC implemented an industrial application platform with tools for building solutions in human-machine interface (HMI), supervisory control and data acquisition (SCADA), and the Industrial Internet of Things (IIoT).

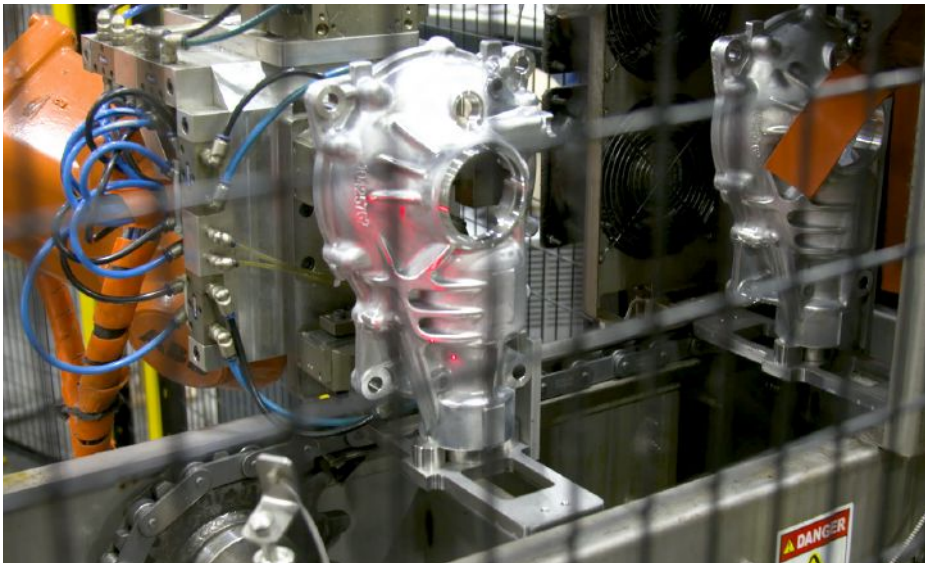
The web-based Ignition platform from Inductive Automation provides unlimited licensing and strong interoperability, both of which help MKC with numerous projects. The company uses the platform for central SCADA, control of Ignition Edge clients, part tracking, part history, reporting, alarms, alarm history, transaction management, API access, predictive control for HVAC, text notifications, and more. Visual capabilities give Madison-Kipp a more accurate picture of what's happening on the plant floor.

"Technology is very important to us," said Bill Johnson, vice president of operations for MKC. "We have to keep ahead of our competitors in many different areas. Using Ignition and taking real-time data from our processes helps us understand our data — which helps us make better decisions."

SOURCE: INDUCTIVE AUTOMATION

New platform enabled development of centralized SCADA, control of Ignition Edge clients, part tracking, part history, reporting, alarms, alarm history, transaction management, API access, predictive control for HVAC, text notifications, and more.

The technology platofrm has made a big difference throughout MKC. "Some of the results we have are in the cost savings realm, and we've also seen improved efficiency," said Johnson. "Before we had Ignition, engineers had to collect data on their own. This would take a long time. Now with Ignition, we're able to pull that data in and look at it and solve problems very quickly."



SOURCE: INDUCTIVE AUTOMATION

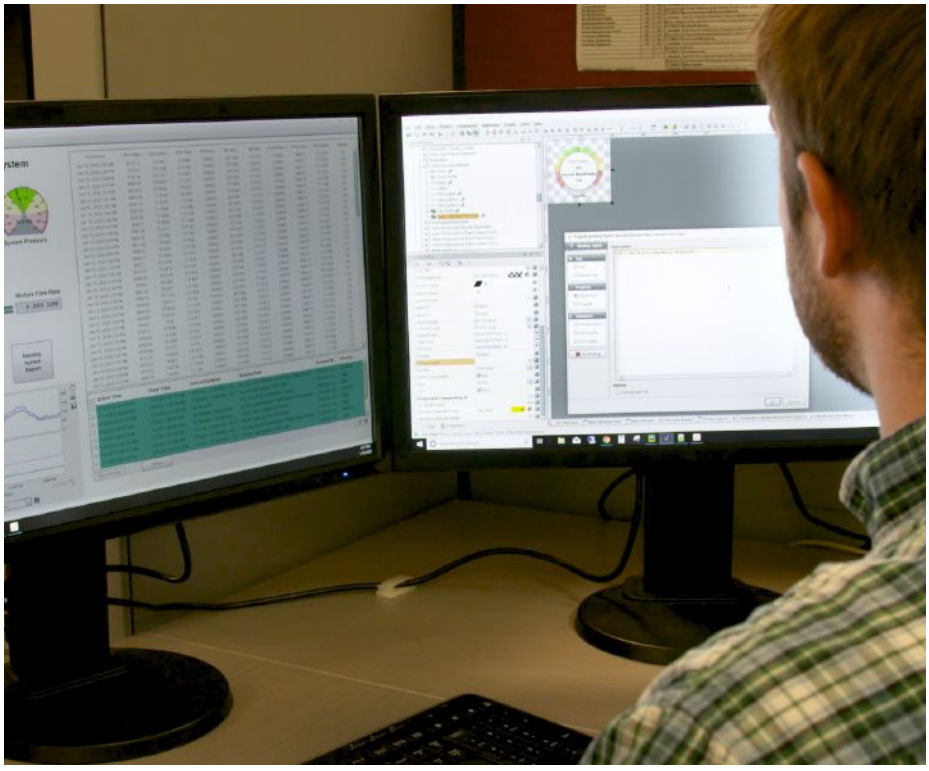
The ability to connect to a wide range of devices has eliminated numerous proprietary roadblocks.

Surprising interoperability

The system can connect to a wide range of devices which has eliminated numerous proprietary roadblocks for MKC.

"The Ignition platform has filled a void for us between multiple manufacturers and platforms," said Jay Sandvick, senior automation controls engineer at MKC. "It's given us interoperability that we didn't believe we could have. We now have accessibility to data streams we didn't have before. And we have the ability to generate seamless reports from machines that were previously thought unconnectable."

Dotti Jacob, industrial integration engineer at MKC, has also been impressed with the platform's ability to connect. "Ignition has been a lifesaver in allowing us to use different programming languages, and tie into all sorts

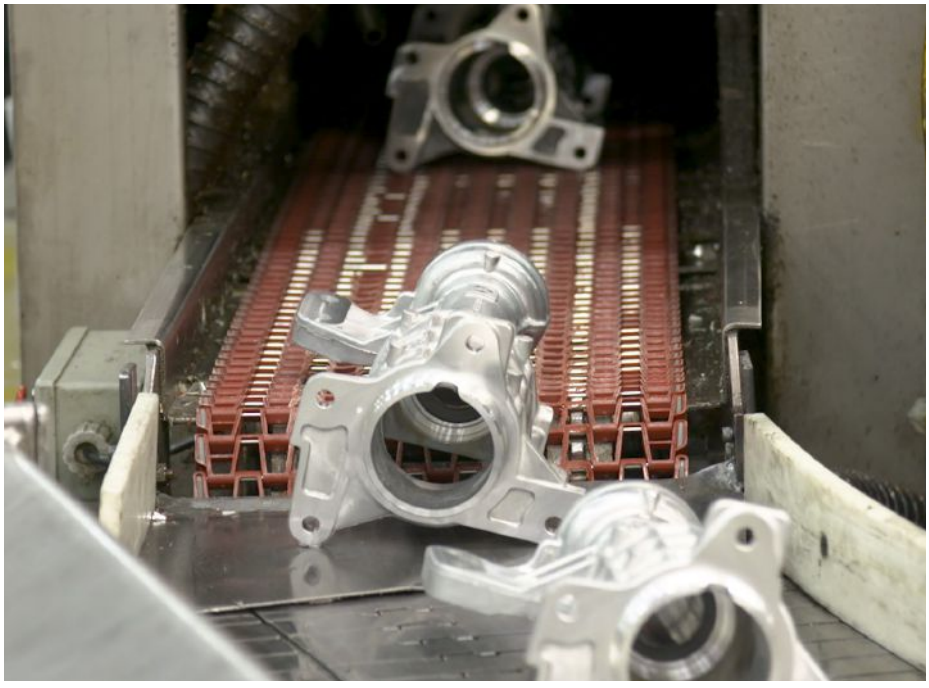


Customers benefit from the ability to see real-time data on products during production.

of different systems, without being held back by proprietary issues," she said.

The platform's interoperability has allowed MKC to streamline its systems. "Before Ignition, we were reliant on various software packages that were frankly a nightmare to maintain and pay for," said Sandvick. "With Ignition, we have a single-point interface, a single cost, and it has more than exceeded our expectations in talking to various machines."

Remote access has been greatly improved. "Before, if I was at a different facility and there were troubleshooting issues, I would have to travel there to help out," said Jacob. "Now that we have Ignition, I can access the SCADA from anywhere and see in real-time actual images of the different machines and what they're doing which is very helpful for troubleshooting. Having real-time data we can access from anywhere allows us to see and address the issue more quickly than we could in the past–which saves us time and money."



Customer can access real-time actual images of the different machines and what they're doing.

Customers see data

More than ever before, MKC's customers want to know how their products are being produced.

"Data access is something that our customers are no longer just asking for; it's becoming a requirement of doing business," said Sandvick. Ignition allows MKC to share data with customers, no matter where they're located.

"Our customers really enjoy the ability to see real-time data on their products being produced," said Scott Sargeant, vice president of sales for MKC. "It allows them to understand things without having to travel to our location -- which of course saves them time and money. We're talking about a paradigm shift in information sharing. It really gives our customers a window into the production environment.

And our ability to provide this helps differentiate Madison-Kipp from other manufacturers."

MKC's customers now have more knowledge about the process than ever before. "In the past, our customers weren't able to understand what variations we had in the process, or just how efficient the process was," said Sargeant. "Now our customers can see that data, can understand impactful events, downtime, and other important issues in production."

Better Graphics

Ignition can use CAD drawings of the plant floor as the background for screens. The screens show real-time movement of robots, so operators always have an accurate view of what's happening.

"Before, we had to use these cookie-cutter images that were not very accurate to what was actually happening on the floor," said Jacob. "Now we're able to take a CAD drawing of the equipment, and it can move in real time with however the equipment's moving, and that's very helpful."

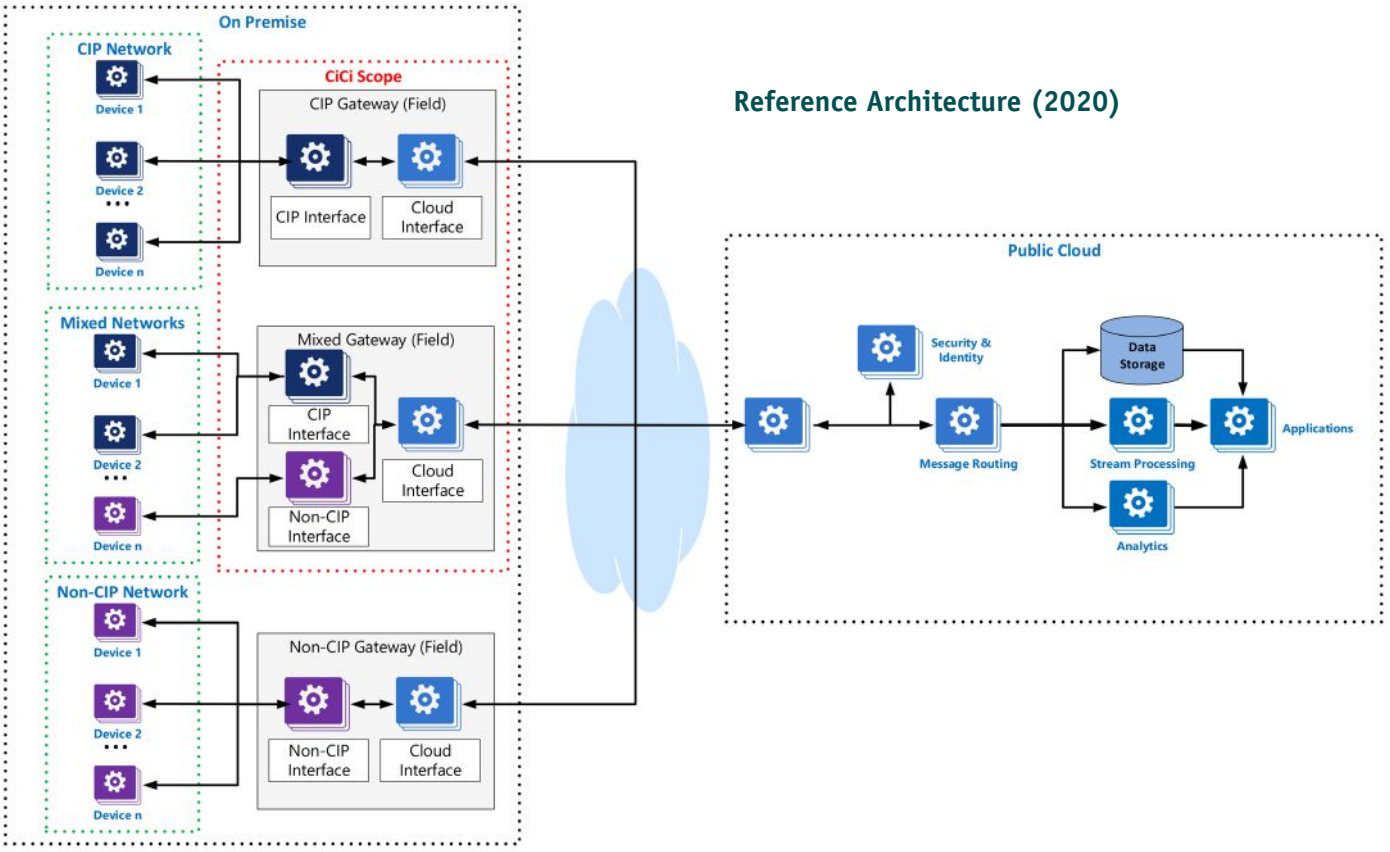
Jacob said Inductive University has also been a big help. The free online educational center has hundreds of videos and allows users to learn at their own pace. "When I started with Madison-Kipp, I'd never heard of Ignition," said Jacob. "I was able to get up to speed very quickly because Inductive University has videos that teach you anything you need to know in order to be successful using the software."

With positive results in so many different areas, Madison-Kipp plans to expand its use of Ignition. "Strategic initiatives are vitally important for any organization," said Johnson. "When we set our initiatives for 2020 on the technology side, Ignition is one of those strategic initiatives that's going to help move us forward this year."

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

Use Cases for a CIP Companion Specification for OPC UA

An OPC UA companion specification for CIP to OPC UA Gateways is based on assumptions that the cloud interface will use an OPC UA information model; it will use OPC UA transport mechanisms (MQTT, AMQP or HTTPS) and the cloud interface will use OPC UA defined cybersecurity roles, authentication and encryption.



SOURCE: ODVA

HAVING CONCLUDED THE FIRST ROUND OF requirements capturing for vertical integration of Common Industrial Protocol (CIP) devices to cloud applications, the Common Industrial Cloud Interface (CiCi) Special Interest Group (SIG) has determined that a key element of an overall solution is an OPC UA companion specification for CIP devices.

Based on this conclusion, a plan is currently under development between OPC Foundation and ODVA for a joint working group to produce this companion specification. In order to ensure that this companion specification meets the requirements of both ODVA members, and of users of CIP technologies the CiCi SIG is now refining those requirements to specifically address companion specification relevant use cases.

This article explores user stories and use cases against which that OPC UA companion specification will be developed. It recaps the work done and benchmarks it against the Device Integration model best practices. It will take advantage of recent lessons learned within OPC Foundation that are being addressed in their Harmonization Working Group and will propose a harmonization model to allow CIP Technologies to integrate seamlessly with the latest OPC UA specifications.

Related work

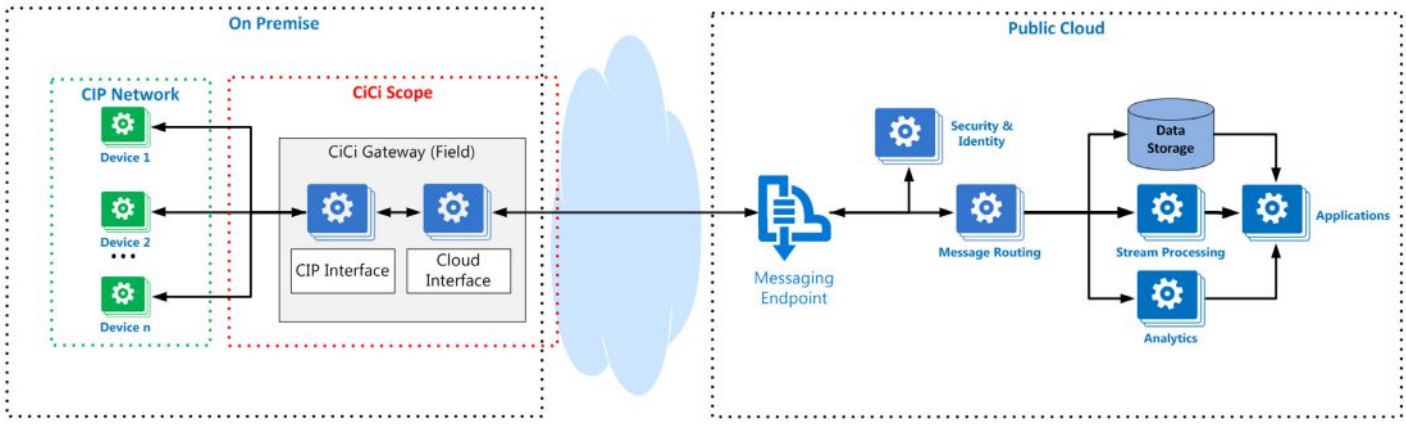
The goal of this initiative is to deliver an open, cohesive approach to implement OPC UA including TSN and associated application profiles. This will advance the OPC Foundation providing vendor independent end-to-end interoperability into field level devices for all relevant industry automation use-cases. The OPC Foundation vision of becoming the worldwide industrial interoperability standard is advanced by integrating field devices and the shop floor. A new set of working groups is identifying, managing and standardizing the OPC UA relevant topics focused on industrial automation including:

- harmonization and standardization of application profiles like IO, motion control, safety, system redundancy
- standardization of OPC UA information models for field level devices in online and offline scenarios e.g. device description including diagnostics
- mapping of OPC UA application profiles related to real-time operations on Ethernet networks including TSN
- definition of certification procedures

Megatrend in global manufacturing

Commonly called Industry 4.0, end users of automation products, machine builders and component suppliers are seeing new opportunities to integrate the automation value chain, reduce costs through new business models and implement new techniques for process optimization. The key technology that makes this possible is the internet, coupled with mass data storage and securable real-time global access to this stored data.

This megatrend is most visibly demonstrated from two angles; national governments are implementing smart manufacturing initiatives to enable competitiveness of their local



Common Industrial Cloud Interface (CiCi) Reference Architecture (2017)

manufacturing base; bottom up corporations are providing delivery platforms to monetize digitization domain expertise.

Two examples from the multiple government led smart manufacturing initiatives, together with their core claims are listed below:

Plattform Industrie 4.0 in Germany: "For Industrie 4.0, it is not the computer that is the core technology, but rather the Internet. Digitalising production is gaining a new level of quality with global networking across corporate and national borders: the Internet of Things, machine-to- machine communication and manufacturing facilities that are becoming ever more intelligent are heralding a new era: the fourth industrial revolution, Industrie 4.0."

Industrial Value Chain Initiative in Japan: "The Industrial Value chain Initiative (IVI) is targeting to turn linked factories and connected manufacturing into reality. In some cases, the result that developing a new system at the enterprise as a whole or at its manufacturing site is needed. In other cases, the challenge may be solved through small improvement efforts by applying IoT tools."

Similarly, two examples of corporate delivery programs and their goals are:

The Connected Enterprise from Rockwell Automation: "New insights that are revealed through better data access can help you reduce bottlenecks, implement demand-based decisions, and improve maintenance."

Azure IoT from Microsoft "Organizations across all industries are using Azure IoT to invent new lines of business, improve productivity, and reduce waste by using AI and machine learning to quickly process massive quantities of data from IoT devices."

Common factors of all these initiatives are:

- Enterprises need to consolidate information across multiple plants
- Supply chain and value chain partners need to share information during the operational phase of a plant
- Cloud technologies must be used to secure and distribute information, abstracted from local assets

Common Industrial Cloud Interface

At the ODVA Annual Meeting in 2017, the CiCi SIG proposed a reference architecture as a basis for their work. In addition, the CiCi SIG presented a number of use cases, which are not duplicated in this document, although some are extended.

These use cases are organized under different phases of a device's life cycle. The use case explored in this document will be extended to consider the life cycle of more complex automation assets, i.e. a machine or collection of machines. Finally, the use case titles were followed by references to a set of communication patterns between a cloud application and a target gateway device.

Reference architecture

The use cases and technical requirements for data transfer white paper proposed a Reference Architecture for a CiCi gateway solution.

This reference architecture assumes that within a plant (on-premises) the user is concerned with only one communications technology. This article will expand the reference architecture to assume a need to support information coming from multiple communications technologies.

The assumption is that OPC UA is a critical partner technology and that joint work will be performed in order to deliver a companion specification. Through the rest of this paper it is assumed that:

- the cloud interface will use an OPC UA information model
- the cloud interface will use OPC UA transport mechanisms (MQTT, AMQP or HTTPS)
- the cloud interface will use OPC UA defined cybersecurity roles, authentication and encryption The use cases/user stories below will attempt to explain why these are reasonable assumptions.

Industrial Value Chain

In this section, we define the stakeholders, both from the perspective of the types of organization, companies and other entities that add value to an EtherNet/IP device through its supply chain, together with the human roles fulfilled across those entities.

Stakeholders represent the legal entities who have interest in a particular story. There may be multiple legal entities who hold a stake in a particular story.

User stories and use cases

Optimizing Production Processes by Role

As a Plant Manager I want to enable my Data Scientist to be able to access data from my assets, so this data can be analyzed and used to optimize production.

As a Data Scientist, I want to be able to discover my assets and their associated devices that may provide useful data for analysis, so these devices can be further queried for the data they may contain.

As a Product Developer, I want to expose only data that are useful for optimizing the specialized asset, so data collection is simplified for customers and plant operators.

As a Business Manager at a Device Vendor, I want to enable my Data Scientist to be able to access some data from my Devices, so that my Data Scientists/specialists can make recommendations that result in operational improvements.

As a Plant Manager, I want to only expose data that will not disrupt the operation of my assets, so that downtime can be avoided.

As a Process Engineer, I want to assign data reading resources, so that there is adequate bandwidth for operating my facility and providing data for analytics.

As a Security Officer, I want to guarantee that only authorized connections can be made to my assets and only authorized devices can be discovered and authorized data can be read.

The native protocols of the devices in these use cases are not important to achieving the desired outcomes. In most operations, there are mixtures of vendors and protocols in use. What is important is enabling these actors to have access to data contained in their assets. The "shape" or context of the data is also very important to the value of the data. More

context makes it easier to provide valuable insights. Also, data scientists use different tools that are aligned with cloud technologies, largely due to the significant amounts of data storage and process power required. These technologies are evolving to be able to take advantage of computing power on the "edge," but they still require services or mechanism that will discover devices on the network, specifically for CIP devices, pull information from the data available and present that data in a standardized way to applications on-premise and on the cloud.

Machine/Skid Builder/Integrator offering remote service of own supply

As the business manager of a machine builder, I want to offer value added annualized services to my customers. In the long term, this will be leasing machines on a usage basis, but the next step my users are prepared to take is outsourcing maintenance.

To deliver these services, I am prepared to invest significantly in instrumentation from multiple vendors and software in machines I deliver. I want to create parts of the information model in controllers that is only available for me to access. I consider this information to be mine and not my customers and not for use by service providers. In order to simplify access, I want to be able to deploy a single gateway function (standalone compute appliance or embedded in the controller I select) which will provide connectivity to my own historical cloud storage.

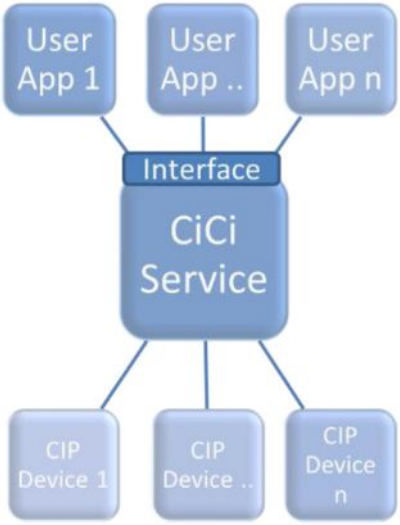
I want this gateway to securely deliver my proprietary information together with standardized and vendor specific information from the components, together with application specific information in controllers and information from discrete devices in the machines. For the machine builder, supporting the native protocol required at a plant is critical to their business – essentially the same machine will be delivered using both CIP and third-party protocols to the different plants – it is only in hybrid plants that the machine builder may have any autonomy.

However, like the data scientist the machine builder will have a strong preference for a single cloud-friendly protocol to deliver consistent information from all of the plants.

This story brings a new requirement which is around role-based security – that the provision of information to the cloud is controlled by the machine builder and not by the user of that machine. Further delivery requires input from the plant network engineer who will be responsible for creation of firewall rules. The fewer technologies deployed, the less work and more importantly, the less risk created.

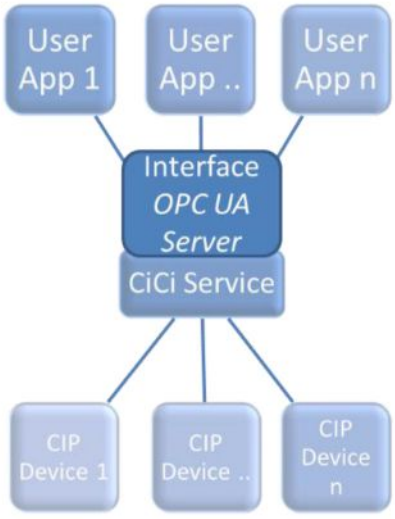
Increased service delivery

As I increase the number of machines on which I deliver these services, I will want to adjust



SOURCE: ODVA

Common Industrial Cloud Interface Services.



CiCi OPC UA North Side Interface.

the information that is delivered to my cloud storage based on experience gained. I must be able to make these changes without physical access to the gateways. I must be able to document and enforce a service agreement with my users about changes that can be made to the running system. Also, like the data scientist, they will have a preference to be able to select variables for monitoring long after commissioning – to avoid replicating the entire machine database in the cloud.

Provide information from inside a machine for Data Analysis

As a data scientist working for a Plant Owner, I want to get "important" or pre-selected data and context from my assets so that I don't have to understand or learn each asset in my enterprise. Extending from Optimizing Production Processes, the data scientist will prefer technologies supported by their cloud vendor, with no concern for the technologies supported by the Device Vendor. The selection of cloud drives communications and not the other way round!

SOURCE: SOFTING

More importantly, the data scientist cannot be assumed to have any domain expertise in either field level devices or communications technologies. Consistent semantics across components, technologies, machines and plants are critical to their success. This means that in the CIP driven plants, all devices must present their metadata using common and well-defined terms and meanings/interpretations. But for the data scientist, whether the plant is CIP driven or third party driven is irrelevant – they want to see the same semantic definitions presented in both cases. This is even more true for the hybrid plant.

To facilitate this device discovery, services to collect the metadata available in each device, and a method to build the metadata into an information model without manual configuration, will be important for adoption.

It is worth noting that the OPC Foundation has a program running called "Harmonization" to address this problem within their own family of companion specifications. Our objective should be to minimize the pain to our users and that we do not increase it.

Device vendor offering remote service

As a Business Manager at a Device Vendor I want to connect to devices when then are used by either machine builders or end users, so that I can offer remote services to ensure the devices I have supplied are operating properly.

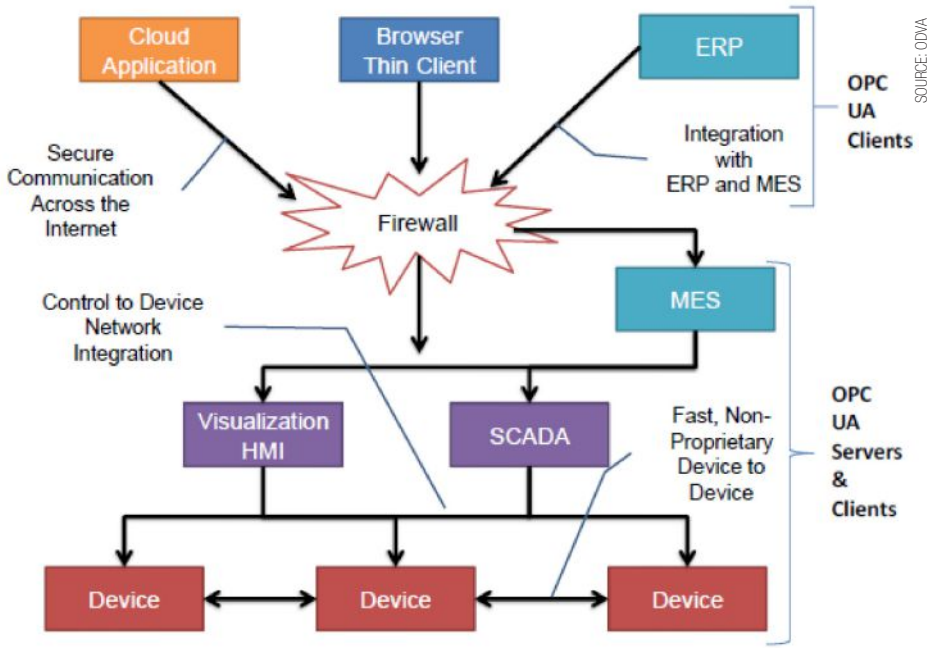
For this purpose, a plant operator needs to grant access to the installed devices for the device vendor but only to the devices of interest. As a device vendor, I want to setup an ad-hoc and exclusive connection to the device and I also may setup a continuous monitoring routine. As a plant operator, in order to allow remote access to devices, I want full control on the permission levels and time, when the access occurs (is allowed to happen). As plant operator, I need to be able to notify the subscribers of a device's data about the potential un-availability of function.

In many ways, this story is identical to the machine builder stories, but with completely different cloud suppliers and information flows involved. Our objective must be to ensure a single approach supports both stakeholders.

A key value is that plant maintenance technicians cannot be practically expected to have expertise in every device in their plant. This support may be delivered in an ad-hoc manner, rather than the programmed and scheduled manner of machine builder support.

Asset management of installed base

As a plant owner I want to be able to establish an asset management system in my plant, which is able to read the asset management and identification parameters from each device/component (hardware/software) that



Scope of OPC UA Within an Enterprise.

is installed in my plant, so that it is possible

- to search for components for which a recall action, Software termination or a hotfix/update exists.
- to create a complete inventory list of all installed and communicating components (hardware/software) for easier root cause analysis in case of failure.

Asset management is typically performed across multiple plants with common identification approaches needed for all devices. Again, this means commonality between CIP and third-party technologies to deliver the anticipated value.

It should also be noted that the security officer is a key stakeholder in the asset management use case, having a responsibility to respond to vulnerability notifications from vendors and put in place remediation plans.

Anyone has access to data in devices

As a product developer of a new and innovative software application, running on a blade server (on-premises or in-cloud) I want to be able to find all of the components (controllers or devices) that have potentially useful information using off-the-shelf browse mechanisms. I do not expect the original developers to have planned for my use. I know that some of those devices will provide me information directly and some will be represented by aggregators or other edge-gateway type devices.

Once I have found useful information I want to be able to read it whenever I want using off-the-shelf mechanisms. While my task will be made easier with devices because of the consistency of their information models, I do not expect to have knowledge of any specific mechanisms (state machine, application relationships etc.) to read that information.

The value of a project is derived from application of software and not directly by the device or automated system. In this case, the communication technology will be determined solely by the software developer and it is the responsibility for CIP devices to provide data for these applications in the desired mechanism(s).

These software applications will be customized based on the installed base of devices and equipment, so discoverability of information contained in CIP devices will be needed. In addition, both on-line and off- line enumeration of information may be needed as some applications may require configuration prior to delivery. The following applications may be considered applicable to this story:

- IoT Gateways
- HMI, SCADA or MES
- Analytics, including Machine Learning
- Energy Management
- Predictive Maintenance

Browsing network for optional information

A story where user wants to browse network to find information – to identify all instruments whose calibration date expires in next 6 months. Not every device has this information.

Common diagnostic view

As a process operator of a machine at a manufacturing plant I want the diagnostics for all of the components in my system to be automatically aggregated into a single user view. I want to be able to filter this view to isolate network diagnostics, component diagnostics and application diagnostics. Where there is time available, in the device (and I know that not all devices will support time), I want it to be presented as a common wall clock time and I want any timestamps to be generated at the lowest level in the architecture where time is available in the system and for that time to be maintained with the diagnostic.

This story requires a significant level of integration between the CIP plant level technology and the OPC UA 'up-link' technology. Some of this integration may require extensions to the CIP protocol to be made possible and others may result in conformance-testable gateway functionality.

Minimize number of Security Servers

As an Engineering Director at a system integrator, I want to deploy the smallest number of security technologies and servers possible to cover all of the sub-systems that I am delivering, of which industrial automation is a subset. Proliferation of security technologies across communications technologies is already becoming a source of pain for many users, generating a need to manage authentication and key servers for each. As the companion specification is developed, it must address the needs for integration of security across technologies as well as the integration of information.

A Common and Consistent Security Policy

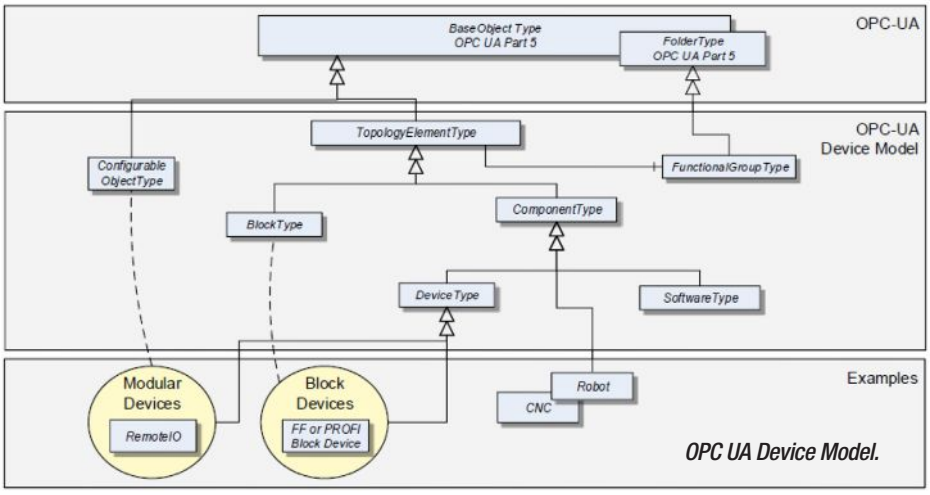
As the Security Officer, my role is to minimize the security risk to the operations of my organization. I want to ensure that the desire for access to production information is achieved in a way that protects the intellectual property of the organization. As well as considering both the IT and OT domains on-premise, I will want to ensure that any off-site storage of my organization's proprietary data is managed in a way that minimizes the chances of it being compromised.

As part of my role, I need to ensure that tools are in place to allow the organization to define and implement rules for access and authentication, whilst providing accounting capabilities so that access can be monitored and reviewed. I will define policies – based on a risk assessment – that need to be implemented to mitigate against these risks.

A specification for cloud connectivity therefore needs to reflect industry best practice, allowing a solution to build on the strengths of each domain, while preserving end-end security. It needs to address aspects such as the interaction between internal and external technologies and policies – as well as to provide the means to address practical aspects such as defining policies and procedures for the management of servers. Definition and rights of roles needs to be consistent from device to cloud.

Alarmable Conditions and Scenarios

As a Process Operator at a manufacturing plant, I need to be able to monitor all devices, including edge devices and cloud interfaces such that if they go into alarm, I need to



SOURCE: ODVA

OPC UA Device Model.

have a common troubleshooting procedures to be able to know what I can do myself, or when to alert a supervisor. If devices create an actionable event, such as a confirmable message on a process control system, I need the content the message to provide clear instructions to take the proper action.

Common Maintenance Activity

As a Maintenance Technician, I need to be able to replace equipment based on regular maintenance schedules, or in the case of faulty equipment, and I need to have clear indications (via logs, alarms or maintenance recommendations) as to which devices need replacing. This could be equipment such as an edge gateway or a cloud interface hardware. I need to have access to spare parts in a timely fashion from a storage depot or maintenance back office. The replacement of this equipment should be intuitive, or clear replacement procedures readily available online, or physically printed on site.

Brownfield Installation with Regulations

As a Plant Manager responsible for a pharmaceutical production operation that is currently validated by the Food & Drugs Agency (FDA) I am being tasked to provide additional data of my processes to support Good Manufacturing Practices (GMP)facilitate an energy management campaign for ISO 50001, and other overall operational improvements.

This data includes asset, diagnostic and process data. Asset data can include device type codes, revisions, catalog, and serial numbers. Diagnostic data may include alarms, fault codes, memory faults, etc. Process data would be values such as pressure, flow, temperature, etc.

My current system has CIP devices with interesting data that I can use. I may also need to add a third- party device (non-CIP) to my network for additional data. I would need a gateway to collect this data, possible contextualize the data, and send it to a cloud for monitoring and analysis.

A variance to the risk assessment for validation protocol can be written since we are not modifying/changing the control program, any devices or functionality to the production operation. It is important that we do not have to undergo revalidation to save time, costs while retaining optimal uptime.

It is necessary to have a gateway that is secure, does not receive inputs from the cloud, only pulls data from devices and pushes it to the cloud. It should have an ability to contextualize data before sending to the cloud if needed. This should not impact the validated process and equipment, and, provide a risk-free way of data collection for analysis. There must be no programming or commissioning changes required at the PLC/DCS.

Thin-slice approach

The premise was that Cloud vendors have "preferred gateways" that can be used by a "User" application to send data to/from cloud. Therefore the task of ODVA is to provide an <interface> that "User" applications could use with the following functions:

- Browsing / Discovery of CIP devices on the local subnet
- Provide Identity Object information from discovered CIP devices
- Provide Connected/Not-Connected status of any valid CIP device address
- Return EDS file from device, if it exists
- Return values of parameters that are defined in an EDS file
- Return values for parameters or assemblies as defined in a Device Profile

The CiCi SIG concluded that a well-defined "interface" would eventually require similar basic functionality as an OPC UA Server for security, diagnostics, discovery as well as data types and the production of data – functionality that does not exist within the CIP suite today in a directly applicable format.

Review of several OPC UA companion specifications confirmed that similar "thin slice" functionality has been defined for other standards i.e. IO-Link.

A CiCi Service should be scoped to provide functionality similar to other OPC UA companion specifications, combined with work to represent any CIP objects in an OPC UA Server

Increasing functionality of the "interface" beyond what could be defined in an OPC UA companion specification would likely be "device management" functions that may be defined by xDS or other SIGs.

OPC companion specifications

"Scope of OPC UA within an Enterprise" demonstrates OPC Foundation's self-declared goal. As can be seen, the focus is primarily on vertical integration from the device to software applications, both on-premise and cloud-based.

However, they recognized that the consumer of information used in devices is unlikely to have detailed knowledge of the field level protocols used in the interaction between controller and device. In April 2019, the Foundation published specification Part 100: Device Information Model to provide the harmonized interface called for to create the north side interface.

Conclusions of CIP requirements

In order to validate the assumptions made in section 3 Reference Architecture, we must address two questions: Do use cases require technologies not available in the CIP family of specifications? Are these technologies readily available within OPC UA and are they acceptable to our actors?

Our conclusion from this is that there is a compelling case for generation of an OPC UA companion specification for CIP to OPC UA Gateways, based on the assumptions:

- the cloud interface will use an OPC UA information model
- cloud interface will use OPC UA transport mechanisms (MQTT, AMQP or HTTPS)
- cloud interface will use OPC UA defined cybersecurity roles, authentication and encryption

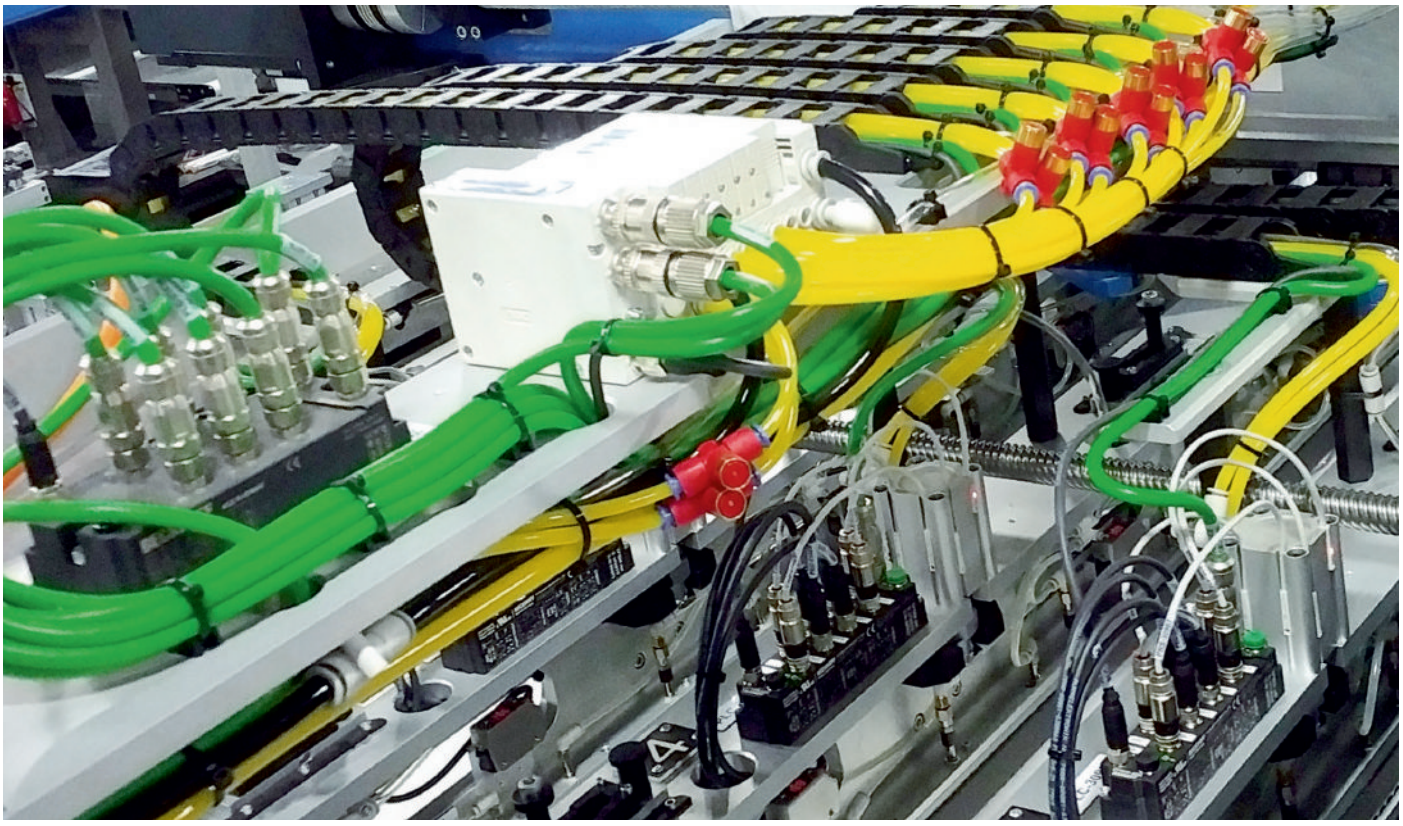
This is because almost all of the functionality missing from CIP is available already in UA; it is a far simpler task to integrate CIP using a companion specification, potentially supplemented with enhancements to the CIP specifications than creating a competing approach from scratch.

The functionality which is missing from OPC UA is typically device centric functionality long-standing in CIP specifications and ODVA core competency.

Paul Brooks Manager, Technology Business Development, ***Rockwell Automation;*** *Ken Hopwood Software Architect,* ***ProSoft Technology;*** *Frank Latino, Product Manager,* ***Festo Corporation;*** *and Steven Roby, Sr. Principal S/W Engineer,* ***Honeywell HPS.***

Scalable automation solution for heat exchanger manufacturing

PC-based automation, drive networking and Ethernet I/O reduces control technology cost and cycle times for OEM machinery builder. Use of EtherCAT technology improved PLC cycle times by 30% and reduced control system costs by approximately 30% when compared with equipment from previous vendors.



SOURCE: BECKHOFF AUTOMATION

By connecting field devices via EtherCAT Box I/O modules, RAMP minimizes wiring distances and reduces cable track requirements.

FOR ITS CUSTOMER CORE ENERGY RECOVERY Solutions, specialty machine manufacturer RAMP based in Waterloo, Ontario, Canada, has developed a solution for manufacturing heat exchangers, or energy recovery ventilators, which increase energy efficiency in buildings. By automating the production machinery with powerful and scalable Beckhoff automation products, RAMP was able to reduce control technology costs, improve PLC cycle times and complete the demanding project on schedule.

For its customers across North America and Europe, RAMP leverages its extensive experience in numerous industries with particular strengths in energy recovery and automotive projects.

The projects range from the design of new manufacturing systems to modernizing existing plants, always by combining custom-tailored solutions with standard components – to deliver maximum efficiency. Jeff Kerr, manager of mechanical design at RAMP, explains: "We cross-functionally examine all requirements and break them down into individual conceptual designs. This way, we ensure that all mechanical and control components are fully compatible, resulting in the best possible solutions for customers."

Recently, RAMP developed a machine for Vancouver-based Core Energy Recovery Solutions. The system, which was installed in 2018, manufactures heat exchangers or energy recovery ventilators (ERVs) that increase the energy efficiency of ventilation systems in residential and commercial buildings. The heat exchange is achieved by conducting cold and warm airflows past each other through internal channels.

The machine takes base materials, including a patented polymer membrane and corrugated aluminum foil, and laminates them in layers of various heights and pitches based on the customer's unique recipe. The second half of the machine takes the laminated materials through a high-precision vacuum conveyor that was designed and built by RAMP. This custom sheet layer then has separating materials placed on it using a unique pick-and-place process with standard pick positions but recipe-driven place positions varying from 250 mm to 1 m.

Finally, the layers are stacked across multiple dimensions and heights according to the last customer specifications and discharged via a conveyor belt.

Powerful open control technology

For the Core project, RAMP relied on PC-based control technology from Beckhoff to implement the scalable drive technology, efficient controls and integrated I/O system.

The programming of PLC and motion control components with TwinCAT 3 in various IEC 61131-3 languages extends the company's standards-based approach to software engineering. TwinCAT also helps RAMP leverage open, vendor-neutral technologies like the OPC UA standard for secure connectivity to higher level databases such as Amazon Web

Services (AWS) and SAP.

For Core Energy Recovery Solutions, RAMP required a powerful Industrial PC (IPC) to handle the company's recipe and data acquisition solutions in addition to the automation software.

"Since we needed an IPC that could run our applications with a one millisecond update rate to have maximum control over the process, we picked the high-power, cabinet-mounted C6930 IPC from Beckhoff," says Steve Slothouber, project control lead, RAMP. The IPC also featured sufficient performance reserves to accommodate the rising requirements from repeatedly adding I/O components during the one-year development phase, and to complete the project within the tight deadline.

RAMP connects the C6930 to advanced CP2916 multi-touch Control Panels from Beckhoff to display dashboards that provide operators with an overview of current production data and overall equipment efficiency (OEE) information.

SOURCE: BECKHOFF AUTOMATION

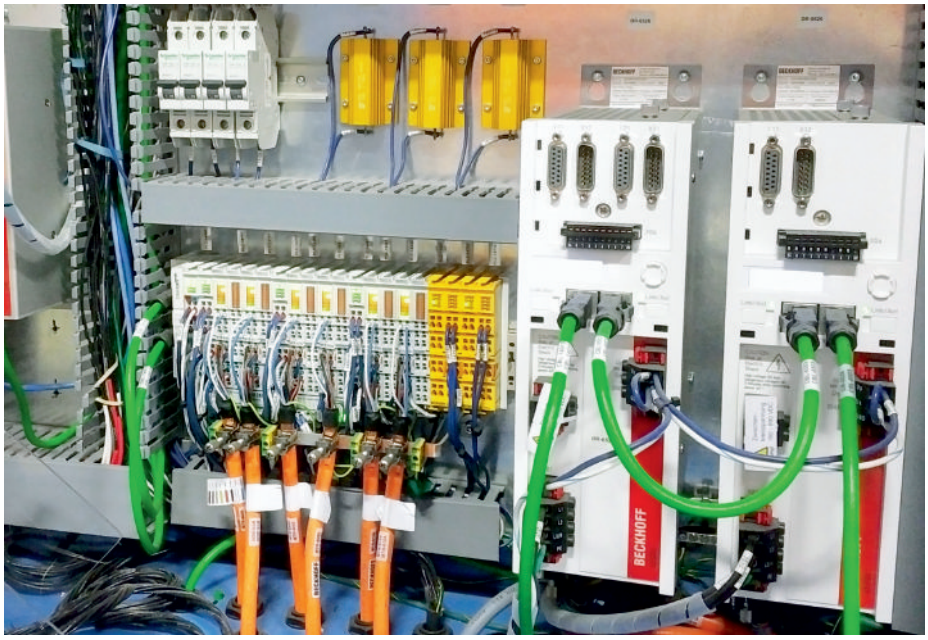
The AM8000 series servomotors with OCT handle conveyance, pick and place, web lamination, tension control and height adjustments.

EtherCAT I/O system

RAMP uses analog and digital I/O components from Beckhoff to cover all data acquisition and machine safety requirements. Space-saving EtherCAT terminals permit a free mix of safe and non-safe I/O in the same segment. High-density (HD) EtherCAT terminals, which offer as many as 16 I/O channels in a 12 mm wide housing, deliver even greater space savings.

"The EtherCAT I/O system provided the high-speed networking and fast scan times we needed while ensuring flexible network topologies," says Matt Buchwald, electrical design lead at RAMP. "The Core application required high-end control technology that can react to production changes and adjust output controls in under 10 milliseconds." The application also had to integrate with various third-party field devices such as EtherNet/IP components for web handling equipment, vision system hardware, automatic power tensioning controls and dispensing units.

RAMP also used EtherCAT Box modules with IP 67 protection throughout the system. "This allows us to place our field inputs and outputs closer to the application and reduce overall cable length and cable track requirements," explains Matt Buchwald. "Integrating all safety systems on the same EtherCAT network via TwinSAFE I/O further reduces the overall cabling costs and installation time."



SOURCE: BECKHOFF AUTOMATION

RAMP selected a C6930 control cabinet IPC (left) with an Intel Core i5 processor as its control platform as well as compact EL7211 drive technology (center) and AX5000 series servo drives.

Highly scalable drive technology

For ultra-compact drive technology, RAMP applied Beckhoff EL7211 servomotor terminals. "The 24 mm wide EL7211 terminals further reduce our cabinet space," explains control systems manager Stephen Gugeler. "We can use one low-cost 48-volt power supply for the EL7211 drives, significantly reducing space and cost requirements for servo drives." In addition, the application features inexpensive AS1020 series stepper motors driven by EP7041 stepper motor modules (50 V DC, 5 A) with built-in incremental encoders for resonance-critical applications.

For higher power and load requirements, the RAMP machine also incorporates AX5000 series servo drives for high-end position control, electronic gearing, velocity control and superimposed position control. The drives are connected to AM8000 servomotors with One Cable Technology (OCT) to handle conveyance, pick and place, web lamination, tension control and height adjustments for the production line.

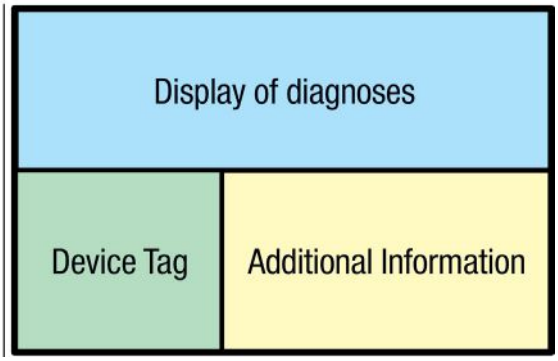
PC-based control technology

Since RAMP first transitioned to PC-based control and EtherCAT technology, the company has had ample time to compare metrics with older-generation PLC- and PAC-based systems. Stephen Gugeler summarizes the findings: "Specifically, we improved PLC cycle times by 30% and reduced control system costs by approximately 30% when compared with equipment from previous vendors. Leading-edge control and networking technology with competitive pricing from Beckhoff helps RAMP increase production throughput and exceed customer requirements every time."

Application report by ***Beckhoff Automation.***

Process device diagnostics leverages NAMUR NE 107

The goal of NAMUR NE 107 diagnostics is to limit downtime and increase plant performance. An effective Process Device Diagnostics Object implementation can help improve process plant maintenance, and provide an expanded set of tools for service technicians, operators and application programmers.



SOURCE: ODVA

Simple and straightforward NE 107 application in a well appreciated monitoring system.

INDUSTRIAL ETHERNET PROTOCOLS IN THE present technological marketplace have become more significant with the application of IIoT concepts for the improvement of process responsiveness and efficiency.

EtherNet/IP based on the Common Industrial Protocol can contribute to the application of IIoT by improving connectivity, efficiency, scalability, time and cost savings for process industrial organizations.

The Process Industries SIG (Special Interest Group) added in 2019 the Process Device Diagnostics Object to ODVA's Common Industrial Protocol. Based on the device's current diagnostics and the NE 107 status (NAMUR), the Process Device Diagnostics Object through the asset controlling and monitoring will bring simplicity, precision and rapidity of execution to the different stakeholders including application programmers, operators and field technicians.

The Dark Ages

The control of fire by early humans was a turning point in the cultural aspect of human evolution. Fire provided a source of warmth, improvement on hunting, cooking food, protection and security. Before this discovery, as soon as the sun set, humans had security issues.

Nowadays, after thousands of years of fire control and technological development, humans are still unsafe in a dark environment. This unsafe state can be viewed in different environments. Being unsafe takes from man the precious thing he has, his freedom. The industrial environment is full of dark spaces, mysterious, and dangerous places. Human eyes are not able to see inside a pipe or to know the status of an electronic card.

The industrial environment plunged humans back into the dark ages. The name black box was not chosen by accident; it is a system which can be viewed in terms of its input and output yet still remains mystical to the majority of people. Some industrial installations are seen as a black box. Many cables, sometimes without denominations, and electrical plans updated without documentation, can really cause confusion. For a field technician, the service continuity has the highest level of priority and, as a result, any incertitude must be minimized.

John is our field technician; he is our eyes on the field side and will inject a little humanity into this article. John is in charge of keeping the plant in a safe state, far removed from the possibility of any downtime. Having downtime in a plant is the worst situation John must face and we are doing our utmost to help him to avoid this occurrence.

Problems in the field

The wide range of activities John has includes, an automation project, installation, commissioning, troubleshooting, calibration, and servicing, which is one of the most time and energy demanding. Field technicians like John in the current process industries have a wide repertoire and are required to do many different tasks with regards to automation.

One of the main problems a field technician has to deal with is the diversity of activities.

There are always fewer technicians in the field, less specialized, and the fact that they need to deal with most of the portfolio and multiple vendors means that more training effort is required.

The main goal a field technician has is to maintain the functional state of the installation, which means keeping the process running and avoid downtimes. In order to avoid downtimes maintenance technicians stick to effective maintenance principles like:

- keeping equipment in good condition;
- developing programs to carry out its services;
- perform quality work;
- anticipate and prepare for future work;
- achieve continued improvement

In addition, these responsibilities include preventive maintenance, predictive maintenance and many more principles.

Preventive maintenance

Preventive maintenance may include service contracts, inspections, cleaning activities, testing, lubrification efforts, and scheduled shutdown service. Inspection is the most significant activity a service technician has, and it should lead to early detection.

John: «inspection looks like a waste of time, it brings us back to the beginning of the previous century." John is, unfortunately not a good candidate for this inspection. Most of us agree with him, our eyes don't have the ability to see inside the process, inside the field devices.

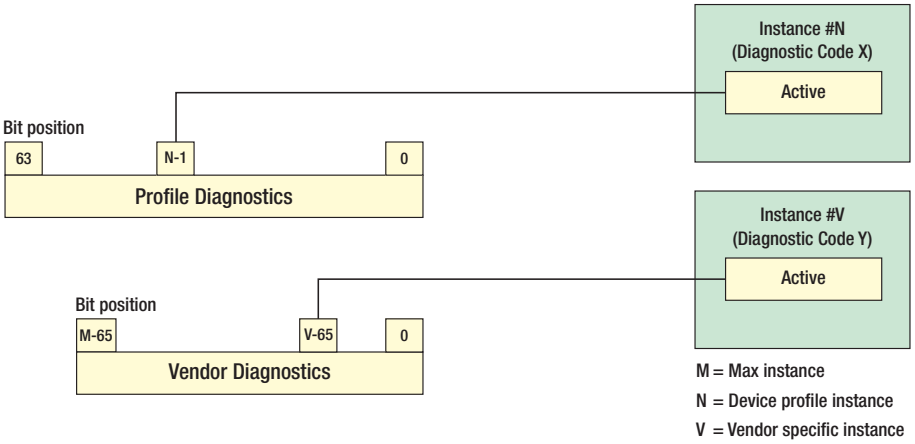
John: «the visual inspection is quite limited because of the miniaturization and the increase of hidden elements".

Predictive maintenance

Predictive maintenance may include vibration

analysis, shock pulse methods, ultrasonic, thermographic analysis and much more to monitor and detect changes in condition to allow more precise intervention. John: "I would like to be able to anticipate earlier when the measurement devices might require servicing."

The number of sensors, actuators constituting an installation is always higher and always more digital and seem like a Blackbox. The more visibility the technician has, the more freedom and time he will have to develop and improve the performance of the installation.



SOURCE: ODVA

Two types of Diagnostics are available: Profile and Vendor specific.

Downtime

John: «When you think that everything is under control then it suddenly happens". Downtime is, by definition, very short stoppage in production but in fact, extremely time-, cost-, and energy- demanding. The sources of downtime are many and result from a series of small, undesirable events.

Downtime and chain reaction

A chain reaction that happens, for example, in chemical process, is when elements have an impact on another element and so on. It is exactly what happens under control in an atom reactor and in an uncontrolled way with a nuclear weapon. An industry has a lot of systems, sensors, and actuators that influence each other and exchange information.

A sequence of undesirable reaction can also happen in this context. When a sensor or an actuator goes in default mode and delivers wrong information, the system can absorb it and continue the production process. However, the field technician must be informed, otherwise this could slowly damage the installation. In addition, if one more sensor or actuator goes to default, the system has good chance to generate a chain reaction and the issue will be the downtime of the installation.

The main point is the financial cost a downtime generates:

- Cost of time
- Cost of repair or replacement of a faulty piece of equipment
- Cost to clean
- Cost of any injury to workers as a result of equipment failure and during the troubleshooting resolution.

It is vital to a plant's survival to minimize the possibility of downtime. A second aspect is more psychological. Downtime is considered as failure for the team, and is the result of the incapacity to structure and to maintain the production process in a safe state.

No diagnostics, no visibility

Visibility and diagnostics are linked and are going to help the field technician to keep his main goal: "keeping the installation in a state in which the production operator can achieve the production output goals".

In the past, visibility in a plant was purely visual, nowadays with the IIOT development, visibility is linked with the ability of a field sensor to deliver the right information at the right moment.

Everyone knows what diagnostic means and the best example is the medical diagnostic. The medical diagnostic is the process of determining which disease or condition explains a person's symptoms and signs. If translated into industrial jargon, it is the ability of a device to generate the performance and health status of all its components e.g. sensor elements, senor electronic, process connection.

John: "Nice 4...20mA analogic output also give the status, means the device is working, or the device needs to be replaced." Analog transmitter output goes to a defined level above 20mA or below 4mA and that the system triggers alarms. When the alarm triggers, it is already too late. More detailed information could help us to avoid this critical situation.

The 4...20mA diagnostic happens during the downtime of the system and need a production stop to bring the process back into a working state.

Modern medicine is the best solution when a healthy person becomes a patient. Digital solutions are going to keep a field sensor healthy and are not science fiction. It is what happens in a plant with intelligent devices.

However, with 4...20mA, the rudimentary diagnostic solution had two main advantages: first it was standardized and second the action after the alarm signal was quite simple, it didn't need interpretation.

Well-engineered systems are keeping the advantage of the previous technologies and are improving it. 350 is the number of pieces of status information an intelligent device can generate. Quantity versus quality is the first idea that crosses the mind of each developer when he sees this amount of information. The volume of information needs to be managed and standardized to get the benefits. In addition, an intelligent device can fail or degrade in many ways, resulting in hundreds or thousands of different diagnostic error codes.

Steven is a charge of the production performance, he's transforming input-based product to output commercial goods in a defined time base.

Steven:" My monitoring screen always has more information. I need a simple message. I do not need details". The operator needs to know if the measurement of the field device is valid or not.

Operators and field technicians don't have the same requirements. A field technician needs more details than the process operator. Both need standardized and mapped feedback from the field device.

Namur NE 107 Diagnostics

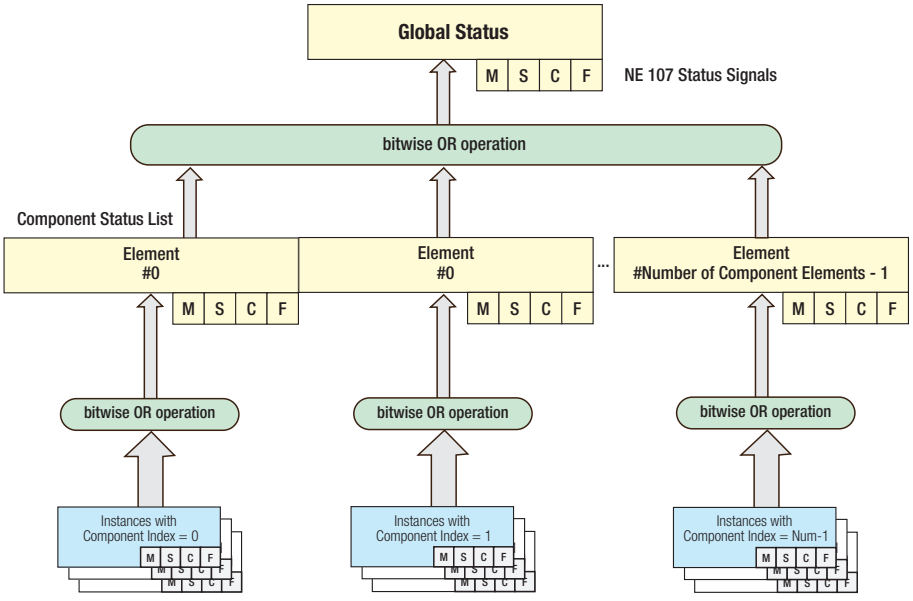
The operator needs to inform the field technician in a short time when something goes wrong in the plant. To achieve this important transfer of information, a standardized way is required. In addition, from the field technician perspective, status information with probable causes and recommended actions could be appreciated.

NE 107 illuminates the plant and keep operators and field technicians out of the dark.

NAMUR NE 107 harmonizes status signals across all kinds of devices. NAMUR NE 107 is the ideal choice to satisfy requirements from the operator and the field technician`s perspective. NE 107 includes continuous monitoring of the internal variables to communicate alarms when internal self-diagnostics detect problems. Early warning results of degradation detection provides precious information to the field technician and helps him to plan daily maintenance and turnarounds.

NE 107 is the perfect bridge between operators and field technicians. Diagnosis through the NE 107 structure is going to avoid downtime and increase plant performance.

The four-status signal proposed by NE 107, in addition to the fast communication



SOURCE: ODVA

From the instances to the Global Status of the device.

of EtherNet/IP, is an obvious benefit for each stakeholder, operator, field technician and much more. In one overview, all status information is available.

Displaying the NE 107 information is one part of the information. Additionally, correct descriptions, data mappings and remedies are functions a field technician and an operator would like to have. Mapping is the action to link the field sensor information with the NE 107 status signal.

In fact, field technicians always spend less time in the plant, self-control is more than needed especially when it is time to resolve an issue. Although the remedy instruction will never replace having a colleague, it is an important support for the field technician.

This NE 107 helps the operator run and supervise the process continuously. NE 107 also helps the maintenance technician keep the plant running (e.g. field devices) by performing reactive, scheduled, condition-based maintenance activities and fixing the issues. However, the brain of the process and the stakeholder in charge of the implementation is the application programmer.

How to implement

The better the communication between the operator, the field technician and the application programmer, the better the performance of the plant will be. The operator's needs are different from those of the technician. Stanley our application programmer should have that in mind, as it is the key to customer satisfaction.

The diagnostic implementation has a lower priority than the process implementation. For Stanley: "In my implementation work plan, the diagnostic implementation has the last priority. It needs to be fast, out-of-the-box". To help Stanley, the NE 107 implementation should be sure, easy and standardized.

The Process Device Diagnostics Object developed by The Process Industries SIG will provide the expected standardized structure that Stanley needs. Attributes and methods standardize the way to implement NE 107 and allow more time for kernel functions. Stanley's kernel function is to adapt the diagnostic display to the customer specification. It could be more operator oriented with, for example, the Failure status or/and more field technicians, in addition to the Maintenance Required status.

Stanley: "The structured and easy to use Process Device Diagnostics Object should definitively accelerate my implementation. I could be more focused on the way to display the diagnostic. In the past, I spent 80% of my time on the diagnostic identification and 20% on the display of diagnoses, nowadays with the Process Device Diagnostics Object, it is quite the opposite."

The problem of collecting the diagnostic data is solved with the Process Device Diagnostics Object which enables access to the current diagnostics information of a field device of any vendor.

Let's help Stanley understand how to perform his control system with the Process Device Diagnostics object. The Process Device Diagnostics Object, like each CIP object, has a class code, in this case 0x108, class attributes, instance attributes, common services and specific services.

For Stanley, the first goal is to get Global Status for his field device. The Global Status is a logical combination of all generated diagnostics. The possibility to get the status of selected elements for a selected channel for a field device is also provided by the Device Diagnostics Object. Diagnostics are not hidden or unreachable data; Stanley also has the possibility to read this information with the Device Diagnostics Object.

Stanley understands that Elements for field devices are channels. Channels like a temperature channel for a Temperature sensor. Stanley would like to know what is behind the concept of instance.

The EDS File from a Flow sensor can have up to 300 diagnostic events. Stanley used to take these diagnostic events and map them. This diagnostic mapping means linking the diagnostic event from the EDS file and converting it in NE 107 diagnostic which took a lot of time to develop. With the Diagnostic Object these diagnostic events are represented and structured in instances.

Two types of instances are defined in the Diagnostic Object:

Profile Diagnostics Instances, which are specified in the Device Profile Object. The Profile Diagnostics Instances guarantees Stanley that all vendors are going to follow the same data structure.

Vendor Diagnostics Instances, which are specified by vendors. Vendors with more specific diagnostic events have the freedom to add them into the vendor diagnostic instance.

Stanley needs to re-map diagnostic codes, a special attribute named User Diagnostic Groups, which are available in the Diagnostic Object for that use case. For example, Stanley could map an over-range and an under-range condition to the same "out-of-range" bit.

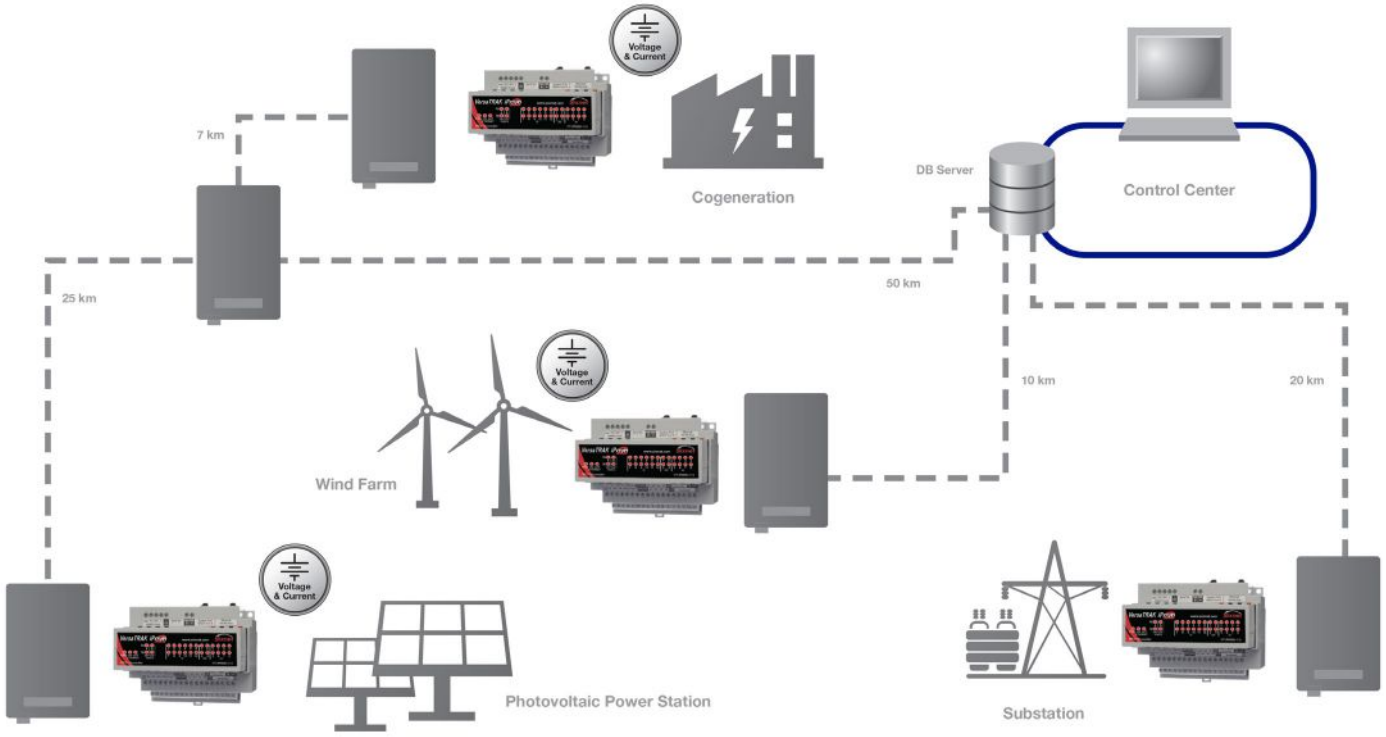
The class attribute gives global information, the first piece of information that appears to Stanley is the Global Status. Instance Attributes are the structure that specifies diagnostic events. The diagnostic event F022 will have a Diagnostic Code: 022 and a Status Signal: F (Failure regarding NE 107 standard). Stanley also has the possibility to activate or deactivate instances, or in a common field technician language to activate or deactivate diagnostics. Stanley can read the diagnostic timestamp information and additional diagnostic messages like "Temperature sensor defective" to provide more clarity and flexibility to Steven the operator.

Stanley has the possibility to scan all instances (all diagnostic events). If Stanley's purpose is to read Vendor Diagnostics, the first step will be to define the right buffer size with Size of Vendor Diagnostics. Then with the Get_Attributes_All service to get a specific Vendor Diagnostic.The diagnostic implementation is no longer a question. The application programmer with the Process Device Diagnostics Object based on NE 107 and Device integration tools are able to answer any diagnostic display requirements the customer has in a suitable and efficient time frame.

Michael Voegel, Marketing Manager Industrial Communication, ***Endress and Hauser Digital Solution.***

M2M protocols offer integration with field devices and meters

Industrial RTUs, which are configured redundantly in the control center, help to ensure reliable network security and management for Deutsche Energie Funk. The end result is a fail-safe communication network that enables the smart grid provider to better serve customers.



SOURCE: RED LION CONTROLS

Network solution uses built-in Modbus gateway to form a seamless interface to existing RTU and PLC devices, and simplify integration efforts.

GERMANY CONTINUES TO ADVANCE THE ENERGY revolution by integrating alternative energy sources into its mainstream electrical grid supply. According to the "German Renewable Energy Act," legislation was created to drive alternative energy costs down through the mass adoption of solar and wind generation facilities.

Not only is consumption being reduced by the implementation of "greener" technologies, production is also being watched and controlled more closely to better meet renewable generation requirements. With alternative energy plants taking up large amounts of land, they are typically remotely located where land is either less expensive or wind patterns are more stable.

Deutsche Energie Funk provides electricity demand and monitoring solutions for the power generation market. Tasked with developing a solution to address the demands of collecting real-time data from different power generation sources, the organization was looking to provide secure communication to remote sites while utilizing native M2M protocols like Modbus for easier integration with field devices and meters. The end goal was to deliver a solution that reliably connects generation plants and substations to many downstream systems such as electrical transportation, storage and substations, which rely on real-time accurate and sensitive data for efficient power source and electrical grid management.

Automation solution

Deutsche Energie Funk combined its own narrowband radio network with industry-leading hardware and software components to offer an optimal solution for the remote monitoring and control of renewable energy generation facilities. Narrowband radios are used in this smart grid application to deliver high quality of service, real-time communication and long reach of low frequencies.

By working with Welotec GmbH to select the Sixnet series VersaTRAK RTU technology from Red Lion Controls, Deutsche Energie Funk is now able to reliably collect and store I/O data points from substation equipment located in or near wind farms, solar plants and co-generation facilities. The Modbus registers in the VersaTRAK RTUs then push data to UHF radios that securely communicate with the energy supplier control rooms. The control servers monitor available energy supply with current demand selecting the appropriate mix of generation methods (wind, solar and co-generation) based on a number of requirements.

Benefits

Red Lion's RTU technology provides Deutsche Energie Funk with a reliable, secure platform for remotely monitoring and controlling energy generation equipment. The built-in Modbus gateway forms a seamless interface to existing RTU and PLC devices, simplifying integration efforts. In addition, Deutsche Energie Funk is able to incorporate different energy meters with a single automation platform.

*Application report by **Red Lion Controls.***

EtherCAT Box for conveyor control

Beckhoff: To enhance control and cabling efficiency for motor-driven roller (MDR) conveyor systems, Beckhoff Automation has released the new EP7402 EtherCAT Box. This compact controller is a two-channel motor output stage for BLDC motors used in MDRs, regardless of the conveyor or roller motor vendor.

The EP7402 offers optimal conveyor control through zero-pressure accumulation (ZPA) logic in its firmware, programming in the TwinCAT 3 engineering environment and high performance EtherCAT industrial Ethernet communication.

Designed for conveying tasks in intralogistics, packaging, food and beverage, assembly and other industries, the EP7402 offers numerous advantages: IP67 rated and compliant with new electrical standards being enforced in 2020; does not require a protective enclosure; mounts in standard C-channel or L-brackets directly on the conveyor frame; One Cable Automation (OCA) via two B23 ENP hybrid connectors; and multiple M8 sockets to support two MDRs per device and digital I/O for peripheral sensors, vision systems or junctions to the entire range of EtherCAT Box modules.

Communications gateway

HMS Networks: A new Intesis gateway makes communication between PROFINET and BACnet easy.

The Intesis protocol translator enables communication between PROFINET PLCs on factory floors and Building Management Systems using BACnet IP/MSTP. With this, full data integration, monitoring, and control is enabled between factory floors and building facilities.

Key objectives can be achieved using factory-to-building communication. In factories, it is essential that environmental dimensions such as temperature, humidity, and air quality are controlled and monitored automatically to ensure optimal conditions for manufacturing and working staff. And, by ensuring efficient control of facilities such as HVAC and lighting systems, factory owners can save a lot of energy and manage emergency situations in a safe way.

However, when system integrators plan for factory-to-building integration, they normally face a heterogeneous and challenging communication situation. BACnet is typically the protocol used in the Building Management System (BMS) to control the facilities inside the building, and PROFINET is one of the most used factory networks for controlling production processes.

Wireless position switches/sensors

Steute: "Wireless Ex" is a technology which simplifies the assembly and operation of switchgear in explosive environments. Switching devices are no longer connected to the receivers in the control cabinet via Ex-compatible cables, but via a low-energy wireless protocol created especially for such applications. It is certified to ATEX and IECEx standards.

Engineers constructing plants and machines for explosive environments can take Ex RF 96 electromechanical wireless position switches, for example, in their slim rectangular design to monitor the position of moving machine components or workpiece fixtures.

Alternatively, positions can also be monitored without any contact – using Ex RF IS wireless inductive sensors in a cylindrical design (M 12, M 18 and M 30). In this case, the Ex RF 96 ST Ex wireless universal transmitter takes care of both wireless transmission and decentralised power supply to the sensors.

These wireless sensors guarantee high transmission availability even in situations (e.g. coexistence with other wireless systems), as is often the case in an industrial environment.

Ethernet cables for e-chains

Igus: New chainflex CAT5e and CAT6 cables offer predictable and guaranteed service life, along with certification for the CC-Link IE protocol.

Two highly flexible Ethernet cables have been designed for use in energy chains, and certified for use in North American markets.

The cables, CFBUS.045 and CFBUS.049, are targeting implementation of Industry 4.0 in automation. The cables have UL certification for North American markets and received the certificate for CC-Link IE protocols for the Asiatic region.

Industrial Ethernet is the future for the digitized factory of tomorrow. Many studies show that the world of fieldbus is stagnating, and the number of Ethernet nodes is increasing, with high double-digit growth rates. These systems offer seamless data exchange on all levels of a production facility, from the highest control level to the manufacturing levels.

The CC-Link IE controller network has been designed for the rapid exchange of large amounts of data in a factory or production plant, whereas the CC-Link IE field network has been optimized for connection of a wide range of devices and their connection to other existing networks such as the standard CC-Link. These increasing requirements for industrial Ethernet communication nodes call for a secure and long-lasting connection between the components to meet the continuously growing amounts of data being transferred.

Secure remote maintenance

B&R Industrial Automation: Machine builders can establish a continuous connection to plants and machinery in the field. With LogTunnel, data from machines all around the world can be archived in a central location. Any irregularities in performance can be detected early to help maintain maximum availability.

LogTunnel is a feature of B&R's Secure Remote Maintenance solution. Secure Remote Maintenance lets users check in on plants and machinery anywhere in the world from the office or on the go. Users can take control if necessary. Through continuous data logging, LogTunnel provides an ability to detect faulty components early and optimize service intervals. Setup is a simple matter of drag-and-drop and requires no special IT know-how.

The ongoing LogTunnel connection is not affected when a technician connects temporarily to perform remote maintenance; logging continues uninterrupted. Machine data can be stored on a central database server, in the cloud or at a data center, where it remains available for later analysis.

Secure remote maintenance functions are

provided in accordance with all the latest IT and cybersecurity guidelines. Machine builders have runtime access to machine parameters from their entire installed base. All access is logged in detail for later traceability.

Pre-validated LTE Connectivity

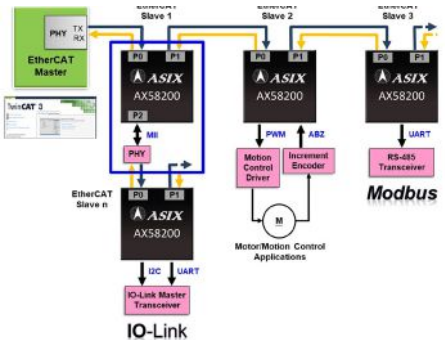
Lanner: Onboard vehicle NVR V3S and V6S have now become Milestone XProtect verified platforms. Lanner's V3S and V6S are designed with multiple built-in PoE ports and a scalable option with uninterrupted swappable 4G LTE modem caddy PGN-series module.

Milestone Systems has added Lanner's V3S and V6S into its online Marketplace, making them the only rugged vehicle PC to join its marketplace with pre-certified LTE connectivity. The pre-validated vehicle NVRs ensure optimal reliability and interoperability for public transit surveillance.

V3S is powered by Intel Atom (Apollo Lake) while V6S is built with Intel Core i7-7600U (Kaby Lake) inside to offer high-compute capability and versatility for vehicle computing. Designed as robust vehicle PCs, both V3S and V6S are made to be highly rugged, E13 standards compliant and MIL STD 810G certified shock & vibration resistant hardware.

The V3S and V6S units come with built-in dual cellular network support for 4G LTE failover. In addition, the high-performance NVR can support CAN bus by option for needs of driver behavior analysis.

EtherCAT Slave IC



ASIX Electronics: This solution targets industrial fieldbus applications that need to support EtherCAT standard communications functionalities. The AX58200 is a 2/3-port EtherCAT Slave Controller SoC equipped with ARM Cortex-M4F core with DSP extension runs up to 192 MHz and EtherCAT Slave Controller (ESC) with two integrated Fast Ethernet PHYs. AX58200 also supports additional communication interfaces such as 10/100Mbps Ethernet MAC with RMII and hardware cryptography accelerator, HS USB OTG, SPI/UART/I2C/I2S/CAN/PWM, etc.

The AX58100 is a 2/3-port EtherCAT Slave Controller (ESC) with two embedded Fast Ethernet PHYs. The AX58100 also provides SPI slave and Local bus Process Data Interfaces (PDI) to provide an easy way for system designers to implement the standard EtherCAT communication functionalities on those traditional non-EtherCAT MCU and DSP industrial platforms.

AX58x00 family is interoperable with all EtherCAT systems with standard EtherCAT protocols such as CANopen over EtherCAT (CoE), File Access over EtherCAT (FoE), Vendor Specific-protocol over EtherCAT (VoE), etc. and is suitable for motor/motion control, digital I/O control, sensors data acquisition, robotics, EtherCAT IO-Link master, EtherCAT Junction slave module, etc. industrial automation fieldbus applications.

Power-Over-Ethernet switch

WAGO: New compact Power-over-Ethernet (PoE) switches expand the company's line of industrial grade Ethernet switches. Just two inches wide and four inches tall, the 852-1411/000-001 PoE switch is designed for applications with limited space.

A wide voltage input of 24 VDC to 57 VDC, makes the 852-1411/000-001 switch an option for all PoE applications. The switch supports both PoE operation modes A and B, with all of the ports supporting 10/100/1000 Mbits/s.

This new ECO (economy) PoE+ switch is unmanaged, supplies 30 watts of power per PoE port and has an operating temperature of -10C to +60C. It eliminates the need to run both an Ethernet cable and power cables to end devices, ultimately reducing cost.

Features include five Ethernet ports, 10/100/1000 Mbit/s, autonegotiation; 4 PoE+ ports (IEEE 802.3at); front-panel diagnostic LEDs; support for Auto-MDI/MDI-X functions; full/half-duplex transfer modes for each port; and store-and-forward switching method.

Next-generation managed switches

Belden: Every year, the number of devices requiring greater bandwidth to remain reliable and well-connected increases. The Hirschmann BOBCAT managed switch is built to help manufacturers keep pace with this change and build next generation networks.

The switches support the new IEEE 802.3bz standard with 2.5 Gigabit speeds to bridge the gap between 1 Gigabit and 10 Gigabit speeds. Legacy devices or networks can be connected with 100 Mbit/s, 1 Gigabit uplinks for current networks or 2.5 Gigabit for future-proof networks. The BOBCAT switches support all speeds by replacing the SFP in the field.

For applications in need of maximum power without device limitations, these next generation compact switches provide Power over Ethernet (PoE/PoE+) with up to 240 W.

The switch is also the first of its kind to enable real-time communication using time-sensitive networking (TSN). Industrial applications require this capability to maximize performance and security, even under the most demanding conditions.

IIoT ecosystem

Endress+Hauser: Its new IIoT solution platform, Netilion, is an ecosystem combining digital services and system components to improve the lifecycle and asset management, maintenance, and support of instruments and analyzers.

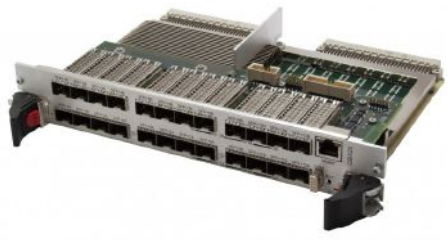
Netilion enables users to keep track of

their installed base, documentation and data management, and instruments' performance and health status. Netilion's digital services available today are Scanner, Analytics, Health, Library and Value.

Netilion Scanner is a free smartphone app that guides the user in capturing field instrument asset data, while utilizing QR code or RFID tag. It can store images and instrument location and accessibility. Critical and quality-relevant information can also be saved , associated with the instrument tag.

Netilion system components such as field gates and edge devices can be used to upload installed base information and create lists of the instruments, without having to interact with the control system. The installed base information in the digital service Netilion Analytics can be used to create a digital twin of the system and analyzed with the help of dashboards to initiate proactive maintenance measures for critical instruments or swap out discontinued instruments.

VME Ethernet switches



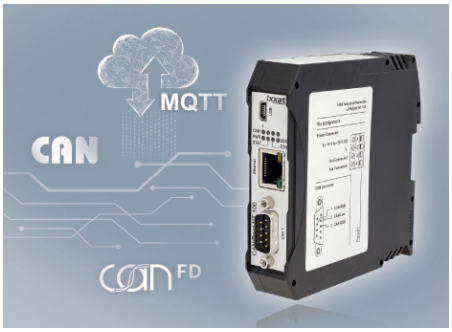
Abaco: The GBX25 6U VME managed Ethernet switch enables users to free up slot space as well as valuable power and cooling resources in existing chassis by using a single switch to replace multiple switch cards while maintaining the range of communication protocols—including 100-FX—and cable types typically installed in legacy systems.

It is available with up to 40 ports (combination of front and rear) that support a variety of copper and fiber cable types. The GBX25's use of standard SMP modules for a variety of basebands including 100-FX, 1000-SX/LX/T, and 10G-SR/LR enables users to combine multiple communications capabilities on a single card, reducing slot occupancy compared with previous multi-card architectures.

The GBX25 is 100% pin-compatible with the GBX24 and RM921, but has been upgraded with Abaco's OpenWare switch management software. OpenWare was created by Abaco at its Networking Innovation Center, and numerous customers have benefited significantly from access to the development team's expertise to smooth transition or to develop application-specific functionality, providing more rapid deployment or a custom networking solution.

Users can access the OpenWare development team for transition and advanced function support for existing or new applications.

CAN-based networking

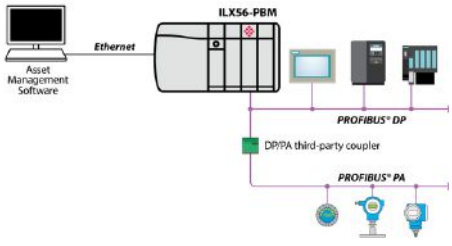


Ixxat: With the new Service Pack 2, the functionality of the Ixxat CAN@net NT and CANbridge NT series has been extended. Users can now add smart, event-controlled network actions and versatile bi-directional MQTT-messaging to cloud applications. The new hardware CAN@net NT 100 complements the CAN@net NT range with new network connectivity.

The CAN@net NT and CANbridge NT product families enable smart and seamless CAN-based networking on site and remotely. The CANbridge NT enables easy coupling of up to four CAN and CAN-FD networks using filter and translation rules. Network wiring can be simplified through tree and star topologies, and all connected segments are protected thanks to electrically isolated bus interfaces. All CAN@net NT products come with an additional Ethernet interface, allowing very distributed networks by coupling up to four CAN@net NT devices using Ethernet. CAN@net NT products also allow remote access to CAN and CAN-FD networks via Ethernet and PC.

The new Service Pack 2 introduces enhanced "Action Rules" programming for flexible definition and execution of events and actions for all CAN@net NT and CANbridge products. Based on LUA script processing, these user-defined actions can be triggered upon e.g. pre-defined message content or status information.

Connecting PROFIBUS & ControlLogix



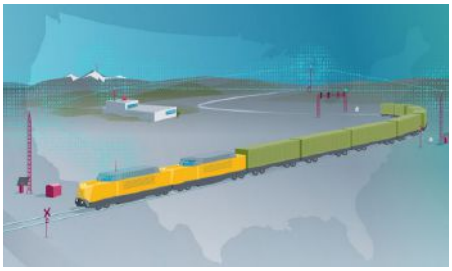
ProSoft Technology: New PROFIBUS solutions and recent updates for high-performance industrial applications include connecting PROFIBUS and ControlLogix controllers.

The latest modules are in-chassis products for Rockwell Automation ControlLogix control systems. With new functionality such as multiple I/O connections back to the ControlLogix processor and the ability for the modules to operate as multiple PROFIBUS DP slaves on a network, these modules provide the performance required for the most demanding applications.

Premier integration tools and each module's PROFIBUS DP packet capture utility will help users reduce configuration time.

New PROFIBUS solutions in the past year have included the in-chassis products for ControlLogix systems, as well as master/slave and multi-slave gateways.

Wireless data communications



Siemens: New modules provide wireless data communications for mission-critical railroad applications and legacy networks.

Railroads will require increasingly more from their communication networks. Advances in private wireless networking and the emergence of new standards (such as, IEEE 802.16s for broadband wireless access systems), railway operators can now build the next-generation of IP-based communication systems for the automated, smart railroad of the future. Wayside and mobile communication solutions will enable railroads to leverage their extensive investment in spectrum and physical infrastructure while meeting stringent demands for high reliability, low latency, availability, and security.

Siemens' system of frequency agnostic (software-defined) wireless base stations, fixed and mobile remote radios are based on IEEE 802.16s (the standard for broadband, wireless, fixed/mobile access systems) that enables wide-area, Internet Protocol connectivity. This allows railroads to transition from multiple, single-purpose networks to a common, managed, multi-purpose/multi-band network and realize significant reduction of infrastructure and operating costs.

Industrial Ethernet switches

Westermo: A next generation industrial Ethernet switch platform is designed to meet the needs of future data communication networks. The

platform is ideal for handling big data and Industrial Internet of Things (IIoT) applications driven by global developments such as urbanisation and infrastructure investments. Integrating hardware, software and network design support, the new switch platform offers advanced capabilities, low total cost of ownership and creates a reliable network across multiple industries.

Designed to meet increasing demands for greater bandwidth and uninterrupted 24/7 service, the new hardware provides high levels of cybersecurity, operational life, and easy configuration, operation and maintenance. The platform will offer a broad range of solutions for every industrial network requirement and will include devices for specific industry applications, such as managed PoE switches approved for onboard rail applications and substation automation solutions.

The new switch platform is powered by the next generation WeOS operating system, which maximises the potential of the new hardware. As with previous generations, WeOS continues to ensure robust interoperability and provide multi-media support, while also helping to provide greater network resilience and cybersecurity. Switches using this latest version of WeOS are backward compatible, future-proofing existing industrial networks and simplifying their design, while the web interface has the same look and feel to ensure easy device management

EtherNet/IP communications

Rockwell Automation: Industrial producers can now improve their network resiliency by using primary and backup adapters for the 1756-EN4TR ControlLogix EtherNet/IP communications module. This new redundant-adapter functionality is provided through a recent firmware update to the communication module.

In addition to helping users improve network redundancy, the module's firmware enhancement also offers more advantages.

No single point of failure: When used with ControlLogix controllers and redundant switches, the communication module is no longer a single point of failure. This can improve uptime and productivity in continuous process applications like oil and gas.

Architecture options: The firmware enhancement can be used with a single ControlLogix controller or redundant controllers. It can also be used with star or Device Level Ring (DLR) architectures. This gives users design flexibility.

Ease of modification: An existing 1756 I/O chassis can be modified for redundant adapters. Slots 0 and 1 are used for the redundant adapters.

The 1756-EN4TR communication module implements network-based access control for users, devices and networks in a 1756 ControlLogix chassis. The module can increase performance in networked operations, with 1-gigabit-per-second communications speeds and the ability to support future network or infrastructure expansions.

Edge automation platform

Red Lion Controls: The FlexEdge Intelligent Edge Automation Platform brings a new degree of versatility to edge computing, while its ease of use makes productivity and efficiency gains from digital transformation initiatives accessible with point-and-click simplicity.

FlexEdge's highly modular design and intuitive software enable quick, straightforward customization and deployment to myriad applications without compromising rugged, reliable operation. The platform carries several certifications that make it ideal for oil and gas, water, wastewater, maritime, hazardous location, and factory automation applications.

Engineered for industrial customers with diverse needs who want to effortlessly connect systems and process data at the edge, FlexEdge's modular architecture boasts a wide variety of wireless and wired communication options. This breadth of options makes it an easily configured communication gateway that connects with any industrial communication requirement, regardless of protocol or manufacturer.

Unlike fixed-function devices that require customers to learn many products, or systems with fixed chassis that take up unnecessary space, FlexEdge offers a form factor and platform that adapts as quickly as application needs change. It's available with advanced networking functionality or advanced automation features, including protocol conversion; virtual HMIs; an advanced web server with Bootstrap, JavaScript and CSS; data, security and event logging; and cloud connectivity.

With FlexEdge, customers can seamlessly connect new and existing devices, reducing overall downtime and allowing for frictionless, future-proof scalabilit. This allows the selection of one platform for a wide variety of edge requirements, so customers can focus on business efficiency without worrying about choosing the right combination of products for their application.

Managed Ethernet switches

Moxa: The MDS-G4000 Series industrial DIN-rail managed Ethernet switches offer a new level of network versatility. With growing connectivity requirements for industrial applications, business owners are looking for versatile, future-proof solutions to scale with these constantly expanding networks.

The MDS-G4000 Series provides a fully modular platform with a variety of hot-swappable media interface and power modules, enabling hundreds of port combinations for on-demand flexibility. The hot-swappable modules and redundant isolated power design combined with an intuitive web interface and MXview support enable the MDS-G4000 Series to provide 24/7 operations while lowering the total cost of ownership.

As industrial networks continue to expand, the MDS-G4000 Series offers five types of 4-port media interface type modules and two types of power modules to mix and match, delivering the flexibility necessary to connect the increasing volume of different devices. The ultra-compact size, together with DIN-rail, wall-, and rack-mounting options provide additional installation versatility when deploying the MDS-G4000 Series in challenging industrial environments such as inside machines and in narrow underground and outdoor cabinets.

The MDS-G4000 Series stands out with its ultra-compact size, robust housing, and convenient tool-free module installation design.

Powerful solar chargers for your outdoor adventures

One downside of our increasingly connected world is that we constantly need power outlets to charge our smartphones, tablets and smartwatches. Solar chargers can keep these devices running wherever we are by soaking up the sun's rays.

SOLAR CHARGERS PROMISE FREEDOM from electricity bills and wall outlets. Today there are several styles and types of solar panels and power banks on the market, to suit different needs from a day out hiking to a week-long camping trip.

Let's take a look at some of the products that can charge a device in the great outdoors.

RAVPower 24W Solar Panel

This RAVPower solar panel has five folding sections. Four of them are solar panels, while the fifth is a carry pouch that also contains the USB charging ports. At 300x170x20mm, the folded package is about the size of a magazine. It unfolds to 300x860mm, which provides plenty of surface area for the solar panels.

As the RAVPower solar panel has no internal battery, it only weighs around 2 pounds. This makes it light enough to attach it to your backpack on a hiking trip. To do this, the waterproof canvas material has four riveted eyelets for carabiners.

PHOTO: RAVPOWER

The charger has three independent USB ports, each with a maximum output of 2.4A. RAVPower claims that its iSmart technology can automatically detect the optimal current to ensure the fastest possible charging of different devices. The maximum total output is 4.8A, so the RAVPower solar charger can potentially charge a tablet and two smartphones at the same time.

www.ravpower.com

BigBlue 28

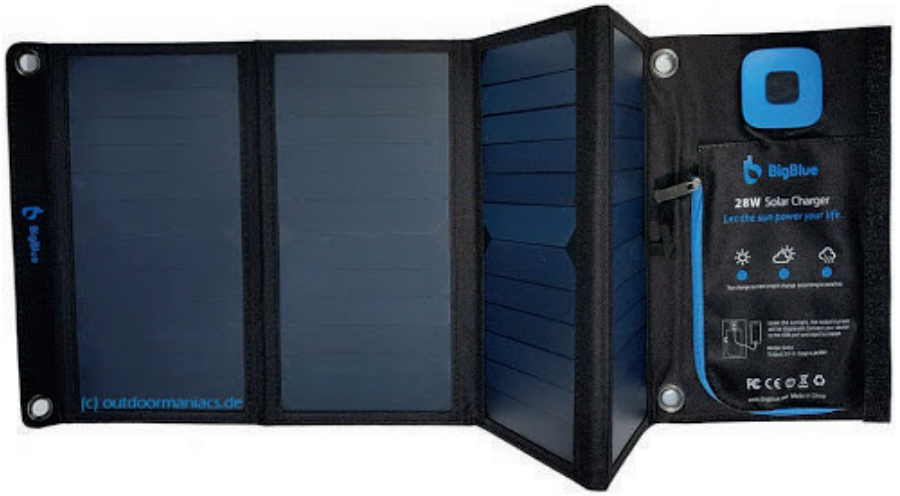


PHOTO: IBIGBLUE

The design of the BigBlue 28 is similar to the RAVPower. It's a folding four-panel charger with two USB ports, which can deliver up to 2.4A each, up to a total of 4A.

It comes with a built-in digital ammeter to provide information about amperage for charging speed. An integrated voltage regulator offers stable power output for safe charging.

One cool feature of the BigBlue is the charge interruption recovery. Many solar panels have the problem that charging does not restart after an interruption. This can happen on a partly cloudy day or when a shadow is cast over the panel. In these situations the BigBlue auto-restart function makes reconnecting to your device a smooth affair.

www.ibigblue.com

BioLite SolarPanel 10+

The BioLite folds to about the same size as the BigBlue and the RAVPower, but it has only two, rather than four panels. Consequently, it has about half the power output, producing up to 10W of electricity. The two solar cells are coated with a plastic protective layer that keeps off dust, and the USB ports are protected by a silicone cap to keep dirt out.

The advantage of the BioLite is, that it comes with a built-in 3000mAh battery, so it can soak up the sun during the day and save some of that power for charging at night. A LED battery indicator with four lights shows how much charge the integrated battery has.

The BioLite has a pair of anchor points, so it can be attached to a backpack with carabiners

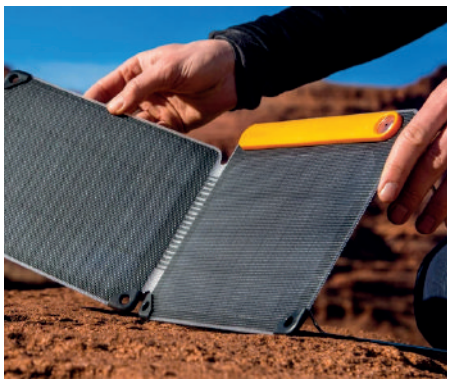


PHOTO: BIOLITE

for solar collection while hiking. The design also includes a 360-degree kickstand, which simplifies positioning on the ground.

One neat feature is a handy sundial on the front, which helps to find the best position for the free-standing panel. The kickstand also doubles as a hook for hanging the panel on a tent or a tree.

PHOTO: BIOLITE

PHOTO: BLAVOR

If you are planning to spend a couple of days outdoors in a mountain cabin or a van, BioLite has a solution for that situation, too. The SolarHome 620 includes the basic elements to transform any structure into an off-grid home. The kit includes a 6W solar panel that charges the 20Wh battery in a central control box. This control box has two USB ports for charging smartphones and other devices. It also powers the three 100 Lm hanging lights that come with the SolarHome kit, and serves itself as a fourth light. With three brightness settings, the individual lights can stay on between 4.5 and 14 hours. One includes a motion sensor to work as a security light.

The control box also includes a speaker with FM tuner and microSD MP3 playback. BioLite thus provides for off-grid energy, lighting, and entertainment.

www.bioliteenergy.com

Blavor

If you are looking for a multi-fuction charger in a portable package, the PN-W05 Solar Power Bank from Blavor may be just right for you.

The focus here is clearly on the power bank. The 150x79mm solar panel can help to keep it topped up, but it would take a very long time to fully charge the 10,000 mAh battery via sunlight alone. There is a solar charging indicator that will illuminate green when the solar panels are in direct sunlight, above 25,000lux. At this point the solar charger replenishes the device at 180ma.

Charging the power bank via an outlet, either through the micro-USB or Type-C input port, you can expect the device to be fully replenished within 6 hours. At full capacity it can then power up an iPhone X up to 2.3 times.

There is a four LED battery power indicator that glows blue whenever the power button is pressed, showing the power left in the unit in 25% increments.

The Blavor also supports Qi wireless charging, giving you the option to power many smartphones without plugging them in. However, using this feature takes up more power in the charger, because the wireless charging is less efficient.

The whole package comes in an ABS fireproof plastic shell, which is ruggedized with rubber-reinforced corners. The housing is IPX4 splashproof, dustproof, and shockproof. There are water-resistant port covers for the micro USB and USB-C ports for charging the power bank, and for the standard USB port for power output. At 180x90x32mm, the Blavor is compact enough to put it in a pocket or strap it onto a backpack.

Designed for outdoor use, the power bank has a small compass attached to it. It also features dual flashlights that you can use in an emergency or simply to have some light in dark areas.

www.blavor.com

Renogy Solar Suitcase

All the solar chargers described above do a good job at charging smartphones, tablets or other portable electronics, but pale in comparison to the Renogy Solar Suitcase.

At 500x690x70 mm and weighing 36 lbs, it is not something you want to drag around with you on a hiking trip. However, if you frequently go camping and boondocking, then the 200W, 12V Solar Suitcase serves perfectly well. It comes with two 100W monocrystalline solar panels, and a protective soft case for safe portability. The frame is made of aluminum and houses adjustable kickstands on the rear.

The waterproof charge controller features a blue back-lit LCD, which displays system information including error codes. Its advanced PWM technology makes it suitable for 12V and 24V batteries with auto recognition. The solar suitcase can charge sealed/AGM, gel, flooded, and lithium batteries, with Lithium Awakening feature.

PHOTO: RENOGY

The charge controller is rated for a maximum of 20A, and includes multiple solar panel, battery, overcharge, and controller protections.

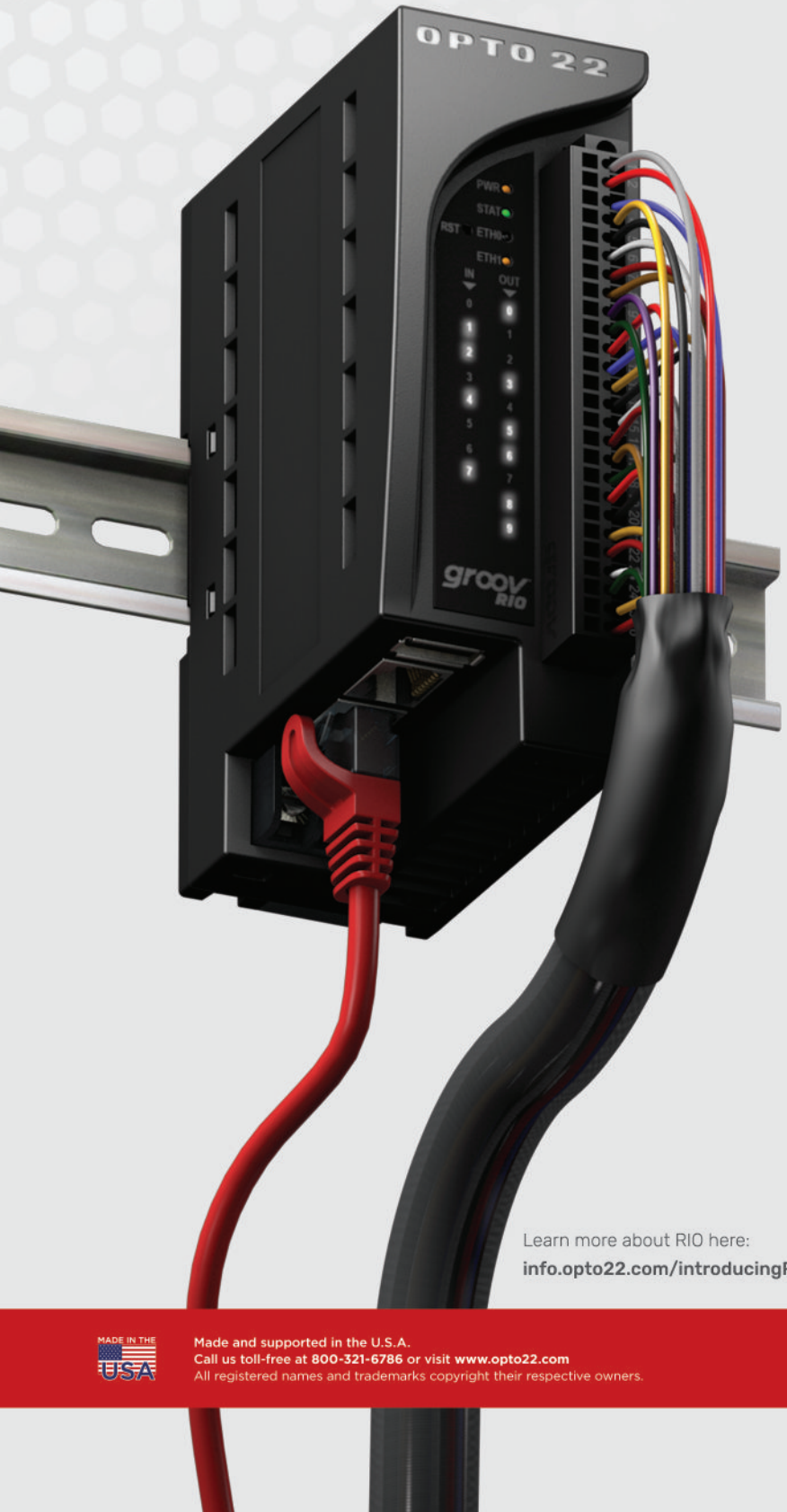
All in all, the Solar Suitcase is a serious alternative to a fuel generator, as it doesn't require regular maintenance and operates silently.

www.renogy.com

Leopold Ploner

Thousands of I/O Options on a Single Module*.

That's RIO cool.



***groov* RIO** - Intelligent, multi-signal, multifunction, PoE-powered, remote Ethernet I/O for IIoT and Automation Applications

- **Configure** up to 8 channels of mixed I/O signals, including temperature, current, voltage, and discrete, plus 2 electromechanical relays
- **Power** the unit and connected I/O with 802.3af PoE Class 0 switches or 10-32 VDC power
- **Integrate** I/O data directly with databases, HMIs, SCADAs, cloud services, and IoT platforms with embedded Node-RED
- **Connect** to existing control systems or building automation systems with Modbus/TCP, OptoMMP, and REST APIs
- **Publish** process data directly into publish-subscribe architectures with MQTT and Sparkplug B or string payloads
- **Log** data to internal power fail-safe memory or an attached USB mass storage device
- **Protect** with built-in security, including configurable firewalls, encryption, user accounts, and VPN client
- **Install** anywhere with wide -20-70°C rating, UL Hazardous Locations approved, ATEX compliant

*Curious how we arrived at thousands of unique field I/O combinations? Check out the details at info.opto22.com/thousands

groov RIO

Learn more about RIO here:
info.opto22.com/introducingRIO

MADE IN THE USA

Made and supported in the U.S.A.
Call us toll-free at **800-321-6786** or visit **www.opto22.com**

OPTO 22
The Future of Automation.