July/August 2022 131
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking & IIoT

Special Supplement

EtherNet/IP solutions update

Page 33

Industrial edge computing on rise: special report 6

Visit us on the web ■ www.iebmedia.com

groov RIO
Power Mon

GET CONNECTED…

Visit our new website at: www.iebmedia.com

5G and the Industrial Edge

A new report from Research and Markets (www.researchandmarkets.com), "Global 5G in IoT Market by Connectivity, Infrastructure, Sensors, Devices" underscores the importance of 5G technology for the Industrial Edge.

This report assesses 5G technologies and solutions in support of the Internet of Things (IoT) and includes an evaluation of key solutions such as 5G enabled Mobile Edge Computing (MEC) and managed services for devices and IoT "things". The report also analyzes the impact of 5G in IoT across infrastructure components including hardware, processors, embedded devices, software, and cloud-based service platforms.

Select Report Findings

- The 5G in IoT market will approach $297.8 billion globally by 2027 at 18.1% CAGR
- 5G and IoT enabled smart machines represent a $3.1 billion global opportunity by 2027
- Device-level SLAs will be crucial for ensuring enterprise and industrial QoS requirements
- 5G is a must for in-building private wireless networks in support of ultra-reliable IoT applications
- Application revenue for edge computing in 5G will exceed 54% of infrastructure spending by 2027

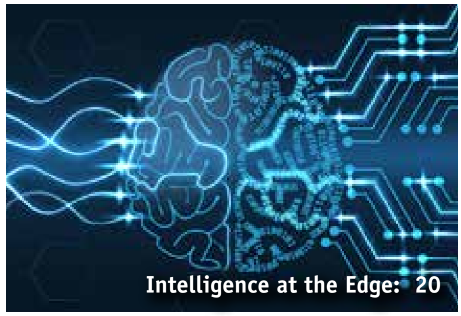
As the size of IoT systems grows to a large scale, their scope will also increase in terms of the impact on enterprise systems and consumers' everyday lives. 5G will optimize IoT networks by way of radio frequency management that meets the needs of both narrowband IoT applications as well as those that require higher bandwidth, which may be on an on-demand basis.

IoT solutions will benefit greatly from the implementation of 5G as cellular providers deploy Low Power WAN (LPWAN) IoT network capabilities. Initial deployments of IoT LPWANs have been non-cellular solutions based on proprietary technologies. However, the author sees emerging standards such as Narrowband IoT (NB-IoT) assuming a dominant role for certain IoT applications.

The use of 5G for Industrial IoT (IIoT) networks in particular will be of great importance to enterprise IIoT in certain industry verticals such as agriculture, logistics, and manufacturing.

It's not a big surprise that 5G will be gaining strength and evolving over the next five years, but it does underscore the breadth of the technology innovations that are driving the IoT. It will be interesting to see its role in the digital transformation of manufacturing.

Al Presher



Intelligence at the Edge: 20

Standardising Data Collection: 26

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2022.**
Deadline for editorial: September 8, 2022 **Advertising deadline:** September 15, 2022

Editor: Al Presher, editor@iebmedia.com

Advertising: info@iebmedia.com

Tel.: +1 585-598-4768

Free Subscription: iebmedia.com/subscribe

Published by IEB Media Corp., Box 1221, Fairport, NY, 14450 USA ISSN 1470-5745

Industrial Ethernet maintains annual growth rate of 10%

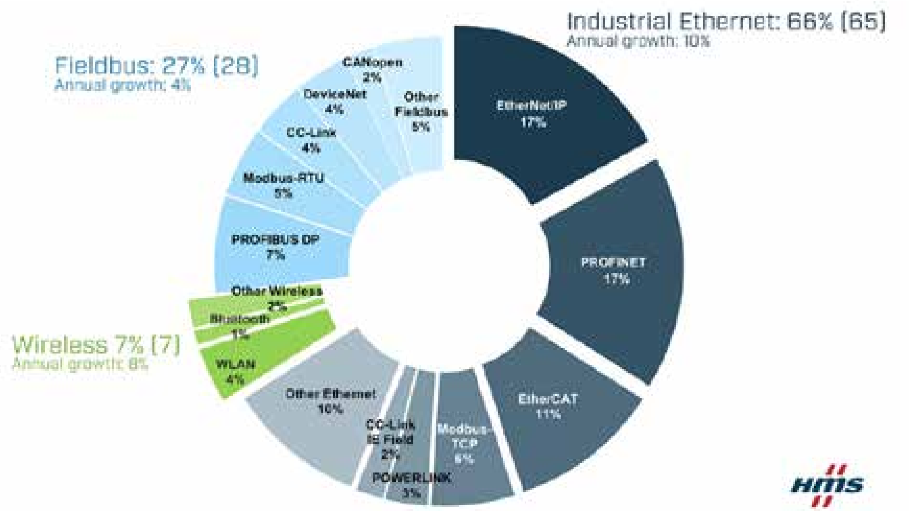
Industrial networks keep growing despite challenging times. Industrial network market shares 2022 according to HMS Networks

EVERY YEAR, HMS NETWORKS ANALYZES THE industrial network market to estimate the distribution of new connected nodes in factory automation. This year's study shows that the industrial network market is expected to grow by 8% in 2022.

Industrial Ethernet still shows the highest growth and now accounts for 66% of all new installed nodes (65% last year). Fieldbuses are at 27% (28) while wireless remains at 7% market share. PROFINET and EtherNet/IP share first place in the network rankings with 17% market share, but EtherCAT closes in fast, now at 11%.

HMS Networks presents their annual analysis of the industrial network market, focusing on new installed nodes within factory automation globally. As an independent supplier of solutions within Industrial ICT (Information and Communication Technology), HMS has a substantial insight into the industrial network market. The 2022 study includes estimated market shares and growth rates for fieldbuses, industrial Ethernet and wireless technologies.

In the study, HMS concludes that the industrial network market continues to grow and that the total market growth in 2022 is expected to be +8%, confirming the continued importance of network connectivity in factories.



Market shares 2022 according to HMS Networks – fieldbus, industrial Ethernet and wireless.

Industrial Ethernet growing steadily

Growing by 10%, Industrial Ethernet continues to take market share. Industrial Ethernet now makes up for 66% of the global market of new installed nodes in factory automation (compared to 65% last year). EtherNet/IP and PROFINET share first place at 17% market share, but EtherCAT takes a big leap forward and reaches double digits for the first time at 11% market share. Modbus-TCP is also doing well as it grows to 6% market share.

Click graphic to view video.

Fieldbuses are growing again

Fieldbuses are at 27% market share compared to 28% last year. However, there is an interesting fact behind these numbers as HMS concludes that despite losing one percent market share, the actual number of installed fieldbus nodes is expected to grow by 4% in 2022 compared to last year, following several years of decline. The underlying reason is believed to be the fact that factories favor established industrial network solutions in uncertain times such as these due to effects from corona and the challenging component situation.

PROFIBUS remains the most installed fieldbus with 7% market share, followed by Modbus-RTU at 5% and CC-Link at 4%. Interestingly, the Modbus technologies TCP and RTU continue to be widely used also in modern factories, together accounting for 11% of the market in 2022 compared to last year.

Wireless use cases emerge – Impact of 5G is yet to come

Wireless grows with 8% which is on par with the overall growth rate of the network market, thus remaining at 7% market share. Typical use cases include cable replacement applications, wireless machine access and connectivity to mobile industrial equipment. The market still awaits the deployment and impact of 5G in next gen factory automation installations.

Networking key for productivity & sustainability in manufacturing

"Industrial network connectivity is an absolute key to reaching productivity and sustainability objectives in modern manufacturing, and this is the main driver for the growth we see in the industrial networking market," says Anders Hansson, Chief Marketing Officer at HMS Networks. "Factories are constantly working to optimize not only productivity and sustainability, but also quality, flexibility and cyber security, and we know that solid industrial networking is key to achieving this as well. While we see growth across all network areas, it is particularly interesting to see that the established fieldbus technologies are getting back to growth again."

Regional network variations

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

*News report by **HMS Networks**.*

New standard for M12 hybrid SPE and power interfaces

SPE Industrial Partner Network driving IEC 63171-7 standard for M12 hybrid Single Pair Ethernet and power interfaces. Developing the hybrid M12 solution is a logical consequence following the initial M8 version.

THE SPE INDUSTRIAL PARTNER NETWORK IS jointly driving a new international standard for M12 hybrid Single Pair Ethernet (SPE) and power interfaces. The new IEC 63171-7 standard, initiated by the Network's founding member TE Connectivity in 2021, is the logical further development of the M8 hybrid SPE and power interfaces, already published by the leading members of the Network in 2020 under the "Industrial Style" IEC 63171-6 standard.

Meanwhile, many industrial customers are following a "one device – one interface" strategy for miniaturized future device generations. Therefore, hybrid SPE connectivity is the key on the way to seamless sensor-to-cloud ethernet communication and power supply.

Developing the hybrid M12 solution is just the logical consequence following the initial M8 version. The roots of hybrid M12 SPE connectivity had been set in the Network's standardization activities for -6. In order to support our customers in their one device one interface strategy, we have been pushing the development of an M12 interface with various SPE and power contact design options.

SOURCE: SPE INDUSTRIAL PARTNER NETWORK

IEC 63171-7 M12 connector and device socket combines SPE and power contacts for a "one device – one interface" strategy for miniaturized future device generations.

The board members of the SPE Industrial Partner Network emphasize in unison the importance of hybrid SPE connectivity: "We are happy seeing an increasing number of companies entering the market with SPE solutions that based on our developments. This demonstrates the acceptance of our initiative and the demand for a uniform single-source solution for all industrial application areas", stated Frank Welzel, chairman of the board. Board member Eric Leijtens of TE Connectivity, who has been leading the establishment of the new standard, sees "the -7 for hybrid SPE connectivity in M12 format as the next inevitable development step for the market."

Device socket.

"We are happy making this step as a strong network of powerful partners. After all, hybrid SPE connectivity will fundamentally speed up the acceptance of SPE in industrial applications, enabling companies to simply and cost-effectively connect devices on the network edge to make data-driven decisions in real time."

Wolfgang Dötsch, Murrelektronik and also member of the board, complemented Eric's statement: "Offering seven codings of data and power contacts provides a very comprehensive solution to the users. Combining them in an industrial standard housing such as M12, the new IEC 63161-7 standard now defines a universal single-interface solution for future IIoT devices. We do listen to our customers – and here we are with an adequate solution providing a standardized interface."

Board member Matthias Eick, HELUKABEL, said: "With the hybrid interfaces and the corresponding M8 and M12 standards, our network has added an important piece of the puzzle, allowing new ethernet infrastructure and by that, new business models. Providing data and power at the same time opens up new opportunities for application in small IIoT devices using data straight from the sensor."

Leveraging the partner network

The SPE Industrial Partner Network, based in Rahden in Westphalia, is an alliance of companies that promote Single Pair Ethernet technology as the basis for rapid and successful growth of IIoT. The aim of the association is to establish SPE on the market as a new Ethernet technology in the sense of a comprehensive ecosystem with all necessary components.

They also see themselves as a partner of the Industrial Ethernet user groups and would like to support them in the adaptation of this new "physical layer" for PROFINET, EtherNet/IP, CC-LinkIE, for example.

Their aim is that the bundling of competences of the individual companies should give users an investment security to invest in this technology.

*News report by **SPE Industrial Partner Network**.*

The rising role of Industrial Edge Computing in the IIoT

In this special report, industry experts provide their perspective on the role of the Industrial Edge in the IIoT. With edge computing processing data where it's generated, using solutions that connect the physical and digital worlds, plants are leveraging data to optimize workflows, save resources and improve quality.

SOURCE: ISTOCK

The Industrial Edge offers an open, ready-to-use Edge Computing platform/infrastructure consisting of Edge devices, applications and connectivity solutions.

INDUSTRIAL EDGE COMPUTING OFFERS A distributed computing framework that is bringing factory and enterprise applications closer to data sources such as IoT devices or local edge servers. This proximity to data at its source can deliver strong business benefits: faster insights, improved response times and better bandwidth availability.

In this special report on Industrial Edge, the Industrial Ethernet Book has reached out to industry experts to gain their insights into the rise of the Industrial Edge and particularly its impact on the IIoT.

Value of open ecosystems

Effective connections and interaction on the automation level.

Benjamin Homuth, Director of PLCnext Technology for PHOENIX CONTACT Electronics GmbH, told IEB that "open ecosystems are the key to a networked future".

"In a world where everything needs to be interconnected in order to obtain the necessary data to optimize processes, automation systems have to be open to improve interoperability and collaboration between various providers and experts. This collaboration between various experts usually takes place at the edge level or in the cloud level," Homuth said.

"Automation providers provide a cloud connection to the various cloud platforms or a connection to other automation providers. The key to this, however, is the connection and interaction on the automation level. Many software experts are able to optimally utilize and process the data originating from an automation application, but they do not possess the necessary automation know-how to obtain this data from an existing automation application. In order to overcome this obstacle, an open edge or automation platform is required so as to integrate the software or at least data connectors into an automation platform."

He added that the challenge here is that there needs to be an easy way to route the data to the cloud or the edge, plus the process data information including the data semantics must also be transferred.

Delivering technology benefits

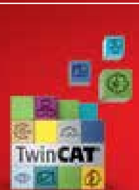
Looking at the specific benefits the industrial edge and cloud computing provides, Homuth said that the possibilities presented by industrial edge and cloud applications give rise to new business models and potential based on the data generated in the automation application. Capturing this data and making it as easy as possible to process the data and transfer it to the cloud presents a challenge not just in existing plants, but also in new plants to some extent.

"There are already many solutions on the market, for example, for data transfer and the processing or analysis of data on the edge or in the cloud. What is critical here is how these solutions can best get at the automation application data without any knowledge of or intervention in the existing plant," Homuth said. "As a standard interface, OPC UA offers

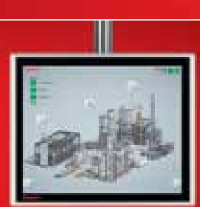
Ex protection and automation combined in a single system: PC-based control

System-integrated explosion protection with PC-based control:

- automation and process technology integrated into one system – barrier-free up to Zone 0/20
- comprehensive range of components for explosion protection
  - ELX series EtherCAT Terminals featuring intrinsically safe interfaces
  - high-quality CPX series Control Panels and Panel PCs
  - powerful EtherCAT fieldbus
  - TwinCAT control software with specific process technology interfaces
- direct connection of intrinsically safe field devices
- integrated control concept for all industries with Ex protection requirements



TwinCAT 3: with process technology interfaces



Complete Ex range: from panels and Panel PCs to I/Os

ACHEMA 2022

Hall 11.1, booth C53

Scan to discover all the benefits of system-integrated process technology

New Automation Technology **BECKHOFF**

"In a world where everything needs to be interconnected in order to obtain the necessary data to optimize processes, automation systems have to be open to improve interoperability and collaboration between various providers and experts." Benjamin Homuth, Phoenix Contact

many advantages for data exchange when forwarding data from the sensors all the way to the cloud. However, to fully exploit all the possibilities of edge and cloud applications, providers of automation solutions must find a way to enable the implementation of software for data analysis, edge software stacks, or cloud connectors."

With the PLCnext Technology Ecosystem, Phoenix Contact provides an open control platform and various possibilities for integrating third-party software on all levels. Installation based on the PLCnext Control hardware platform even makes an edge layer optional. When a PLCnext Control device is used, the PLC level already offers all possible functions, such as the seamless integration of third-party software, the aggregation and preprocessing of data, transmission including semantics via OPC UA, and direct connection to cloud systems.

The optional use of PLCnext Control on the edge layer simplifies interoperability with other automation providers and existing applications, and enables the bundling of data from larger installations.

Homuth added that, with PLCnext Control, know-how can be pooled from different areas. Various programming languages, such as IEC 61131-3, C++, C#, Python, or Java, can be used to program an application and can be combined, if required. The ability to integrate open-source software and easy-to-integrate apps from the PLCnext Store allows the controller to be tailored to the specific application. The programmer has an almost unlimited array of options at their disposal when creating the application.

The application program can be implemented using native implementation or encapsulated in a docker container. If required, the code can also be executed in real time and at cyclic intervals (in accordance with IEC 61131). In many applications, the use of AI and especially machine learning on the edge or in the cloud offers significant potential for optimizing production plants. By using different methods of implementation on a PLCnext Control device, it is possible to also integrate machine learning algorithms and execute them together with a control program. In the case of ML applications with fast response times or in the event that the bandwidth is not sufficient, execution on the edge or directly in the control level is an advantage over sending all the data to the cloud.

Edge application targets

Homuth said that it is evident that more and more small and medium-sized companies are using public cloud solutions with direct connection to the automation application. It is only larger companies with their own IT departments that are able to operate a private cloud, e.g., as an on-prem installation. Both versions offer different advantages and disadvantages and the companies in question need to weigh up which option will be best suited to their applications.

With both versions, an edge layer offers the option of bundling data from larger installations or connecting to an existing application. The data can then be analyzed, processed, and visualized on the company's own servers or in partnership with major cloud providers. With Proficloud, Phoenix Contact offers another option for collecting data from the automation application, especially for small and medium sized applications.

Transmission to the cloud is implemented quickly and without any additional programming by means of a Proficloud connector that is preinstalled on the PLCnext Control device. In Proficloud, the user can record, evaluate, and visualize the data. This provides an easy way to exploit the potential of cloud applications, without having to select the right cloud components from the wide and complex range offered by the major cloud providers.

"The networking of automation technology enables the transfer of data to a cloud, which "increases the need for cybersecurity measures to ensure the security of the plant and to protect against unauthorized access and manipulation," Homuth added. "Cybersecurity incidents are increasing at a rapid pace and can, in a worst-case scenario, damage the image of a company and result in financial losses due to production downtime. Along with the transfer of data to a cloud application, including the semantics of the process data, the proper and adequate implementation of these security measures presents a challenge for many automation users."

With PLCnext Technology, devices and applications can be professionally installed and protected in accordance with the IEC 62443 cybersecurity standard. The PLCnext Control device is already certified in accordance with standard IEC 62443 and therefore provides the basis for the implementation of cybersecurity in machines and plants. So, with the possibilities afforded by PLCnext Technology, including the appropriate security, it is possible to benefit from all the advantages of edge and cloud applications.

SOURCE: MOXA

"A robust and long-term support operating system (OS) and an execution environment for software containers are the infrastructure for modern edge applications. Examples are Moxa Industrial Linux, a 10-year support robust Linux OS, and container environments like docker, Microsoft's Azure IoT Edge or AWS Greengrass." Hermann Berg, Head of IIoT, Moxa

Hardware, software & service

Easy-to-manage, long-term platform-level solutions.

Hermann Berg, Head of IIoT for Moxa, said that the key components of any Industrial Edge and Cloud Solution are hardware, software and (cloud) service. Robust hardware for industrial environments has been around for a while and continues to improve and get more cost effective. The most relevant advances of recent years however have been made on the software side.

"A robust and long-term support operating system (OS) and an execution environment for software containers are the infrastructure for modern edge applications. Examples are Moxa Industrial Linux, a 10-year support robust Linux OS, and container environments like docker, Microsoft's Azure IoT Edge or AWS Greengrass," Berg told the Industrial Ethernet Book recently.

"This should integrate seamlessly with a device lifecycle management or fleet management system that is often provided in the form of a Software-as-a-Service (SaaS) cloud platform."

Berg said that all together this provides an easy-to-manage long-term platform where data engineers, scientists and software developers can quickly add and manage their apps without ever going on site to fix or improve the software on the IIoT gateway or edge computer.

Industrial Edge Benefits

IIoT projects have to be easy, fast and scalable to succeed. They have to be fast, so engineers and data scientists can quickly determine, if the data collected is "good enough" to create the desired outcome.

The platform should be easy to use, so internal resources can focus on developing and strengthening digital core competencies: making best use of data related to their own equipment, processes, material, and deliverables. And the platform has to scale quickly, once proof of concepts (PoC) and first deployments show the value of the new software. So, from the start hardware, software and services should be selected that are suitable for large-scale rollouts.

Berg said that, initially most companies focus on simple data collection to increase transparency: What is the status of my equipment? What is the performance of an important process, e.g., measured by indicators like overall equipment effectiveness (OEE)? This already allows for a quicker reaction to unforeseen issues and better short-term and long-term planning.

Another benefit of these open platforms is the fact that third-party applications and services can be easily combined with different hardware options. Moxa has started to establish partnerships with different types of partners to take advantage of the easy integration: https://moxa-europe.com/iiot-partners/.

"That way a stronger and stronger IIoT and edge infrastructure serves as the basis to offer the tools that allow workers and managers to successfully manage an increasingly volatile, uncertain, complex, and ambiguous production environment," he added.

Solutions for industrial applications

Berg said there are multiple ways to implement such a scalable IIoT platform with the option to add and manage your own software apps from the cloud.

A high-end solution could be based on Microsoft Azure which provides a seamless integration of the Azure IoT Edge software modules into their cloud-based Azure Container Registry. Azure IoT Hub and their device and module twin framework is a perfect foundation for managing both edge devices and edge software containers from the cloud at scale. Increasingly third-party software applications are available through the Azure Marketplace and Azure allows for a rich integration with the cloud back-end and the rest of the IT stack of a company.

A more simple and cost effective solution, outlined by Moxa and qbee in recent project called "IIoT on a Shoestring Budget", was centered on a very simple, but extendable open-source Python-based IIoT edge software that made very efficient use of GitHub, optionally Docker Hub, and fleet management software from our IIoT partner qbee.io (https://github.com/MEUIIOT/moxaiiot-


SOURCE: MOXA

The goal of the Industrial Edge is an easy-to-manage, long-term platform where data engineers, scientists and software developers can quickly add and manage their apps without ever going on site to fix or improve the software on the IIoT gateway or edge computer.

uc2100-qbee-io).

In both cases, devices in the field can be easily monitored, upgraded and troubleshooted from remote. In particular, the software running on the devices can be managed and continually adapted and improved at scale without ever visiting the respective sites.

Potential industrial applications

When asked what are specific application areas are the newest Industrial Edge and Cloud solutions targeting, Berg responded that companies today seem to be looking less for closed third-party point solutions, rather they are prepared to build their own end-to-end data infrastructure on top of and integrated with their existing IT and OT environments.

"Based on this new and growing infrastructure they develop their own data capabilities complementary to their existing traditional core competence. Those digital capabilities can then be used to saving costs, avoiding outages and delays, and generally providing better service to the customers," he said.

"One visible sign of this increased digital ownership has been the surge of After Sales Service Portals. Machine and plant builders along with other vendors and users of high value industrial assets in segments as diverse as marine, mining, energy, and transportation have applied industrial IoT technology to provide more, better, and more digital service to their customers during the pandemic," he added.

Since the beginning of 2022, Berg said that a strong and growing challenge is the efficient use of energy in Europe. Keeping operations up, while dramatically reducing gas and electricity consumption might become the single biggest challenge in 2022 and 2023 for many large industrial companies in Europe that currently depend on Russian gas or oil. IoT connectivity will be the basis of many solutions developed to address it.

Up until recently connectivity and security issues represented a significant hurdle during the deployment of IIoT solutions. As IIoT infrastructure matures and deployments scale up, new challenges arise.

"Building one integrated infrastructure for IIoT application means that data will be used by more than one application," Berg said. "As a result, a common data model across applications has to be agreed between the development teams. The common data model becomes part of the IIoT infrastructure, so developers and data scientist can focus on the task of developing code and models based on the available data, rather than solving infrastructure problems."

This helps to address the more commercial challenges that determine whether a good business idea will turn into a success in the real world or not: speed, scale, resources, and cost. Easy access to quality data allows developers to quickly develop, test, and deploy their apps at scale. Resources can be focused on core competencies, while the infrastructure is handled by other teams or outsourced.

"Separating IIoT edge infrastructure from the actual apps is the foundation for more valuable insights and more automation and thus better and faster service at lower cost," he said.

Industrial infrastructures

Compatibility, scalability, security and artificial intelligence.

According to Georg Stöger, Director Training and Consulting for TTTech Industrial, four key technology trends are enabling the latest generation of Industrial Edge and Cloud Solutions.

"In addition to the wide adaption of open technologies and standards for compatibility and scalability, and the use of IT technologies such as virtualization and containerization for system management, we consider the integration of OT systems into IT security as a third key technology trend to further enable IIoT and OT-to-cloud solutions," Stöger told IEB recently.

"With the rising threat to industrial systems from increasingly professional and state-sponsored cyberattacks, the security aspect has risen in importance in recent months. Fortunately, these trends are not opposing each other; in fact, the security architecture of open standards such as OPC UA tends to be up-to-date and sophisticated, and flexible application management using virtualization and containerization can – if done right – also contribute to security," he added.

Nevertheless, the challenges to achieve secure and efficient system management in a cloud-enabled industrial infrastructure are tremendous and will likely become even more so with the fourth trend, the use of artificial intelligence at the Industrial Edge.

This trend will blur the line between cloud and edge further, offering even more flexibility to optimize existing applications and create new functionality that could not be effectively implemented in a fully cloud-centric architecture.

Benefits of the Industrial Edge

When asked about the specific benefits that industrial edge and cloud computing provides, and the potential impact on manufacturing, Stöger replied that each have their separate benefits but there are also substantial the benefits of combining industrial edge and cloud.

"With field level interfaces connected to the industrial edge, access to real-time process data is possible. This is essential for use cases which require a lot of storage and processing power, such as powerful digital twin models," Stöger said.

He added that the process data for creating these models needs to be sent to the cloud. However, the same data might also be used immediately at the edge, e.g. for rapid diagnostics to avoid machine malfunctions that could affect product quality. Not all data may be needed in the cloud; users could send only the data required for analysis or storage to the cloud, thus saving bandwidth and cost, while processing the full data set at the edge.

An industrial edge computing platform such as TTTech Industrial's Nerve, needs to support not only this flexible management of process data, but also the management and execution of multiple functions at the edge, ideally supporting various technologies for efficient use of hardware resources: virtualization and containerization of applications make it possible to maintain and update applications, devices, and software remotely. This saves hardware cost and enables remote maintenance as well as easier handling of devices (e.g. via a web-based management system).

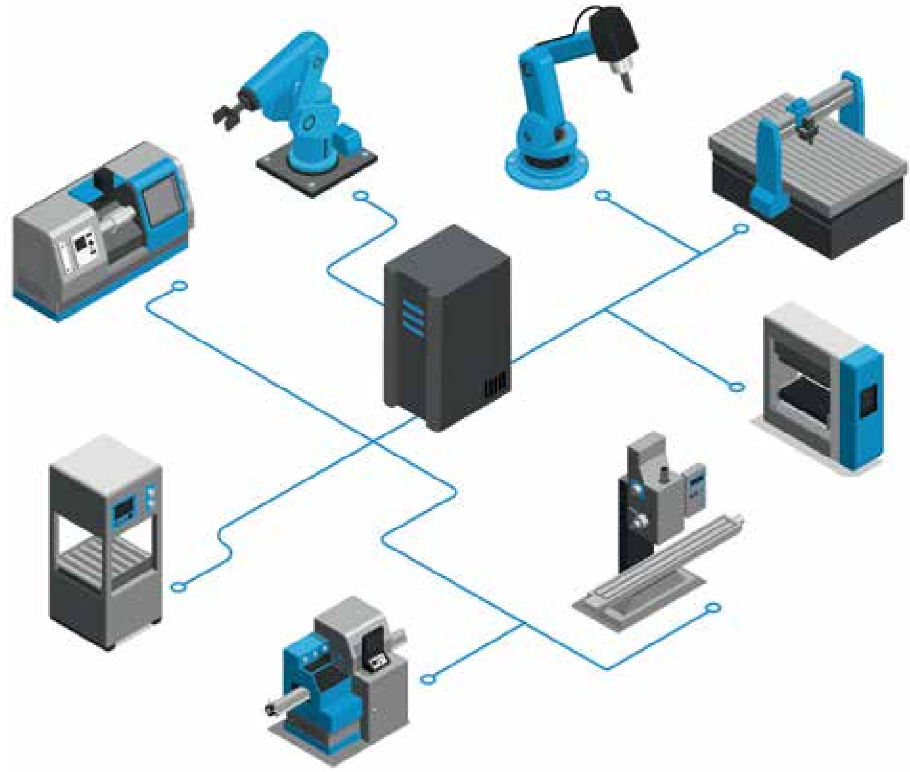
Industrial application solutions

One key benefit is that Industrial Edge computing brings IT technologies to the shop floor and OT data into the data center. Applications using OT data can be run close to the data source (e.g. the machines on the shop floor); this allows data to be processed with lower latencies and can help mitigate network bottlenecks, but also security issues.

OT data made available to the IT infrastructure can also be used to provide additional services to customers, e.g. in connection with predictive maintenance and service packages, decreasing the risk of production standstills. Remote maintenance is based on real-time data as well – it helps to reduce travel cost and allows issues to be resolved more quickly and without customers having to wait for a technician to arrive.

"At a time of severe supply chain issues with electronics, virtualization can become a very interesting benefit of industrial edge computing. With this technology, which is well established in the data center, a single powerful IPC can host multiple applications and even entire virtual computers simultaneously. This saves cost and simplifies system management. However, specialized virtualization technologies (real-time hypervisor) are required to address the specific needs of some industrial applications. Our edge computing platform Nerve uses Linux Foundation's open hypervisor ACRN™ and Intel® Time Coordinated Computing (Intel® TCC) to improve hard real-time virtualization," Stöger said.

"The application areas that our customers and project partners are currently focusing on include condition monitoring of machines and field equipment, remote access for service, and predictive maintenance. These applications all need reliable access to real-time OT data



SOURCE: TTTECH INDUSTRIAL

"In addition to the wide adaption of open technologies and standards for compatibility and scalability, and the use of IT technologies such as virtualization and containerization for system management, we consider the integration of OT systems into IT security as a third key technology trend to further enable IIoT and OT-to-cloud solutions." Georg Stöger, Director Training and Consulting, TTTech Industrial

provided by field I/O and controllers to industrial edge devices. Cloud analytics can enhance the picture by showing an aggregated picture across production sites and countries," he said.

Machine learning for optimization of parametrization, anomaly detection, and digital twins are newer applications that make use of edge computing technology. They also need large amounts of real-time data for training, which has to be made available reliably and securely.

Machine learning builds on often large samples of data and enables machines to make predictions and decisions based on "examples of previous experience with this kind of process".

This is an important step towards smart factories and more autonomous production. Digital twins are a digital representation of an asset such as a machine or a factory. They are trained on real-world data and allow companies to build and test parameters in the digital world before rolling them out in the physical world. This helps optimize processes and machines before they are built or reconfigured, saving resources and adaptation costs.

Addressing engineering challenges

Stöger said that a major challenge often encountered by automation engineers is networking. IT and OT networks are typically managed in very different ways, which makes sense in a traditional federated architecture with "closed" and tightly controlled production systems.

With more openness, more internet-connected applications, remote access, remote maintenance, and increasing frequency of software updates and patches, gateways and firewalls become a liability.

"This challenge is addressed by integrated industrial edge platforms that support secure tunneling, forwarding, and other mechanisms to provide the necessary flexible connectivity for multiple applications and devices at the edge, while maintaining full control over all traffic that enters or exits the factory network through the firewall. Thus, the automation engineer is not required to become an IT networking expert to address network performance and security," Stöger said.

Edge computing can also address software security issues. Less secure applications (e.g. legacy software) can be containerized and isolated so that they can only access the intended resources within the edge. As the applications are running completely separately from each other, the system is only partially affected if one of the applications/devices is successfully attacked and compromised. Edge computing devices should support role-based access control which limits the risk of unauthorized access to critical data and resources.

Edge-to-cloud connectivity

Solutions that connect the physical and digital worlds.

According to Arun K. Sinha, an engineer at Opto 22, key technology trends that are enabling the edge-to-cloud solutions include Internet protocols and technologies being driven into systems at the edge, where the physical world and the digital world connect.

"Layers of complexity are being removed from the communication process between physical assets and cloud solutions. Modern IIoT system architectures are being flattened, streamlined, optimized, and secured," Sinha said. "Edge computing systems must easily and securely access the cloud through the open, standards-based communication technologies the internet is based on."

He added that most devices on an OT (Operational Technology) network today communicate using the request-response model. Edge-to-cloud architectures pose a problem of scale, and with this model network traffic can quickly become an issue. The trend is towards a model that is more effective in IIoT applications, which is publish-subscribe, or pub-sub. In the pub-sub model, a central broker becomes the clearinghouse for all data. Because each client makes a single lightweight connection to the broker, multiple connections are not necessary.

Technology benefits

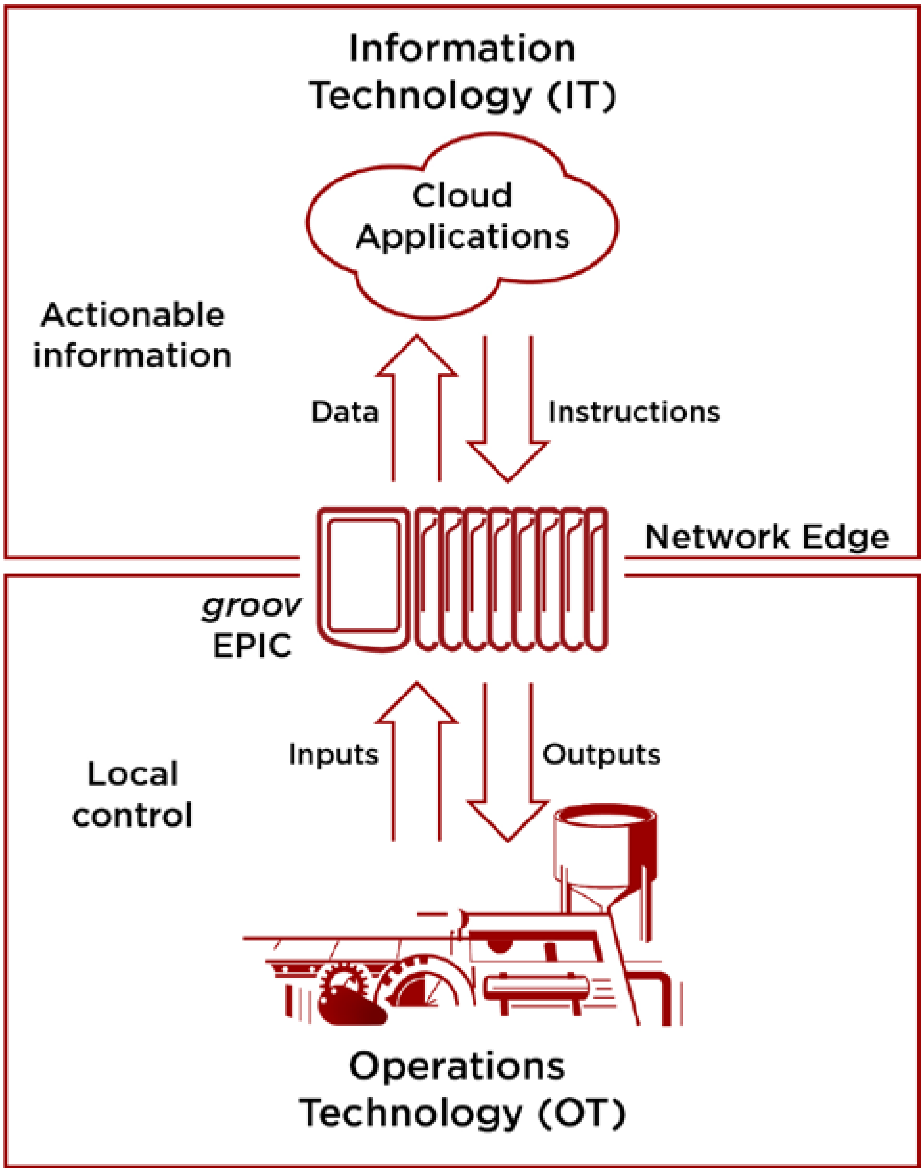
"Industrial edge and cloud computing ideally create a cohesive system of devices and applications able to share data seamlessly across machines, sites, and the enterprise to help optimize production and discover new cost-saving opportunities. The benefits include making it easier to connect industrial equipment with computer networks, software, and services, both on premises and in the cloud," Sinha said.

The impact on manufacturing companies as well as OEMs is that they can now take advantage of analytics tools from software companies such as AWS, Microsoft, Google and others to improve their manufacturing processes and streamline their business. Manufacturers can then start to identify real opportunities for operational efficiency improvement and meaningful revenue generation. To foster such business benefits, data from the physical world of machines and equipment must be available to the digital world of the internet and information technology systems, quickly, easily, securely and continuously.

Sinha added that new software and communication tools have emerged onboard automation systems that help facilitate edge-to-cloud connectivity, industrial IoT, digital transformation, and Industry 4.0 for manufacturing, process and OEMs. These are unique in that they combine traditional automation and control with technology more common in IT and software development tools, data formats and communication methods.

MQTT with Sparkplug B is a secure, lightweight, open-source publish-subscribe communications protocol with a data payload designed for mission critical applications. Node-RED is a low-code, open-source IoT programming language for managing data transfer across many devices, protocols, web services, and databases. RESTful APIs allow software or cloud systems to get data from remote edge devices, without the layers of complexity and conversions that exist in traditional industrial automation systems.

Further, cybersecurity features commonly found on IT devices such as user authentication, configurable firewalls, encrypted communications and even LDAP are critical for edge devices when used in industrial applications involving cloud connectivity.



"Industrial edge and cloud computing ideally create a cohesive system of devices and applications able to share data seamlessly across machines, sites, and the enterprise to help optimize production and discover new cost-saving opportunities. The benefits include making it easier to connect industrial equipment with computer networks, software, and services, both on premises and in the cloud." Arun K. Sinha, Opto 22

Industrial Edge and cloud solutions

Sinha said that one of the most exciting use cases for industrial edge and cloud solutions is predictive maintenance of machinery. Most analytics tools using anomaly detection, artificial intelligence or machine learning executed their algorithms in the cloud. The data is first gathered and pre-processed at the edge, and then communicated to the cloud for the heavy computational resources required.

"Remote monitoring of distributed assets is another application area where IIoT solutions such as MQTT with Sparkplug can play a key role," he added. "Where field signals are distributed over large geographic areas or multiple sites, edge devices can facilitate data transmission to networked applications and databases, improving the efficiency and security of local infrastructure or replacing high-maintenance middleware such as Windows PCs. IoT enabled edge controllers can act even as IoT gateways to legacy control systems. All disparate devices can share data across the organization through the cloud with a unified namespace."

Machine builders and OEMs are also utilizing these solutions to provide value add services to their end users. These include not only hosting but analyzing client data to provide proactive service measures as well as improve operational efficiency of their machine at the customer facility. MQTT is ideally suited for this application as it does not require a port to be opened by the customer IT department, as all data is communicated securely via device originated, outbound connections.

Connectivity challenges

One common challenge that automation engineers face is one of connectivity. At the edge, things like sensors, circuits, relays, and meters are attached to industrial control systems used to operate equipment and machines. These sensors translate what's physically happening (temperature, light, vibration, motion, flow rate, and so on) into an electrical signal like voltage or current, which is then interpreted by a controller.

Traditional PLCs typically are not capable of edge computing or communicating directly to cloud platforms. They typically use OT protocols for communication that are seldom internet compliant, and do not include information security standards like encryption and authentication.

Sinha added that another challenge is the large volumes of data that can be generated at the edge with industrial automation systems. Moving that much data onto existing network and internet infrastructures for cloud-based analytics and centralized management will clog networks, vastly increasing network and internet latency. For many industrial IoT applications, that is not acceptable, because real-time control and monitoring are mandatory. For the industrial internet of things to reach critical mass, intelligence must be pushed to the network edge, where the physical world meets the digital world. Computing systems at the network edge must have the capability to collect, filter, and process data generated at the source, before it's transmitted up to the IIoT. And at the same time these edge computing systems must be able to complete the local real-time process control and automation tasks of traditional industrial applications.

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

The price of network transparency

Convergence of information technologies (IT) and operational technologies (OT) has led to new cybersecurity challenges. Integrating IT and OT to achieve greater flexibility and visibility on the shop floor has turned proven cybersecurity strategies on their head, leaving major security vulnerabilities.

CYBER DEFENSES LIKE NETWORK ISOLATION, a strategy to keep OT systems physically and electronically separated, and security through obscurity (STO), which enforces secrecy and confidentiality within IT systems, are losing their defensive foothold against cyberattacks.

Current security challenges

Securing devices and infrastructure after they've already been implemented is an arduous and costly undertaking, impeding the adoption of better security measures. And, because the IT/OT convergence is exposing network vulnerabilities, increased isolation and obscurity will not solve the problem at its source.

Anyone, even an employee, could inadvertently install compromised devices and USB sticks with malware to make it past firewalls. Additionally, although field devices that bridge on-premises networks and machinery to the cloud are beneficial, they also carry cyberattack risks.

In short, new network security countermeasures are required to meet the growing threat of cyberattacks while still maintaining the openness of IT/OT integration.

Current regulatory efforts

To regulate cybersecurity for field devices, the International Electrotechnical Commission (IEC) developed the IEC 62443 standard, which has 14 components and considers the entire automation system supply chain. Many plant operators now require their suppliers to adhere to IEC 62443 when developing and manufacturing their field devices.

SOURCE: ISTOCK

New network security countermeasures are required to meet the growing threat of cyberattacks while still maintaining the openness of IT/OT integration.

Hardware and software solutions can alleviate these security growing pains with modern security already in place. Manufacturers that adopt IEC 62443 early and incorporate IEC 62443-compliant features into their devices will be ahead of the curve as the rest of the industry catches up.

Security hardware/software

Installing devices with built-in security functions will make IT/OT integration easier and safer, and facilitate the addition of more advanced security functions later on. Look for security-hardened solutions with advanced features like a system on a chip (SoC) with Secure Boot to verify firmware integrity before completely booting up. Implement protocol firmware such as Ethernet/IP with CIP Security or PROFINET Security to ensure secure communications at the field level. And, proven technologies like Transport Layer Security (TLS) offer device and user authentication data integrity as well as IO-data encryption.

The flexibility and power to future-proof your infrastructure in this way will be an invaluable advantage.

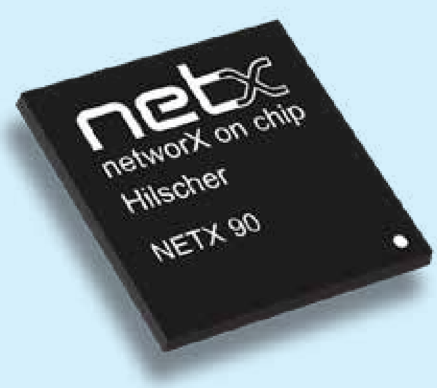
*Technology report by **Hilscher**.*

Visit Website

Future-proof your secure networks

Hilscher says that the netX 90 is the smallest industrial communication chip on the market with advanced, out-of-the-box security features like CIP Security as protocol stack firmware and Secure Boot functionality. This system on a chip (SoC) provides industrial real-time Ethernet to connected devices, while its state-of-the-art crypto core enables complex cryptographic algorithms without sacrificing performance.

A robust controller, the netX 90 is compatible with many protocols like PROFINET, EtherNet/IP, EtherCAT, Modbus TCP, CC-Link IE FB and Sercos III. It is also ideal for reliably transferring process data between devices and their controllers, without the risk of third-party manipulation.



Industrial Edge ecosystem offers connectivity solutions

An ecosystem of hardware, software and connectivity solutions is required to create effective Industrial Edge platforms and infrastructure. Some of the newest innovations cover the diverse needs of network connectivity including security protection, edge computing software and reliable cloud integration.

Anomaly-based intrusion detection for industry

Digital transformation for industry based on reliable OT (operational technology) networks needs efficient security solutions. Furthermore, deterministic OT communications have special security considerations.

For instance, the security hardware should be rated for industrial environments and operate reliably without batteries for minimal maintenance. Moreover, the software must provide maximum transparency without network disruptions, especially when the cyberthreat is internal.

Passive anomaly-based intrusion detection with the Guardian and the Central Management Console from Nozomi Networks in combination with Scalance LPE offers a simple, integrated approach to monitor, detect, and respond to threats within the network. It is a passive monitoring intrusion detection system with no disruption to network operations during installation or operation. You can deploy the Nozomi Networks' Remote Collector on the Scalance LPE within trusted zones of the network to obtain complete visibility on OT/IoT assets and processes.

This is a comprehensive solution of field-proven hardware, advanced software, and OT network expertise from a single, trusted source. It enables security personnel to respond to anomalies in real-time, with context-based smart alerts, always keeping your production environment safe and operational.

Learn more

SOURCE: SIEMENS

Passive anomaly-based intrusion detection with the Guardian and the Central Management Console from Nozomi Networks in combination with Scalance LPE offers a simple, integrated approach to monitor, detect, and respond to threats within the network.

Processing data locally ensures that bandwidth and latency issues are addressed, while forwarding only relevant data to the cloud.

Edge computing for industrial applications

As edge computing creates new opportunities for industries, the demand to run applications at the Edge using high-performance industrial-grade devices is growing. Essential in IIoT solutions, the portfolio of Edge computing devices from Siemens provide a reliable, flexible, and secure platform for deploying Siemens, third-party and self-developed Edge computing applications into networks in industrial and harsh environments, bringing intelligence and data processing closer to the source in real-time.

Processing data locally ensures that bandwidth and latency issues are addressed, while forwarding only relevant data to the Cloud.

Devices such as Scalance LPE, a local processing engine with a powerful CPU, Ruggedcom APE for the RX1500 family, an industrial application hosting platform and Ruggedcom RX1400 + VPE, an ARM-based virtual processing environment, can easily integrate Edge computing applications to perform advanced analytics, machine learning, artificial intelligence (AI) and other tasks. Additional applications can be installed for predictive maintenance, secure remote access, network management and anomaly-based intrusion detection.

Siemens provides cost-effective and customized solutions that help businesses make informed decisions, while reducing costs, improving operational efficiency, safety, flexibility and security.

Learn more

Easily transmit data from field devices to the cloud

To benefit the digitalization comprehensively, cloud connectivity is essential. The possibility to simply transfer the data to any cloud system without unnecessary additional costs and process them there, where it is most economical, is key element to successful project completion.

The introduction of the new firmware V5.0 in SIMATIC RTU3000C, the remote terminal units, is enabling simple connection to all standard cloud systems like MindSphere, Microsoft Azure or AWS via MQTT protocol. In addition to telecontrol tasks, this expands the range of potential applications for SIMATIC RTU3000C. The new possibility to combine monitoring process data from RTU (remote terminal unit) with cloud processed and fed context and data sources, allows improved process quality, malfunction identification and in general data (or big data) analysis-based measures.

The RTU3000C monitors remote measuring points even in locations without external power sources and records and buffers values of the connected sensors with a time stamp. New firmware V5.0 extends the possibility to send the data either to the remote-control center as it used to be or to a cloud application.

SOURCE: MOXA

Data collected from advanced IoT gateways can be transferred to Azure IoT Edge and then on to the Azure IoT Hub with a few simple configuration steps.

For the RTU3000C, that supports a wide range of telemetry protocols like DNP3, IEC 60870, TeleControl Basic and SINAUT ST7 and allows connection to peripheral devices and sensor technology, the extension of the MQTT communication protocol is therefore strong and futureproof enhancement.

Learn more

Advanced IIoT gateways for remote management at unmanned sites

When embracing the new era of the Industrial Internet of Things (IIoT), many system integrators and engineers face the critical challenge of finding a secure and reliable IIoT-gateway solution that offers regular security patches to remedy system vulnerabilities in a timely manner. Moxa's newly launched AIG-300 Series IIoT gateways come with Azure IoT Edge integration that adds significant value in the form of unique features that help build a cost- and time-efficient IIoT system.

Azure IoT edge integration

IIoT gateways need to be highly secure and reliable to facilitate seamless edge-to-cloud data acquisition and device management. The AIG-300 IIoT gateway, seamlessly integrated with Azure IoT Edge and powered by ThingsPro, is a market-leading solution for reliable, quick, and easy data acquisition and device management.

Data collected from devices can be transferred to Azure IoT Edge and then on to the Azure IoT Hub with a few simple configuration steps. Conversely, devices can be effectively managed via the route of Azure IoT Hub to the Azure IoT Edge on the AIG series IIoT gateways. This seamless one-stop edge-to-cloud platform can greatly help customers shrink the system development time and cost.

Most IIoT applications are deployed in remote, unmanned, and harsh environments such as a smart grid, energy storage systems, solar fields, oil and gas refineries, and rail-wayside applications.

Maintaining normal operations and monitoring statuses effectively is crucial to these systems. The AIG series gateways, with their wide-temperature design and low power consumption, are well-suited for use in these environments.

Learn more

SOURCE: SIEMENS

The RTU3000C monitors remote measuring points even in locations without external power sources and records and buffers values of the connected sensors with a time stamp.

Edge computing for easily implementing IoT applications

Intelligent IoT edge solutions can close the gap between the IT and OT worlds. With preinstalled software packages as well as universal graphical user interfaces and programming environments, powerful Edge PC hardware are enabling simple development and implementation of edge applications.

SOURCE: SHUTTERSTOCK

Universal graphical programming reduces software development expenditures. (Image source: whiteMocca@shutterstock.com)

THE ADVANTAGES OF EDGE APPLICATIONS ARE already known. However, a traditional PLC cannot locally preprocess incoming data. That's why Phoenix Contact has developed Edge PCs with preinstalled software tools for easy implementation of IoT applications (lead).

The discussion of whether edge computing lends itself to industrial applications comes up with increasing frequency today. The concept involves a decentralized computing infrastructure that is close to the data source. Edge computing solves the challenges of cloud computing in the production industry, as the cloud applications are pushed into the production applications. Cloud computing is already established in many office-related IT applications.

Many of these application areas, such data analysis and storage, are also relevant to the manufacturing industry – that is, operational technology (OT). There are some challenges in this environment, however, in terms of data protection and data security, lag time in information processing, data transfer rates, and computing power and storage space costs. Edge computing brings data processing closer to the machine and thus closer to the data source. Relocating the cloud application to the edge (that is, the edge of the network) allows such problems to be overcome.

It is important to realize, however, that there isn't just the one edge. Rather, there is potential along a spectrum from the machine edge to server-based solutions for entire production sites. And the actual functionality of the edge solution differs from application to application. Cited as typical edge applications are data collection and compression, data (pre)processing and analysis, the use of artificial intelligence, and cloud connection.

Edge computing does not replace cloud computing, though. Instead, it complements it. The edge and the cloud thus have a partnership in which the distribution of tasks between the two solutions can differ according to application.

Benefit from openness of ecosystem

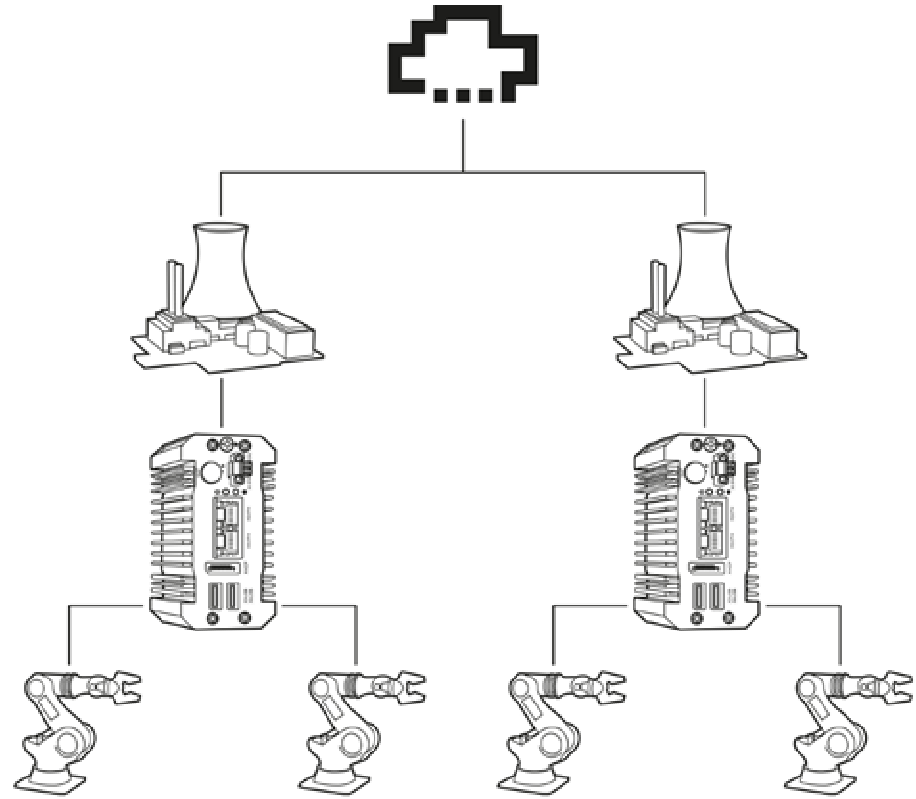
Behind PLCnext Technology is an open control platform for industrial automation technology that is part of a complete ecosystem. The ecosystem consists of the following components:

- PLCnext Control as a robust piece of hardware in the form of a PLC or industrial PC to which an I/O system can be connected
- The engineering and configuration software PLCnext Engineer, which supports IEC 61131-3
- The PLCnext Store as a digital marketplace where software related to PLCnext Technology can be downloaded
- The PLCnext Community, which serves as an information source and is there

for exchanging knowledge about the ecosystem

Because of the openness of PLCnext Technology, any customer application can be integrated into the complete project, regardless of programming language. The openness and completeness of the ecosystem thus creates the ideal foundation for edge computing in the manufacturing environment. PLCnext Technology already offers numerous advantages here:

- The inclusion of various programming languages reduces development time
- The OT communication protocols most widely used in the production environment, such as OPC UA, PROFINET, or Modbus/TCP, are already supported by the hardware
- PROFICLOUD or multi-cloud connection is possible with a Cloud Coupler
- The components are based on a security-by-design development in accordance with IEC 62443
- Customer-specific and open-source software can easily be integrated into the overall application
- New apps can be reloaded to the controller easily through the PLCnext Store



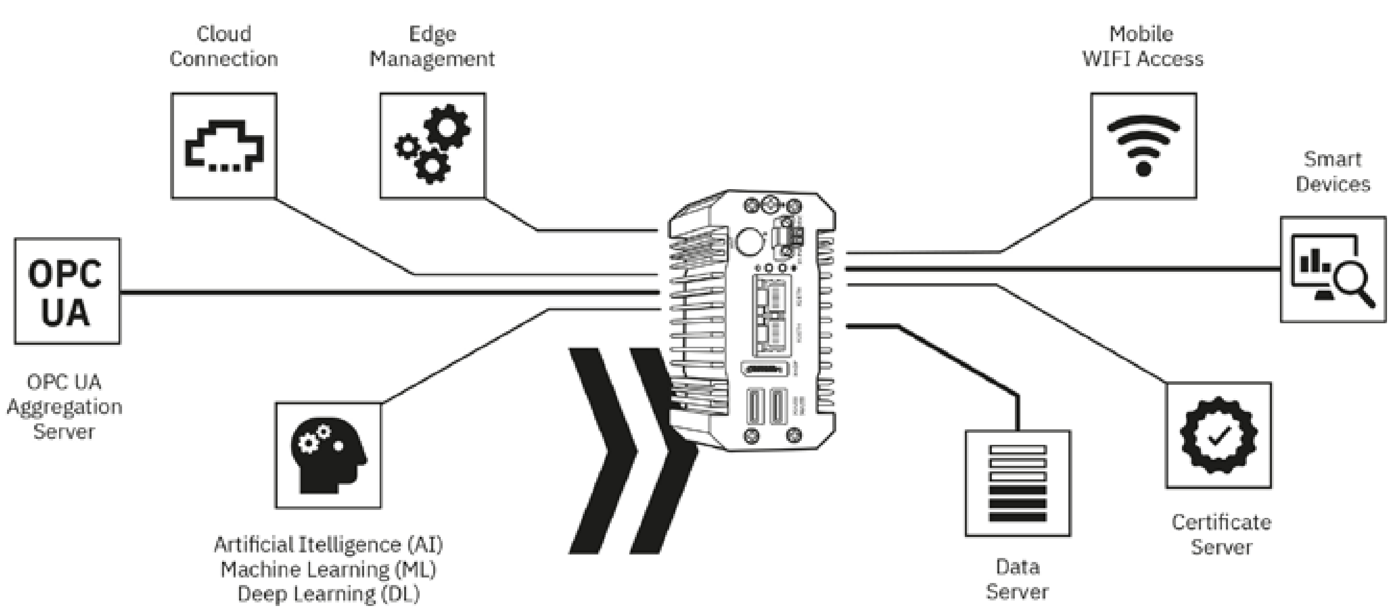
By definition, edge devices are installed at the edges of the network.

Software tools already integrated into the devices

The market for edge-programmable devices is currently evolving. While most providers offer edge-ready hardware, they lack the integrated software tools needed for a ready-to-use programmable edge device. That's why Phoenix Contact Edge PCs are equipped with preinstalled software tools and were developed such that a wide range of IoT applications could easily be implemented.

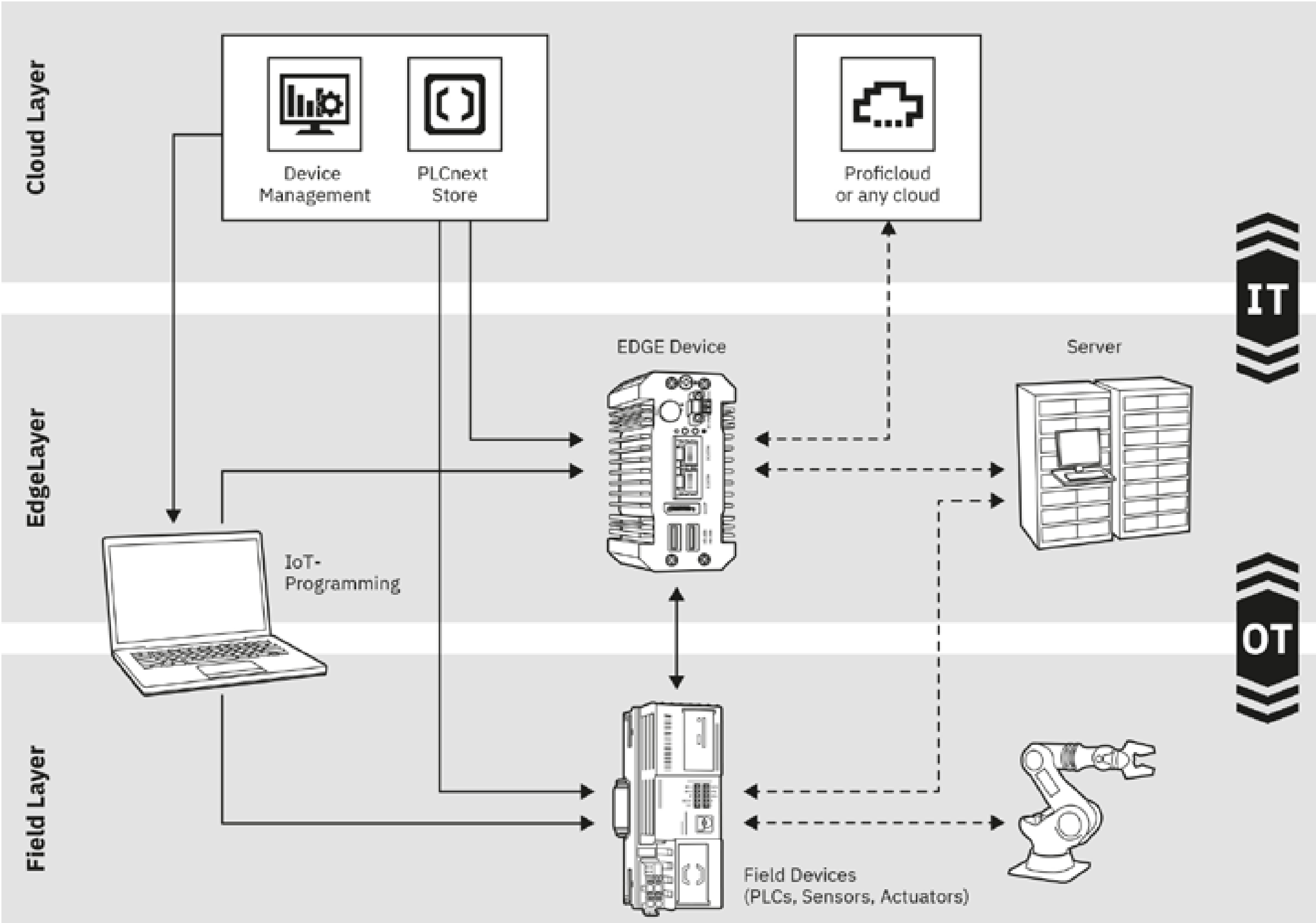
With preinstalled software tools such as Node-RED, a local time series database, and a simplistic cloud connection to many cloud systems (e.g., PROFICLOUD by Phoenix Contact, Amazon Web Services, Microsoft Azure, or Google Coral), special nodes make the realization of IoT applications easier.

The Edge PC connects the IT and OT layers. Data processing happens at the edge of the network, as opposed to today's usual process in which large volumes of data are sent to a cloud where they must then be processed and evaluated. The objective of processing data locally and upstream of the Edge PC reduces the bandwidth load on the network while simultaneously ensuring faster execution. Delay times are thus reduced. With a traditional PLC, though, data cannot be preprocessed. That's why Phoenix Contact is currently developing Edge PCs that sort and preprocess a large portion of their sensor data at the point of origin.



The Edge PC serves as the ideal device for edge applications within PLCnext Technology.

SOURCE: PHOENIX CONTACT



Functionalities of the Edge PC.

Applications with high computing power and storage requirements

The company's new Edge PCs combine the robustness of a proven industrial PC with the openness of PLCnext Technology. The devices, which are equipped with an Intel Celeron N3350 dual-core processor, offer up numerous interfaces. These include two Ethernet ports, two USB ports, one display port, and two serial RS232/RS485 interfaces. With 2 GB RAM (upgradeable to 4 GB) and 32 GB flash storage with an optional 128 GB M.2 SSD, even applications with high computing power and storage space requirements can be developed.

A user interface that can be called up via web server or locally via the display port allows access to the many functions of the Edge PC. The integrated TPM chip (Trusted Platform Module) ensures the integrity and security of the communication. The user can easily incorporate customer-specific applications and third-party applications into the solution via the PLCnext Store digital marketplace. In addition, support from Docker or Portainer enables intuitive implementation and management of containers and volumes. Consistent application of user interfaces and graphical programming environments means that users can easily develop and deploy their own edge application.

Combining the advantages of two platforms

More and more users require a decentralized, resource-sparing processing of the application data at the edge of the network. They would also like to reap the benefits of modern cloud concepts - because by processing large volumes of data close to the source, the application can respond more quickly and flexibly. It is against this backdrop that the new edge devices from Phoenix Contact combine the robustness of a proven industrial PC platform with open PLCnext Technology.

This is how intelligent IoT edge solutions can be built, which closes the gap between the IT and OT worlds. With preinstalled software packages as well as universal graphical user interfaces and programming environments, the powerful hardware of the Edge PCs enables simple development and implementation of edge applications.

Connect hardware to common cloud platforms

Among other things, an edge application aims to reduce the bandwidth of the network through local (pre)processing of the incoming data while also ensuring faster execution and thus shorter delay time. Such an application cannot be implemented with a conventional PLC. Conversely, the user first sets up the Edge PC in the familiar PLCnext Engineer engineering environment. Data can be collected by all common communication protocols (e.g., OPC UA, Modbus TCP/RTU, or PROFINET) and can easily be stored in Node-RED with the existing nodes in the InfluxDB database.

The data can then be visualized and managed in the Chronograf user interface. Data can be compressed here, and rules can be established and alarms initiated. The opportunities appear to be endless and conform to the user's needs in an optimal way. With nodes and the use of MQTT, connection of the Edge PC to the Phoenix Contact cloud as well as other cloud platforms can be pulled off without a problem.

*Daniel Korte (Technology Manager, PLCnext Technology) and Daniel Mantler (Product Manager, HMI/IPC), both **Phoenix Contact Electronics GmbH.***

Intelligence at the Edge: boost productivity and improve costs

As factories strive to boost productivity and improve operational costs, the demand to deliver new technology that Empowers Intelligence at the Edge is increasing. "What does the edge mean?" The Edge is where the machine meets or interacts with the real world.

IN FACTORY AUTOMATION, EMPOWERING Intelligence at the Edge means reducing the amount of lost productivity a factory experiences in a year. The biggest contributor to this is factory down time or when the production line stops causing the company to lose money. In fact, according to an article from McKinsey published in October 2018 on Digital Enables Reliability Beyond Predictive Maintenance, factories experience on average 800 hrs./yr. of production line shutdowns or an average of 15 hrs./wk.

This is a substantial impact to revenue and profit for a company. Take for instance that a car manufacturer loses close to $22,000 per minute when the factory stops manufacturing. This means it loses $1.3M/hr. or close to $20M per week. Empowering intelligence at the edge has already made an impact on the manufacturing line improving productivity by 10% and achieving a 20% savings in maintenance cost. So, the net result of empowering Intelligence at the edge in factories works to keep production lines running by preventing costly production line shutdowns.

While it's clear that Empowering Intelligence at the Edge provides a boost in productivity and reduces operating costs, the real question is "What does it take to Empowering Intelligence at the Edge"?

A new way of thinking

As semiconductor suppliers, we need to deliver solutions that enable Intelligent Sensors and Actuators, support Software Configurable IO, and provide advanced diagnostics. Let's review the importance of these four critical elements and the key capabilities they provide in Empowering Intelligence at the Edge.

Intelligent sensor technology

Sensors are found everywhere. They have become ubiquitous in our everyday lives. In the manufacturing environment, all manufactured products require an array of sensors that work in unison to help machines detect an object, determine the distance to an object, configure the colors and composition of an object, and monitor the temperature and pressure of an object or liquid.

Commissioning new sensors to replace damaged sensors or adapting a piece of equipment to enable the manufacturing of a different product is labor intensive and it contributes a significant cost burden due to loss productivity. The cost of sending a technician to the factory floor to change a sensor and then re-calibrate it to the correct manufacturing parameters impacts factory throughput. If we multiply this same level of maintenance for every sensor across a factory, changing or reconfiguring a sensor is the single-most expense all manufacturing lines incur.

SOURCE: ANALOG DEVICES

Intelligent Actuators: PD42-1243-IOLINK Stepper Motor and EoAT Gripper (TMCM-1617-GRIP REF)

IO Link is an exciting new technology that allows intelligent sensing all the way down to the machines on the factory floor. This new technology enables flexible manufacturing to improve factory throughput and operational efficiency. IO-Link is a technology that converts traditional digital or analog sensors into an intelligent sensor by providing bi-directional information exchange with the sensor. This technology adds a new level of intelligence and capability to remotely commission the sensor as well as the ability to react in real-time by making on-the-fly adjustment to the sensor parameters. Industrial Automation machinery now has a newfound intelligence to dynamically respond to real-time operation conditions based on the health and status of a network of sensors located across the factory floor. By tapping into this reach sea of end-to-end information across a network of intelligent sensors, a facility can create a mapping of its factory floor to provide better real-time information to an overarching AI monitoring solution that can rapidly identify manufacturing bottlenecks, points of failure as well as provide a new capability to optimize the entire factory floor for better operational efficiency.

The way IO-Link technology simplifies the commissioning process and improves factory throughput is by making sensors interchangeable through a common physical interface that uses a protocol stack and an IO Device Description (IODD) file. This allows technicians to quickly commission a sensor which results in reducing factory down-time and allowing the manufacturing line to be re-configurable on-the-fly.

The adoption of IO Link sensors continues to accelerate as companies realize the benefits of having a common interface that makes exchanging various sensors such as pressure, proximity, and temperature as easy as plug and play. According to ResearchAndMarkets, the IO-Link market continues to grow, and it is expected to reach $12 billion USD by 2023 from $3 billion USD in 2018, at a CAGR of 33.56%.

IO Link hub and software configurable IO

While it's clear that IO Link technology is the catalyst behind a set of new intelligent sensors, IO-Link is also providing new opportunities that bring intelligence to the edge through IO Link Hub solutions. These new IO Link Hubs provide a simple way to add Analog and Digital IO expansion channels as well as the integration of intelligent actuators such as Solenoid and Motor Drives.

The IO Link Hub provides a simple way to expand the type and number of channels needed to support unexpected manufacturing line re-configurations. These IO expansion Hubs provide a solution that leverages all the benefits of IO Link technology and simplifies the task to add Digital and Analog IO ports. These new class of products enable the commissioning of the sensors via the IO Link Hub which reduces factory downtime. Examples of these solutions can be seen from

Omron's IO Link Hub NXR product family where they boast achieving a 90% reduction in setup and commissioning times.

Software Configurable Digital and Analog IO solutions allow Automation Engineers and Technicians the convenience of providing a universal IO port that can be commissioned remotely. Comparable to the benefits that IO Link provides, these new class of Digital and Analog Software Configurable IO products simplifies a factories Wire Marshalling burden and provides flexibility to physically connect any Digital and Analog IO Sensors or Actuators to any unassigned Digital and Analog IO port. This software -configurable technology is more cost effective and increases the channel density the factory floor.

Intelligent actuators

Actuators are used to influence and control the direction and speed a product moves across the factory floor. Since all applications require a unique set of motion control and motor drive characteristics, these smart actuators will need to dynamically adjust to its environment to form that perfect Mechatronic Cyber Physical System. Currently, Intelligent Actuators are evolving to provide an Auto-configuration capability that autonomously adjusts its performance parameters to meet the demands of its operational environment.

This is the first step in making the actuator become self-aware of its environment and allow the system to optimize its performance for maxim throughput or maximize the long-term reliability and operational performance of the actuator. In either case, the result yields lower operational costs and higher efficiency. To empower this combination of Intelligent Motion, it requires the integration of two key elements.

1. The first critical element is power efficient Analog Drive technology to allow high voltage operation while providing health and status of the local environment to enable optimization of the motors to achieve a balance between high efficiency and faster throughput.

2. The second critical element is the ability to provide Motion Control algorithms to enable a smooth range of motion. This consists of the ability to detect loads placed on the motor during operation to avoid line failures and minimizing power consumption.

Motion control algorithms provide smooth and precise movement, while the Chopping Algorithms focus on making the motor more power efficient. In addition, sensing the position of the armature is important to know if the motor has moved to the correct position. This is done with magnetic sensing typically using Hall Sensors or some type of optical encoding solution.

To demonstrate the value of these next generation Intelligent Actuators, here are two new examples, the PD42-1-1243-IOLINK and the recently released End of Arm Tooling (EoAT) Gripper reference design TMCM-1617-GRIP-REF. Both solutions demonstrate the power of combining intelligent motion, driver, and IO Link communication technology from Maxim and Trinamic. These new Intelligent Actuators simplify commissioning and boost factory productivity by providing Industrial Automation Engineer access to 50 percent more configuration and performance parameters over the IO Link communication interface. Finally, these Intelligent Actuator can be adjusted on-the-fly to accommodate changes in operating environment and the implementation of advanced AI derived productivity solutions. This ability to shape the actuators performance based on its operational environment is the future of Intelligent Motion Control.

SOURCE: ANALOG DEVICES

Omron: NXR-Series IO-Link Controller & IO-Link I/O hub with MAX14819A, MAX14827A, MAX14912/15.

Diagnostics and real-time decision-making

Higher levels of diagnostic capabilities continue to provide a richer data set that improves real-time, edge-based decision-making to improve productivity and operational integrity on the factory floor. These powerful manufacturing-based AI algorithm platforms are expected to grow from $1B in CY18 revenue to over $17B by CY25, or a CAGR close to 50%, according to a MarketsandMarkets report published in January 2019 entitled, "Artificial Intelligence in Manufacturing Market."

During this time, machine learning is expected to be the highest growth segment in AI due to the rapid investments being made to implement smart factories. The driving force behind this growth stems from the abundance of health and status information being generated from a network of IIoT-powered devices, algorithms providing predictive analytics, and machine-vision cameras monitoring the quality of products as well as evaluating the status and operational health of the machines.

At the IC level, more and more information is monitored, collected, and communicated via SPI bus to and from a microprocessor. The volume of these IC datagrams continues to multiply as they carry critical information such as temperature status of a device, overvoltage, overcurrent, open wire detection, short circuit detection, overtemperature warnings, thermal shutdown, and CRC. If we take a step back now and multiply the number of semiconductors providing datagrams across the entire breath of equipment on a factory floor, it becomes clear that a diagnostic mapping of the factory floor can be achieved to anticipate, identify, and diagnose manufacturing line failures.

The next big thing

One thing is clear, by empowering this "New Way of Thinking", Smart Factories can take advantage of these new capabilities to improve throughput and increase productivity. As these new technologies continue to mature, the next generation of AI algorithms will become the beneficiaries by leveraging the higher quality of real-time data being generated from these solutions.

As a result, these new self-aware capable machines will automatically implement AI generated solutions to keep a manufacturing line operational until it is repaired or serviced by a technician. This era of self-aware machines will inspire "The Next Big Thing" in Industrial Automation.

Jeff DeAngelis, Vice-President - Digital Factory, ***Analog Devices.***

Visit Website

5 ways smart factory analytics bridge data & communication silos

Manufacturing companies across the world are trying to figure out a way to integrate data and simulate it for meaningful decision-making. Complete deployment of smart manufacturing with IIoT and cloud technology has brought the industry to the doorstep of this end-to-end connectivity.

SOURCE: ISTOCKPHOTO

The transition from traditional to tech-driven manufacturing seems daunting. But with the right strategy, it can turn out to be seamless and hassle-free.

DESPITE THE WIDESPREAD POPULARITY OF THE Industrial Internet of Things [IIoT], relatively few manufacturing firms have put the theory into practice and deployed IIOT technologies in their plants. There are a plethora of benefits that lie beneath the surface of the initial investment in the transition to this digital technology, equipment, and processes.

The 2020 Gartner Smart Manufacturing Strategy and Implementation Trends survey shows that:

- 86% of respondents agree that smart manufacturing is an integral component of their digital supply chain strategy.
- 84% expect smart manufacturing to increase their competitiveness.

Yet, less than 50% of manufacturing leaders are implementing or have a fully deployed smart manufacturing strategy.

As manufacturers expand and their businesses go global, those with more granular and real-time insights into their systems win. A quick answer to every question enables agility and competitiveness. Without this, they fall behind in this highly competitive market.

Most of the shop floor questions can be answered with real-time visibility for end-to-end processes and knowing the where, why, what, and how for all your assets. The traditional factory setup does not offer these insights as the data obtained from each system is either incomplete, independent on its own, non-standard, or obsolete by the time it reaches decision-makers. And they create gaps in communication across departments within the enterprise.

Operational challenges due to gaps in communication

Gaps in action plans for interdependent operations: Every time there is a glitch or deviation in shop floor operations, the shop floor engineers have to track it down physically or the cause remains unknown. It is a time-consuming process and the operations can be slowed down or even halted.

Inability to track orders: In a traditional setup, the supply chain has a single point of contact with shop floor management. As a result, there are so many gaps that they hamper decision-making and there is no certainty of when the shipment will reach its destination.

Inaccuracies in order quantities, schedules, etc.: Without close synchronization between a purchase manager and a warehouse manager, inventories cannot be ordered in proper quantity or on time. It impacts both departments and causes disruptions in production schedules.

Wasted storage space: When the orders are over-ordered, they need storage space in the warehouse, causing inconveniences in managing inventories. Also, the project cost could skyrocket.

Data integrity: Duplicated, non-updated or obsolete data compromises data integrity and accuracy. It leads to faulty decision-making, impacting the overall project schedule, cost, inventory, etc.

By adopting a smart factory approach with sensor-controlled data, dashboards, analytics, and automated solutions, data silos can be removed. Factory owners can get a clearer picture of what is happening on the shop floor and across the supply chain to raise overall productivity.

Here are five ways smart factories help improve seamless data exchange and communication:

Reliable and timely data helps save costs through digital twins

The Gartner statistics quoted above state that only 50% have fully deployed smart manufacturing strategies.

The interpretation of the word 'fully' is important. It means collecting data from all touchpoints and establishing a link between all of them on a central database.

This gives a 360-degree picture of the factory using reports, dashboards, conditions of machines, operational accuracy, etc. on a single screen.

With such real-time reporting on a computer or mobile device screen, one can virtually set up the digital factory shop floor – essentially a digital twin of the factory. This integrated data with simulation generates a digital twin to help bring down costs by predicting the interplay of machines first digitally and then physically.

This way the shop floor managers know the final impact beforehand and processes can be optimized to save costs – while keeping all concerned departments in the loop.

Lean operations with digitally connected supply chain and logistics

Transportation often accounts for about 30% of planned expenses. Likewise, storage costs in the US are $4 to $7 per square foot. Depending on your storage facility, as well as labor and equipment charges, production companies often end up spending 40-90% of the business' total budget. Any overheads in these areas weigh heavily on budgets.

Common strategies like reducing fleets, finding cheaper alternatives, etc. are insignificant for massive manufacturing firms. This is where smart manufacturing helps by optimizing inventory, storage costs, and planning logistics.

Digital tools such as fleet management software, centralized inventory management software, etc. connected with ERP and CRM systems, provide real-time insights for all stakeholders. They provide collaborative visibility into the entire supply chain with shipping updates, receipt acknowledgment, tracking orders, etc. with RFIDs.

Digital tools for inventory tracking enable maintaining a check on inventory levels to help you plan and order bought-out parts, raw material, etc. on time and avoid delays. An Australian freight company reduced fleet costs by 9-17% through fuel economy, reduced idling, and improved purchase habits, along with a 90% reduction in safety issues and breaches using digitization with Deloitte.

Plan and schedule machine maintenance in advance

Datasets in silos are not valuable. But using the same datasets – when connected and talking to each other – a hefty amount of valuable information is derived. For example, if a shop has the details of when each lathe machine was purchased, it can also provide information on how many orders the shop needs to complete in any particular month. Additionally, the maintenance engineer has a detailed schedule for machine maintenance plans.

Despite all these datasets, if the maintenance engineer and production engineer do not communicate, the delivery schedules cannot be planned accurately: the latter might dedicate three random lathes, one of which might have downtime scheduled around the delivery date. This will result in a miss or pushing the timelines further.

A centralized platform for insights into all your assets helps draw a dashboard where all details about the production floor are available in the form of tables, graphs, charts, etc. that are easy to understand, and enable proactive maintenance.

Documentation regarding warranties, contract renewals, discarding, etc. can be managed easily.

Ensure high-quality products

Smart factories can efficiently and immediately detect process or operational malfunctions, deviations, and deliver an in-depth economic evaluation of the entire plant. For example, a sensor fixed on an axel measures and sends signals to the dashboard to detect anything unusual. Thus, any out-of-order axel vibrations and their impact on the final product can be rectified before it is too late.

An integrated system of sensors provides the monitoring personnel with detailed information about the system under observation. Anomalies are detected before complete breakdown or wrongdoings to save cost, raw material, time, and other resources.

These systems also enable scheduling prescriptive maintenance to avoid obstacles during peak time and save the machine from failing. LEWA GmBH installed such a sensor-backed system for their pumps to leverage data analysis to make maximum use of the smart monitoring system on production operations.

Monitor and reduce energy consumption

Smart monitoring can also be equipped to keep a check on the energy consumption of the production shop. Often called Energy Monitoring Systems or EMS, these sensor-triggered checks are accurate in flagging excess energy consumption. These are particularly helpful for energy-intensive companies that not only focus on reducing waste but also save costs to offer affordable products.

A sensor network is attached to energy meters and data loggers to keep a constant and real-time check. This data is then transferred to a cloud server so that it can be monitored remotely on any device, and so that surplus energy consumption can be cut immediately.

Conclusion

Manufacturing companies across the world are trying to figure out a way to integrate data and simulate it for meaningful decision-making. Complete deployment of smart manufacturing with IIoT and cloud technology has brought the industry to the doorstep of this end-to-end connectivity. They bridge the existing gap in traditional manufacturing and deliver higher ROIs by improving existing processes.

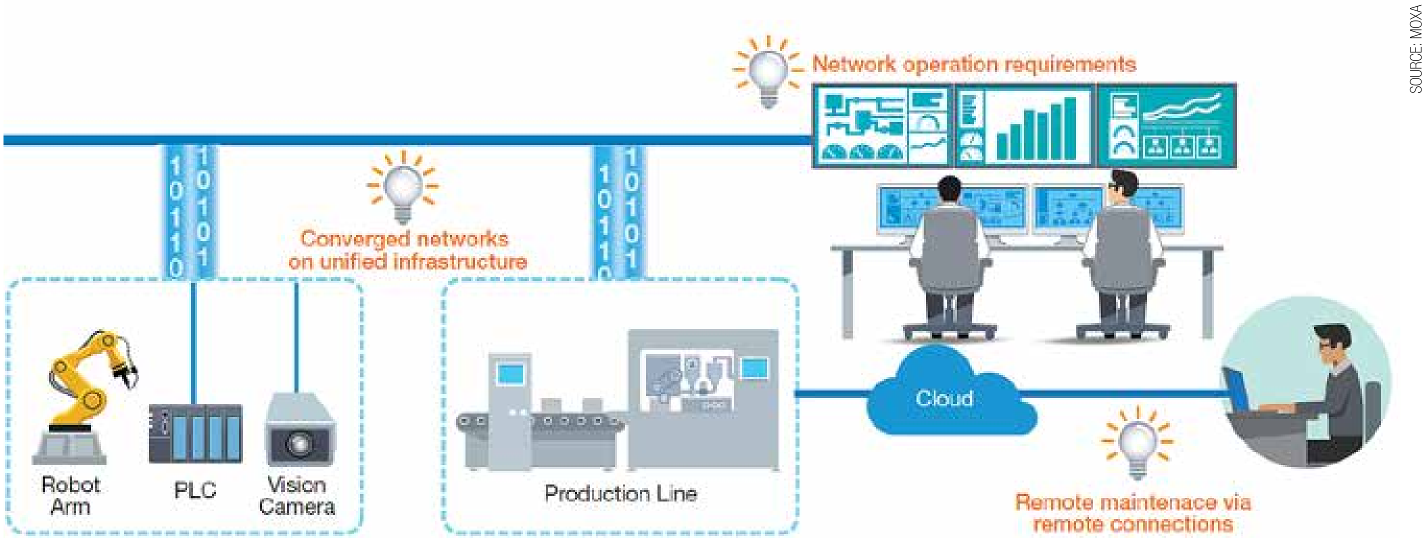
The transition from traditional to tech-driven manufacturing seems daunting. But it can be seamless and hassle-free. It helps you get all stakeholders on the same page through real-time, accurate reporting and by avoiding delays. Accurate integration, connectivity, and the right queries for dashboards and charts using analytics set you apart.

Eric Whitley, Director of Smart Manufacturing, ***L2L.***

Visit Website

Getting IIoT networks ready for the future

Three keys help create more effective, future-proof IIoT networks. Achieve a greater level of integration by using an unified infrastructure. Create an ability to access remote machines anywhere with hassle-free cloud services. Implement tools for visualizing network status by both OT and IT professionals.



Future-proof IIoT networks are converged on a unified infrastructure, meet operational requirements and provide remote maintenance access connections.

FUTURE-PROOF IIOT NETWORKS REQUIRE unified infrastructures, support for remote access applications, and powerful management tools.

It may be tempting to rest on your laurels when you finally have your IIoT networks up and running. Nonetheless, change remains the only real constant in life, and the world of industrial networking is no exception. Your IIoT network may be sufficient for your current needs—it may even be ready for your foreseeable application requirements over the next several years. But what about the next decade or more? Change is always on the horizon, and we need to be prepared.

Since the early days of industrial automation, manufacturers have adopted a variety of purpose-built protocols and systems, instead of standard Ethernet technologies, for highly specialized industrial control applications. However, as the IIoT market is expected to grow at a CAGR of 24% by 2023, industrial networks of the future will in all likelihood be required to transmit large amounts of data between interconnected devices or collect data from remote devices. With these growing demands on the horizon, how well-prepared you are for the future of industrial networking may determine your success in tackling new challenges. This section provides three considerations to help you prepare your IIoT-ready industrial networks for the future.

Achieve greater integration with unified infrastructure

Over the years, various devices using different industrial protocols have been deployed on industrial networks to provide diverse services. Under these circumstances, network integration usually costs more than expected or becomes more difficult to achieve.

Manufacturing companies can either choose the status quo, that is, maintain their preexisting isolated automation networks with numerous purpose-built protocols of the past, or alternatively seek solutions to provide deterministic services and integrate these "islands of automation".

If our goal is to be ready for the growing demands on our IIoT network in the future, the choice is obviously the latter. The rule of thumb is to take potential industrial protocols into consideration and ensure you can redesign your networks in case any new demands arise in the market. Time-sensitive networking (TSN) is a set of new standards introduced by the IEEE 802.1 TSN Task Group as an advanced tool box.

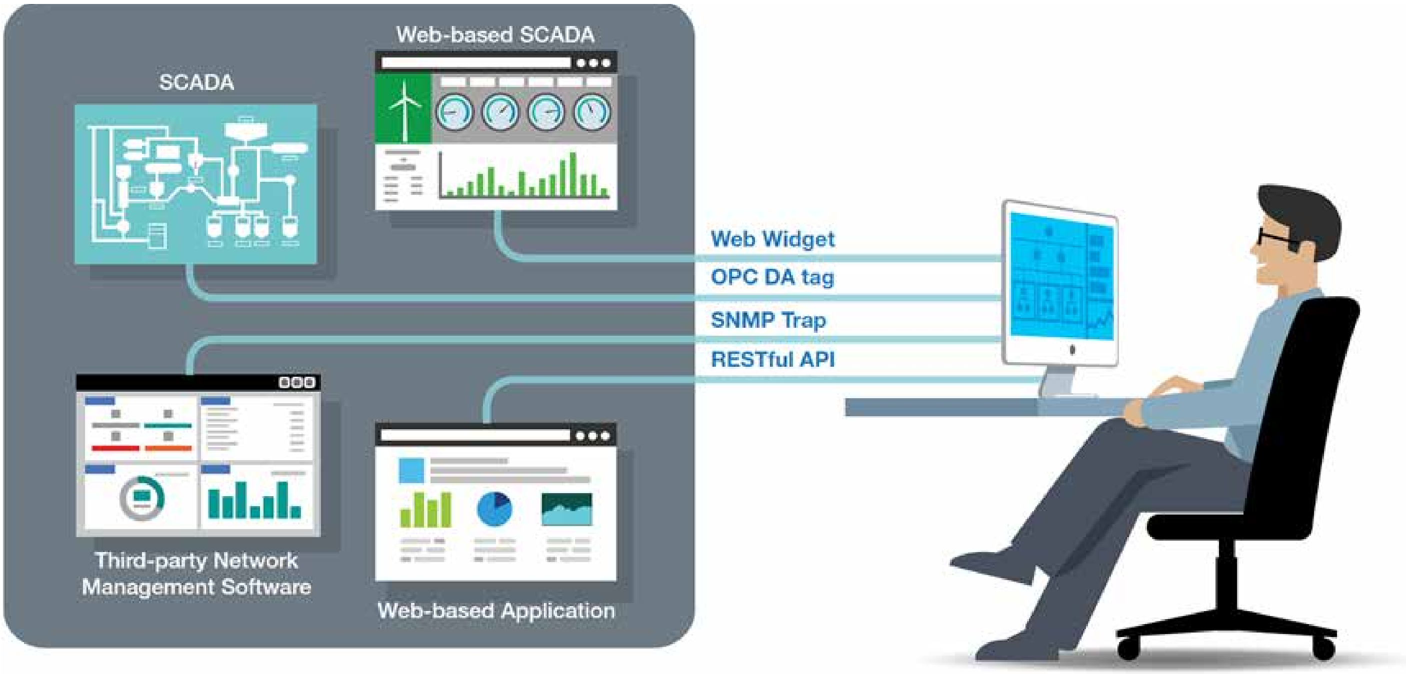
With TSN, you can build open, unified networks with standard Ethernet technologies that reserve flexibility for the future. Furthermore, you may consider selecting solutions offered by the key players who are advocating this new technology because they actively participate in TSN plugfests to complete the ecosystem and ensure compatibility among different industrial automation vendors.

Access anywhere to your remote machines with hassle-free cloud services

Cloud-based remote access offers many benefits to IIoT customers, such as reducing the traveling time and expenses of sending maintenance engineers to multiple remote sites. Furthermore, cloud-based secure remote access can provide flexible and scalable connections to meet the dynamic, changing requirements of the future.

However, operational technology (OT) engineers for water and wastewater treatment plants, machine builders, and other IIoT customers may find it cumbersome to set up and maintain their own cloud servers to provide new services and applications. Indeed, considerable efforts are associated with setting up new infrastructure, even if it is in the cloud. Fortunately, OEMs and machine builders can now deliver secure cloud-based services and remote access to their customers without having to maintain their own cloud servers.

One key issue you should definitely scrutinize is the cloud server license scheme. Often, upfront costs may seem low for limited server hosts. However, these apparent cost



Both plant managers and operators need a variety of software visualization tools to quickly judge current situations and take action according to the information aggregated on the screens in front of them.

savings on server hosts may actually make your project uneconomical due to a limited scale of connections. Secondly, you may also need to consider central management capabilities in order to flexibly expand remote connections in the future.

With this said, carefully weigh the costs and benefits of incorporating secure remote access to your industrial networks. Always select solutions that can eliminate the hassles mentioned and help you focus on delivering more value and benefits to your customers.

Visualize your network status for both OT and IT professionals

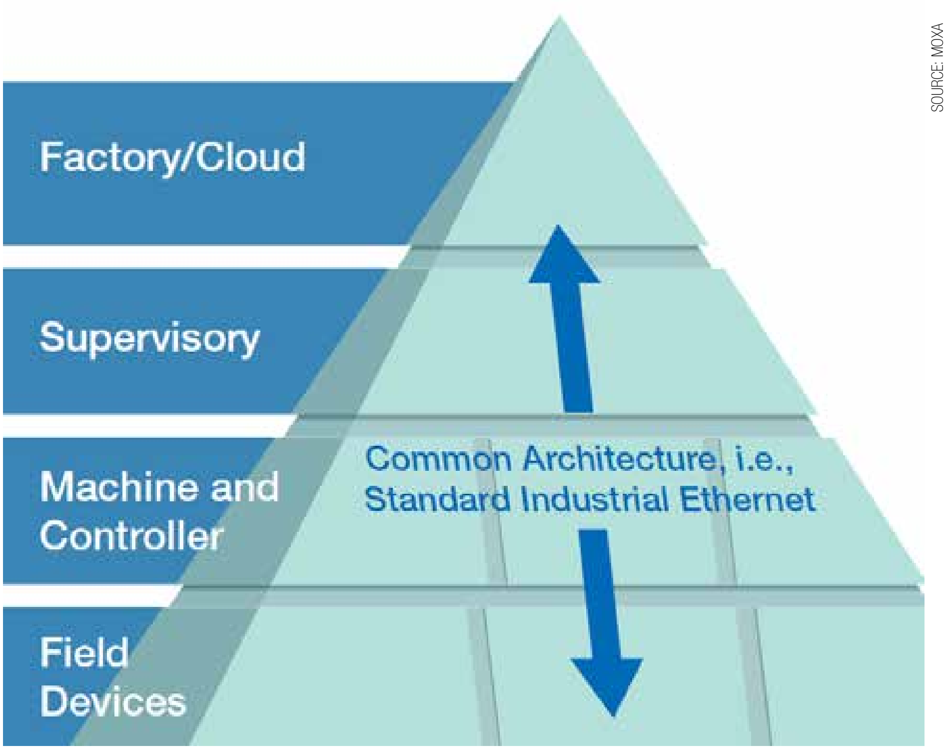
You may have seen the following scene in a movie or photograph in the news. The control room of a metro system has a group of monitors showing the current status of each metro station in the system, the locations of all the moving trains, and so on. Managers or operators need to quickly judge the current situation and take action according to the information aggregated on the screens in front of them.

This visibility helps them keep everything under control. When complexity increases with greater connectivity on industrial networks, it can become very difficult to identify the root cause of problems and maintain sufficient network visibility. Control engineers often have to revert to trial and error to get the system back to normal, which is time-consuming and troublesome.

Therefore, in order to facilitate and manage growing industrial networks, network operators need an integrated network management software to make more informed decisions throughout network deployment, maintenance, and diagnostics. In addition, as your systems continue to grow, you will need to pay attention to a number of network integration concerns.

First, only managing industrial networks in local control centers may not be feasible three or five year later, especially when existing systems need to be integrated with new ones.

It is therefore important to use network management software with integration interfaces, such as OPC DA tags for SCADA system integration or RESTful APIs for external web services. Furthermore, an interface to facilitate third-party software integration is also a key criteria to ensuring future flexibility.



Future-proof networks offer solutions at all levels from the factory/cloud to field devices.

Technology report by ***Moxa.***

Visit Website

Standardising data collection in breweries

As the beer industry continues to expand globally, brewing companies that operate across multiple international sites face issues with data management. There is often little consistency in how these sites track data, making it impossible to optimise performance across the brewer's entire production landscape.

A powerful case can be made for cross-facility digitalisation in the brewing industry, and how data collection in breweries is vital for this process.

INDUSTRY 4.0 CAN DELIVER TANGIBLE operational benefits for manufacturers, according to McKinsey & Company, including inventory cost savings of 20 to 50 percent. Meanwhile, the US National Institute of Standards and Technology predicts smart manufacturing could save businesses $57.4 billionper year in energy, materials and labour.

Breweries are no exception, and are increasingly turning to automation and the Internet of Things (IoT) technologies to become more efficient, lean and scalable in light of increasing production and energy costs.

This is more challenging for brewing companies that operate different sites worldwide. For breweries, as with any type of manufacturer, poor or outdated data management can negatively impact overall equipment effectiveness (OEE), cause unplanned downtime, decrease throughput and ultimately damage the company's bottom line.

IoT technologies will prove crucial as the beer industry penetrates into new markets. For instance, a large multinational brewer might install sensors throughout its production line to monitor OEE, and upgrade its manufacturing execution systems (MES) to analyse the brewery data collected by these sensors.

This process is where some larger breweries are encountering problems. Managing these large reams of data consistently across multiple international sites simply isn't feasible without software.

Bird's eye view

Fortunately, industrial software, like COPA-DATA's zenon, can play a vital role in supporting larger manufacturers with data management. zenon makes it possible to analyse data more efficiently and effectively within individual plants, and new and legacy systems can be integrated into the software platform to allow overall system improvements.

Features of zenon, like its Industrial Performance Analyzer, can present statistical analysis of equipment faults.

Production issues, like bottlenecks, can be identified and resolved quickly to stop them affecting the bottom line. Take the case of a brewery that, according to a study by the American Council for an Energy-Efficient Economy (ACEEE), was losing up to 10 per cent of its overall product. Even worse, the cause was unknown.

To solve the problem, the brewery used software and installed 40 sensors at key points throughout its production line. It was able to spot exactly where on the production line losses were being made, and address the issue. This put an end to the manufacturer's 10 percent loss.

Solutions like this rely on better data capture. By linking sensors to software platforms like zenon, it becomes possible to evaluate the frequency and duration of problems, and source their origin. A brewing company may find that production issues are caused by pressure and temperature imbalances, and resolve these issues accordingly within a predictive maintenance strategy.

Industrial software can also support massive improvements in production output. A brewery might use digital twinning to compare its actual line capacity, of 100,000 cases of beer a week, against a desired capacity of 2,000 cases.

Once the digital simulation has identified performance improvements that can be made to the line, the manufacturer can link its software to an MES and leverage this data to improve its production capacity.

Multisite improvements

Once an individual brewery has used data capture to spot flaws or improvements, this information can be shared with other multinational sites. zenon Analyzer can relay data to operators at other facilities, who can then investigate if they have the same problems or opportunities. Don't underestimate the scale of the benefits manufacturers can achieve with software.

Going forward, there also is potential to combine zenon with other management systems, like control charts, to make data management even more integral to the production process. Brewing companies should turn to industrial automation software to avoid falling behind in the global market. Automated data collection in breweries will be crucial for preventing downtime and managing data across multiple international sites, helping breweries expand globally.

Martyn Williams, managing director at ***COPA-DATA UK.***

Visit Website

How Wi-Fi 6/6E enables Industry 4.0

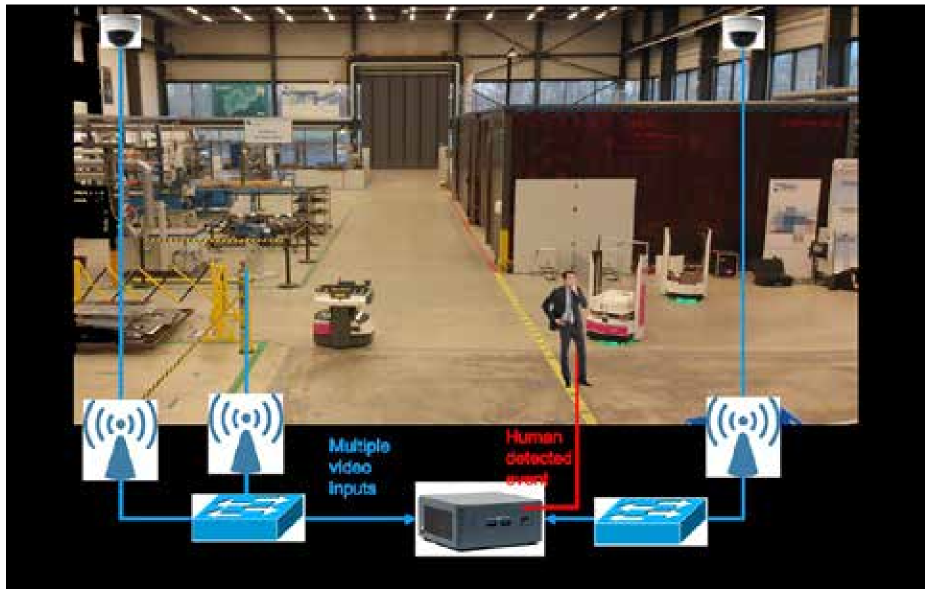
A Wireless Broadband Alliance (WBA) report explores how autonomous Mobile Robots, Automatic Guided Vehicles, Augmented and Virtual Reality use cases can be addressed with Industrial Internet of Things deployment guidelines.

THE WIRELESS BROADBAND ALLIANCE (WBA) has published "Wi-Fi 6/6E for Industrial IoT: Enabling Wi-Fi Determinism in an IoT World." This paper explores how Wi-Fi's latest features are ideal for meeting the unique, demanding requirements for a wide variety of existing and emerging IIoT applications.

This includes manufacturing/Industry 4.0 and logistics, involving autonomous mobile robots (AMRs), automated ground vehicles (AGVs), predictive maintenance and augmented/virtual/mixed reality (AR/VR/MR).

For example, manufacturers are increasingly using IIoT sensors for vibration, temperature and lubricant viscosity to catch emerging equipment problems before they result in extensive, expensive downtime. Other IIoT sensors provide real-time insights about production output, inventory levels and asset locations. Wireless has become the preferred way to network these sensors because it's faster and cheaper to deploy than copper or fiber.

"As more equipment is monitored, wiring becomes prohibitive," the white paper says. "Industry is moving towards the inclusion of wireless technologies to lessen the cost of obtaining more information about their processes. In one recent case in the oil and gas industry, moving to a wireless installation resulted in a 75% cost reduction in installation."



SOURCE: WBA

WiFi 6 is providing key technology for a broad range of industrial IIoT solutions.

Produced by the WBA's Wi-Fi 6/6E for IIoT work group, led by Cisco, Deutsche Telekom and Intel the white paper provides an overview of Wi-Fi 6 and 6E capabilities that are ideal for sensors and other IIoT applications, such as:

Scheduled access (SA) enabled by trigger-based (TB) uplink (UL) orthogonal frequency domain multiple access (OFDMA) in Wi-Fi 6 provides the ability to reduce or eliminate contention and bound latency (e.g. 99 percentile). This leads to increased levels of determinism applicable to all real-time and IIoT applications.

Wi-Fi 6 provides many *deterministic QoS capabilities*, such as the traffic prioritization that is a key component of Time-Sensitive Networking (TSN) for Industry 4.0 applications. Another example is Multi-link operation (MLO), a capability that helps provide high reliability for applications that cannot tolerate any packet loss.

The *Fine Timing Measurement (FTM) protocol* specified in IEEE 802.11-2016 enables both time-synchronization but also precise indoor range and position/location determination. This can be used for Autonomous Mobile Robots (AMR) and Automatic Guided Vehicles (AGV) applications such as route planning, exception handling and safety-related aspects including collision avoidance based on proximity. This capability does not require additional Wi-Fi infrastructure, so manufacturers can implement it immediately, for instance as part of their Industry 4.0 migration.

The *target-wake-time (TWT) feature* added to Wi-Fi 6 provides more efficient power-save and

SOURCE: WBA

Wi-Fi 6 and 6E capabilities are well-suited for sensors and other IIoT factory automation applications.

WiFi 6/6E infographic illustrates current market drivers and emerging IIoT use cases.

scheduling enhancement. This capability is a good fit for battery-powered IIoT nodes that need to transmit only infrequently, such as a sensor that uploads data only when a motor's temperature exceeds a certain threshold.

Wi-Fi 6E supports up to 1.2 GHz of spectrum, making it ideal for use cases that require both multi-Gb/s throughput and determinism, such as industrial AR/VR/MR and sensor fusion.

The 52-page report also includes RF/network deployment guidelines for factory, warehouse, logistics and other use cases. For example, it provides recommendations for leveraging 802.11ax/Wi-Fi 6 scheduling capabilities to optimize traffic patterns and manage critical QoS requirements. Another example is using high-gain directional antennas to increase channel re-use rates and work around metal racks and other signal-attenuating features commonly found in warehouses.

Current Projects

Over three dozen vendors, service providers and other organizations participated in developing the white paper, which describes many of their current projects. Examples include:

- Cisco, Intel and partners are working on use cases involving AMR and AGV, where key requirements include <10-20ms latency, <50km/h speed and .99.9999% reliability.
- Cisco and Mettis Aerospace are working on sensor applications, where requirements include very high reliability, low power consumption and high device density.
- Further work taking place on video-AMR fusion use cases such as collision avoidance, where technical requirements include <20ms latency and <1ms jitter.
- Cisco is working on safety control applications, which require <1-ms latency for applications such as automatically stopping a machine after a sensor detects that the person has left the operating position.
- Cisco, Mettis Aerospace and Intel are working on AR/VR applications with resolutions up to 80K and 90fps, where throughput requirements can be as high as 100 Mb/s.
- Cisco is working on automotive uses cases such as logistics in high-density storage lots, where <60dBm interference is key for reliable operation.

Tiago Rodrigues, CEO of the Wireless Broadband Alliance, said: "Wi-Fi has been a key enabler of the global IIoT market, which is on track to have a compound annual growth rate (CAGR) of about 23% between 2017 and 2023. Wi-Fi 6 and 6E are expanding capabilties by providing the multi-Gb/s data rates, additional spectrum, deterministic performance and other advanced capabilities necessary to support demanding applications such as Industry 4.0."

Matt MacPherson, CTO, Cisco Wireless, said: "The next industrial evolution will not only depend on the ability to connect more things, but to also add greater reliability, intelligence and security. This can only be done when the world's leading companies work together with progressive Industry 4.0 customers to explore and implement new, game-changing technologies. Cisco is proud of the work it has done with the WBA to ensure customers understand how, when and where to apply the latest innovations. It is because of advancements in wireless technology that Industrial IoT sits at the center of the forthcoming industrial revolution."

Ahmed Hafez, VP of Network Convergence at Deutsche Telekom said: "Deutsche Telekom's industrial partners are demanding ubiquitous high performance wireless connectivity to take their production processes to the next level. Converged Access combining 5G cellular and Wi-Fi6/6E Networks will play a vital role to deliver comprehensively on their application and process demands in the near future".

Eric McLaughlin VP, Client Computing Group & GM, Wireless Solutions Group, Intel Corporation, said: "The industrial IoT market is experiencing a major transformation, and Wi-Fi is an essential ingredient enabling this transition. Applications like Autonomous Mobile Robot (AMR) and Remote Human Management Interface (HMI) industrial devices require the mobility, functional safety, high reliability, low latency, robust security and determinism that Wi-Fi 6/6E can deliver particularly when combined with TSN (time sensitive networking) solutions. Intel is pleased to be leading this Wi-Fi technology evolution, and applauds the work that the WBA is doing in this space."

Article by ***Wireless Broadband Alliance.***

Download White Paper

OPC UA for the Field Level: UAFX multi-vendor demo

OPC UA is establishing itself as an industrial interoperability standard not only for the vertical integration from the control level to the edge or up to the cloud, but also as an interface for exchanging process data between controllers regardless of which protocol communicates with underlying field devices.

SOURCE: OPC FOUNDATION

The OPC UA FX Multi-Vendor Demo shows the interaction of controllers and network infrastructure components from different vendors to exchange process data at the field level.

THE FIELD LEVEL COMMUNICATIONS (FLC) initiative of the OPC Foundation was launched to establish OPC UA as a uniform, consistent and vendor-independent industrial interoperability solution also at the field level.

To this end, extensions to the OPC UA framework are being specified that standardize the semantics and behavior of controllers and field devices from different manufacturers, both for discrete manufacturing and for the process industry.

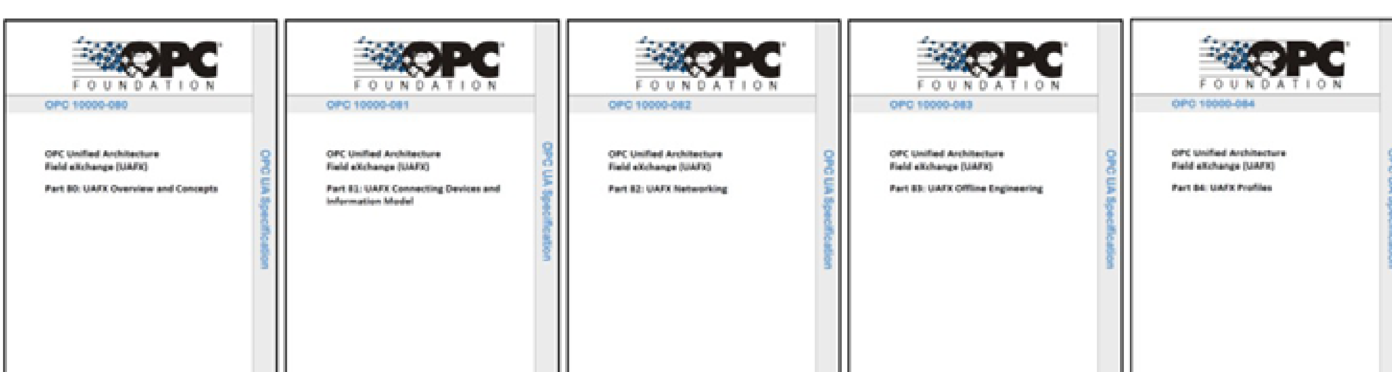
Three and a half years after its launch, the initiative has completed the final release candidate of the first specification version, which is being named OPC UA Field eXchange (FX).

This first specification has the focus on cross-vendor controller-to-controller use cases that support flexible and reconfigurable processing and manufacturing operations. A multi-vendor demo was created to test the interaction of UAFX controller prototypes that exchange process data on the basis of OPC UA and the OPC UA FX extensions.

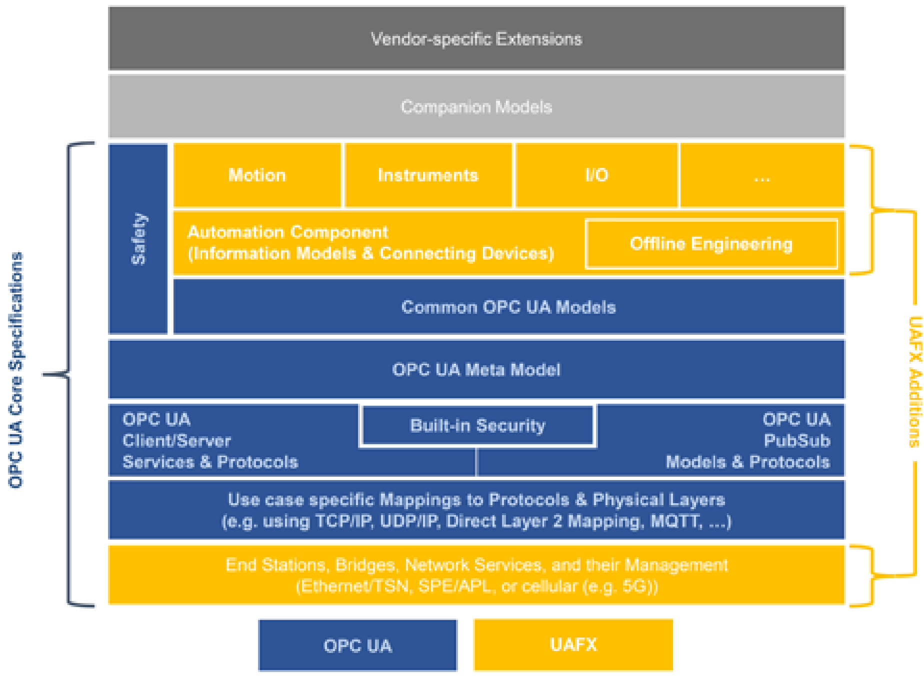
Application example

To illustrate the application of OPC UA FX an example is given in the following: A machine operator buys two identical machine tools from manufacturer 1 and two identical robots from manufacturer 2 to automate the loading and unloading of the machine tools.

To control and synchronize the processes between the machine tool and the robot, the respective controllers must exchange defined process data with each other. Neither the machine tool nor the robot changes its function or operation after installation, but there is no pre-planning of which machine will be connected to which robot, and possibly the network identification of the different controllers is not defined in advance.

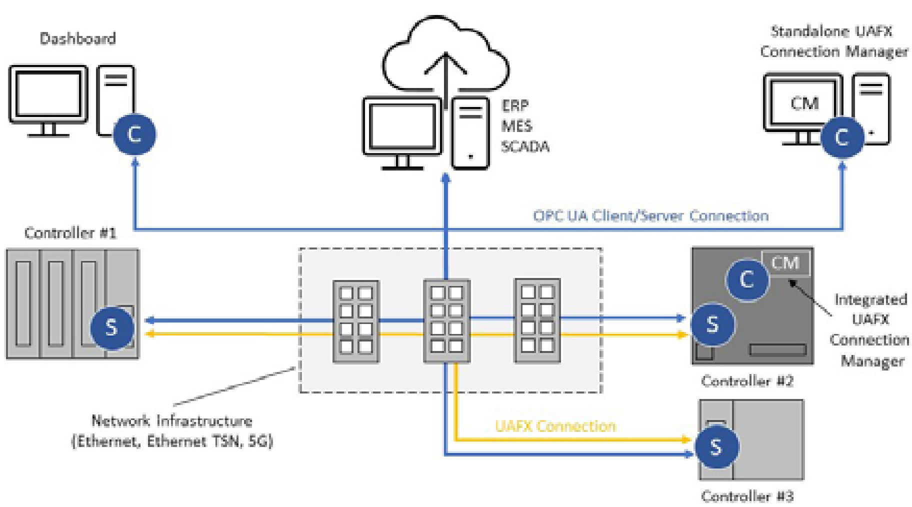


OPC UA FX Specifications (Parts 80-84)



SOURCE: OPC FOUNDATION

OPC UA and UAFX System Architecture.



SOURCE: OPC FOUNDATION

Schematic structure of the first OPC UA FX multi-vendor demo.

At the time of commissioning, each machine and robot (or more specifically, the controller in each machine or robot) must be assigned their network identification and the network identification of the respective communication partner. No other configuration should be needed on the part of the user to enable plug-and-produce operation with an exchange of real-time and safety data.

Technical Solution Approach of OPC UA FX

To enable the plug-and-produce concept described above, the OPC UA framework is extended by corresponding features, which are described in the following.

UAFX controllers must expose selected information via a prescribed OPC UA information model, the so-called Automation Component (AC), which contains both the functional model and the asset model. The scale of an AC is up to the vendor.

It could be as small as an individual standalone 8 point I/O controller or as large as a complex, room-sized machine. The asset model describes physical items, but can also include items that are not physical, such as firmware or licenses.

The function model describes a logical functionality. It consists of one or more Functional Entities (FE), each of which encapsulate input/output variables, communication and device parameters, as well as communication connections. A Functional Entity is abstracted from the hardware, which enables applications to be ported to new hardware. The Connection Manager (CM) is a service that is usually located in one of the controllers and is responsible for establishing or managing connections between FEs in different controllers.

A UAFX connection is first established via client/server mechanisms, where information for establishing a bidirectional PubSub connection (including compatibility checks, parameterization) is exchanged. The PubSub connection is then prepared and put into operation.

Offline engineering is an important element for the development, operation and maintenance of an automation system. By allowing the user to be able to understand the operation of the automation system before deploying the system in physical hardware, the user will know that the system will perform the control function reliably and correctly once the physical system is in place.

To make this possible, so-called descriptors are used. The descriptor of an AC is a set of documents containing an OPC UA information model and possibly other useful information for configuration purposes. The information can be for a single AC or a group of ACs (like a machine, machine module or skid). The AC descriptor is delivered in a packaged container format containing both product and configuration information.

A product descriptor contains the product data of the controller and is usually provided by the controller vendor. The configuration descriptor contains information such as functional units, communication DataSets, required quality of service (QoS) and data necessary for one or more connections. The configuration descriptor is created in the engineering process, usually with the intention to share engineering information between two engineering tools.

Safety data can also be exchanged between controllers. For this, OPC UA Safety, a safety protocol that is transmitted via standard UAFX connections, is used. The advantage of this approach is that the evaluation and testing effort by a notified body (e.g. TÜV) is limited to the safe transmission protocol, whereas the underlying UAFX connections do not require any additional evaluation and testing.

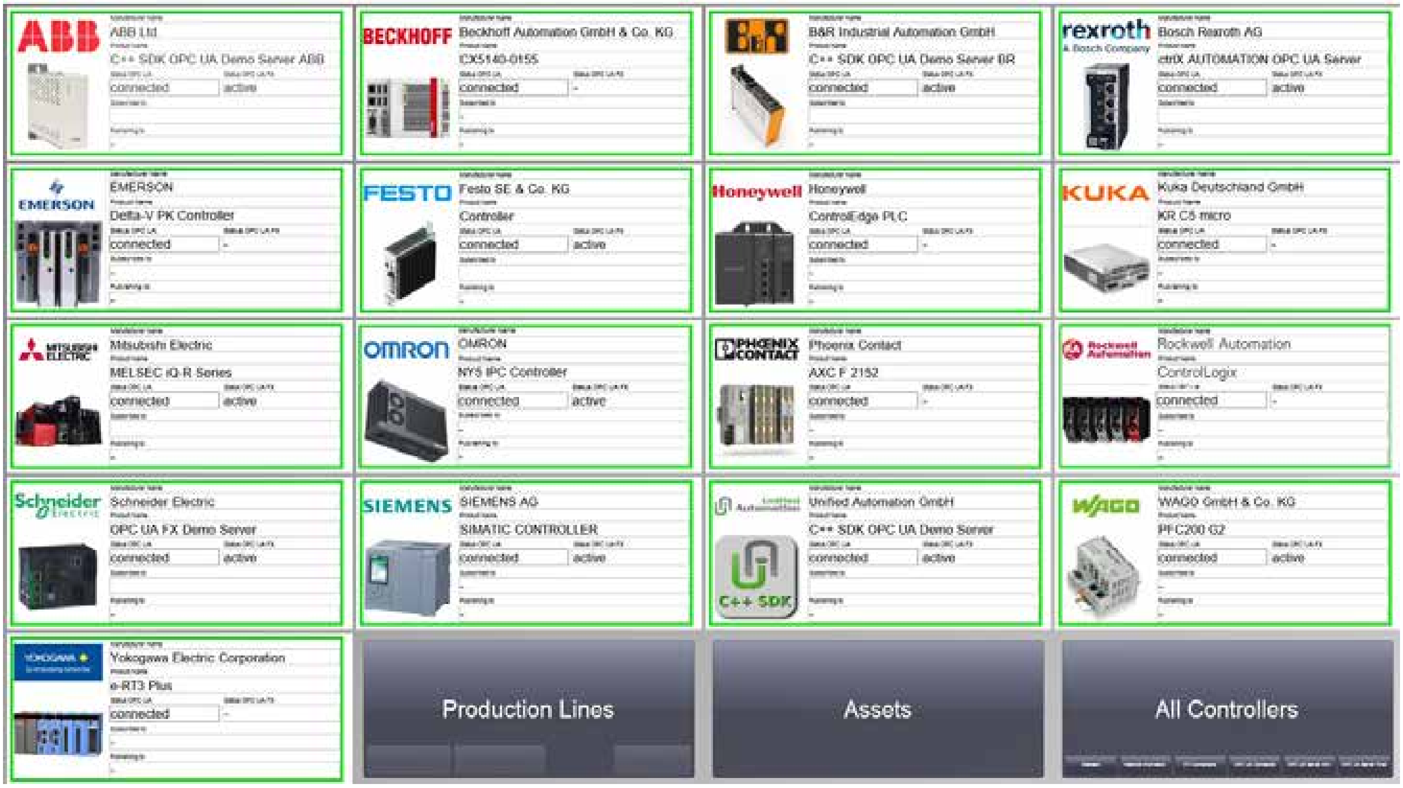
Each UAFX connection can be authenticated and optionally encrypted by standard OPC UA security mechanisms specified for the Client/Server and PubSub communication. The connection establishment is entered after a OPC UA Secure Session establishment is completed using asymmetric cryptography with certificates and private keys.

First OPC UA FX Specification Version

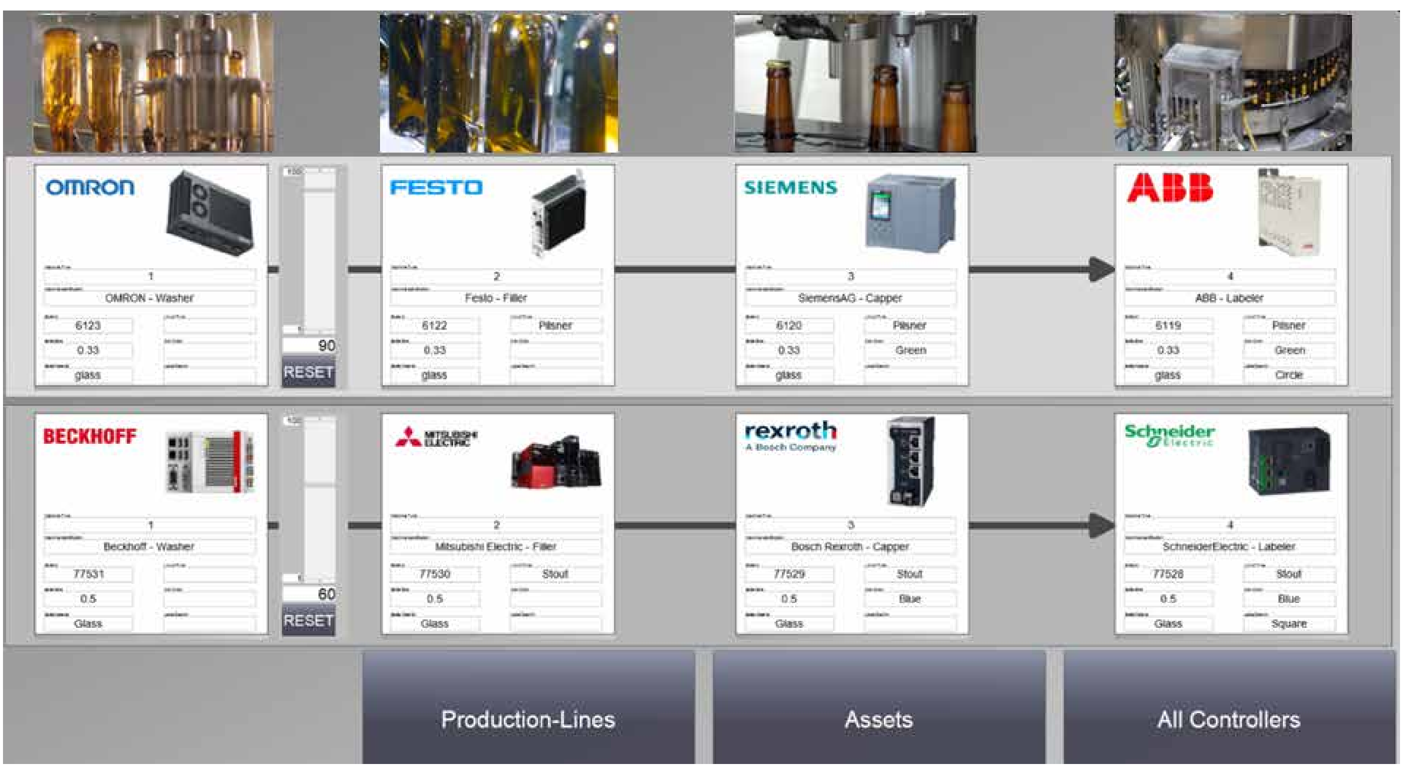
The first OPC UA FX specification version consists of five specification parts:

- Part 80 (OPC 10000-80) provides an overview and introduces the basic concepts of using OPC UA for field level communications.
- Part 81 (OPC 10000-81) specifies

SOURCE: OPC FOUNDATION



Dashboard of the UAFX Multi-Vendor Demo (All Controllers View).



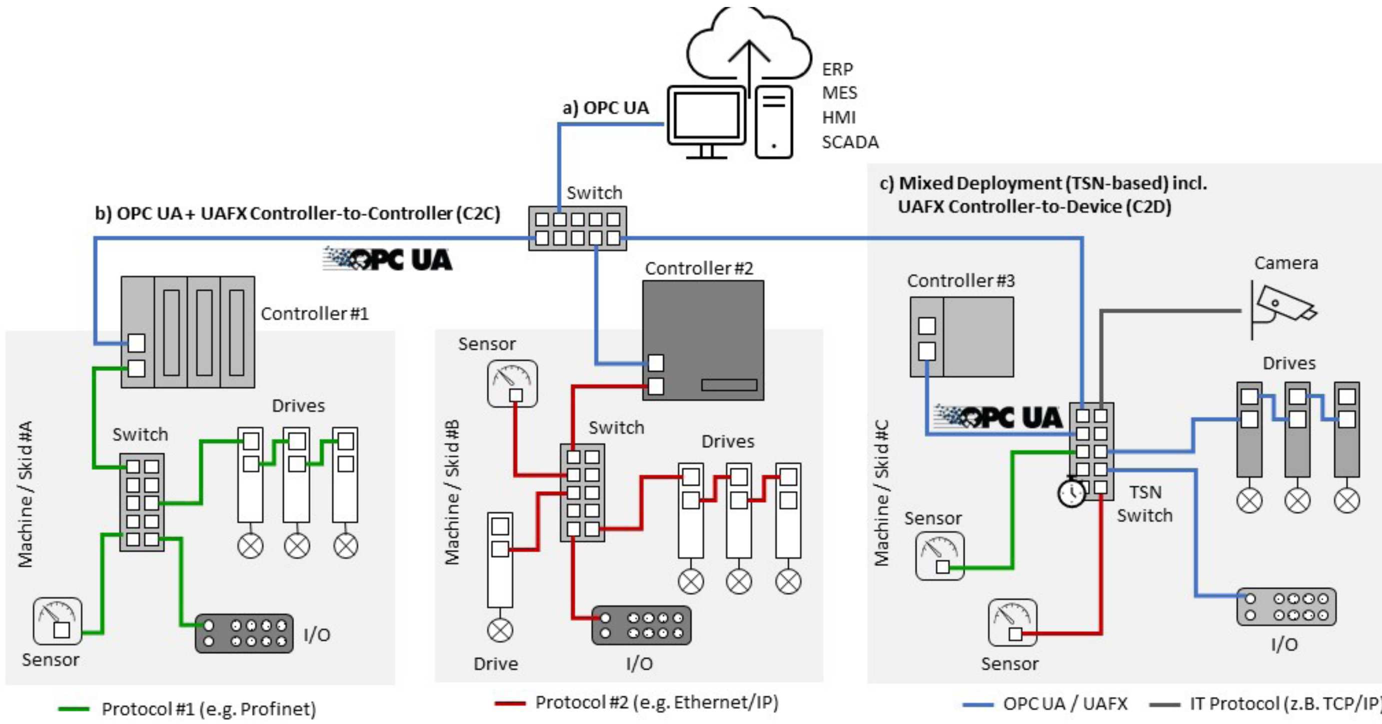
Dashboard of the UAFX Multi-Vendor Demo with the visualization of 2 production lines.

the base information model and the communication concepts to meet the various use cases and requirements of Factory and Process Automation.

- Part 82 (OPC 10000-82) describes networking services, such as topology discovery and time synchronization.
- Part 83 (OPC 10000-83) describes the data structures for sharing information required for Offline Engineering using descriptors and descriptor packages.
- Part 84 (OPC 10000-84) describes the UAFX Profiles that are used to segregate OPC UA FX features with regard to testing of OPC UA products implementing OPC UA FX functionality.

First OPC UA FX Multi-Vendor Demo

In November 2021, a first multi-vendor interoperability demo was realized, in which automation and network components were combined to illustrate cross-vendor data exchange via OPC UA and the OPC UA FX extensions. For this purpose, 17 controllers (including PLC, motion and robot controllers,



SOURCE: OPC FOUNDATION

Unification of horizontal and vertical communication via OPC UA (a) and UAFX (b), as well as migration to a continuous, convergent network (c) that full scales from the field to the cloud and vice versa.

as well as Distributed Control Systems) from different vendors - including the largest automation manufacturers in the world - were interconnected via a common network infrastructure.

This infrastructure consists of conventional Ethernet switches, Ethernet TSN (Time-Sensitive Networking) switches, and a 5G testbed using the millimeter-wave frequency range.

All controllers of the demonstrator provide current status and asset information via an integrated OPC UA server, which is queried and visualized via a central dashboard. The "All Controllers" view displays the status of OPC UA connections for all 17 controllers in the multi-vendor demo, as well as status information about the PubSub-based UAFX connections configured by each of the UAFX controller prototypes. The dashboard itself is interactive and, when clicking on one of the 17 controllers, switches to the "Asset View", which displays the UAFX asset information modeled and exposed by the controllers.

In order to demonstrate the possibilities and advantages of the UAFX extensions, a modular bottling line was simulated in the demonstrator, in which 4 machine units for washing, filling, capping and labeling the bottles are combined to form a production line. For demonstrating cross-vendor interoperability, each of these units is equipped with a control system from a different manufacturer.

The configuration of the communication connections and the process data exchanged via these connections to implement a functioning production line is carried out via a UAFX Connection Manager, as already described above. In the demonstrator, a stand-alone (external) Connection Manager from Unified Automation, based on UA Expert, and a Connection Manager integrated into the SIMATIC PLC from Siemens, each with its own graphical user interface, are used. The Connection Managers act as OPC UA clients and use the OPC UA servers integrated in the UAFX controller prototypes to configure UAFX connections between the respective controllers.

The corresponding process data is then exchanged via these UAFX connections using OPC UA Pub/Sub. The controllers act as UAFX publishers and/or UAFX subscribers depending on their role & position in the configured production line. The process data can be real-time data or, for example, safety data for fail safe operations. The configured production lines can be visualized and monitored in the dashboard.

Summary and Outlook

The first OPC UA FX specification defines extensions to the OPC UA framework that enable uniform networking between controllers via a common network infrastructure in order to exchange process data on the basis of a manufacturer-independent interface.

OPC UA is thus establishing itself as an industrial interoperability standard not only for the vertical integration from the control level to the edge or up to the cloud, but also as an interface for exchanging process data between controllers, regardless of which protocol these controllers use to communicate with the underlying field devices, e.g. servo drives, distributed I/Os, sensors.

In the next project phase that will be launched end of July 2022, the concepts developed for the "controller-to-controller" use case will be extended for "controller-to-device" (C2D) and "device-to-device" (D2D). This supports additional use cases, including further functions and device-specific models, e.g. for motion control, instrumentation and distributed I/Os. OPC UA will then provide a uniform communication standard that scales completely across all levels, from the field to the cloud, both vertically and horizontally .

Ethernet TSN (Time-Sensitive Networking) and the IEC/IEEE 60802 TSN IA (Industrial Automation) profile of IEC/IEEE 60802 are particularly important because it enables different protocols, regardless of whether they are IT or OT protocols, to coexist in a uniform and common network infrastructure.

This enables a step-by-step migration of conventional industrial Ethernet protocols to a uniform OPC UA-based communication solution and barriers due to incompatible protocols and profiles can be removed step by step. A decisive success factor here is that OPC UA is supported by all major automation suppliers in the world, so that users will be free to decide in the future which systems and components they use in their production plants and factories.

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

Visit Website

industrial ethernet book

Industrial Networking & IIoT

Special Supplement

EtherNet/IP Solutions Update

Learn about the technology and trends, applications and products shaping the newest generation of EtherNet/IP solutions.

EtherNet/IP focus on digitization and process industry applications

EtherNet/IP™ is a best-in-class Ethernet communication network that provides users with tools to deploy standard Ethernet technology (IEEE 802.3 combined with the TCP/IP Suite) in industrial automation applications while enabling Internet and enterprise connectivity.

The Common Industrial Protocol (CIP) encompasses a comprehensive suite of messages and services for a variety of manufacturing automation applications, including control, safety, security, energy, synchronization & motion, information and network management.

ETHERNET/IP AUTOMATION, MOTION AND machine control offer a standard industrial network solution that adapts a Common Industrial Protocol (CIP) for use with standard Ethernet technologies in the factory.

For the Special Report on EtherNet/IP in this issue, the Industrial Ethernet Book reached out to Paul Brooks, manager of technology business development at Rockwell Automation and Dr. Al Beydoun, ODVA President and Executive Director, to learn more about the current state of the technology and to provide readers an update on this key Industrial Ethernet network protocol.

Focus on digitization

The drive to leverage information

According to Paul Brooks, manager - technology business development at Rockwell Automation, a series of key technical trends are helping to driving forward the adoption of EtherNet/IP for automation, control and networking solutions.

"Digitization and the thirst for information coming out of automation devices and automated equipment are significant drivers. In many ways, EtherNet/IP is a mature technology," Brooks told the Industrial Ethernet Book recently. "Reasons for adopting EtherNet/IP are evolving from better machine and plant control (e.g., increasing machine speed and getting plants running faster) to better overall asset management across many plants. Users want an excellent software experience so they can effectively manage many machines and automation devices."

Brooks said that automation systems that utilize EtherNet/IP technology solutions are able to leverage primary technology benefits designed specifically for factory automation and control networking.

Importance of digitization

"We believe that systems built with EtherNet/IP are better positioned for digitization than other technologies. We use standard unmodified Ethernet and IP centric technologies. Our design approach is built around the same technologies that are used in the software (cloud to on-prem) environment and we follow a strictly object-oriented model," Brooks added.

Single Pair Ethernet (SPE) and Ethernet-APL, in particular, are offering new capabilities and enhancing automation network solutions especially in process industry applications.

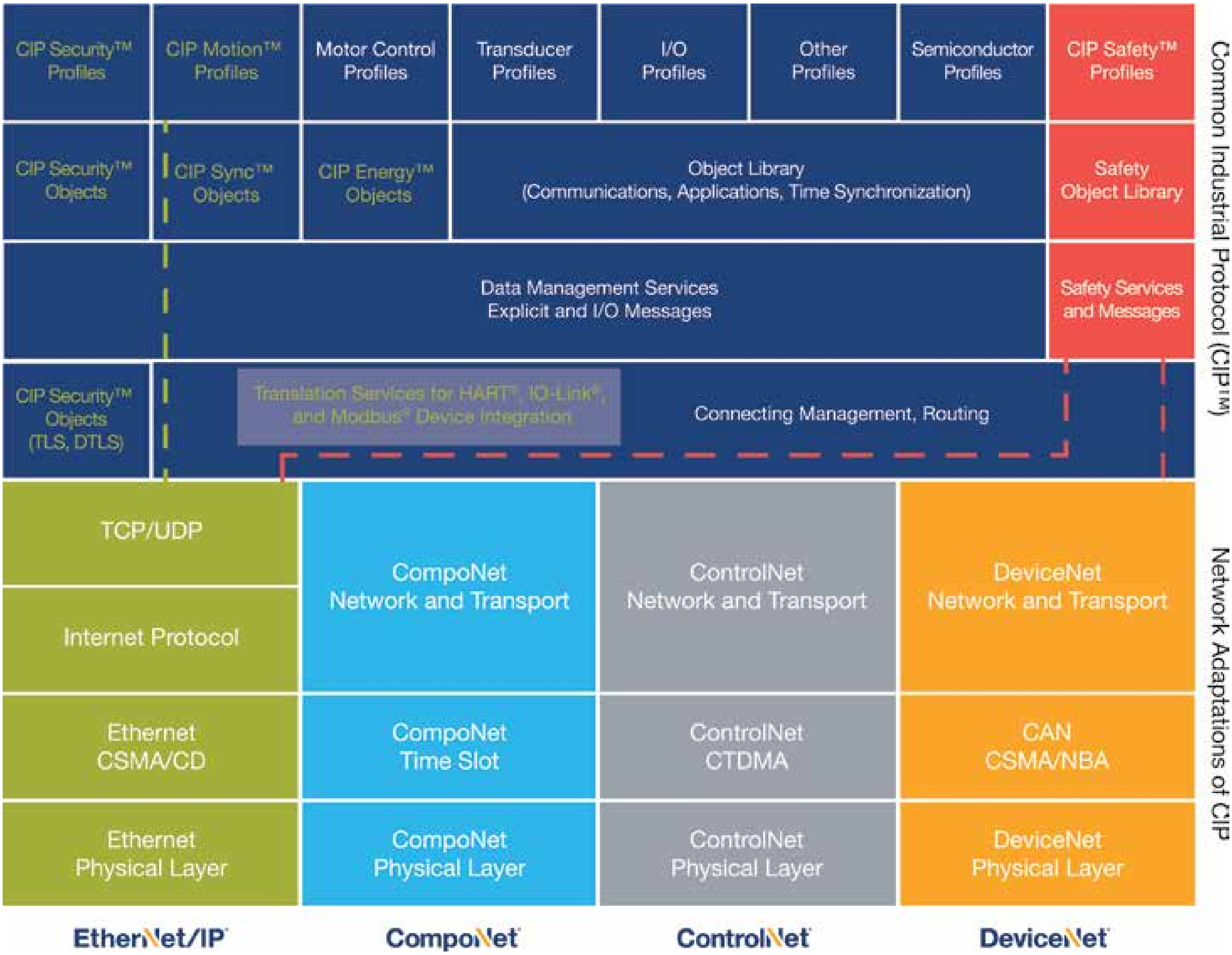
Brooks said that SPE and APL have some network architecture implications, but what truly sets them apart is that they allow new classes of devices to be connected to Ethernet (with EtherNet/IP).

"Process instrumentation has long been one of the biggest gaps and biggest customer demands for EtherNet/IP, but classical 4-pair Ethernet was technically not a viable option for most applications. Allowing long cable runs into hazardous areas makes it possible to meet this demand by implementing EtherNet/IP on these components and achieving digitization driven by information delivery," Brooks said.

These technologies are helping to drive interest in specific application areas, and the ability to offer solutions for IoT and enterprise connectivity.

"Clearly, we see process instrumentation and continuous process control as the most important emerging application space for EtherNet/IP, complementing its success in discrete and hybrid applications," Brooks said.

"Digitization through IIoT solutions is a bottom-line driver for most of our customers and here EtherNet/IP is an important contributor, but these solutions will also rely on technologies like OPC UA and MQTT. EtherNet/IP's contribution will generally remain within the four walls of a plant, and



below 'the Edge'. A non-device focus area for EtherNet/IP development is to provide integration with these technologies to deliver information with context from device to cloud, generally with pre-processing at the edge. Two examples of this include EtherNet/IP and OPC UA companion specification development and FactoryTalk Edge Gateway. The outcome is software application development that takes advantage of the rich data and meta-data already in EtherNet/IP devices," he said.

Addressing engineering challenges

The developments in APL to support process instrumentation in the context of value delivered by software applications is making an impact through the value delivered by expansion into new classes of previously unconnected devices.

Brooks said that these two themes are also addressed by two major ongoing developments in the ODVA community. The first is the xDS project, which is a reworking of ODVA's product descriptor mechanisms using contemporary technology. It is about software enablement and providing the tools to allow app developers to understand and automatically expose highly innovative and vendor-specific information within devices to the users of those apps.

Second, the "resource constrained in-cabinet solution," which makes innovative use of short-range SPE and a reduced capability variant of EtherNet/IP and makes it practical to deploy communications technologies on simple electromechanical control components. Overall, EtherNet/IP is evolving to allow more types of devices to deliver user value through innovative software apps.

Industrial Ethernet solutions

Automation control networking technology

Dr. Al Beydoun, ODVA President and Executive Director, said that Industrial Ethernet has overtaken fieldbus and now makes up the majority of new connected nodes due to the increased speed and omnipresence of Ethernet that enables precise control, additional diagnostic data for the enhancement of existing operations, and increased interconnectivity across the business.

EtherNet/IP™ is a leading industrial automation network solution as a result of relying on commercial-off-the-shelf (COTS) technology and standard, unmodified Internet Protocol and Ethernet (IEEE 802.3 combined with the TCP/IP Suite).

"This gives users unparalleled access to information from Industrial IoT devices, allowing for visibility and insights into how operations are performing, which results in better business decisions," Beydoun said. "Reliable, real-time communication on the factory floor is made possible with EtherNet/IP through a properly planned network design that leverages segmentation via managed switches allowing for both efficient communication and greater security. EtherNet/IP also uses profiles that define how the information in a device should be presented, which ensures interoperability."

Beydoun said that EtherNet/IP utilizes the Common Industrial Protocol (CIP™) for the session, presentation, and application layers per the Open Systems Interconnection (OSI) model, which enables media independence (e.g. wireless transport) and a consistent information format. The Ethernet based physical, data link, and network, and transport layers are what makes EtherNet/IP unique from other CIP networks such as DeviceNet®.

Key technology trends

EtherNet/IP utilizes ODVA's CIP application layer and deploys it on standard networking technology such as Ethernet, Wi-Fi, or 5G. CIP is an object-oriented approach to designing Industrial IoT devices, which shortens the learning curve for developers. EtherNet/IP also defines a suite of CIP services for delivering real-time, safe, secure and application specific functions that industrial automation practitioners require with CIP Safety, CIP Sync, CIP Motion, CIP Energy, and CIP Security.

"Encapsulation of CIP along with TCP and UDP into an IP packet is used to route messages vertically through an organization's enterprise to allow the data to be consumed by business systems such as manufacturing execution systems, enterprise resource planning software, and even to cloud-based applications. Using TCP, UDP, and IP ensures that EtherNet/IP is IT friendly. Furthermore, the same class of switches and routers used in established Enterprise networks can also carry EtherNet/IP OT traffic," he added.

CIP Security on EtherNet/IP allows users to extend a defense-in-depth approach to the EtherNet/IP network to help protect EtherNet/IP IIoT devices from cyberattacks. Additionally, CIP Security enables policy-based application authentication and authorization for EtherNet/IP IIoT devices.

EtherNet/IP supports a range of topology options and functionality that allow end users and OEMs to tailor the EtherNet/IP network to their needs. For example, device level ring (DLR) with specially enabled EtherNet/IP IIoT devices provides an option for single-ring network resiliency. QuickConnect™ functionality is also an option to rapidly exchange different discrete IIoT devices.

Since EtherNet/IP is compliant with IEEE Ethernet standards, users can take advantage of speeds of up to 1 Gigabits per second (Gbps) and more as needed. Media installation options include copper, fiber, fiber ring, and high speed and bandwidth wireless solutions such as Wi-Fi and 5G. Reliance on IEEE and IEC standards also means that users can take advantage of new advancements in Ethernet technology. This includes Single Pair Ethernet reaching resource-constrained devices in cabinets and using the Ethernet-Advanced Physical Layer for accessing devices in the field for process automation hazardous applications.

Impact of SPE and Ethernet-APL

Beydoun said that it's important to note that Single Pair Ethernet (SPE) encompasses 10BASE-T1L General Purpose SPE applications, 10BASE-T1S in-cabinet applications, and 10BASE-T1L Ethernet-APL applications. Furthermore, there are multiple IEEE SPE standards in addition to those discussed here.

The functionality in EtherNet/IP for in-cabinet resource-constrained device connectivity powered by SPE (10BASE-T1S) allows for the usage of a flat cable to reduce material cost, space used, and installation time. The flat cable includes both switched power, network power, SPE, and a select line to enable multi device connectivity at a low cost. This compact low-cost flat cable allows devices to be easily attached via a safe and simple piercing connection.

Ethernet-APL (10BASE-T1L) supports trunk and spur, line, and star topologies as well as Type A fieldbus cable to meet the requirements of the process industries. The trunk and spur topology will be seen in the vast majority of instances for powered and intrinsic safety applications, but a ring topology is possible for non-powered and non-IS applications to enable redundancy for critical applications in sectors such as Water Treatment Plants. Ethernet-APL also enables the use of Parallel Redundancy Protocol (PRP) for network technology that have this as an option, as EtherNet/IP does.

EtherNet/IP will be able to expand precise, efficient Ethernet-based control and commissioning across process field instrumentation via the Ethernet-APL physical layer. The full use of EtherNet/IP in process automation will enable concurrent seamless connectivity from the field devices to the controllers, to Industrial IoT applications, as well as the edge and cloud for prognostic analysis.

EtherNet/IP targeted applications

"Wireless and wireless safety are some of the newest applications where EtherNet/IP is being leveraged as a solution. Motion control and other applications requiring high speed reaction times are still typically best served by wired solutions," Beydoun said. "However, for time-critical safety and I/O applications, wireless is increasingly becoming an option.

An Automated Guided Vehicle (AGV) in a factory that is moving on a fixed route to supply components to a machine or to transport finished goods from a packaging line to a delivery vehicle loading area in an environment with people working on other tasks is an example where EtherNet/IP and CIP Safety can be used."

The individual devices can use the CIP Safety protocol to detect failures in communications and bring the system to a safe state. This is made possible through the "gray channel principle", which is laid out in IEC 61508. The concept is that two safety devices must have enough intelligence in themselves, and enough diagnostics in their communications, that the entire communication network has zero impact on the ability of the device to detect communication errors.

Wireless AGVs can transmit data about the number of components or finished goods that have been transported over a given period of time to provide a better understanding of operations and how to improve them. This data can be transported either to the edge or to the cloud for further processing or inclusion in KPI dashboards making the promise of IIoT a reality. Furthermore, a degradation in AGV functionality measured via decreased speed and/or increased vibration could be used to predict future failure thereby allowing for preventative maintenance efforts to maintain maximum OEE.

Engineering challenges

EtherNet/IP already has and will continue to undergo enhancements to meet engineering challenges such as connectivity beyond wires, simpler and less expensive SPE cabling for process and discrete applications, increased speed, and enhanced coexistence on the wire.

The challenge of network convergence is particularly noteworthy given both the scope of the task as well as the expected benefits of manufacturing optimization and flexibility. EtherNet/IP plans to support the currently in process IEC/IEEE 60802 Time Sensitive Networking (TSN) standard upon completion, which is expected to improve coexistence in an effort to offer end users better visibility into operations and to more easily implement their systems.

"EtherNet/IP is already strongly positioned to meet the needs of time sensitive applications, flexibility in network design, and Industry 4.0/IIoT with implementation of proper network segmentation. EtherNet/IP is designed to both move I/O traffic deterministically and quickly via low overhead UDP while at the same time allowing for more complex messaging to higher network levels including ERP systems and the cloud with TCP," Beydoun said.

Through the use of a planned gateway device, EtherNet/IP will have a unique advantage with the addition of 60802 TSN by being able to both fully adhere to the mechanisms outlined in the IEC/IEEE 60802 TSN profile as well as the IEEE 1588 Precision Time Profile through CIP Sync and CIP Motion. CIP Sync is an existing network mechanism for applications where tight real-time synchronization is vital between distributed intelligent devices and systems. CIP Motion is a current deterministic network solution for multi-axis, distributed motion control.

60802 based TSN will serve as an additional layer of control and interoperability that EtherNet/IP users can utilize to enable network convergence with other types of Ethernet traffic, such as coexistence with cameras for high-speed scanning or security, while having all applications respect the same Quality of Service considerations.

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

Single Common Conformance Test Plan: IEC/IEEE 60802 TSN

Avnu Alliance, CLPA, ODVA, OPC Foundation and PROFIBUS & PROFINET International are collaborating on a single conformance test plan for IEEE/IEC 60802 Time Sensitive Networking (TSN) profile for industrial automation.

SOURCE: ODVA

THE TEST PLAN WILL BE USED AS A BASE TEST by all the participating organizations and made available to the broader Industrial Automation ecosystem. This collaboration contributes towards end user confidence that 60802 conformant devices from different manufacturers which support different automation protocols will coexist reliably at the TSN level on shared networks, including with devices using TSN for applications other than automation.

The focus of the collaboration is to work together towards a jointly agreed and owned test plan for the industrial automation market. This formal collaboration provides value by creating a structure in which all these organizations can work together and exchange ideas towards the end goal of interoperability and coexistence on open, standard networks for all protocols, without needing to establish a separate, formal organization.

The TIACC marks a commitment by these organizations to develop an interoperable ecosystem of devices from different manufacturers to comply with the IEC/IEEE Standards Association 60802 profile and enable end-users to confidently deploy these devices on open, standard networks. The goal is to have the final version of the single, shared test plan available soon after the IEC/IEEE 60802 profile is published.

"Avnu's purpose and mission is to transform standard networks to enable support for many time sensitive applications and protocols in an open, interoperable manner. This collaboration among organizations will be critically important to facilitating coexistence of multiple workloads and protocols according to IEEE 60802 on a network, while leveraging foundational network interoperability that is used across industries," said Greg Schlechter, Avnu Alliance President. "We are committed to working with the industries to enable an interoperable ecosystem of devices that allow end users to confidently deploy on open, standard, and converged networks."

"The creation of the Connected Industries of the future requires different systems and devices to communicate in order to deliver the necessary process transparency required. This is a core principle for the CLPA and is at the root of why the organization was founded. This is why we are delighted to be part of the TIACC and look forward to supporting the creation of a unified, common test plan for TSN-compatible products. By doing so, we can help further boost the adoption of futureproof technologies for smart manufacturing," said Manabu Hamaguchi, Global Director at CLPA.

Learn more about the TSN Industrial Automation Conformance Collaboration #TIACC here: https://www.tiacc.net/.

Standardized Common "Power Consumption Management"

A NEW INTERFACE STANDARD FOR ACQUISITION of energy consumption data in industrial manufacturing is being developed by ODVA, OPC Foundation, PI, and VDMA based on OPC UA technology.A key objective of the future mechanical and plant engineering sectors is to achieve climate-neutral production. This is backed up by the European Union's "European Green Deal", which aims to make Europe climate-neutral by 2050. To achieve this goal, and to implement many other use cases, energy consumption data in production is an important prerequisite.

ODVA, OPC Foundation, PI and VDMA founded the "Power Consumption Management" group in May 2022 with a focus on the development of this OPC UA interface standard.

Karsten Schneider, Chairman of PI, said he is looking forward to cooperation with the ODVA, the OPC Foundation, and VDMA: "The acquisition and analysis of energy consumption in machines and plants is an immensely important topic for the future."

"The four organizations are working at full speed to harmonize and standardize energy consumption information on the shop floor," said Andreas Faath, head of VDMA Machine Information Interoperability Department. "With this, a crucial building block, supporting the goal of global climate-neutral production in all sectors of the machinery and plant engineering industry, is under development."

"Rapid transition to environmentally-sustainable energy use is the greatest challenge of our time and, as such, I am glad that we are proceeding together: PI and ODVA contributing their in-depth know-how on energy interfaces at the field level, with the internationally recognized OPC UA data modelling standard defining semantics and secure data transport, serving as the foundation of the Global Production Language developed by the VDMA", said Stefan Hoppe, President OPC Foundation.

"ODVA is pleased to be an active contributor to this key initiative to optimize energy usage and thereby reduce the detrimental impact on the environment from waste," said Dr. Al Beydoun, President and Executive Director of ODVA. "This Power Consumption Management collaboration will help ensure end users have a highly standardized and interoperable means to reach their environmental, social, and corporate governance (ESG) goals."

The results of the working group will be published as a new OPC UA specification. Future releases of the OPC UA for Machinery specification will leverage these results, ensuring that energy information from all machines and components on the shop floor can be provided in a standardized way as part of the Global Production Language.

"The activity is based, in particular, on the existing standards of the participating organizations; but also on other standards from the OPC Foundation, the VDMA, and external research," said Heiko Herden, VDMA and elected chairperson of the new joint working group. "In combination with other OPC UA for Machinery use cases, such as status monitoring or job management, the calculation of the product and production-specific carbon footprint will be possible."

*News report by **ODVA**.*

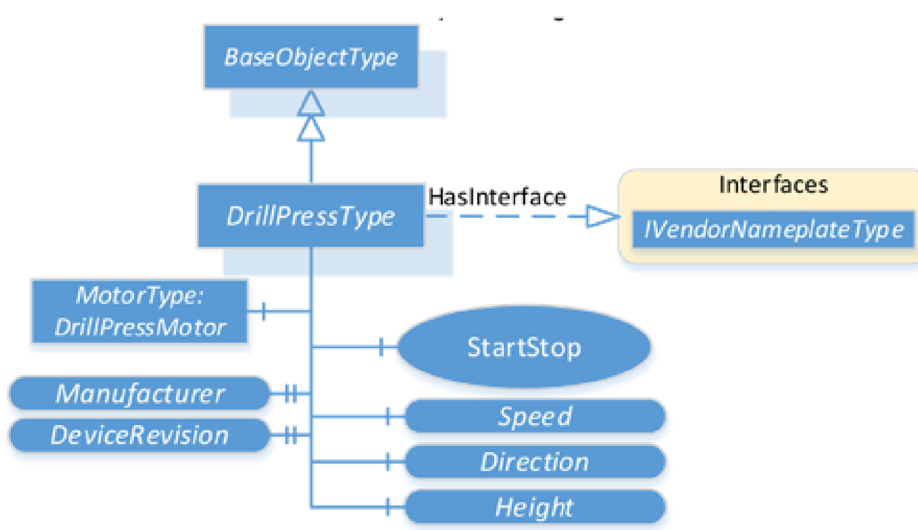
Mapping CIP to OPC UA: companion specification update

OPC UA continues to gain momentum as a vendor-independent mechanism to collect data. The publication of an ODVA companion specification will be essential to help end users realize the potential of intelligent devices. This article discusses progress towards an OPC UA Companion Specification for CIP.

THE WORLD IS ABUZZ WITH TALK OF THE next industrial revolution, or Industry 4.0. Digitization, smart technologies, machine-to-machine communications, Internet of Things deployments, the list goes on, and on. All these innovative concepts will benefit from the standardized exchange of information between all levels of an industrial system.

New products will evolve over time, but existing technologies can be adapted now to leverage the massive installed base of CIP-enabled products around the world. One such technology that is gaining acceptance is OPC UA. Many vendors, end users, and industry consortia have converged on OPC UA as a vendor-neutral mechanism to exchange data. ODVA and OPC Foundation are jointly developing a CIP Companion Specification to support this data exchange.

This article documents the approach taken by that joint working group to map the CIP information model to the OPC UA information model. With this mapping, applications utilizing OPC UA and its associated companion specifications can obtain data from CIP devices without the need to understand CIP. This solution will bring value to end users seeking to extract more data from existing installations for evolving application needs.



SOURCE: ODVA

OPC UA Model for a Drill Press.

Introduction

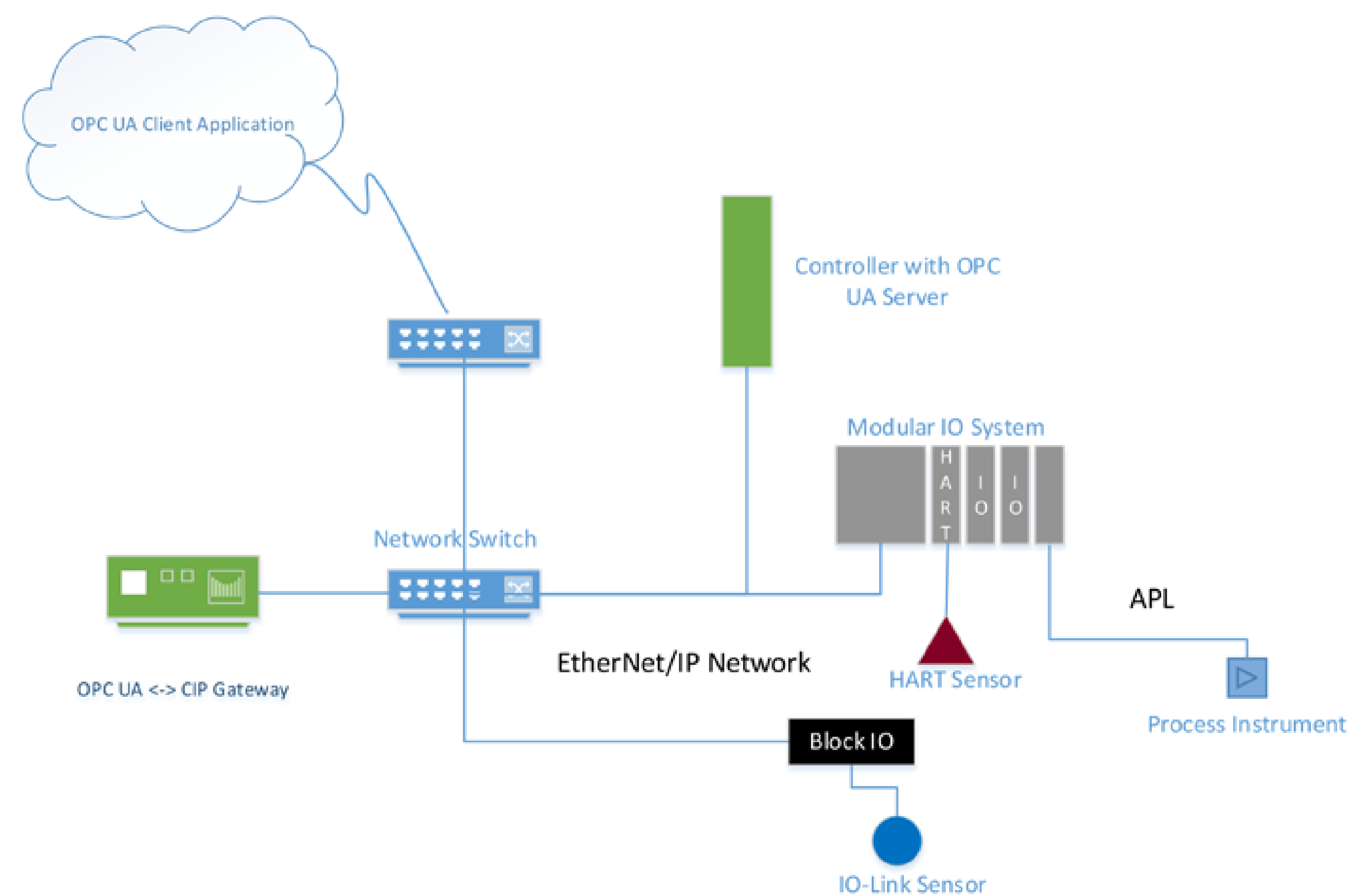
The original OPC standard was born out of a need to "abstract PLC-specific protocols into a standard interface". That need still exists today. End users choose field level protocols based on application specific needs, but there is an increasing desire to collect and use data from devices on all those disparate fieldbuses. The users of that data may not understand the details of each field level protocol and they wish to get data consistently across all of them.

SOURCE: ODVA

Attribute	Value				
BrowseName	DrillPressType				
IsAbstract	False				
References	**Node Class**	**BrowseName**	**DataType**	**TypeDefinition**	**Other**
Subtype of the BaseObjectType defined in OPC 10000-5					
0:HasComponent	Object	DrillPressMotor		2:MotorType	M
0:HasComponent	Variable	Speed	0:Int32	0:PropertyType	O
0:HasComponent	Variable	Direction	0:Boolean	0:PropertyType	M
0:HasComponent	Variable	Height	0:Int32	0:PropertyType	M
0:HasComponent	Method	StartStop	Defined in x.y.z		M
0:HasInterface	ObjectType	1:IVendorNameplateType			
Applied from IVendorNameplateType (defined in OPC 10000-100)					
0:HasProperty	Variable	1:Manufacturer	0:LocalizedText	0:PropertyType	M
0:HasProperty	Variable	1:DeviceRevision	0:String	0:PropertyType	M

Table 1 - Drill Press Object Type Definition.

SOURCE: ODVA



Industrial Network Accessed by OPC UA Client Application.

Many are choosing OPC UA to achieve that. ODVA's Common Industrial Cloud Infrastructure Special Interest Group (CICI SIG) was formed to enable interactions between cloud applications and ODVA CONFORMANT™ devices that support EtherNet/IP. At ODVA's 2020 Industry Conference, members of the CICI SIG presented a paper documenting use cases for a *CIP Companion Specification for OPC UA*.

This article outlines the progress towards meeting some of those use cases.

What is OPC UA?

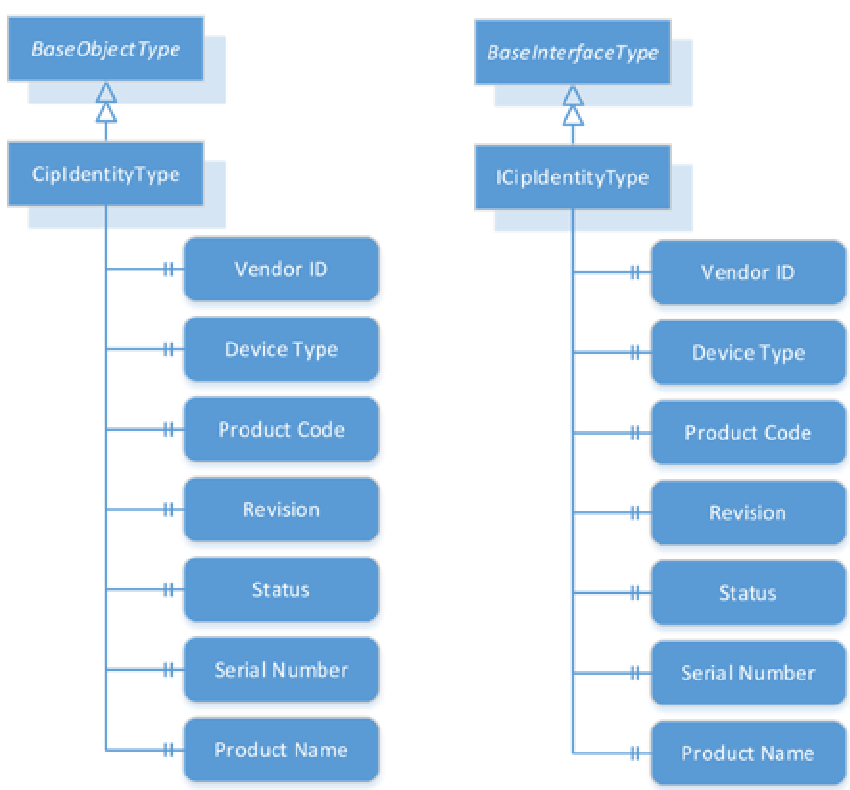
OPC UA is an open, royalty free set of standards designed as a universal communication protocol. It makes use of standard internet technologies, like TCP/IP, HTTP, and Web Sockets. It defines sets of core services and a basic information model framework. That framework allows vendor-specific information to be exposed in a standard way using metadata. This enables OPC UA Clients to discover and use that vendor-specific information without prior knowledge of it.

Information Modeling in OPC UA

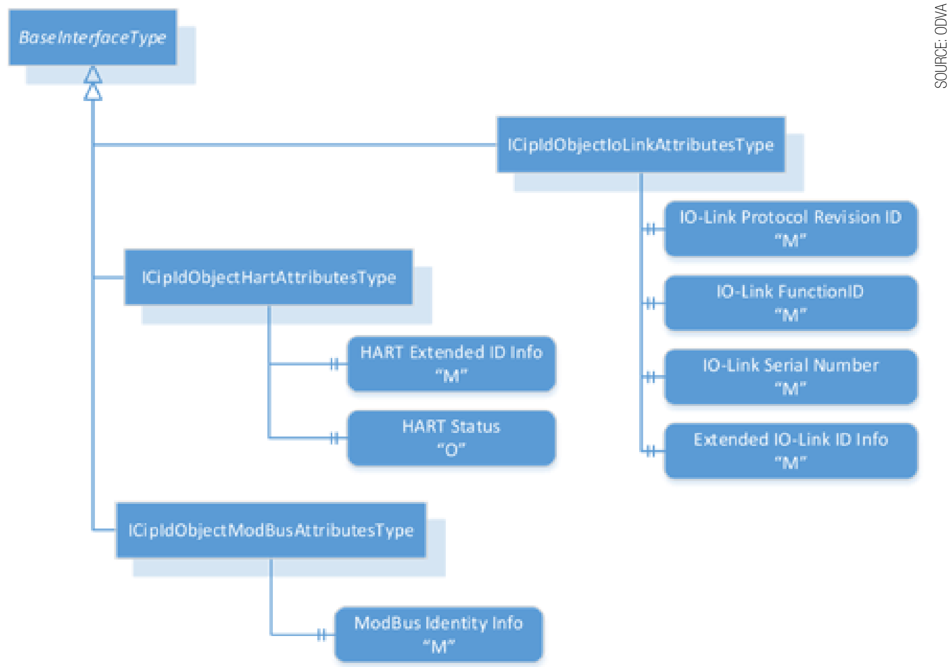
The elemental modeling concept in OPC UA is the "Node". Everything is implemented using Nodes: objects, methods, variables, references, etc. All Nodes are described by a set of required attributes such as the NodeId, NodeClass, and BrowseName. Different node classes have additional attributes – for example, Variable nodes have a Value, DataType, and other attributes which describe the contents of the data. These attributes are the metadata that allows clients to discover the information that a server has to offer.

OPC UA uses inheritance, and each new derived type can add required and optional attributes, or require an optional attribute

SOURCE: ODVA



Modeling the Identity Object.



Optional Functionality Modeled using Interfaces.

from a base class be mandatory in the derived class, but cannot remove support for inherited attributes. This technique is used by all OPC UA information modeling elements.

Much like CIP, OPC UA uses Objects to represent complex information. The information modeling framework defines a textual representation and a graphical representation that is similar to UML. A simple information model shows how a drill press might be modeled in OPC UA.

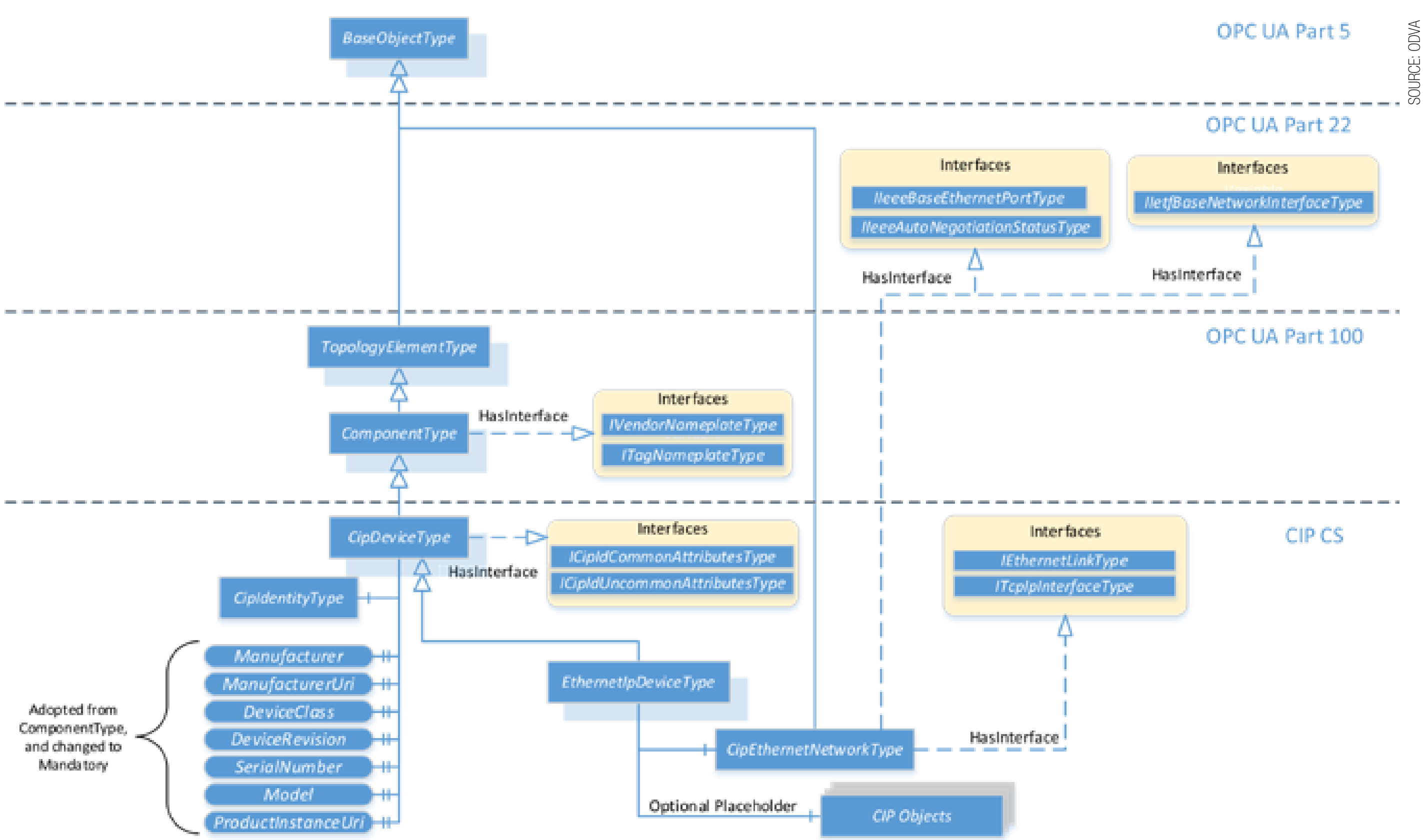
You can see from the figure that the DrillPressType inherits from the BaseObjectType. The BaseObjectType is defined by OPC UA 10000 – 5 Information Model. OPC UA's Part 5 is a core specification that defines the required attributes that all Object Types must support for consistency.

The newly defined DrillPressType object has components (an object representing the motor, a method to control operation, Speed, Direction, and Height) and properties (Manufacturer and DeviceRevision). The object also includes an OPC UA "Interface". Two of the optional properties from the interface (Manufacturer and DeviceRevision) are defined as mandatory for this object so they are specifically shown in the drawing.

The textual representation for this model is shown in Table 1. Each element of the object definition is further defined in this table. References indicate the relationship between the object and each element. The Node Class tells you which fundamental modeling construct (Node Type) is used. DataTypes can either be fundamental data types defined in the core specifications, or derived types. To help readers identify where something is defined, namespaces are included in the definition. If a number and a colon precede an element, it means that it is defined elsewhere.

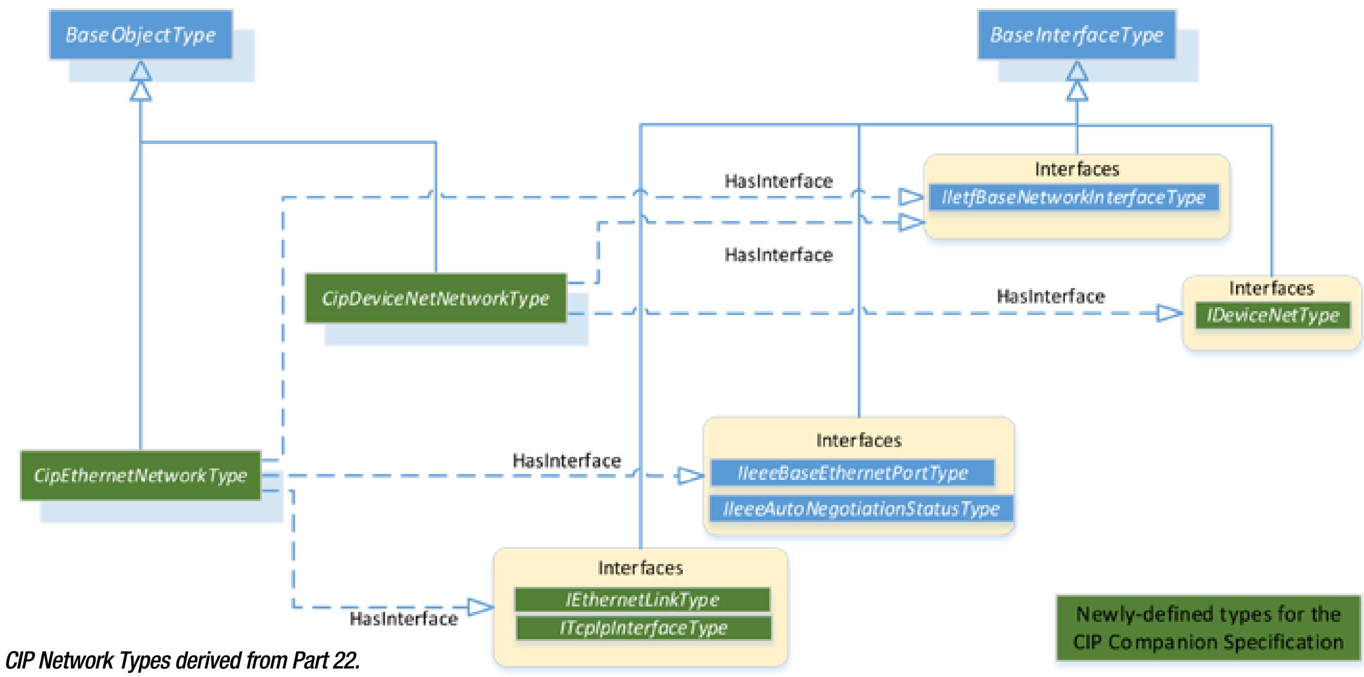
Specifications are required to supply a namespace table containing an index and a URI of any referenced type definitions. The "Other" column documents the need in implementation. Mandatory (M) and Optional (O) are shown here, but OPC UA defines additional classifications not demonstrated in this simple example.

Finally, you will recognize that all the elements have a BrowseName. The BrowseName is a required attribute of all elements in OPC



CIP EtherNet/IP Device Information Model.

SOURCE: ODVA



CIP Network Types derived from Part 22.

UA. The BrowseName is human-readable, but its primary use is for clients to build paths of BrowseNames. Clients gain access to a server's address space through some known entry point and then start navigating using BrowseNames and references between the elements.

Once the client finds the specific information it needs, it invokes a service on the server to translate a BrowsePath into a NodeId. Once the client has the NodeId, it will use that to access the information in the future. This whole model is very similar to the directory structure on a computer.

What is a Companion Specification

A companion specification uses OPC UA's information modeling framework to describe common information found in an industry vertical (e.g., Plastics and Rubber), or standard types of machines (e.g., Pumps and Vacuum Pumps).

These specifications attempt to harmonize the representation of the information in that vertical or machine by defining objects, variables, data types, methods and references specific to their operation. Simply put, companion specifications define a common interface to information represented by the model that could be supported in any instantiation of that model.

The CIP Companion Specification

CIP does not represent any one industry vertical or specific machine. It is used everywhere throughout industry. The purpose of the CIP Companion Specification is to provide a translation that would allow information found in CIP devices to be represented in the form needed by existing and future OPC UA client applications regardless of what companion specifications those applications use. An example of the translation that is needed is presented in this article.

The translation rules defined by the CIP companion specification can be implemented in any device that has an OPC UA server, however the most efficient and expedient way to enable this capability in existing installations would be for it to exist in a gateway appliance, or gateway function in a product already on the network.

The result is that an industrial network can be accessed by an OPC UA Client Application. OPC UA clients can discover OPC UA Servers and browse their address spaces. Either the controller or the gateway appliance could contain the gateway functionality that would gather data from devices and translate it for the OPC UA client. This could be done for EtherNet/IP devices as well as non-CIP field devices integrated through CIP's Integration Volumes 7A-C. The client could see each proxied device as an individual OPC UA server as if it were communicating directly with it.

CIP Device Information Model

To build our model we considered the elements that are common to all CIP devices: an identity, a network interface, and a collection of device-specific application objects. We created a standard representation for the Identity Object and CIP network interfaces by defining several OPC UA object and interface types. For all other device-specific application objects we plan to create OPC UA types that could model any CIP object generically.

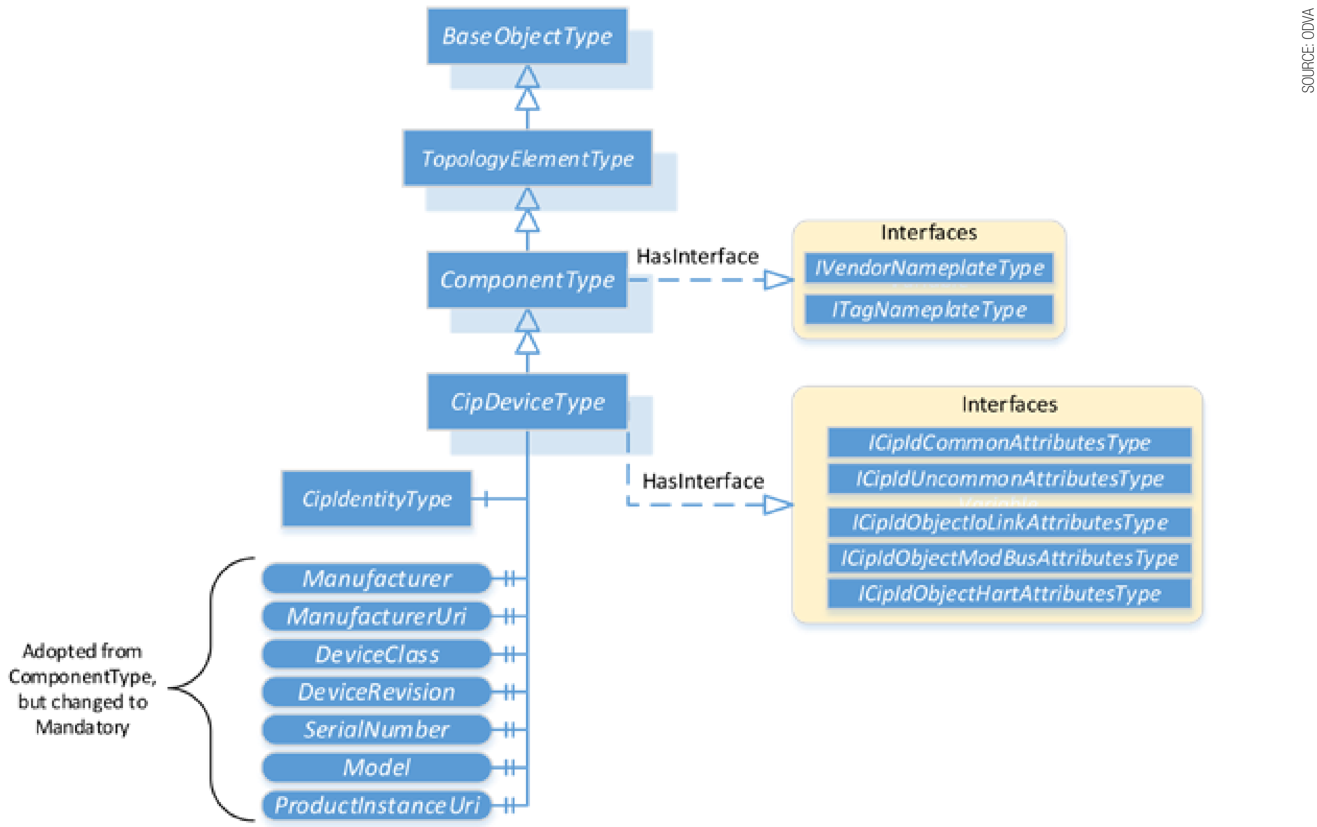
Many of the use cases outlined in deal with asset management. For OPC UA this kind of information is defined in OPC 10000-100 (Devices). While there is considerable overlap between the information in OPC's Devices specification and CIP's Identity Object, we decided to model both. We wanted to preserve all the attributes of the Identity Object in a lossless way and be able to represent a CIP device as modeled in OPC's Part 100: Devices.

CIP Identity Model

To model the CIP Identity information, we defined a CipIdentityType Object. The object inherits from OPC UA's BaseObjectType; the root for all object definitions. Each required CIP attribute is modeled as a property of the CipIdentityType.

In addition to this ObjectType, we also defined an identical InterfaceType so that existing models could expose the CIP Identity Object attributes simply by including the interface. Interfaces are an OPC UA modeling construct that enables you to build object functionality by referencing the interface (i.e., composition). When referencing an interface, the source object must include mandatory elements in the interface and can optionally include any optional elements

The optional attributes of the Identity Object were also added to OPC UA Interfaces. We grouped optional attributes into five interfaces: common, uncommon, HART, IO Link, and ModBus. This was a tradeoff between defining many interfaces and one very large interface that contained everything the Identity Object defines. This grouping should allow for more sensible implementations. For example, CIP can model the Identity of HART, IOLink, or ModBus devices. The optional interfaces needed for these attributes can be applied only where needed to represent



CipDeviceType Derived from Part 100 Types.

devices on those networks.

OPC UA's Part 100: Devices specification defines information for the identification of devices. Those properties are contained in two interfaces, IVendorNamplateType and ITagNameplateType. The CIPDeviceType is inherited from the ComponentType which is defined in Part 100. The CIPDeviceType further mandates several optional properties from the Part 100 interfaces to align with many existing companion specifications (e.g., PA-DIM). This collection of OPC UA properties and CIP Identity Object Attributes represents all the identification functionality from both specifications.

Some CIP attributes have a close equivalent property in an OPC UA object, while others require significant translation. For example, OPC UA makes extensive use of string data types in many properties that have numeric equivalents in CIP attributes. Table 2 demonstrates examples of the translation rules being proposed for the CIP companion specification for the identity information inherited from Part 100.

CIP Network Interface Model

OPC UA 10000 - 22 Base Network Model defines a very basic InterfaceType to be used by all networks. We defined object types that referenced that InterfaceType and new InterfaceTypes that model the information for the specific CIP network of the device. Part 22 defines a well-known location in the server's address space for network interfaces. Our new types will be located there so that any client can learn about a device's interface to its network.

Generic CIP Object Model

The CIP specifications define doTablezens of application objects and vendors are free to define more of their own. There are several alternatives to modeling these for OPC UA. We could provide a translation for only the most common publicly defined objects.

That would provide some benefit but would neglect some applications due to the missing translations and it does not address vendor specific objects. We could provide a translation for all publicly defined objects. That would take a long time and still would not address vendor-specific objects. The most comprehensive solution is to provide some type of generic mapping of the CIP object model to OPC UA.

The EthernetIpDeviceType has an "Optional Placeholder" for CIP Objects. OPC UA uses the Optional Placeholder modeling rule for open-ended situations. It allows you to place any number of objects with an unspecified BrowseName at that point in the model. We will use this to represent all other CIP objects in a device.

The details behind the GenericCipObjectType are still being developed. The figure above demonstrates how this generic type might be used. It shows a device that supports two instances of the Discrete Input Point Object. It supports Class Attribute 1, and Instance Attributes 3 and 4. The gateway would use some algorithm to generate unique BrowseNames for each Node in the model. In this case we used the pattern "CIP Class X Instance Y Attribute Z". For brevity the pattern could have been "CXIYAZ". The important part is that the name is unique within the path. Using this generic object, we believe we can represent any CIP object in OPC UA.

Example Integration with other Information Models

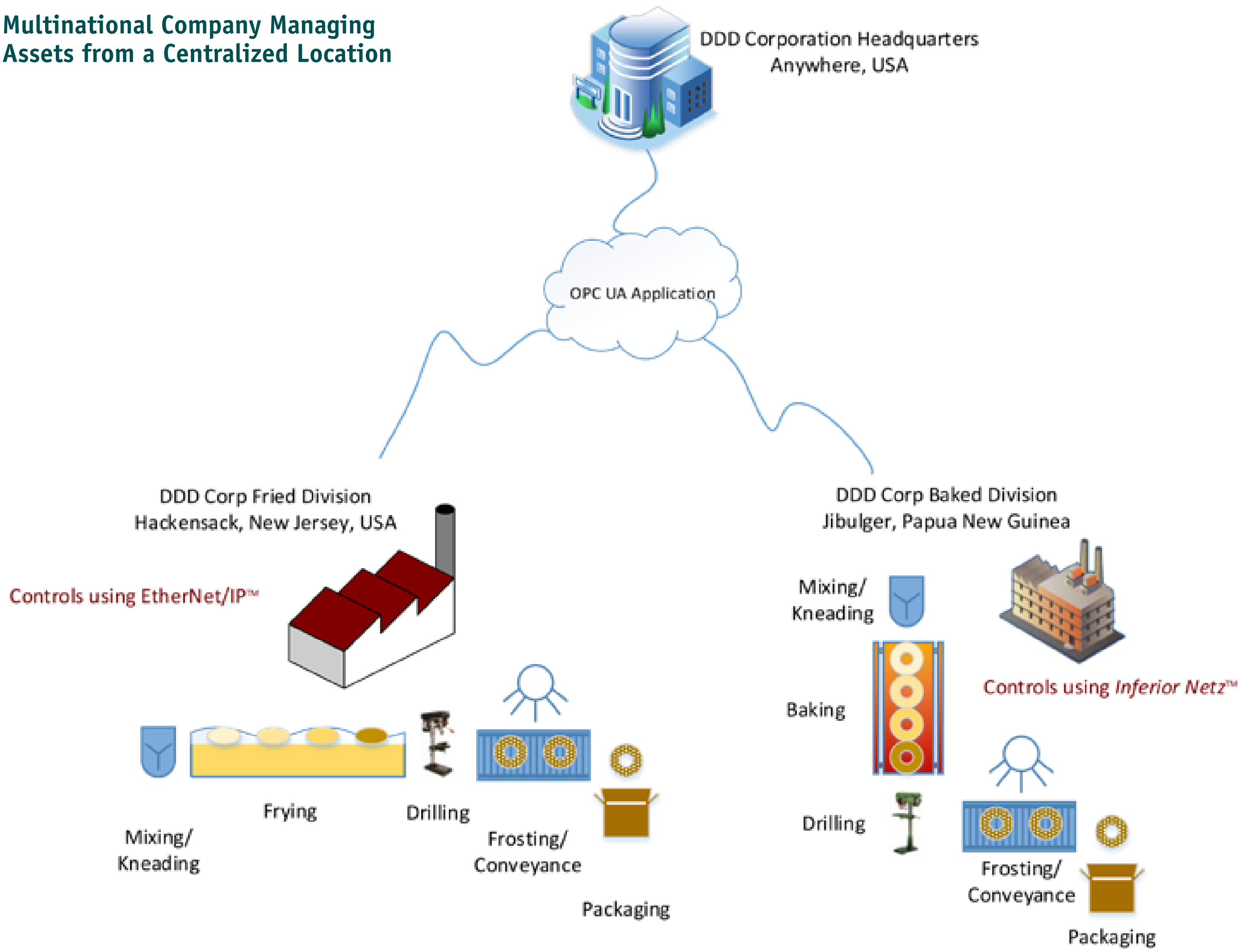
Let's finish with an example to understand how this model might be used. The Downright Delicious Doughnut Corporation is a multinational company with production facilities around the world.

They buy machines and control equipment locally where their production facilities exist. As such they need to manage equipment from many different suppliers. They want to harmonize their asset management function so that it can be performed and accessed from any location.

The high-level processes at DDD's locations are similar: dough is formed, cooked, drilled (likely the best way to make the holes in donuts), dressed, and packed in continuous batches. Some equipment used at both factories is identical, while other equipment is different. The Fried Division has standardized on EtherNet/IP, while the Baked Division uses Inferior Netz.

The two network technologies use different information to represent the identity

Multinational Company Managing Assets from a Centralized Location



SOURCE: ODVA

of products even for identical pieces of equipment. EtherNet/IP uses the numerical attribute values defined in the Identity Object. Inferior Netz uses all string datatypes with a heavy use of animal names to differentiate products. For both networks there are vendors that produce OPC UA gateway products.

The Quality Assurance department at the Jibulger plant has recently reported uneven baking resulting in raw and burnt donuts that are out of specification. Plant engineers researched the issue and determined that it could be addressed with a firmware update available for the oven. Following this update, product is produced within specifications. When headquarters learns of this issue and resolution, they order the asset management team to find all the firmware updates available for their equipment.

The asset management team maintains a database of all equipment in DDD's facilities using an OPC UA application. The application was built using the Donut Industry Companion Specification (fictional, but certainly needed). That specification defines object types to represent all the equipment used in the donut-making process (e.g., DrillPressType) and those types are built referencing interfaces defined in OPC's Part 100.

The asset management team finds a security bulletin from the drill press vendor indicating that attackers could change the direction of motion during operation. This attack would lead to imperfect holes of varying sizes. The remedy is a firmware update from the vendor. This vendor uses EtherNet/IP controls and has identified the affected products using the Vendor ID, Device Type, Product Code and Revision. The team first searches the database for this Vendor's products. It uses the Manufacturer property from Part 100.

CIP products will have their numeric Vendor ID mapped to a vendor name. Once all occurrences of this vendor are found in the database, the asset management team can filter for the Device Type and Product Code. Both values are available because the gateway used at the Hackensack plant uses the CIP Companion Specification to incorporate common OPC data with CIP data. All devices are represented with the CipIdentityType which includes both the Identity Object information as well as the Part 100: Devices model.

This demonstrates merging of data from core OPC UA specifications, industry companion specifications, and the CIP object model.

Conclusion

OPC UA continues to gain momentum as a vendor-independent mechanism to collect data. The publication of our companion specification will be essential to help our end users realize the potential of their intelligent devices. This article discussed progress that has been made towards an OPC UA Companion Specification for CIP.

There are still many challenges that need to be addressed like offline and online representation of all the data a device has to offer, metadata that fully describes CIP attributes, handling of complex data and services, and adoption of the UAFX asset model. All these issues still need to be investigated to achieve a feature rich solution that satisfies all the use cases we envision. The material we have today provides good coverage for many asset management functions and will provide immediate benefit if released as a first version while we continue to develop the model to cover more diverse use cases.

*Gregory Majcher, Principal Engineer, **Rockwell Automation, Inc.***

Learn More

12 time-tested principles for architecting EtherNet/IP systems

Learn what every control engineer needs to know about constructing properly engineered Ethernet/IP control networks. Excerpts from a new book offer a resource and insights into proven technologies, architectures and recommendations for designing and deploying EtherNet/IP control networks on the factory floor.

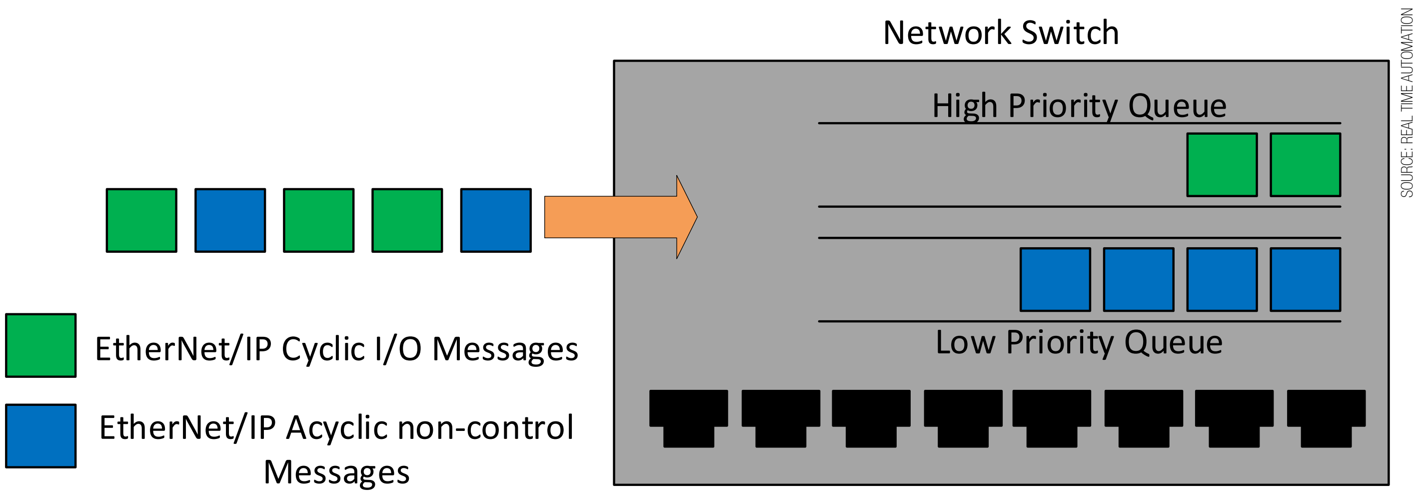


Figure 1 - Priority 0-3 form the lower priority and 4-7 form the higher priority.

WHILE NOT OLD, ETHERNET/IP CAN CERTAINLY be labeled "mature." The specification was first introduced over 25 years ago, and the first EtherNet/IP conformed product left the ODVA test lab a little more than 20 years ago this year. Since then, tens of thousands of words have been written detailing the inner workings of the protocol, and thousands of EtherNet/IP control systems have been deployed across the globe.

The majority of these reliable and well-functioning control systems are the product of testing and experimentation: tweaking what's worked in the past, testing new functionality and experimenting with new infrastructure.

Until now, no one has attempted to collect and document the best practices for deploying effective and reliable EtherNet/IP control systems. The EtherNet/IP specification from ODVA is a descriptive, not a prescriptive specification. For example, network designers will find that the specification does not specify an architecture for the underlying Ethernet network. There are numerous types of Ethernet networks that fit within the boundaries of the ODVA specification, but many of them would be inappropriate foundations for EtherNet/IP control traffic exchanges.

A new book, *The Everyman's Guide to EtherNet/IP Network Design*, fills this gap and details 12 specific guidelines an EtherNet/IP network designer should use to create practical, optimized and reliable EtherNet/IP control systems. It is a unique resource of proven and time-tested technologies, architectures and recommendations control engineers can use to design and deploy EtherNet/IP control networks on the factory floor.

To provide a snapshot of what this book encompasses here are two, highly abbreviated, segments of our recommendations.

Recommendation 3: "Control System Messages Get Priority. Period!"

The most important traffic an EtherNet/IP control system conveys is control signal traffic. Control traffic should preempt any non-control traffic. The impact of even momentary traffic congestion on an EtherNet/IP network could be significant and should be minimized. Non-control traffic, even network management traffic, should defer to control system traffic on an EtherNet/IP control system network.

The foundation for an EtherNet/IP network is an Ethernet network, which is also the foundation for most current IT networks. Because they share the same foundation, some facilities try to mix more traditional IT traffic with control signal traffic on an EtherNet/IP network. That creates the possibility of contention and/or congestion on that EtherNet/IP network.

Contention (access to the network) is easy to avoid by never using shared network infrastructure devices (Ethernet hubs) and always using full-duplex communication. Congestion occurs when multiple messages need to be simultaneously transmitted over the same link. There is a brief message transmission delay while one message is temporarily stored in the outgoing message queue of a switch waiting for the transmission of the other message to complete.

Congestion is managed using priority. The priority of an Ethernet message is indicated by the value of the priority field in the Ethernet frame. There are eight possible priority values, with 0 indicating the lowest priority and 7 indicating the highest priority. These priorities are mapped to specific message queues in a switch.

Two priority queues are sufficient for EtherNet/IP networks: high- and low-priority. EtherNet/IP implicit message traffic should get assigned to the high-priority queue. All other traffic should be assigned to the low-priority queue. No exceptions.

Recommendation 9: "Right Size Your EtherNet/IP Network."

Right sizing means properly architecting the broadcast domains of both the Ethernet network as a whole and the EtherNet/IP TCP/IP subnetwork that is superimposed on that Ethernet network. The broadcast domains for each are not necessarily congruent.

It is only when devices certified by ODVA to conform to CIP and the EtherNet/IP specifications use a portion of an Ethernet network to exchange CIP communications that we have in an EtherNet/IP network.

An Ethernet network where most of the traffic is not EtherNet/IP traffic is not classified as an EtherNet/IP control network. An Ethernet network containing non-EtherNet/IP devices is a blended network and is also not an EtherNet/IP control network. Blended networks are strongly discouraged for machine control systems.

Right sizing an EtherNet/IP network means architecting an EtherNet/IP network to exist on its own subnet, with its own broadcast domain(s). It means deploying an EtherNet/IP broadcast domain such that all broadcast traffic is only delivered to the EtherNet/IP network devices that conform to CIP and EtherNet/IP specifications.

The network in Figure 2 is such a network. It consists of two production system switches with a number of controller switches, each having a PLC and a linear I/O network. A VLAN limits the broadcast domain to just the I/O devices on the linear network. Another VLAN connects all the PLCs, HMIs, and other operational devices across each system zone.

There are many advantages of this architecture, including line speed I/O communication, identical I/O device addressing, easily transportable logic programs and low resource devices that only see address resolution traffic from other I/O devices. The VLANs are architected very specifically to restrict broadcast traffic to the individual I/O networks, to restrict broadcast traffic to the controller network and to restrict corporate broadcast traffic to the corporate network. Class C networks are purposely selected to simplify device troubleshooting, training and easy sharing of PLC programs.

Right sizing an EtherNet/IP network means architecting it for the optimal size of the control system applications that it supports, limiting the broadcast domain of the EtherNet/IP network to the control network devices, excluding devices that are not part of the EtherNet/IP control system and organizing the devices to achieve optimal efficiency and reliability of the EtherNet/IP control system.

Other recommendations include:

- *Use Fully Switched, Full-Duplex Ethernet:* Architect EtherNet/IP control networks so that there is no possibility of contention between devices for access to the control network.
- *Maximize Control Traffic Throughput:* Architect an EtherNet/IP Device Network to Minimize Control Traffic Transmission Delays.
- *Use Unicast Communications:* Unicast traffic is the better choice for EtherNet/IP network traffic. It is far superior to both Broadcast and Multicast communications. Unicast traffic comprises most of all EtherNet/IP network traffic.
- *Implement Redundancy Only When Needed:* Only implement redundancy mechanisms where and when the expected value from implementing them exceeds the costs associated with implementing them.
- *Continuous Monitoring of EtherNet/IP networks:* Continuously monitor an EtherNet/IP network behavior to improve network performance and decrease response times to network disruptions.
- *Use One Exclusive Plant Backbone Connection:* Architect an EtherNet/IP control network so that there is a single connection between the control system and the corporate IT plant backbone.
- *Define a Well-Architected Address Space for EtherNet/IP Devices:* A well-architected EtherNet/IP address space is easily understood and explain-able to plant team members. It is an address space that is easily implemented without extraordinarily complicated router and switch configuration. And it is an address space that is easily maintained by a controls department.
- *Properly Manage VLANs to Optimize Network Performance:* Define logical networks to segregate traffic and ensure that Ethernet broadcast and multicast traffic stay within the VLAN boundaries and that any unicast Ethernet traffic can't be switched but must be routed between VLANs.
- *Make Your IT Department an Ally Not an Enemy:* The problem between the IT and Controls groups is two very highly professional organizations that have good intentions but are separated by common objectives.
- *Use Linear Network I/O Properly:* EtherNet/IP network architects should use the 7 "rules of the road" when using embedded switch technology and linear networks in EtherNet/IP systems.

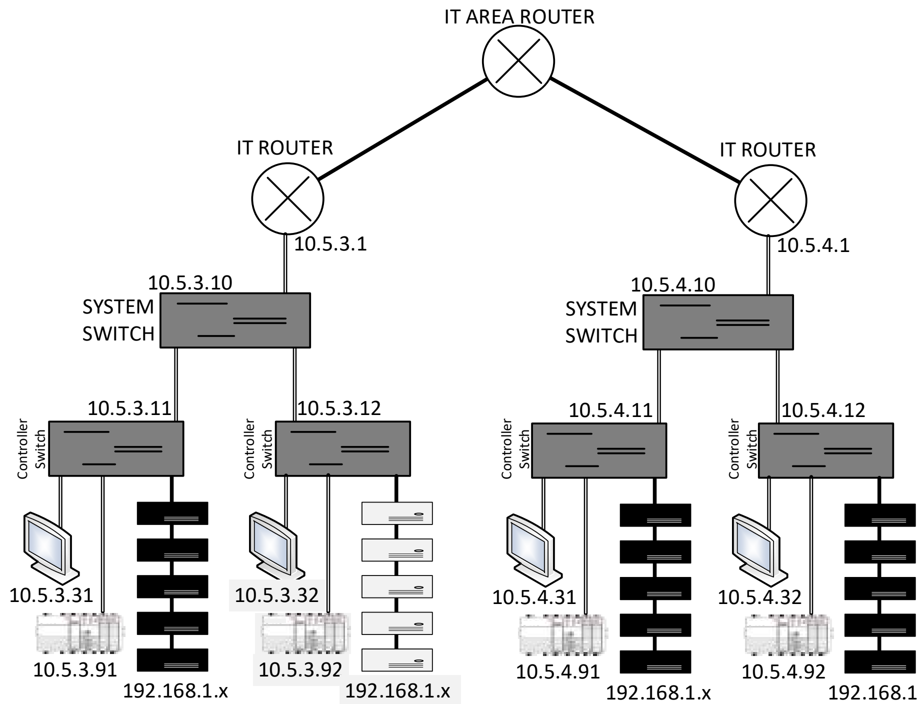
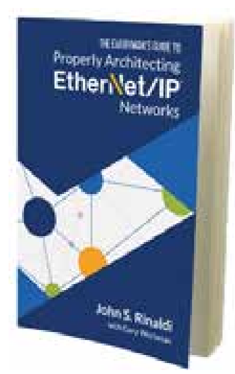


Figure 2 – Production zone with four EtherNet/IP control networks.

Get a Free Book



To learn more about these recommendations and building effective and reliable EtherNet/IP control systems, you can get the book, The Everyman's Guide to EtherNet/IP Network Design, using the link below.

Fifty (50) free books are available to the readers of this publication. Simply click on **www.rtautomation.com/IEB/freebook** to get the book at no cost.

John Rinaldi is Chief Strategist and Director of WOW!, ***Real Time Automation (RTA).***

Gary Workman is a coauthor of the book. Gary led much of the effort to identify and codify into practice the principles GM used to architect hundreds of reliable EtherNet/IP control systems at GM plants around the world. Each recommendation is followed by a "Gary View", containing a personal, sometimes acerbic, story from his days fighting the GM IT department.

Request Free Book

Commissioning cabling infrastructure for OT networks

Fieldbuses are in decline. Industrial Ethernet is now estimated to be more than 60% of newly installed nodes and SPE/APL are rolling out to wire the remaining edge devices. Review your organization's internal standards for the network physical layer, and specify the latest norms for Industrial Ethernet.

ALL ETHERNET APPLICATIONS REQUIRE THE transmitted data to reach receivers without excessive loss of signal or interference from electrical noise. If the signal-to-noise ratio is too high, applications like EtherNet/IP™ will not function correctly, and data may be lost or require re-transmission.

By employing good commissioning practices, one can ensure that the cabling installation will support traditional Ethernet physical layer requirements like 100/1000BASE-T as well as Single-Pair applications such as 10BASE-T1L and Ethernet-APL™.

This article describes key aspects of a quality commissioning practice:

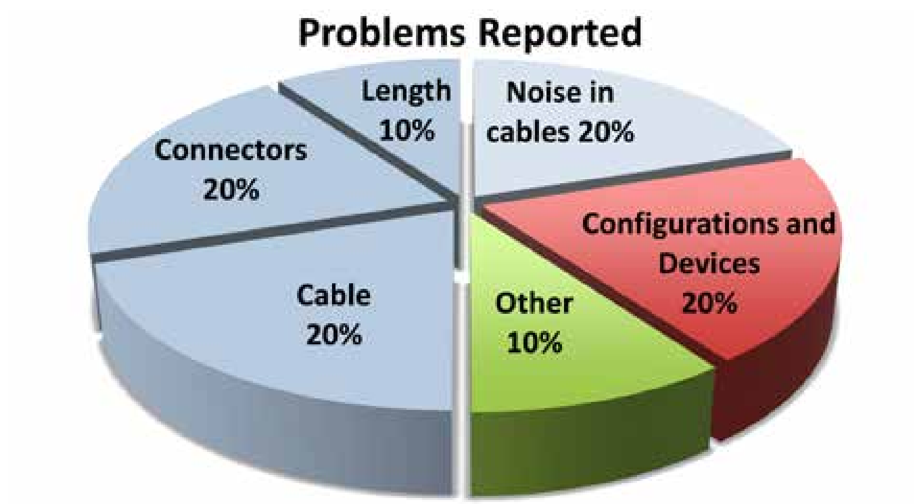
- standards for specification of OT network wiring systems including power delivery
- common network topologies and wiring practices
- specific commissioning tests for point-to-point links to identify non-compliant cable or connectors, as well as workmanship issues
- measurement properties and associated industry standards for physical infrastructure
- and re-purposing legacy fieldbus cabling for Industrial Ethernet

Current context for industrial cabling infrastructure

Market research data provided by HMS Networks indicates that new installations of all types of fieldbuses are in decline, and wireless installation rates are stable, The Industrial Ethernet market share has reached 64% of all new installations, up from 59% in the previous year. Note: EtherNet/IP and Profinet are the dominant Industrial Ethernet variants with 17% market share each.

Recent research conducted by Fluke Networks (a business unit of Fluke Corp.) has found that greater than 50% of problems operating Industrial Ethernet can be traced to cabling problems. Data for the study came from reviewing industry reports, interviewing facilities staff, controls engineers, equipment manufacturers, and system integrators. The research covered a broad mix of primary users, systems, and industrial network types.

This finding is also corroborated by recent findings of the International Society of Automation (ISA) where more than half of failures in the industrial network were found in the data-link and physical layer.



Results from Fluke research.

What follows is a short list of the most common defects:

- Wrong cable used for the application
- Needed to re-terminate cables on-site (too long)
- Cables damaged during installation or operation
- Connectors wired incorrectly
- Wire-pair separation causing noise ingress
- Poorly bonded cable shielding

The potential downtime from these types of defects directly affects OEE and can be costly for the end user. Our experience, and that of our partners in the cabling industry, shows that plants with best-in-class OEE (those at the 90%+ level) do more planning, specification, and testing for data-link and physical layer reliability.

Put another way, if one doesn't baseline the performance of the original cabling installation, one won't know the capacity of the system to grow or support future upgrades. This is especially important when you consider the likelihood that the active hardware in the network will typically be replaced 4x over the life of the cabling.

In summary, installation of Ethernet connected industrial devices are increasing along with the need for more real time data. Using a disciplined approach to planning and deploying the network physical layer can reduce risks and improve long-term process reliability. System baseline testing will improve your knowledge of the system capacity and workmanship, and leads to reduced troubleshooting costs for both for the system integrator and those responsible for system maintenance and future upgrades.

Standards for specification of OT network wiring systems

Network Physical Layer standards defined by the Telecommunications Industry Association (TIA)

TIA is recognized across multiple "premises" by IT organizations in North America as the standards making body for network design and deployments. If you are sitting in a commercial building today your network is extremely likely to be distributed following the commercial standard – accordingly data centers, healthcare and Industrial premises also have unique standards. These standards make systems consistent, predictable, and easier to manage the changes needed to accommodate growth and improvements in the network.

The primary TIA standards for Information and Communications Technology (ICT) are found in the TIA/EIA-568 series. This group of cohesive standards defines copper and fiber optic cabling types, distances, connectors, cable system architectures, cable terminations, installation requirements and methods of testing installed cable. And perhaps most importantly, they define cabling transmission performance and noise immunity necessary to assure reliability in the various premises. In all cases the TIA standards define cabling and infrastructure in support of IEEE 802.3 Ethernet (LAN, MAN).

The TIA standard most relevant to OT networks is the TIA-1005-A standard for industrial premises. This standard is referenced directly from the 568-series parent documents and concerns itself with specific differences necessary for industrial applications. Specific examples being:

- Additional cabling transmission performance and noise immunity requirements
- Requirements for utilizing the M12 connector form factors
- Allowance for greater number of connectors per channel (max. 6 connector channel)
- Definition of MICE component ratings (Mechanical, Ingress, Chemical/Climatic, Electromagnetic).

TIA standards are also largely harmonization with the IEC and ISO standards bodies in Europe. Nearly all of the concepts and requirements described so far are also found in ISO/IEC standards.

Network Physical Layer standards defined by the ISO and IEC

Much the same as TIA standards, the ISO/IEC standards define cabling, infrastructure, and management in support of IEEE 802.3 Ethernet (LAN, MAN). The primary standards for Information and Communications Technology (ICT) infrastructure are found in the ISO/IEC 11801 series. Like the TIA standards this series defines copper and fiber optic cabling used across multiple "premises".

The primary standard applied to industrial premises is ISO/IEC 11801-3 which should be specified in support of any of the primary industrial Ethernet protocol types (e.g. Profinet, EtherNet/IP, Modbus-IP). Other standards of interest, but not necessary for commissioning practices, are the IEC 61784-1 & -2 fieldbus profiles. Of special interest are the Real-Time Ethernet communication profiles (RTE) defining solutions that are able to run in parallel with other IEEE 802.3 based applications.

Three additional ISO & IEC standards that have particularly useful guidance and specifications for commissioning are:

ISO/IEC 14763-2: defines planning, installation, and acceptance testing of 11801 standards compliant infrastructure

ISO/IEC 14763-3: specifically defines testing of optical fiber cabling

IEC 61918: defines installation of communication networks in industrial premises. IEC 61918 is specific to the installation of cabling within and between the automation islands. It deals with the roles of planner, installer, verifier, acceptance test personnel, and gives comprehensive guidance.

Environmental elements and severities

Mechanical	M_1	M_2	M_3
Ingress	I_1	I_2	I_3
Climatic	C_1	C_2	C_3
Electromagnetic	E_1	E_2	E_3

SOURCE: FLUKE ELECTRONICS

M.I.C.E. levels.

Network topologies and wiring practices

The universal TIA model (see graphic on next page) includes naming the parts of a network cabling system. This is a physical infrastructure model for cabling and connectivity design that is flexible and scalable.

Conceptually it starts at the bottom where "EO" indicates an equipment outlet. Then there are two, and sometimes three sets of patching systems or "distributors" on the way up to the network core at the top. From the bottom up these are depicted as "DA" (Distributor A), "DB" (Distributor B) and "DC" (Distributor C). Distributor C is the link patching that is collocated with the actual network core equipment.

In actual practice, cabling subsystems also start at the bottom and move up toward the network core. The collection of links that connect the edge-equipment outlets is "Cabling Subsystem 1", then moving up you have Subsystem 2 (intermediate distribution) and Subsystem 3 attaching the network core. Within the distributors are where the patching interconnects occur (a.k.a. cross-connects).

This provides a testable and scalable plant floor cabling infrastructure that lends itself to good commissioning practice and testability for any incremental moves-adds-and-changes.

You will also notice the model is quite flexible, allowing structured cabling to be implemented across various network topologies that often include fail-over redundancy. One can see that different portions of the network may have multiple cabling subsystems or none at all (like the EO third from the right).

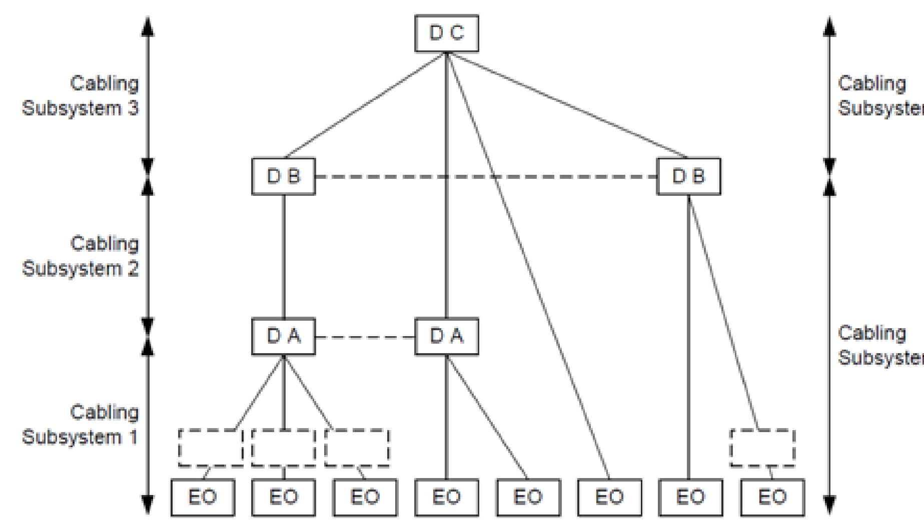
The example on the far right side of the diagram, with only one distributor between the equipment outlets and the core, just implements Subsystem 1 and 3. Also note that Subsystem 1 is usually copper media and Subsystems 2 and 3 are usually some kind of fiber optic medium. The reason fiber links are often broken into two subsystems is that these could be very different kinds of fiber links (e.g. single-mode, multi-mode, or trunked fiber) depending upon distances and environments in the plant.

The TIA 1005-A is a premises standard for the industrial building, and we can describe directly where that structured cabling model fits within the typical Plantwide Ethernet Levels.

At the top of the Manufacturing Zone, network Level 3 corresponds to structured cabling Subsystem 1. Level 2 Distribution Frames or intermediate distributors (switches on the plant floor) correspond to structured cabling Subsystem 2. And the Levels 1 and Level 0, industrial switches in the Access Layer, in turn correspond to structured cabling Subsystem 1. The later are typically deployed in control panels or within network zone enclosures in the Cell Area, automation island, or on-machines.

One final consideration when implementing structured cabling topologies like TIA 1005-A are the M.I.C.E. level considerations. Whatever particular path one may be on, it's going to be important to take a look at updating how the plant is laid out for future growth and apply the standards appropriate to the various environments.

Most quality cabling suppliers provide suitable guidance about products rated to withstand the severity associated with the M.I.C.E. elements. Keep in mind that environments may change over time, and one should allow consideration for the worst-case use in a particular area. It's also possible to use the M.I.C.E. concepts, and product guidance, along with the structured cabling



SOURCE: FLUKE ELECTRONICS

Structured cabling for industrial premises

approach, to control costs. A specific example is to utilize commercial-grade components as much as possible in the M.I.C.E. Level 1 environments.

Installation testing practices

Let's start by describing why we test cabling during the commissioning process. The world has almost 30 years of network testing experience now (both IT and OT). These tend to be the major motivations for testing:

To be sure that the installed cabling has the performance the customer is paying for and is free of defects.

An untested cable is a source of uncertainty. The cabling may appear to be working, but does it have the margin for continued reliability? Can it support growth in the network and modernization of the edge devices?

Experience has shown that tested networks: reduce New Machine Start-up Time (one can eliminate the cabling as the source of any start-up errors); reduce CRC/FCS errors that lead to re-transmissions and latency problems (RTE); reduce intermittent production down-time due to material defects or workmanship; and have a longer service life due to verified design margins. And if you are an installer or machine builder, it helps you get paid faster and leads to higher customer satisfaction.

It then becomes important to specify installation testing. As an example, ODVA has required cabling performance tests for some time now (EtherNet/IP Network Infrastructure Guide – ODVA Pub 35).

"Each cabling segment (consisting of cable and connectors) must be tested to confirm that, after installation, the segments all conform to The EtherNet/IP™ Specification* for performance." (*The CIP Networks Library, Vol. 1 and 2)

Including standards references for TIA 568, 1005-A, and 1152-A (or ISO/IEC 11801 and associated installation requirements) in any bid specification for materials and installation is key to getting the necessary assurance from the commissioning process.

Returning to the TIA model and the definitions for a cabling subsystem; the testing methods are defined within the TIA 568 series common standard – TIA 568.7-C for copper cabling and TIA 568.3-D for fiber optic cabling. Cable installation testing is typically be done just prior to commissioning stage in most projects. Channel testing that verifies cable and connectors should be done at each cabling subsystem level. This includes Subsystem 1, the field Level 1 & 0 connections.

Modern hand-held cabling testers, in use today, demonstrate varying levels of simplicity, sophistication, and basic accuracy. At the simple end of the spectrum are testers that perform wire-tracing, length measurements, and indicate a pass/fail result for transmission at some maximum data rate. These testers are very useful but are not sufficient to demonstrate conformance to standards or to calculate system margins.

At the more sophisticated end of the market are testers that perform full frequency analysis with high accuracies which are capable of guaranteeing standards compliance. These higher-end testers typically employ a graphical user interface and features to aid more detailed trouble-shooting for any failed links. The testers typically come pre-programmed with the necessary standardized tests and associated pass/fail criteria and are fairly intuitive to operate.

Some can even be remotely configured by project managers, in advance of commissioning, to assure all specified tests are applied correctly. In all cases the test results can be saved and used to document the system baseline performance.

Standards-based measurement

Here we will describe the standardized parameters that need to be measured to assure long-term system performance. The capacity of a cabling system to support high-speed data is based on measurements of signal and noise. Continuity testing, or wire-tracing, while necessary, is not sufficient assurance for even the slowest Ethernet. Signal strength, or loss, is measured as attenuation; a.k.a. Insertion Loss. Noise is measured with two parameters, NEXT and Return Loss. Putting these measurements together one gets a total picture of the Signal to Noise Ratio (SNR). The greater the frequency where we can maintain a positive SNR, the faster and farther our devices can communicate.

Wire-tracing or Wire-map Testing

Typically an automated test to sequentially check the continuity of all wire-pairs and the correct isolation of all combinations of wires and wire-pairs. Test results are typically straight forward. Wire-map testing is typically accompanied by cable length measurements as well as resistance measurements of the wire-pairs and individual conductors, both of which can cause a test failure for certain standards. All are quite important for the implementation of PoE power delivery.

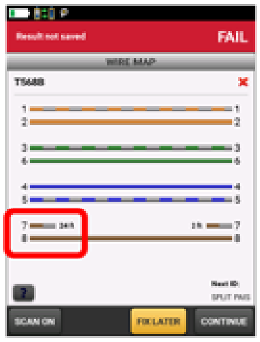
Signal Strength – Insertion Loss Testing

Insertion Loss is measured in units of decibels (dB) and indicates the signal loss down the cable into a calibrated load. Signal Loss will typically increase with cable length, transmission frequency, and ambient temperature. Note that the various communications data rates have different frequency and signal strength requirements (e.g. Gigabit Ethernet requires an upper test frequency of 100 MHz, 10 Mb single-pair Ethernet only 20 MHz). It is most prudent to choose a cabling category for the maximum application speed and then test the cabling to those performance minimums. This will guarantee the worst-case transmission performance. The cabling category is easily specified in the tester.

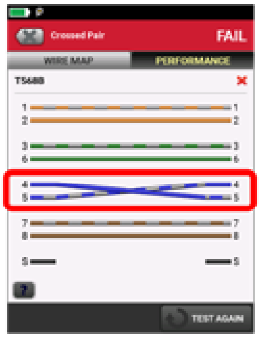
Noise – Return Loss Testing

Return Loss is also measured in units of decibels (dB) and indicates the reflected signal on a single wire- pair; a kind of echo if you will, that cannot be avoided in practical applications. The name Return Loss sounds like an attenuation measurement i.e. a signal loss measurement.

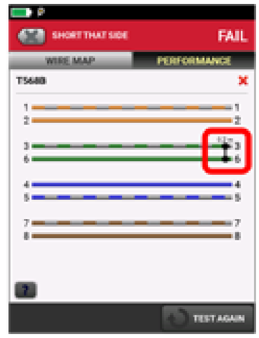
However, it's the actually the level of reflected transmission energy in the cable that shows up as noise in the receivers after reflection. So high amounts of loss are a good thing, because it's a loss of reflected energy noise). Low Return Loss can be found due to defective or damaged cabling, wire-pairs being separated, water in the cable, and sometimes just choosing the wrong cabling with incorrect impedance characteristic.



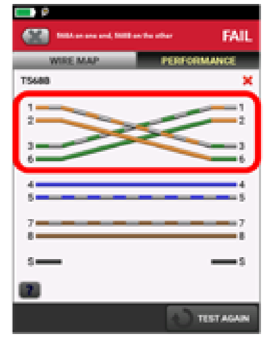
Open Pairs



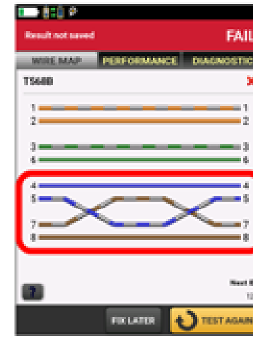
Flipped Pair



Short



Crossed Pairs



Split Pair

Noise – Near-end Cross-talk (NEXT) Testing

NEXT, also indicated in dB units, is a measure of unwanted signal found on another wire-pair when a test signal is applied to an adjacent wire-pair. (see Figure 8.) Put simply, Near-end Cross-talk is the measurement of noise coming from the other pairs within a multi-pair cable. (Obviously, this does not apply to single-pair cables.) NEXT noise is increased by some connector geometries and pin configurations, defective or damaged cable or connectors, untwisting wire-pairs, or just choosing the wrong category of cable or connectors.

SNR - Attenuation Cross-talk Ratio (ACR) Testing

ACR is a derived parameter, displayed in units of dB, and indicates a signal-to-noise ratio of a given pair. ACR values are obtained by subtracting insertion losses from cross-talk measurements across the frequency range of interest. It is typically measured at the near-end and the far-end of a cabling channel. Higher ACR values on a cable at higher frequencies will support faster communications. Therefore higher category cable has more stringent requirements.

Shield Integrity and Cable Balance (TCL) Testing

CRC errors can slow down or even crash a network. These errors occur when data packet checksum values generated by transmitting devices don't match those calculated by the receiving device. The network operator may not know they are happening. Devices will 'throw out' a defective frame and re-try many times. A few bad frames can cause some machines to shut down, and this is especially true for high RPI applications. These errors can be caused by internal noise products or external interference. The possibility for external interference is why we want to recommend these last two test types.

Susceptibility to electromagnetic interference (EMI) can also be tested during acceptance testing. Cabling is designed to meet certain noise rejection characteristics, and some of these parameters can be tested after the cabling has been routed, pulled, and terminated. These tests are not required by standards, they likely take just one or two seconds of extra test time during an auto-test, but they are well worth it.

Shield Integrity testing measures the shield continuity on shielded network cabling. However this is not a typical DC continuity test. This is a radio-frequency test of the shielding all the way through the link regardless of any grounding connections presented along the way. If the shield does not follow the path of the cable along its entirety an open shield will be reported.

Twisted-pair Ethernet cable is inherently balanced and differential mode signaling takes advantage of this characteristic to reject common-mode noise, like EMI. When common-mode noise is coupled equally onto the two conductors in a perfectly balanced twisted-pair, very little energy will be detected by the differential receiver. This is called common-mode rejection. Well-constructed and properly installed cabling will reject EMI to a high degree. However, installed balanced twisted-pair cables are never "perfectly" balanced, which is why we have test parameters for balance specified in industry standards.

The two balance measurements that indicate noise rejection performance are Transverse Conversion Loss (TCL) and Equal Level Transverse Conversion Transfer Loss (ELTCTL). In field testers these are implemented as optional choices for an automated commissioning suite.

Re-purposing legacy cabling for Industrial Ethernet

Here we must confine our conclusions to Single-Pair Ethernet and the use of existing controls cabling (I/O), which is also single-pair wire. IEEE 10BASE-T1 (10SPE) popularly known as Single-Pair Ethernet was designed to take advantage of existing low-voltage wiring. (It must be balanced twisted-pair of course.)

However not all field bus cabling was designed with the frequency range and performance required for 10SPE, and even if it was, and it functions fine for the current use, wear-and-tear, workmanship and terminations must be considered before connecting new Ethernet devices. The use of shielded wiring and/or well-balanced cabling being chief among them, especially where MICE considerations must be taken into account. (Examples being; long runs in open space and cabling densely packed in closed spaces or near higher voltages, motors, VFD, etc.)

That said, there is much potential for high quality, recent vintage, control cabling to perform well for SPE traffic. The quickest and most certain way to tell is to test it. Certification tests provide high accuracy, total parametric coverage, and the highest level of assurance. Verification tests typically cover less parameters, have slightly reduced accuracy, but provide reasonable assurance. Also one doesn't necessarily need to test every link under consideration. Statistical sampling is recommended for reuse of large populations of cabling (given that the supplier and age is fairly uniform).

Examples exist in the cabling standards for the use of Statistical Sampling methods. The best example being the ISO/IEC 14763-2 Cabling planning and installation standard recommendations, which are consistent with ISO 2859-1 for the attainment of statistically acceptable quality levels (AQL).

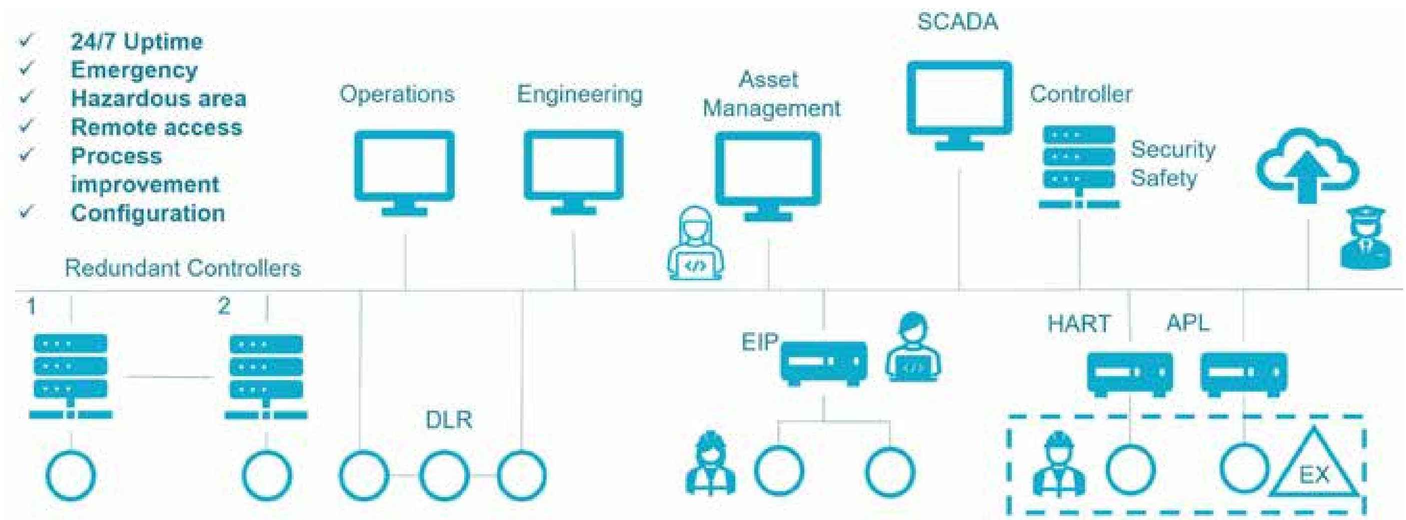
Summary

- Fieldbuses are in decline; Industrial Ethernet is now estimated to be more than 60% of newly installed nodes and SPE/APL are rolling out to wire the remaining edge devices.
- It is recommended to review your organization's internal standards for the network physical layer and specify the latest norms for Industrial Ethernet.
- It is recommended to utilize the M.I.C.E. concept to improve designs and mitigate environmental factors in advance.
- Greater than 50% of problems operating industrial ethernet can be traced to cabling problems.
- Assessment tests are a recommended best-practice that can catch common defects and provide greatest assurance over the lifetime of the network.

*Theodore Brillhart, Technology Director, **Fluke Electronics Corp.***

Process applications framework using CIP technologies

Advanced Physical Layer (Ethernet-APL) is gaining attention due to the opportunity it presents to extend the reach of EtherNet/IP into areas in which Ethernet has not been deployed. However, this is just one of several areas where development is taking place to facilitate the use of EtherNet/IP in process applications.



SOURCE: ODVA

Typical EtherNet/IP process automation network architecture.

THE USE OF THE ETHERNET COMMUNICATION technologies has become significantly more prevalent in recent years, with market share data indicating that EtherNet/IP is one of the market leaders. Although EtherNet/IP has been adopted by a broad range of industries, it is recognized that the process industries are an opportunity for growth.

The term "Process" encompasses many different industries, from applications in the Life Sciences, the production of oil & gas, chemical manufacture and the treatment of Water and Wastewater. These industries all have different needs and priorities. These industry sectors in turn will have their own characteristics and requirements. Whilst a skid for producing pharmaceutical reagents may share characteristics with a packaging machine, a refinery is likely to have its own unique requirements. For example, the physical characteristics and size of a refinery or chemical plant is likely to lead to automation components that are separated by long physical distances. This type of application is likely to take additional measures to avoid the risk of explosion.

Regardless of the industry, what differentiates process applications from discrete applications are relatively slow control loops, and update rates between devices that can be on the order of 100's of ms. The impact of this is that the performance demands on EtherNet/IP target devices is lower than applications in the discrete industries. In contrast, the scale of some process applications means that scanner class devices may have additional demands in terms of the number of connections.

In general terms, although this means that devices developed in the discrete industries can also be deployed in process, the environment in which they are deployed, and specific application needs drive an additional set of requirements that are needed to facilitate the use of EtherNet/IP devices in these industries.

Initiatives such as the Advanced Physical Layer (Ethernet-APL) are gaining significant attention owing to the opportunity it presents to extend the reach of EtherNet/IP into areas in which ethernet has not been deployed previously. However, this is just one of several areas where development is taking place to facilitate the use of EtherNet/IP in process applications.

This article provides an overview of the state of the industry, documenting areas where the state of the CIP and EtherNet/IP technologies are mature enough for adoption and identifying areas where additional effort is needed in order to facilitate the use in real applications.

Personas

To illustrate how process applications are designed, installed, used, and maintained, we will define a number of Personas:

Cassie: A Control Systems Engineer. Cassie has a background in traditional automation concepts, and has experience with controllers, instrumentation and actuation. She also has experience with fieldbuses such as ControlNet but has had limited direct exposure to IT herself. She is well aware of the need for IT and OT personnel to collaborate – as a prerequisite for delivering the converged architectures needed for contemporary digital manufacturing solutions.

Edward: An Instrument Engineer with responsibility for selecting instrumentation to meet the needs of the process.

Isabelle: An Instrument Technician who has to maintain a broad variety of instruments from a number of different vendors.

Ned: A Network Engineer who spent the first part of his career supporting network infrastructure for a software development company. He chose to move into manufacturing in order to take on a fresh challenge. He has a good understanding of networking as applied in IT but is developing his knowledge of the operations domain.

Sam: A Security Architect. Like Ned, he has a background in IT, but with the increased convergence of IT and OT, he now has responsibility for ensuring that the complete installation follows industry best practices. His job is to ensure that all aspects of the facility are designed in a way that ensure the key requirements of Confidentiality, Integrity and Availability are all met.

Facility Design

Cassie has been tasked to create a process plant network that fulfills the following requirements:

- 24/7 uptime for the highly available part of the process.
- Protection from an emergency event for the critical system operators.
- A hazardous area for both new and legacy devices.
- Remote access to the system for troubleshooting.
- Access to process data for process improvement analytics.
- Simple set up and configuration of instrumentation

Cassie knows about controllers and instrumentation but is not as knowledgeable about network security and topologies, so she elicits the help of two IT professionals from her company - Ned, the Network Engineer and Sam the Security Architect. Cassie has experience with ControlNet, so she turns to other CIP technologies to meet her needs.

To learn more about CIP technologies, Cassie attended a workshop where several of the technologies were described. Cassie learned that device profiles are standardized collections of CIP objects that allows similar device types from different manufacturers to expose control, configuration and diagnostic data the same way. She also learned that the industry has developed a standardized information model, called PA-DIM, to upload data to the cloud. Cassie is very excited to see how these concepts can be used to fulfil her needs.

SOURCE: FLUKE ELECTRONICS

ODVA technologies are well-suited for process applications but there are areas where work is needed. The includes providing guidance on achieving process safety, further clarity regarding the use of CIP Security to meet industry standards, defining a standard way for managing redundancy and in enhancing the way in which EtherNet/IP devices are configured and managed.

Architecture

As a starting point for developing their architecture, Cassie, Ned and Sam consider ODVA's guidelines for EtherNet/IP Network Infrastructure, Cybersecurity, as well as vendor documentation to create a network.

Controller and Device Redundancy

Looking at the details of the specification, the team notes that the application on which they are working on requires a very high level of fault tolerance. The common mechanism by which this is achieved in process industries is through the use of controller redundancy consisting of at least a pair of controllers (primary and secondary). The most crucial applications can require yet more controllers.

The primary controller operates the input/output (I/O), and it executes control logic and communication tasks. Physical I/O and other smart devices are arranged on one or more fieldbus network for access by both processors. In addition, the primary controller must update or mirror itself to the secondary continuously to ensure that I/O status, memory values, and any program changes are shared between the controller pair. This ensures that the secondary controller is ready to assume control seamlessly if needed.

In the event of a major fault—such as a power failure, rack fault, or processor error the primary controller switches over to the secondary, which should seamlessly continue with operation without any LOC (Loss of Control) or LOV (Loss of View). This action is known as switchover or failover.

Cassie notes that at present, controller vendors have proprietary mechanisms implemented with CIP devices to ensure there is no LOV or LOC during switchover/failover. Techniques used include the use of IP address switching, Gratuitous ARP (GARP) and hold/freeze of process values. With this approach, there is potential for unexpected results as device vendors are not following a standardized mechanism for achieving the switchover from primary to secondary. Furthermore, she notes that some of the devices she wishes to use within her architecture do not support GARP, and therefore a connection loss is experienced when control switches from primary to secondary.

These observations suggest that although redundancy solutions are available, there is a need to standardize the Redundancy and Controller failover/switchover scheme to have seamless integration of CIP devices in process industries – and to achieve full application coverage.

High Availability and Media Redundancy

In line with many process applications, the specification with which Cassie is working with calls for high availability – defined as the ability for the system to tolerate a single failure. Looking initially at the media, Ned notes that a number of options are possible – for example the Rapid Spanning Tree Protocol (RSTP). Cassie points out that although this might work for the connection to the SCADA and the broader plant, the convergence speed of this standard protocol is not sufficient for maintaining a connection between a controller and a device.

Based on this feedback, Ned chooses to implement the Device Level Ring (DLR) protocol. The DLR protocol provides the means to detect, manage, and recover from single faults in a ring-based network. It is intended primarily for implementation in EtherNet/IP end devices that have multiple Ethernet ports and embedded switch technology and allows applications requiring media redundancy to be realized. The protocol provides for fast network fault detection and reconfiguration to support the most demanding control applications. Cassie agrees this is a sufficient approach since the instrument technician staff is readily available to replace any failed device.

One of the ways in which this is achieved is through the use of a protocol such as the Parallel Redundancy Protocol (PRP). From Cassie's experience, she knows that this works well with EtherNet/IP devices because the media redundancy protocol works completely independently of the application.

However, she notes that in many cases, the devices that she wishes to use do not support PRP natively, and that switches with Redundancy Box (RedBox) capabilities are needed to realize the architecture. She feels that being able to purchase more devices with native PRP support would simplify her architectures

Long Cable Runs and Connectivity to Hazardous Areas

Cassie notes that as per the requirements of the facility and there are some parts that need to be located more than 100m from the nearest ethernet switch. Cassie also has to install devices within a hazardous area. Whilst fiber optic cables can be used for the network infrastructure, this cannot be used for connecting to instruments directly as it would require separate distribution cabling to provide power to the devices.

Cassie knows that not every device or switch can be installed in a hazardous area, so she and Ned work together to create a network solution that complies with hazardous area approvals. Cassie finds existing devices that support 4-20mA HART® protocol – in which the transmitters are powered by the control loop. They also identify newly introduced devices that support Ethernet-APL in which the power for the instrument is supplied over the network.

They note the simplicity in using this technology owing to the ability to use existing two-core cable that is already present in the facility. They also note that functionally, EtherNet/IP instruments for Ethernet-APL are identical to other EtherNet/IP instruments. They see that this presents an opportunity to collect information from devices from which the level of diagnostic information had been limited to either a standard analog loop or to what was available over HART – noting also that the move from HART to EtherNet/IP also provided a much faster update rate.

From a network architecture perspective, Ned explains that standard industrial Ethernet switches cannot be used for either type of devices so Cassie and Ned research the types of switches needed and realizes a HART translator is needed to communicate with the 4-20mA HART devices and an Ethernet-APL switch is needed to integrate the Ethernet-APL devices.

They conclude that Ethernet-APL is a advanced technology that has an opportunity to significantly enhance the information available regarding the performance of their facility.

SOURCE: FLUKE ELECTRONICS

The term "Process" encompasses many different industries and types of applications.

Connecting to Legacy Technologies

Cassie is told by her management that part of the installation will make use of a skid that will be transferred from another facility. As she investigates the specifications of this skid, she realizes that it is 20 years old. From her history in the industry, she expects that it might have some ethernet connectivity, but that its capability is likely to be limited. Her expectation is that the instrumentation is likely to be using 4-20mA HART.

Isabelle and Cassie have long recognized the difficulty in using HART instrumentation. Process maintenance teams have long been challenged with gaining access and connectivity to service their lowest-level field devices. Traditionally, plant personnel needed to walk out to the processing area and use a handheld communicator or web server to connect to each device individually – a process that can take hours. This, together with the need for better real-time information on the performance of devices has driven a desire for better EtherNet/IP device connectivity.

Although Cassie would like the skid to be upgraded to use EtherNet/IP instrumentation, her management tells her that she has a limited budget for the integration of the skid. Furthermore, she notes that some of the more specialized devices on the skid do not have an EtherNet/IP equivalent on the market. She notes however that the EtherNet/IP Specification from ODVA defines a standard mechanism for integrating

HART devices into the Common Industrial Protocol (CIP). Using this mechanism, a CIP originator (such as an industrial control system) can communicate with a HART device as if it is a native CIP device. The result is seamless communication between CIP-based devices and HART-based devices, without needing any changes to the HART devices or the CIP originators: from the CIP originator's perspective, the HART device appears as a CIP target device, with CIP objects and with CIP communication mechanisms. However, from the HART device's perspective, all HART commands originate from the Translator in the form of standard HART commands.

In summary, Cassie notes that the ability to use a HART to CIP translator meets the immediate need for integrating HART devices into a CIP architecture.

Meeting Safety Requirements

Safety in process can mean different things depending on the specific industry. The chemical, oil and gas industries all aim to avoid the release of hazardous or explosive substances into the environment. Like the discrete industries, all facilities have a goal of protecting their employees from injury or death.

In the case of the facility being designed by Cassie, the safety specification calls for the use of Safety Instrumented Systems (SIS) as defined by the IEC61511 standard, which covers the application of electrical, electronic and programmable electronic equipment in the process industries.

This requires the components of the system to meet a Safety Integrity Level (SIL) rating. The complete application also has to have a SIL rating. This calculation is based on the ratings for the complete process loop, covering the sensors, control logic and actuators. Cassie is aware that the IEC61511 standard references the IEC61508 for the design of safety components.

She is also aware of the CIP Safety standard. In studying the CIP Safety standard, she sees that it has some useful characteristics: it ensures that the behavior of components in the event of a failure is well defined. She sees that the features of the protocol provides the means to protect against faults arising for the corruption of data, unintended repetition, incorrect sequence, loss of data, unacceptable delays, insertion, masquerading and addressing faults. Cassie notes that it operates at the application layer and uses the black channel principle, meaning that only the end nodes need to be safety certified and that that there is no need to certify the intermediate networking hardware – something which will no doubt be of interest to Ned, the Network Engineer.

However, she struggles to find any guidelines to help her use CIP Safety certified devices in applications that need to be built according to the 61511 standard. She also notes that offerings from vendors are often segmented, with specialized safety solutions being sold as a separate offer to standard DCS systems. She decides to engage a specialized process safety contractor to help her meet the needs of her application.

Security

The specification to which Cassie and Sam are working calls for them to follow industry best-practice for ensuring that their facility is well protected. They have three key goals: to ensure that company assets (recipes and other confidential information) are not compromised, that the integrity of the operation is not impacted, and that production can continue 24 hours a day, 7 days a week. At the same time, they have a requirement for real-time sharing of production information with management elsewhere in the world, and they also need remote access to facilitate maintenance by global suppliers. This need rules out an air-gap system.

Sam is aware that the industry standard for securing OT systems is IEC62443. Like Safety, this defines a number of security levels and they believe that Security Level (SL) 3 – the provision of protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation is a realistic target.

Sam notes that two parts of the standard are most relevant. The 62443-3 standard applies to their installation as users, and the 62443-4 standard applies to the devices that they deploy within the facility. Cassie is also aware of the existence of CIP Security™ – which allows the communication between devices to be secured. They note that there appears to be alignment between the needs of the standard and the capabilities of the devices. Overall, Sam and Cassie feel that as with safety, further guidance is needed to help them navigate the complexity of meeting 62443 certification and in understanding how ODVA technology can help them to achieve this.

Commissioning and Integration

Aside from the architecture, Cassie and Edward are aware of the time it takes for the team to commission and integrate devices into the control system and are looking for ways to simplify and speed up the activity. They note that EtherNet/IP devices are coming on to the market with standardized device profiles. They see these profiles as a way for her programmers to further standardize their interface modules – and allowing the team to concentrate on developing and implementing their core control loops and visualization concept.

Device Configuration & Management

Edward, the instrumentation engineer recognizes that this is an installation with a large number of instruments supplied by a number of different vendors. He has extensive experience using Asset Management solutions to configure instruments and uses the software tools to create backups of the configurations in each device.

Edward works with Isabelle to ensure that all the instruments in the installation are configured correctly and the backup configurations are maintained. However, when Isabelle replaces an instrument, she does not want to have to walk to an Engineering Workstation to restore a configuration. Having spent many years maintaining devices, she prefers to use the front panel of the instrument.

She has a paper notebook where she writes down the parameter settings from the failed instrument (if she can) and after replacing the instrument she enters the parameters from the old instrument into the replacement unit. Her experience has meant that she has a sense for what the parameter settings in an instrument might be, but she does not have the full insight into the functionality of the process held by her colleagues Cassie and Edward.

As they investigate the capabilities of CIP devices, they see that mechanisms exist to facilitate the integration of EtherNet/IP instrumentation into their DCS. However, they are surprised to see that different manufacturers have interpreted the requirements in different ways. Consequently, they find that some devices cannot be added to the control system at all. Other devices can be added but lack the capability to be configured over the network. A third class of instrument can be added and configured but there is little standardization between the interfaces.

They are also surprised to see that there is no equivalent to the Asset Management

Software used by Edward – although they do see that their existing tools can be used over the EtherNet/IP backbone network – and that it has been recognized that a solution based on combining EtherNet/IP with other standards such as FDI can help deliver strong benefits to the user community.

Although they are aware that some DCS suppliers offer some interesting capabilities in terms of device configuration (and in some cases, for device replacement), and they are aware of ODVA's xDS initiative, they note that this latter solution is not yet complete and opt to remain with their existing asset management software owing to the lack of standardization that exists across the devices they wish to use.

Device Maintenance in Use

In her role as instrument technician, Isabelle has to maintain the functional state of the process. Inevitably, devices fail in operation and Isabelle has to replace them.

Her life is made easier when the instruments can report potential problems in advance of failure. Given that she has to support a range of instruments, her work is made easier when problems are reported in the same way. She is tired of every manufacturer designing instruments to report issues using proprietary definitions.

Isabelle airs her grievances to Cassie, and Cassie notes that ODVA has recently published the Process Device Diagnostics object, which is based on the NAMUR NE 107 standard. When instruments implement the Process Device Diagnostics object, the instruments provide Isabelle with a standardized way of reporting instrumentation malfunctions and an indication if a process is operating out of specification. Isabelle can easily see which error reports are failures and need to be acted on immediately and which are less critical and can wait for action.

Isabelle is especially happy when Edward, the Instrumentation Engineer, specifies instruments with the Process Device Diagnostics object implemented. Now all Isabelle needs to do is convince Edward to specify devices that can perform predictive maintenance.

If she had techniques to help determine the condition of the instruments in order to estimate when maintenance should be performed, she would not have to make so many late-night calls due to failed instruments. Her maintenance activities would become much more predictable and she would not waste the company's money on performing tasks that were not warranted.

The team notes that the functionality they need is available in a limited range of devices to date and that their needs will be best met when more manufacturers choose to implement the Process Diagnostics Object.

Device Replacement & Interchangeability

Although Isabelle makes her best efforts to maintain instruments to the best of her abilities and to address potential problems during scheduled downtime, inevitably, there are times when devices do fail during production. Oddly, failures often occur when the facility is operating with a reduced staff – for example at night or during the weekend. Naturally, it is imperative for users to be able to replace failed equipment quickly in order to return to production.

Having worked in different industries, he notes that there are different perspectives on how this scenario should be managed. Owing to regulatory compliance, a life science application will require a failed device to be replaced with an identical unit to align with what has been validated by the relevant regulatory authority. In contrast other process applications do not require the same level of regulatory compliance.

For this scenario, Edward recognizes that the primary need is to allow the on-site maintenance staff to be able to use whatever instrument is available in stores, without having to worry about the manufacturer or backwards compatibility with the firmware version. For example, a pressure transmitter manufactured by Company A fails in the facility, but the maintenance store only has a pressure transmitter manufactured by Company B on the shelf. Edward notes that ODVA is working on a series of device profiles to standardize the data definition within EtherNet/IP instruments.

ODVA recognizes that the user is looking for the ability to work with "whatever works" – in other words, the ability to use an instrument or actuator from any vendor and for it to be integrated into a Control System without anyone having to make any changes to the program controlling the application. The Coriolis Flow profile is an example of the type of definition that is needed in order to facilitate this use-case. Edward notes that the profile standardizes the configuration parameters across similar measurement devices – which Isabelle's commissioning time more efficient.

Overall, Edward and Isabelle note that ODVA offers the capability they need; however, as with maintenance, their ability to use it is limited by the class of device in which it is available as well as the number of devices supporting it.

Compute and Cloud Connectivity

One of the strategic goals that Cassie needs to meet is for continuous process improvement. She is aware that data from the operations needs to be collected for analysis, and that this can be done using compute capabilities either on-site or off-site. She is aware that OPC-UA is becoming a standard that is gaining significant traction for cloud connectivity, and also that work has been done on mapping CIP objects onto an OPC UA Information Model.

Further investigation reveals that a Device Information Model for representing Process Devices has been published. She also aware that ODVA has documented the Use-cases for a CIP Companion Specification for OPC UA and confirms that these are in line with the requirements of her facility. She is also pleased to see that there is alignment between the device profiles and the PA-DIM standard. Overall, she concludes that her needs are well understood and the infrastructure she is selecting will deliver the connectivity she requires, however she also notes that products based on these concepts are not yet available.

Summary

In summary, the process plant network that Cassie was tasked to create had several diverse requirements and Cassie and her team was able to fulfill them by using ethernet as a backbone and CIP technologies where appropriate. They conclude that the state of ODVA technologies allows them to realize the architecture of their operations in the way they see fit.

Conclusion

In conclusion, it is clear that many aspects of a process application can be achieved using ODVA technology today. The fundamental function of exchanging information between sensors, controllers and actuators can be achieved using EtherNet/IP. Features exist that facilitate high availability topologies, full system redundancy, deployment of devices over long distances, installation of equipment in hazardous environments – all with a feature set that aligns with industry best practices. In addition, the integration of older technologies into a CIP based architecture can be achieved with ease. In use, there are means by which diagnostic information can be presented in a standardized way and there is a move towards facilitating the exchange of devices without having to make changes to the control application.

There are however some areas where more work is needed, specifically in terms of providing guidance on achieving process safety, further clarity regarding the use of CIP Security to meet industry standards, defining a standard way for managing redundancy and in enhancing the way in which EtherNet/IP devices are configured and managed.

*Vivek Hajarnavis, **Rockwell Automation**, Dawn Kelsch, **Micro Motion**, Rizwan Mohammed, **Honeywell** and Michaël Voegel, **Endress + Hauser Digital Solutions.***

Visit Website

Powerful, open control automation for “Baumkuchen 4.0” bakery

An ultra-compact Industrial PC uses the power of TwinCAT software to power robot-based cake production, and the "Theo" robot that bakes high-quality Baumkuchen. Theo is also supported by an artificial intelligence (AI) application in the oven that monitors the process and ensures highly precise baking.

SOURCE: BECKHOFF

The process of making Baumkuchen is simple. A rotating core rod is repeatedly coated with raw dough and placed in an oven until 13 layers are evenly baked.

MANY PEOPLE IMAGINE LARGE-SCALE ROBOTS in manufacturing plants, collaborative robots (cobots), and hospitality and care applications when thinking about robots used in Japan. A novel solution for food manufacturing has been unveiled by Juchheim Co., Ltd., a confectionery manufacturer that has been in business for over 100 years.

The "Theo" robot bakes high-quality Baumkuchen. Theo is controlled by an ultra-compact Beckhoff Industrial PC with TwinCAT software and supported by an artificial intelligence (AI) application. The engineering firm Matsuura Denkosha Co., Ltd. provided support during the development of the control system, including the integration of a Denso Wave robot.

SOURCE: BECKHOFF

With PC-based control and AI support, Juchheim can offer pâtisserie-quality “Baumkuchen” layered cake at all its locations.

Founded in 1909 and operating in Japan since 1922, the Juchheim Group, with administrative headquarters in Kobe, runs more than 350 stores in the high-end Baumkuchen segment and is a supplier in Japan and Singapore. Baumkuchen is a German style of layered cake that is also popular in Japan. Ever since the company was founded, the Juchheim confectioners have been baking the delicacy according to the same recipe – without any food additives.

"Baking Baumkuchen requires advanced skills and experience on the part of the confectioner," emphasizes Mr. Matsumoto, Managing Director of Juchheim's central plant. However, if the oven's parameters can be captured and set remotely, and if the baking temperatures can be displayed precisely, Juchheim's pastry chefs can remotely control local machines to produce top-quality Baumkuchen. "With Theo, Juchheim is taking

SOURCE: BECKHOFF

The precise skimming of the dough after applying a new layer of cake also needs to be "learned" via an AI inference.

one step further," said Mr. Yokoyama, a Juchheim consultant. "Through integrated AI and the expertise of master confectioners, Baumkuchen can be made anywhere in the world with the same Juchheim quality." "The idea for Theo originally came from Hideo Kawamoto, the President of Juchheim," adds Mr. Matsumoto.

In parallel with the development of Theo, the company planned the construction of a new building complex with the theme of food innovation – the "Baum Haus" in Sakae, Nagoya. Part of the concept was also a transparent baking studio, which was further developed with Theo into a fully automated Baumkuchen studio.

The perfect 13 layers of dough with PC-based control

The process of making a Baumkuchen is simple in itself. A rotating core rod is repeatedly coated with raw dough and placed in the oven until 13 layers of dough are evenly baked.

Before baking, the dough container and core rod must be transported to the oven and pushed in. This is normally done by operating personnel but can be automated easily using a conveyor belt and robot arm. However, the baking itself requires an expert. Theo replicates the expert's skills with the help of AI. For this unprecedented task, Juchheim selected the engineering firm Matsuura Denkosha as its development partner.

The company not only has expertise in AI, but also extensive experience in the control of articulated robots. "The Baumkuchen plant consists of three Theos, a vertical articulated robot and a conveyor belt that transports the dough containers and rods," explains Mr. Kitano, Managing Director of Matsuura Denkosha. All components are controlled by an ultra-compact Beckhoff C6030 Industrial PC with Intel®-Core™ i7 processor and networked via EtherCAT.

The high-tech bakery installed in the Baum Haus is almost completely automated. All the operator has to do is prepare the Baumkuchen dough and the core rods, and place them on the conveyor belt, select one of the three ovens on the control panel and start the baking process. Then the conveyor belt automatically transports the dough container and core rod to the specified position. The robot picks up the container and rod and places them in front of the oven. Then the robot begins to coat the core rod with dough and apply the layers one by one. The AI functionality implemented in the oven monitors the process and ensures highly precise baking.

Mr. Kitano explains, "The advantage of the Beckhoff IPC and TwinCAT software is real-time process control via EtherCAT and the Windows integration." In this system, TwinCAT 3 PLC controls the conveyor belt, the rotation of the oven, and the opening and closing of the door using EtherCAT drives and motors that are precisely synchronized with the robot's motion.

In addition, the IPC offers high scalability so that Juchheim's own Windows applications can be used as can solutions for remote system maintenance. The I/O components from Beckhoff also play an important role. After all, there are many sensors and cameras to integrate. The compact housing and the wide range of EtherCAT I/Os enabled the system integrator to save control cabinet space and minimize engineering complexity.

AI inference and TwinCAT PLC on a single platform

The AI functionality runs as a Windows application on the same IPC as TwinCAT. "We use multimodal AI technology to monitor the quality of the Baumkuchen," Mr. Kitano points out. For this purpose, high-performance cameras are installed in front of each oven to capture images of the cake surfaces. This data is linked to other sensor data, including those from radiation pyrometers. The AI model is based on a Convolutional Neural Network (CNN), and was previously trained in Python in a separate environment. It is implemented in the standard IPC as a Windows application.

As the number of dough layers increases, so does the diameter of the Baumkuchen. Accordingly, various parameters can vary, such as the distance from the oven wall and the baking time required to achieve a perfectly baked dough layer. It is an extremely delicate process that requires careful monitoring of baking conditions up to removal from the oven at the optimal time, and for the application of the next layer of dough. In addition, the surface of the dough must be smoothed with a spatula to give the Baumkuchen its characteristic cylindrical shape.

Five to six batches of Baumkuchen are usually required for the system to reproduce the expert baking process of a master pâtissier. A batch requires 30 min to bake, so the total time for data collection is about 3 h. "Based on this limited amount of data, it takes about 20 hours to train the AI model, including the

SOURCE: BECKHOFF

Mr. Yokoyama, a consultant at Juchheim (left), and Mr. Matsumoto, Managing Director of Juchheim's central plant, have used Beckhoff technology to cast their master pâtissier's expertise with Baumkuchen into software.

final tests," explains Mr. Kitano.

During operation, Theo checks the image data from the camera and the data from other sensors in real-time to determine the quality of the Baumkuchen: when a dough layer is in optimal condition, it is reported back to the control system. TwinCAT then stops the rotation of the dough tube and opens the door so the robot can remove the Baumkuchen. The total time required from data input into the trained model, including the inference output, until feedback to the control is around 100 to 200 ms. Mr. Kitano states, "This extremely fast response time for AI applications is possible because the AI inference and PLC control are integrated in a single control platform, the Beckhoff IPC."

Another technical challenge is the constant coating of the dough rolls with identical amounts of dough. For this purpose, TwinCAT controls the optimum position and angle of the rotating rod so that the robot can apply exactly the same dough thickness for each layer. This is a huge advantage over the manual process, as material loss is minimized. "From this point of view, Theo is a better Baumkuchen baker than a master pâtissier," Mr. Yokoyama points out. In addition to baking, the other conditions must remain stable for consistent quality, i.e. the dough should always be the same. "If the dough recipe is changed, the trained model no longer works perfectly," Mr. Yokoyama continues. Then, in collaboration with the master pâtissier, a new inference model must be created based on the modified dough.Control flexibility supports easy optimizations

The system configuration was optimized during pilot operation in the Baum Haus. The position of the safety light curtain and the layout of the conveyor belt were changed to improve the workflow for the operators. It was possible to do this easily because of the high degree of freedom with the EtherCAT network topology. System updates could also be configured in a straightforward manner, thanks to the flexible TwinCAT engineering platform.

The Baum Haus is home to the world's only automated Baumkuchen studio with AI ovens, conveyor belts and robots. Several stand-alone ovens with AI functionality and Theo, on the other hand, are in operation across Japan – even as mobile Baumkuchen studios. In addition, Juchheim is expanding its activities, as Mr. Matsumoto explains: "We are developing a model for baking chocolate-based dough and a system with compact vertical articulated robot arms. Beckhoff and our engineering partner Matsuura Denkosha will continue to provide optimal support for our ambitious and creative initiatives in baking."

Stefan Ziegler, Editorial Management PR, ***Beckhoff Automation.***

Visit Website

SOURCE: BECKHOFF

A Beckhoff IPC C6030 not only controls the conveyor systems and oven doors via TwinCAT; the trained AI model also runs on the same device under Windows.

Effective control systems key to nationwide equipment network

ALTA Refrigeration uses automation control technology to achieve faster, easier product development and servicing with groov EPIC and MQTT technologies.

WHAT'S THE SECRET TO PROVIDING SUPERIOR service and staying competitive in a changing industrial equipment market? Well, you might learn something from ALTA Refrigeration's experience. Over ten years, it transformed itself from a custom engineering services company into a scalable industrial equipment manufacturer, using an edge-oriented control architecture to efficiently manage a growing installed base.

Originally started in 1975 as Industrial Refrigeration Services, ALTA has been designing and installing refrigeration systems across the United States for more than 45 years. And for a long time, they were large, custom-designed systems that used a central machine room to deliver refrigerant to various facility areas through long, overhead piping runs.

"Our customers' biggest concern is their power bill," notes Peter Santoro, controls engineer at ALTA. So ALTA's systems stood out for the level of control they offered, including multiple operating modes that allowed the equipment to be tuned for optimal efficiency.

However, it required significant time to design and program each unique system, and competitors were able to steal some of their market share with cheaper, simpler offerings.

SOURCE: OPTO 22

Each EXPERT follows a standard, reliable design that can be mounted on the roof above the area it serves.

"Competitors could use 20-30 cheaper units with control limited to a dumb thermostat to compete against one of ALTA's large systems," Peter adds.

ALTA knew it couldn't compete by reducing its product quality, so the company looked for a way to standardize its offering without sacrificing features.

SOURCE: OPTO 22

ALTA upgraded the EXPERT control system to Opto 22's groov EPIC to gain access to more flexible control and communication options.

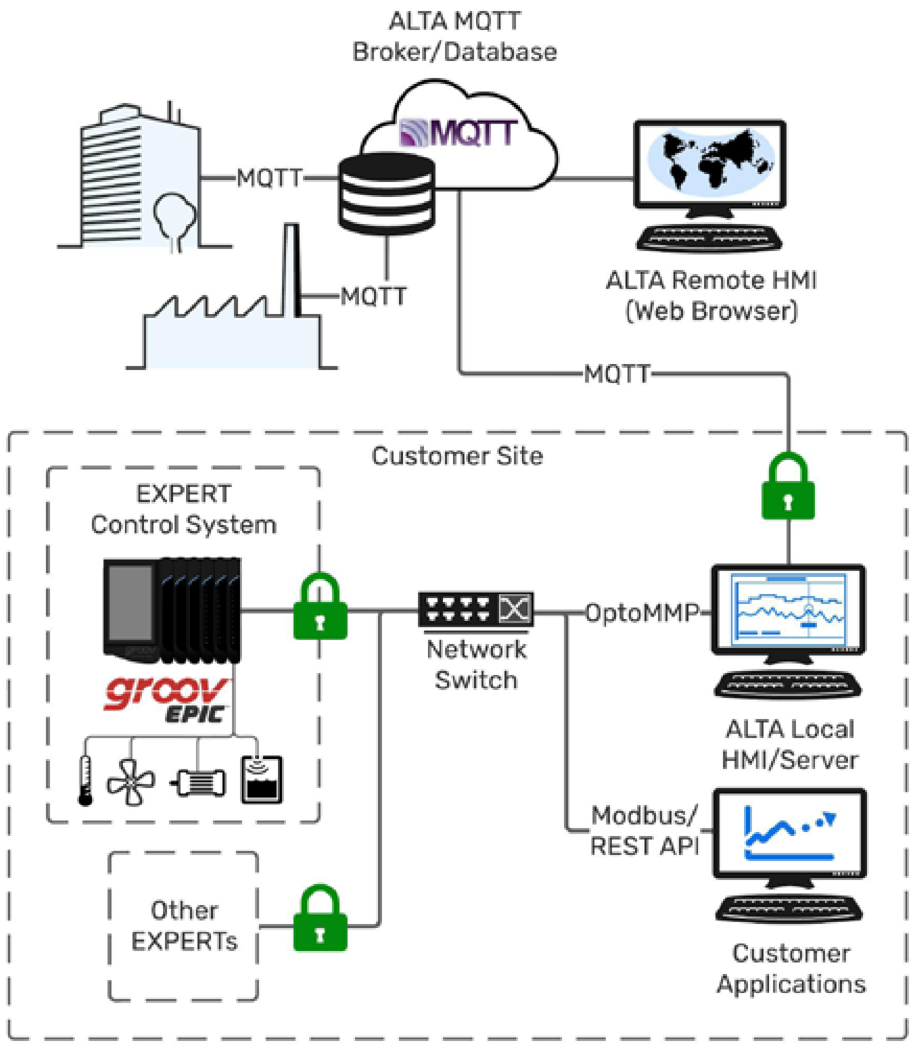
We're the Experts

In 2013, ALTA introduced its EXPERT series of modular refrigeration control units. Each unit used a standard, more reliable design, and could be mounted on the roof above the area it served, simplifying installation.

According to Peter, ALTA poured its previous years of experience with system design into creating the EXPERT product line.

"A single EXPERT has almost as much I/O as an entire centralized system, and because the units are much smaller, the wiring and conduit runs are incredibly short, allowing us to cram in a ton of sensors. The units themselves are also incredibly efficient. We analyze both the external ambient conditions and refrigerated space and do real-time thermodynamic calculations. This lets us do variable capacity refrigeration, and only run exactly the amount of refrigeration as needed."

"All motors are on variable speed drives.



SOURCE: OPTO 22

ALTA's nationwide network connects each EXPERT to its central server through a local HMI and MQTT gateway.

We also design many of the sensors we use on the system, allowing us to get precise valve positioning and to monitor refrigerant levels throughout the system. We make good use of Hall effect sensors in various configurations to monitor refrigerant levels and motor positions. There is also a dedicated energy monitor on each unit so we can monitor voltages and power usage."

Since all EXPERT systems are essentially the same, Peter and his colleague, Todd Hedenstrom, could put a higher degree of focused engineering into creating a robust and complete solution that works with many different applications.

A Good Problem to Have

The product rollout worked. EXPERT sales quickly grew to become the bulk of ALTA's business. ALTA has sold nearly 600 units and is typically sold out into the next year.

But growth brings its own challenges. While a handful of EXPERTS can replace one of the older, custom systems, ALTA now averages eight units per site. And service contracts drive ALTA's revenue. With only a small controls engineering team, servicing the growing installed base became time-consuming.

"Since we are installing sites at a much faster rate, scalability was our main concern," says Peter. "We service the vast majority of our sites, so we need visibility into everything… Our systems have a long lifetime and service is super important to our customer relationships… but we sell probably 70 of these a year and it gets hard to manage all that."

On top of that, there were some aspects of their previous designs related to system maintenance that got in the way. Their control system required many steps to properly update control strategies in the field, including exchanging files between the control engine and the web server they used for remote connectivity. It was a sometimes fragile process that made it difficult to train technicians.

Previously, ALTA had also left the details of remote connectivity to each customer. This increased the team's workload, since they usually checked in on each site every day and had to use a different method to connect to each one (VPN, Citrix, LogMeIn, TeamViewer, etc.).

If they were going to keep up with the pace of growth, Peter and Todd needed a way to remove these bottlenecks in service delivery.

Where to Start?

ALTA's centralized control system design was built around an industrial PC (IPC) running custom C++ code on top of a distributed I/O system from Opto 22. "We've been Opto people for something like 37 years," Todd adds, so when he and Peter designed the original EXPERT, they simplified the system by replacing the IPC with an Opto 22 PAC controller.

This approach was an improvement in some ways since all the components of the system could be managed through the PAC Control engine. But it didn't go as far as they needed. It still required a multi-step update process and didn't give them as much data access as they wanted. So they began exploring Opto 22's newer groov EPIC system.

EPICs, or edge programmable industrial controllers, provide a new option for industrial control systems that combines the best features of PLCs and IPCs. PLCs offer a rugged, purpose-built design with many, typically expandable, options for I/O and device communication. IPCs offer general-purpose processing power, storage, and networking options to support more demanding applications and broader functionality like cybersecurity, database management, and high-level programming languages.

EPICs support all of these functions on a single backplane but typically without the complexity of maintaining a full Windows OS environment.

Peter and Todd wanted to use the power and flexibility of an EPIC to develop a custom solution that reduced the effort required to deploy bug fixes and product updates. They also wanted a single solution for remote monitoring, and thought that groov EPIC's array of communication options would make that easier.

Building a Better Fridge

Peter and Todd dove seriously into using groov EPIC's operating system shell to port their PAC Control application to C++, passing over other control engine options to leverage the language they were most familiar with. "We tried CODESYS on the EPIC," says Peter, "but the freedom and flexibility of going with C++ was too good to pass on."

groov EPIC uses a custom Debian Linux distribution that has been stripped down to the essential components, reducing its memory footprint and potential cyber attack vectors. Additionally, it has been cryptographically signed with Opto 22's private key to prevent installation of any unapproved software. However, Opto 22 also exposes access to the EPIC's Linux command-line using the secure shell protocol (SSH) and a free Shell Access license (GROOV-LIC-SHELL).

"All development is done remotely through the SSH connection in [Microsoft] Visual Studio," Peter explains. You can find the guide Todd posted in the Opto 22 user forums explaining how he set up this connection, which allowed him to develop programs in VS and compile them directly on his EPIC. Once Todd figured out this basic process, he and Peter were able to consolidate most of the control program into their C++ application along with many new features.

The program controls the installed I/O modules—voltage and current sensing inputs and discrete AC outputs—using Opto 22's C++ OptoMMP SDK, or software development kit. The application also includes its own Modbus server that creates and manages connections to variable frequency drives, the local energy monitoring unit, and other remote devices.

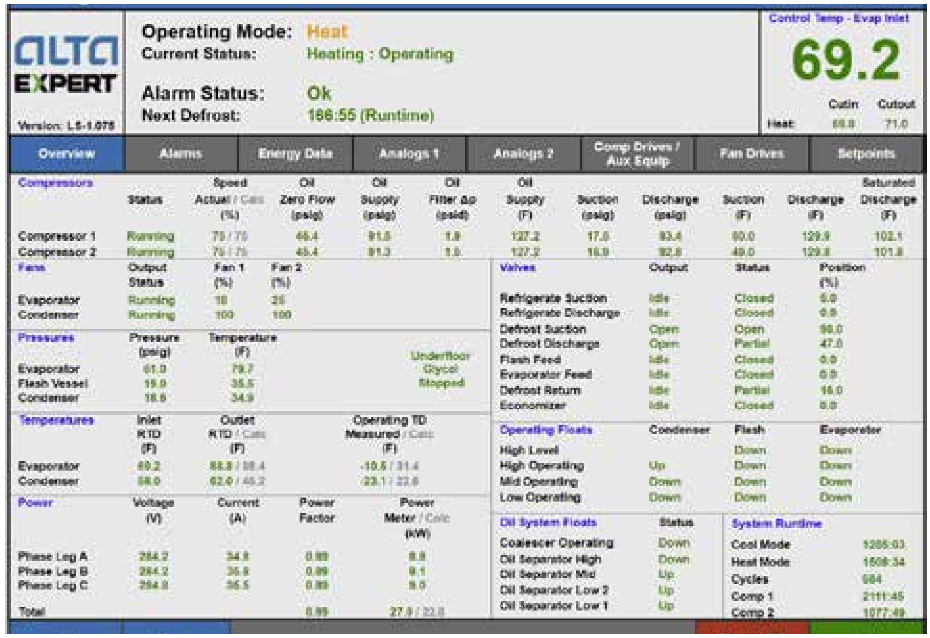
"We [also] have our own REST API and webserver running on the C++ application," Peter adds, "allowing us to create our own web page interfaces in HTML and Javascript… It's a lot easier to build HTML stuff in familiar tools than with an HMI package… You can do anything." That includes things like using Google's Chart API to display energy metrics in the HMI.

Each EXPERT's web interface is served up from its EPIC controller. It includes prebuilt templates for different unit configurations and verifies system settings to help technicians identify configuration values that are out of range or not recommended. It also generates alarms as needed. Alternatively, customers can access unit data through the EXPERT's Modbus server or REST API.

For managing groups of EXPERTs, ALTA uses a separate HMI server to read data from each unit and present a unified view of the entire system. "All of our sites are required to have a local interface for operators to see a global view of their refrigeration units, instead of having to manage network connections to hundreds of individual units," Peter explains.

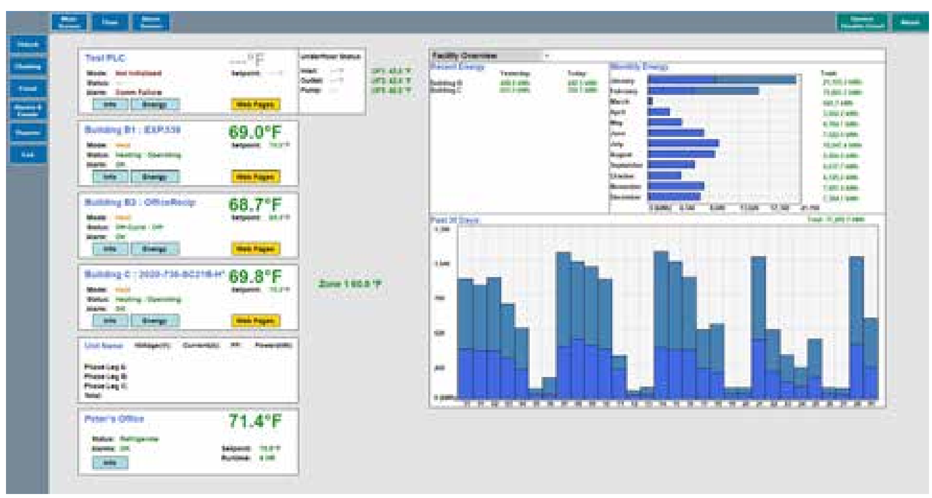
To create this site-level HMI, each EXPERT stores transient data in the shared memory "scratchpad" area of its groov EPIC. ALTA's HMI server runs on Windows and uses Opto 22's .NET OptoMMP SDK to retrieve this data from all units in 1-second increments. Data is stored in cyclical files that maintain a 1-week buffer, and the HMI server uses this data to generate trends, charts, and email notifications.

ALTA can also access this data remotely for troubleshooting recent events. By default, groov EPIC does not route traffic between its Ethernet ports, so ALTA can use the controller to create a security zone for each EXPERT.



SOURCE: OPTO 22

Each EXPERT provides a local unit interface through an embedded web server that runs on the unit's EPIC.



SOURCE: OPTO 22

ALTA's central HMI aggregates data from across its installed base of EXPERT systems.

One port on each EPIC connects to a private network exclusively for the controller and its remote devices. The other port is connected to a common network between all the units at a given site, as well as the local HMI server.

This server is connected to the internet and uses MQTT to send and receive data, acting as a middleman for each individual EXPERT to the MQTT broker that resides in ALTA's headquarters. When ALTA's remote HMI requires new data, it sends a request to the local server over MQTT. The data is queried and sent back. External connections to local HMI servers are restricted so that the only traffic allowed through is from outbound MQTT TLS connections.

Recently, ALTA also made it possible for their customers to access this remote server. The server has its own database that records temperatures and energy usage for each EXPERT in 10-minute intervals. Customers can log into a private web portal to generate reports directly from this data.

Since groov EPIC provides an embedded MQTT client and network firewall, ALTA "also tried doing unit-level MQTT [communications] to the broker," Peter clarifies. "But with some of our units running on customer networks, it was impossible to guarantee they would allow a direct internet connection to the [EPICs]. That is why we shifted focus to only have our local site server be the device connected to the broker."

The Coolest Service Around

How are Peter, Todd, and the ALTA team doing now? In Peter's opinion, "Our service and warranty programs are unprecedented."

SOURCE: OPTO 22

Each EXPERT provides a local unit interface through an embedded web server that runs on the unit's EPIC.

ALTA has built a nationwide HMI that aggregates data from its network of EXPERT units and highlights any issues the team needs to act on. Instead of spending hours every day to check on each site, they can monitor their entire installed base in minutes. They know when there is a problem, can input and track necessary work orders, track technicians' locations, and monitor energy usage per unit. When an alarm occurs, the system creates an interactive timeline of events before and after.

"Often, we know what the problem is before the customer calls. We just need to drive there and fix it," says Peter. "With the amount of data we get from our units we are capable of diagnosing the vast majority of problems remotely. This allows many of our end users to not even staff on-site maintenance… And no interfacing with third-party systems anymore. It's all integral."

"When we used to do centralized systems, a lot of IoT stuff was near impossible with how the old systems were structured. Because all the central systems could be drastically different, it was difficult to even consider a 'dashboard' to display them. Having a central web server or database was not even considered until we made the full transition to our EXPERT product line."

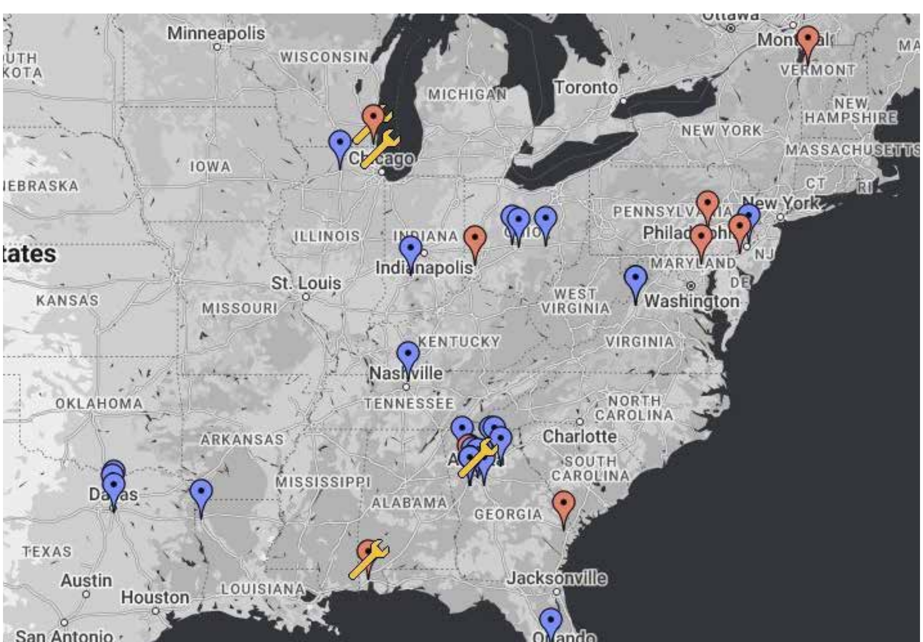
"This solution was mostly developed to make our lives easier to support the systems. Having customers on here is just a big bonus now that everything is externally visible."

Servicing the systems themselves has also become much simpler now that Peter and Todd can manage the entire platform—I/O configuration, control strategy, communications, and networking—through a single device. "One of the best features we introduced was the ability to update the programs through our web interface… Now a batch program packages up all the program files into a .gz (compressed) file. Technicians can upload the file and restart the system… We send the tarball, they click update, and the system takes care of the rest. Much easier," Peter says.

"We have a lot of experience with C++ here, so applying that to the EPIC controllers using Shell Access has allowed us to rapidly ALTA's central HMI continuously monitors its entire installed base, providing intuitive representation of system health across the country. develop these custom solutions with a very small team… The lead engineer loves to make changes so we've gone through hundreds of revisions."

ALTA also uses the groov EPIC's touchscreen as a maintenance interface inside the control cabinet.

The native groov Manage application allows them to view and modify I/O and network settings directly on the controller without using a separate computer interface. Using the EPIC's native HMI server, groov View, ALTA also provides technicians with local control options and basic information about the Linux program's status.



ALTA's nationwide network serves up performance data on every unit and allows the team to track and manage necessary work orders.

But Can It Get Even Cooler?

With EPICs as a foundation for their control platform, Peter and Todd continue to dream up even more service offerings. They are working on the ability to remotely update both the local servers and each individual EXPERT unit from their central webserver.

The server will soon have its own REST API as well. With the correct key, a customer could grab the information from ALTA's nationwide system without needing to interface with their local hardware at all. Additionally, ALTA is considering using the larger storage capacity of the groov EPIC PR2 processor (GRV-EPIC-PR2) to store the EXPERT's process history buffer directly on the EPIC, rather than its local Windows servers.

Other new features are on their way as well, potentially including real-time operational adjustments based on local power rates. And with a large network of performance data to draw on, the team has also been evaluating integration with a cloud IoT platform for long-term data storage and predictive control.

Peter sums it up by saying, "It's nice to have the EPIC as the IPC with I/O. It's just simpler… We can do a lot with a little." As of writing this case study, ALTA has deployed 200 EPICs in the field. EXPERT sales are booked solid through the coming year.

Technical article by ***Opto 22.***

Visit ALTA Website

CC-Link IE network keeps power on track at Euston Station

To ensure reliable and fast inter-substation data transfer, a proven high-bandwidth open network technology was needed for the High Speed Two (HS2) railway line at London's Euston station. The technology used to deliver the high-speed network for this project was the open gigabit industrial Ethernet solution, CC-Link IE.

SOURCE: CLPA

The technology used to deliver an exceptionally reliable and accessible high-speed network for accommodating the High Speed Two (HS2) railway line at London Euston station was the open gigabit industrial Ethernet solution, CC-Link IE.

ACCOMMODATING THE HIGH SPEED TWO (HS2) railway line at London Euston station in the UK meant installing a new substation for the control of traction and electrical power to address the needs of the expanded facility. The technology used to deliver an exceptionally reliable and accessible high-speed network for this project was the open gigabit industrial Ethernet solution, CC-Link IE.

HS2 will use Euston station as its main terminus hub, with the number of seats out of the station during peak hours set to double. To support this increased capacity, the terminal is being enlarged to include 11 new 400-meter-long platforms for high-speed trains to and from London, the Midlands and north of England.

In order to meet the new electrification requirements of the expanded station, the telemetry system for the rail network's electrical supply also needed to be upgraded.

When Sella Controls were asked to upgrade the substation control system, they proposed the use of TRACKLINK® remote terminal units (RTUs) developed in partnership with Mitsubishi Electric. This utilises a PLC to process signals from field devices, acting upon the information provided in a timely manner, as well as reporting data to SCADA systems in the control room.

Since Euston station has always featured an extraordinarily large infrastructure, the control system uses an uncommon framework. Unlike smaller railway terminals, which only use a single RTU to address their needs, the London railhead's electricity generation, transmission and distribution system is divided into multiple subsidiary parts.

Known as substations, they are key for effective power distribution and control. The master RTU is used to link to remote I/O panels placed at each substation. Thanks to this setup, the main controller can complete auto reconfiguration procedures in the event of a power loss at the station.

Jay Sampat, Project Manager at Sella Controls, explains: "An RTU is typically a single panel deployment within a substation. However, depending on the structure of the railway terminal and its substations, some I/O can be remote. An example is Euston terminus, which comprises Euston Concourse, Euston East, Euston West and the new master location at Barnby Street Station. Whilst this type of setup is needed to successfully cover the entire infrastructure, it makes inter-substation communications particularly challenging."

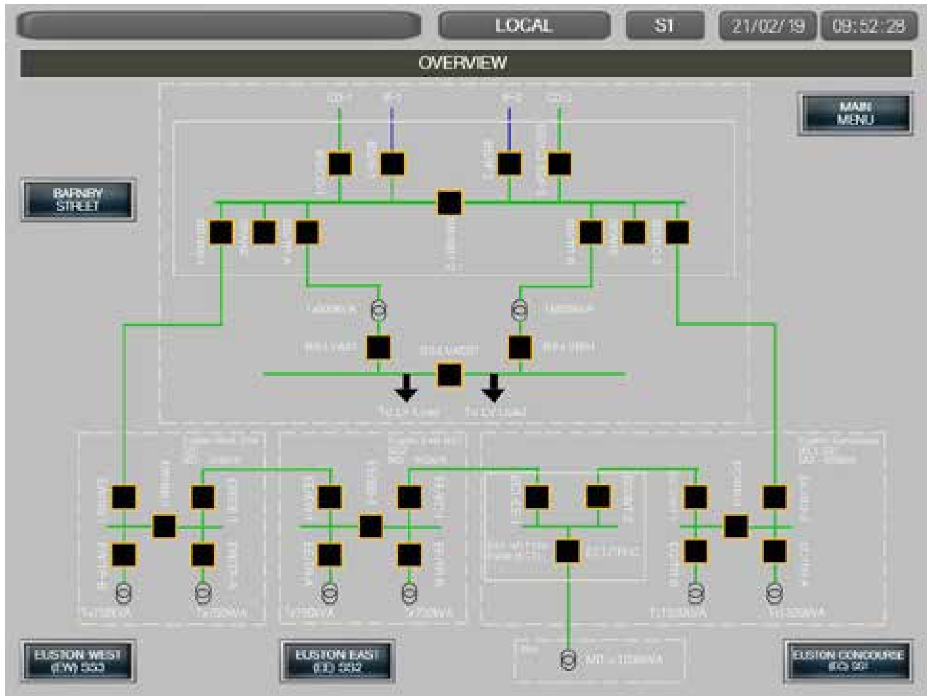
Fast-tracking traction power communications

To ensure reliable and fast inter-substation data transfer, a proven high-bandwidth open network technology was needed. This is why Mitsubishi Electric recommended to Sella Controls that it selects CC-Link IE.

This open industrial Ethernet technology offers gigabit bandwidth and uses a token passing method to provide real-time, deterministic communications. This minimises latency and jitter, facilitating the transmission of large volumes of data without congestion.

John Browett, General Manager at CLPA, comments: "The industry-leading functions of CC-Link IE were crucial to creating a high-speed telemetry system that can also address future data loads. The network that has been created is highly responsive and can be easily modified or upgraded as needed."

Chris Elliott, Business Development Director for Rail at Sella Controls, adds: "The setup developed is unique, marking the first application of CC-Link IE for railway traction power control to deliver inter-substation connectivity. We look forward to setting up more cutting-edge control systems like this across the country soon."



SOURCE: CLPA

A remote terminal unit (RTU) is typically a single panel deployment within a substation. However, depending on the structure of the railway terminal and its substations, some I/O can be remote. An example is Euston terminus, which comprises Euston Concourse, Euston East, Euston West and the new master location at Barnby Street Station.

SOURCE: CLPA

To ensure reliable and fast inter-substation data transfer, a proven high-bandwidth open network technology, such as CC-Link IE, was needed.

Full speed ahead

To ensure an exceptionally responsive control system, CC-Link IE was combined with Mitsubishi Electric's iQ-R series modular PLC as the new building block of the RTU. Also, a GOT 2000 HMI was incorporated within the master RTU panel to maximise visibility and accessibility.

David Bean, Solutions Group Manager at Mitsubishi Electric, says: "Our advanced automation components have been used for multiple Tracklink RTUs across the country and are delivering best-in-class performance. In this specific application, we were able to truly get the most out of our equipment to deliver interconnectivity between the main controller and the remote I/Os."

Since the important completion of the upgrade project at Euston station, the new telemetry solution has been key to ensuring a highly reliable traction power infrastructure within the railway terminal. John Browett concludes: "We are extremely proud to see our open network technology, CC-Link IE, being used to support this large-scale infrastructure project. As railways continue to advance and incorporate new technologies, we are well-positioned to deliver cutting-edge connectivity solutions to help realise reliable and accessible networks."

Application article by ***CC-Link Partner Association (CLPA).***

Visit Website

Simplified development for real-time Industrial Edge systems

A high-performance software platform has targeted edge computing use cases, such as industrial control and real-time signal processing applications. It provides extended OT connectivity, auto-discovery for easy device onboarding, and a new MQTT API combined with improved performance and scalability.

AN EDGE SOFTWARE PLATFORM HAS BEEN designed specifically for time-critical and resource-constrained embedded Industrial OT (Operational Technology) and IoT (Internet of Things) systems. It provides a powerful edge software framework that supports key capabilities such as Southbound OT connectivity, edge data processing and Northbound IT/Cloud connectivity.

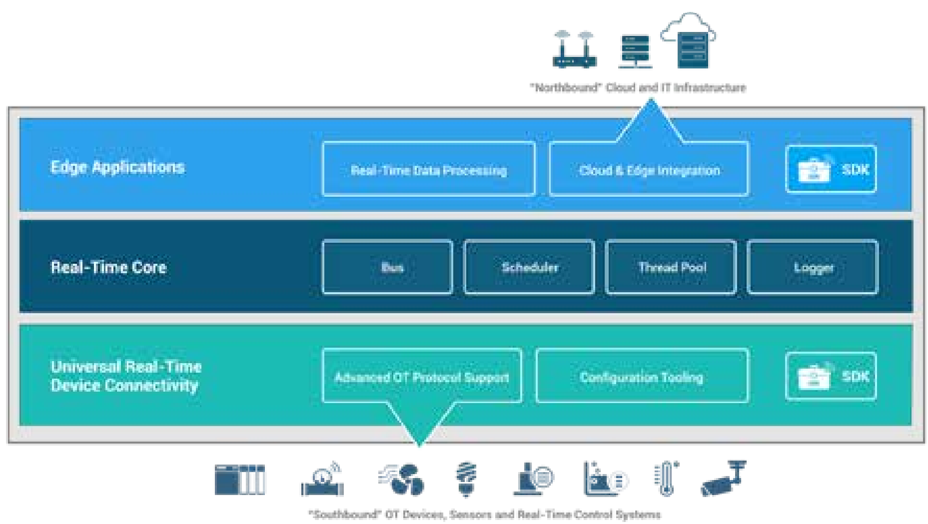
Edge XRT technology delivers these capabilities while also supporting the following key non-functional properties:

- Small memory footprint (e.g. less than 100 KB)
- Ultra-low latency data processing (e.g. less than 100 microseconds)
- Predictable and deterministic real-time execution
- Easily ported legacy hardware and/or operating systems

Edge XRT is targeted at high-performance edge applications such as industrial control, high-frequency signal processing and real-time analytics in different vertical markets including factory automation, oil and gas, utilities, autonomous systems and smart energy. It also enables integration between the real-time industrial edge applications and higher-level SCADA, MES and IT/Cloud systems.

Due to its small memory footprint XRT is perfectly suited for resource constrained embedded applications such as those enabled by the next generation of connected microcontrollers, for example Microsoft's Azure Sphere devices.

Edge XRT is a complementary commercially-licensed extension of the Linux Foundation's EdgeX Foundry platform. It enables the EdgeX ecosystem and commercial derivatives such as IOTech's Edge Xpert to support the full spectrum of secure hard and soft real-time Edge Computing requirements.



SOURCE: IO TECH

Edge XRT technology enables integration between real-time industrial edge applications and higher-level SCADA, MES and IT/Cloud systems.

New Edge XRT 2.0

Edge XRT 2.0 provides extended OT connectivity, auto-discovery for easy device onboarding, a new MQTT API to simplify integration and management, combined with improved performance and scalability. This is a major release of the open software platform is designed for time-critical and embedded OT applications at the industrial IoT edge.

Edge XRT 2.0 greatly simplifies the development of OT applications and enables faster time-to-market for new edge systems. It is hardware agnostic, independent of the silicon provider (Intel or ARM) and operating system. Users have complete deployment flexibility. They can deploy it as a native application, containerized and/or into a virtualized environment.

With its small memory footprint and efficient use of computing resources, Edge XRT 2.0 is also suitable for microcontroller-based applications where CPU and memory resources are limited. This makes it ideal for use cases such as connected commercial or consumer electronic devices (e.g., refrigeration unit), medical device applications or automotive engine management systems.

The technology's open APIs make third-party application integration very easy. Major industrial OEMs and ISVs are leveraging the product's multi-vendor OT connectivity, cloud interoperability and high-performance, real-time edge processing capabilities to create a new generation of protocol-agnostic edge solutions.

"As a configurable, embeddable, high-performance OT platform, Edge XRT 2.0 is unique," said Andrew Foster, Product Director at IOTech. "It provides a rich set of OT and IoT capabilities that our customers can easily use to create their own edge solutions. In most cases, this is through simple configuration without the need for lots of custom code."

New release highlights

The new release adds a number of important features including:

OT connectivity: In addition the existing pluggable OT connectivity for Modbus, EtherNet/IP and EtherCAT, BACnet and OPC UA protocols, the platform now supports PROFINET, S7, GPS and BLE.

For protocols that support device discovery such as OPC UA, BACnet and EtherNet/IP, devices can be discovered and then onboarded easily without any manual configuration.

A new MQTT API allows Edge XRT clients to easily manage the lifecycle of connected device/sensors, support read/write OT data access, control device discovery and resource scheduling.

When deployed on an Azure Sphere device, an Edge XRT application can now be dynamically configured and reconfigured via a Device Twin running on Azure IoT Hub.

IOTech has made scalability and performance improvements to address customer demand for concurrent access to an increasing number of OT devices and their data.

Technology report by ***IO Tech.***

Visit Website

Compact multi-axis system

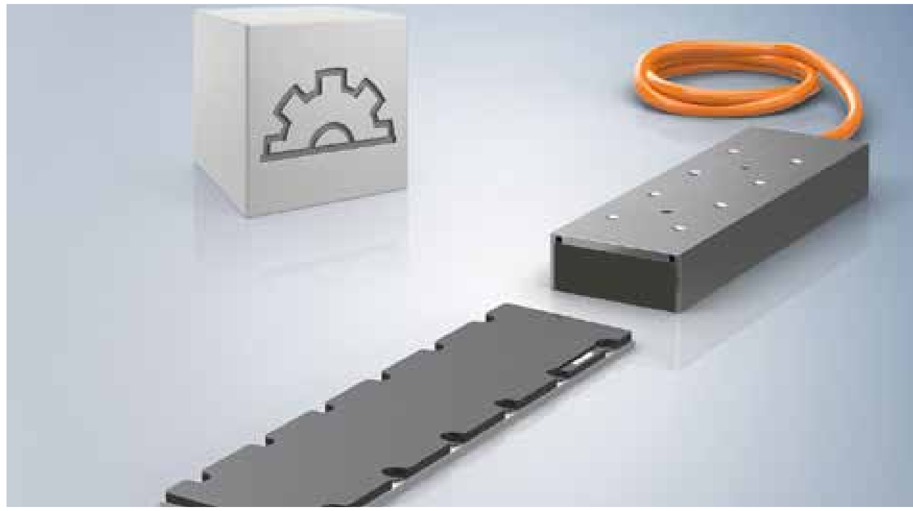
The internal media feed for data, power and fluids is designed so that all axes rotate endlessly.

With ATRO, Beckhoff is presenting a new concept for robotics applications. This is a modular system from which the right robot kinematics can be put together extremely flexibly for any application. A highlight of the system is the internal media feed for data, power and fluids. This has been implemented in such a way that all axes are designed to rotate endlessly.

With ATRO, users can create almost any robot design for their application from the modules provided – from a simple 1-axis rotary indexing table application and delta kinematics, through to multi-axis articulated robots. Beckhoff's holistic perspective is decisive for simple commissioning and handling, because only the direct integration of the robot system into PC-based control enables a truly optimized complete solution for the machine or plant. This reduces the number of controls needed on one industrial PC, even with multiple robots.

ATRO kinematics are made up of active joints – the motor modules. The motor modules are available in different designs: straight modules in I-shape or angled modules in L-shape, which are designed in five power sizes. Each motor module forms a complete drive system for one axis of the robot. The only external components required are a power supply and a control, which significantly reduces the space required in the control cabinet.

All modules are interconnected via the ATRO interface, which guarantees a rigid connection and also passes through the media that is fed in. Data, power and fluids (compressed air, vacuum or water) are thus guided internally through the modules in the ATRO kinematics.



SOURCE: BECKHOFF

ATRO kinematics are made up of active joints – the motor modules.

Beckhoff

Learn More

Eight-port Ethernet switching hub

Designed for compact, wide-temperature applications, with Plug-and-Play simplicity.

A new series of unmanaged switches makes it easier to expand Ethernet networks in the most demanding environments. The EISW8-100T is an eight-port Ethernet switch that provides 10/100 Mbps performance on all ports to accommodate a range of control devices and workstations used in automation systems. A wide operating temperature range of –40°C to +75°C make the EISW8-100T suitable for outdoor applications.

This low-cost, compact unit is encased in a rugged steel enclosure, with both DIN-rail and wall mounting installation. The EISW8-100T requires a rail space width of only 41 mm, making it ideal for control panel installations where DIN-rail space is at a premium. A metal DIN-rail clip attached to the steel enclosure can survive the toughest installation.

"Ethernet continues to evolve as the network of choice for automation systems due to its high speed, familiarity among users, and easy Internet connectivity. But the environment can be demanding," said Joe Stasiek, sales manager at Contemporary Controls.

The switch supports plug-and-play operation and requires no configuration. All ports automatically configure their data rate and duplex using auto-negotiation protocol. Depending on the capability of the link partner, communication is set at 10 or 100 Mbps and at either half- or full-duplex. The EISW8-100T has eight Auto-MDIX ports for attaching local devices. Each port has one LED that glows with an established link and flashes with activity which assists in troubleshooting connection issues.

SOURCE: CONTEMPORARY CONTROLS

This eight-port Ethernet switch provides 10/100 Mbps performance on all ports to support a range of control devices.

Contemporary Controls

Visit Website

Advanced valve systems with OPC UA

Digital twin solution solves interoperability challenges while improving productivity and efficiency.

SOURCE: EMERSON

Valves comes preinstalled with Open Platform Communications Unified Architecture.

The AVENTICS Series Advanced Valve (AV) valve system with Advanced Electronic System (AES) Profinet andEthernet/IP is now available with preinstalled Open Platform Communications Unified Architecture.

OPC UA functionality makes it the first and only valve system to offer this directly integrated capability. The AES helps users solve interoperability challenges and access data more easily while the integration of the digital twin can improve productivity and efficiency.

A valve system with integrated OPC UA functionality simplifies communication with upper systems since data and analytics are received via the valve system and communicated directly to upper systems, no gateway necessary unless deeper analysis or local dashboards are required.

OPC UA functionality also expands the connected capabilities of the valve system itself, making it easier for users in industries such as automotive, food and beverage, packaging, pulp and paper industries and more to digitally transform. When organizations undergo digital transformation, key protocols such as OPC UA embedded in technologies enable device monitoring and machine connectivity when sending data from a valve system to an upper system.

The AES is simple to integrate and connect to new or existing applications and machines and provides easy access to data and analytics without changing the programmable logic controller (PLC).

Developed by the OPC Foundation, OPC UA is a platform independent, information technology standard for sensor-to-cloud data exchange that features integrated security.

Emerson

Visit Website

CompactPCI blades

Benetel and ASOCS provide industrial sector with technology needed for 5G private network installations.

SOURCE: KONTRON

Both blades offer a remarkable performance-per-watt ratio and a highly scalable power budget that gives users the flexibility to tailor the power dissipation precisely to their needs match requirements.

The new Kontron CP6007 blade series is designed for long-term computing tasks and for server applications based on PICMG2.16 and relies on 6- or 8-core CPUs from Intel's 11th Gen Xeon processors with 10nm technology. At the same time, it is largely backward compatible with many earlier Kontron Blades, e.g. the CP6007-RA variant of the Successor to the CP6004-RA blade.

Both blades offer a remarkable performance-per-watt ratio and a highly scalable power budget that gives users the flexibility to tailor the power dissipation precisely to their needs match requirements. The CP6007-RA version has a soldered 32 GB of memory, while the CP6007-SA variant also comes with a SODIMM module can be equipped can add up to 64 GB total memory with Error Correction Code (ECC) to provide support. A wide range of Communication and media interfaces are also part of the package as an improved hardware and software-based system security through the Trusted Platform Module (TPM 2.0).

There are various expansion options such as mass storage, XMC, PMC and rear I/O are available. These include industrial ones M.2 flash devices (NVMe and SATA) and a 2.5 " SATA hard drive or SSD, which can be accommodated on a corresponding rear I/O module. XMC compatibility based on XMC.3 is also available at x8 PCI Express support, or alternatively PMC to accommodate other different extensions available on the market.

Kontron

Visit Website

OPC UA server and MQTT options

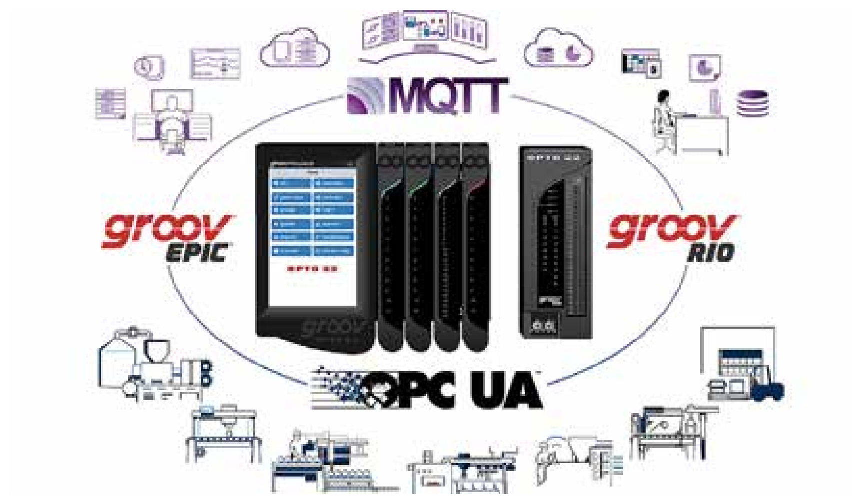
Latest firmware updates offer new data services capabilities plus updated software for security.

Opto 22 announces the latest firmware version 3.4 for the groov EPIC edge programmable industrial controller from Opto 22, along with firmware version 3.4 for the groov RIO edge I/O module. Both are available as a free download for all existing groov EPIC and groov RIO users, adding even greater capabilities for sharing OT data with SCADA systems, databases, HMIs, and historians, and with other functions like Quality and Process.

New data democratization capabilities include an additional, embedded OPC UA server and much more flexibility in MQTT services. The release also adds support for SNMP and the Scratch Pad memory map area.

New embedded OPC UA server. Opto 22 was instrumental in developing the original OPC specification and in founding the OPC Foundation. With the new PAC Control and I/O OPC UA server now on board, both groov EPIC and RIO offer this familiar, platform-independent way to exchange data among devices and software within your OT network. For example, you can smoothly integrate your control and I/O systems into SCADA software using OPC UA—no special drivers required.

With these new data service capabilities, users can communicate operational data through both OPC UA and MQTT protocols simultaneously. Tried-and-true OPC UA is client/server based and, because it requires an open incoming port, is best used in a secure OT network such as an in-plant network. MQTT is a more secure publish/subscribe method, offering a simpler architecture that doesn't require opening incoming firewall ports, which is ideal for sharing data with remote servers over standard IP networks, including cellular and the public internet.



SOURCE: OPTO 22

New data democratization capabilities include embedded OPC UA server and more flexibility in MQTT services.

Opto 22

Learn More

Raspberry Pi-based DIN rail PCs

STV Electronic introduces second generation of its Raspberry Pi-based DIN rail PCs.

Two new, even more compact variants of its Raspberry Pi-based 64-bit DIN rail PC family for control cabinet are available: the Smart Manager Basic and the Smart Manager Light. Both are available immediately, which is important to emphasize given today's supply chain challenges. Based on the 1.2 GHz Broadcom BCM 2837 quad-core processor, the new systems have no front interfaces, which allows for installation in extremely slim spaces. Thanks to their shallow depth of 62.2 mm, compact width of 6HP (108 mm) and top/bottom interfaces, these industrial DIN rail PCs fit into any control cabinet – even flush-mounted small distribution boxes that permit maximum installation depths. The new DIN rail PCs can be used in a variety of edge computing applications.

Featuring 1 GB LPDDR2 SDRAM and between 8 or 32 GB eMMC onboard flash memory, the real-time capable systems provide an HDMI interface, up to two Ethernet ports, four USB 2.0 ports and two programmable RS-485 interfaces. Further interfaces – including WLAN, fieldbuses such as M-Bus, Modbus, LonWorks and KNX, as well as digital, analog and custom I/Os – are easily added to the Smart Manager Basic using wireless expansion modules. A wide voltage input range of 12 to 30 V facilitates the integration of industrial applications. Based on Debian Linux, the Smart Manager Basic and Light supports a wide choice of programming software: CoDeSys, NodeRed, Node.js, C or C++ offer solutions for all application areas. FHEM, openHAB or Mosquitto can also be easily installed.

SOURCE: STV ELECTRONIC

Based on Debian Linux, the Smart Manager Basic and Light supports a wide choice of programming software.

STV Electronic

Learn More

Motor control MPU & Ethernet

Combines high performance motor control and TSN-Compliant Industrial Ethernet network on a single-chip.

SOURCE: RENESAS

Highest-performance RZ/T2M motor control MPU enables fast, high-precision control of servo motors.

The RZ/T2M combines fast and highly precise real-time motor control capabilities and the latest industrial Ethernet on a single chip, while also supporting functional safety operation. By providing all essential peripheral functions for motor control, the RZ/T2M enables customers to reduce the number of external components.

The RZ/T2M is built around two Arm Cortex®-R52 cores with a maximum operating frequency of 800 MHz. Connecting the peripheral functions used for motor control to a dedicated bus linked directly to the CPU enables the CPU to access these functions with low latency. In addition, the large memory capacity (576 KB) is tightly coupled with the CPU, reducing the fluctuation in execution time that can occur when cache memory is used and delivering deterministic, fast-response processing. These advantages enable the RZ/T2M to deliver rapid and highly precise control for applications such as AC servos, inverters, and industrial robots.

In addition to major industrial networking protocols such as EtherCAT, PROFINET RT, and EtherNet/IP, Renesas has added support for the PROFINET IRT protocol in the RZ/T2M. The new MPU also includes an Ethernet switch that supports the next-generation Time-Sensitive Networking (TSN) standard, allowing multiple devices to operate in precise synchronization.

In most cases, building industrial equipment that complies with functional safety requirements involves two external MCUs for safety monitoring, which increases BOM costs. The RZ/T2M has a hardware configuration designed with functional safety operation in mind, so only one external MCU is needed to implement functional safety.

Renesas

Visit Website

Test and validate IoT solutions

u-blox XPLR-IOT-1 enables end-to-end proofs of concepts for IoT products and applications.

SOURCE: UBLOX

XPLR-IOT-1 makes it easier than ever to explore the potential of IoT applications.

The u-blox XPLR-IOT-1 IoT explorer kit is an all-in-one package to test, evaluate and validate IoT applications. Integrating all relevant u-blox technologies and services into a capable prototyping platform with a vast selection of sensors and interfaces as well as cloud connectivity, XPLR-IOT-1 makes it easier than ever to explore the potential of IoT applications.

The increasing complexity of IoT devices, which often require satellite-based positioning, Bluetooth low energy, Wi-Fi, and cellular connectivity via, for example, LTE-M is raising the importance of prototyping and validating ideas before bringing them to production.

The XPLR-IOT-1 gives users everything they need to prototype low-power IoT use cases such as logistics container trackers, industrial automation, sensor-to-cloud applications, and fleet management solutions. The board's u-blox NORA-B106 Bluetooth LE 5.2 radio module doubles as its main MCU, hosting the application software and controlling the other modules. These include a u-blox SARA-R510S for LTE-M and NB-IoT cellular connectivity with built in cloud security, as well as a u-blox NINA-W156 for 2.4 GHz Wi-Fi.

The board also hosts an ultra-low-power MAX-M10S positioning module capable of concurrently tracking four global navigation satellite system (GNSS) constellations, delivering highly reliable location data wherever GNSS coverage is available.

UBLOX

Visit Website