11.2020 Issue 121
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking and IoT

AI and edge computing for industrial applications 20

CC-Link IE TSN

OPEN the FUTURE of CONNECTED INDUSTRIES

SEE & MEET US AT
sps connect
The digital automation hub
Visit eu.cc-link.org to claim your **FREE ONLINE TICKET**

CC-Link IE TSN: Time-Sensitive Networking joins open gigabit Ethernet to deliver the world's most advanced automation network technology for Industry 4.0.

- **Performance:** Combines gigabit bandwidth with TSN to deliver the highest productivity network solution for Industry 4.0.
- **Connectivity:** Open technology provides freedom of choice for end users, OEMs and device vendors.
- **Intelligence:** A wealth of intelligent features reduce time to market and downtime while increasing productivity.

Contact us now to see how CC-Link IE TSN can meet your needs or visit our websites to download your free copy of the white paper – **Time-Sensitive Networking: The Case For Action Now**.

Europe: **partners@eu.cc-link.org** | **eu.cc-link.org**
Americas: **Info@CCLinkAmerica.org** | **am.cc-link.org**

CC-Link CLPA PARTNER ASSOCIATION
OPEN AUTOMATION NETWORKS

20th Anniversary CLPA

CC-Link IE TSN

HIROSE ELECTRIC EUROPE B.V.

iX Industrial™

Buy Online on SINBON webshop https://ix.sinbon.eu/

Ethernet communication between electronic equipment has increased with Industry 4.0 which brings efficiency of manufacturing with ICT technology. In response to this increasing demand HIROSE had standardized a new miniaturized Ethernet mating interface in compliance with IEC 61076-3-124. The ix Industrial™ socket size is reduced by 75% compared to the existing RJ45 modular connectors, and offers ideal space saving cabling for applications with miniaturized requirements.

- **Compact: 75% smaller in size than a RJ45**
- **Robust: 5000 mating cycles**
- **High-speed: Ethernet 1Gbps/10Gbps**
- **High EMC resistance**
- **Complies with IEC 61076-3-124**

► Security System

► Transportation

► Data Center

► Robotics

► Communications

► Factory Automation

www.hirose.com/eu - eu.info.3d@hirose-gl.com

C_ber Securi_y

AI 05-19.000.L1

Incomplete security?

Our 360° cybersecurity solutions protect your industrial network!

Industrial control and automation systems are increasingly exposed to cyber risks and unintentional changes due to the growing networking of these systems and their connection to the Internet. By means of secure products, services, and industrial solutions, Phoenix Contact helps you protect your systems and safeguard your know-how. Don't hesitate to contact us for more information and advice.

For additional information call +49 5235 3-00 or visit **phoenixcontact.com**

PHOENIX CONTACT
INSPIRING INNOVATIONS

Benefits at the edge ...

This issue of the Industrial Ethernet Book takes an in-depth look, using a series of articles authored by industry experts, into edge computing technology and its benefits for IIoT applications.

Edge computing, by definition, is the practice of processing data near the edge of the network where the data is being generated, instead of in a centralized data warehouse.

The benefits of edge computing include local, more secure storage of data, increased flexibility, innovations in the areas of software updates and data security—along with access to what is becoming a fertile ecosystem of edge technology solutions.

Edge technology solutions are emerging at a rapid rate ranging from a new generation of distributed I/O, Edge-located HMI solutions and even how edge computing is being combined with artificial intelligence to create Industrial AIoT applications.

On page 6, the article "Distributed I/O and control build IIoT from edge to cloud" discusses how distributed edge I/O, edge controllers and associated networking technologies support data transfer through the edge, fog, and cloud portions of an industrial architecture.

Use of next generation digital I/O and more distributed global architectures are enabling connectivity to the cloud for sensors and actuators, and for the I/O systems and controllers linked to them. Edge-to-cloud architectures are creating new options at the edge for acquiring, securing, storing and processing field data.

The article "Edge computing and AI create Industrial AIoT applications" on page 20 investigates how enabling Artificial Intelligence (AI) capabilities at the edge can improve operational efficiency and reduce risks and costs for industrial applications. System designers choose the right computing platform for an industrial AIoT application by addressing specific processing requirements during implementation.

Additional articles "Data integration for the Industrial Internet of Things" on page 10 and "No edge computing without an appropriate network" starting on page 18 provide insights into how network setup and architecture play an important role in edge computing success.

As is the case with many technologies, creating solutions takes a lot of development and tools to effectively implement systems. Our goal as a publication is to provide you with the latest information from industry experts. The advantages of end-to-end Ethernet networking, including edge computing, can only be fully utilized if the network is equipped with necessary resources.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **January/February 2021.**
Deadline for editorial: December 15, 2020

Product & Sources Listing

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

Update your own products

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

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

Editor: Al Presher, editor@iebmedia.com
Contributing Editor: Leopold Ploner, info@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +49-8192-994-9928 · Fax: +49-8192-994-8876
Online Editor: Adela Ploner, info@iebmedia.com
Circulation: subscriptions@iebmedia.com
Published by IEB MEDIA
IEB Media, Bahnhofstrasse 12, 86938 Schondorf am Ammersee, Germany
ISSN 1470-5745

PEFC™
PEFC/04-31-1873

IIC report defines framework for distributed edge computing

Moving computing from the cloud to the edge increases the performance, trustworthiness and efficiency of industrial IoT applications, according to a technical report from the Industrial Internet Consortium.

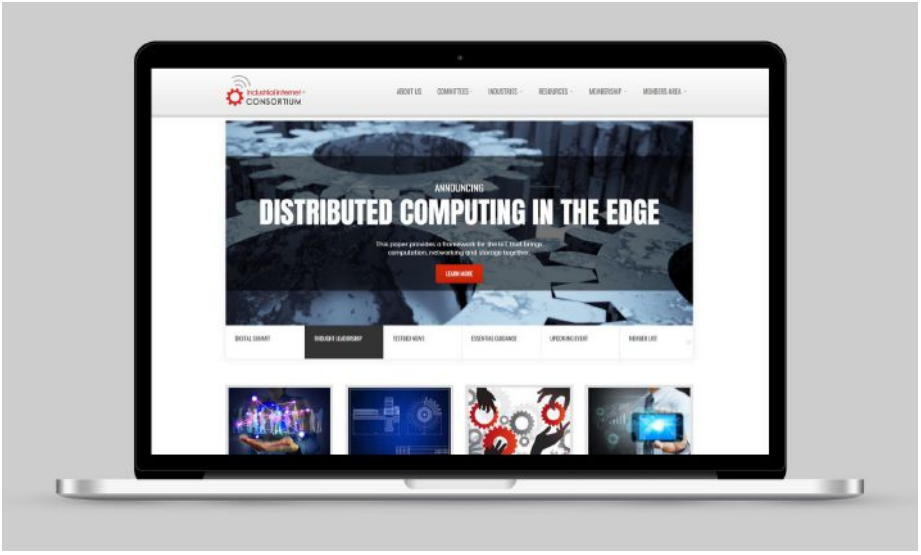
THE INDUSTRIAL INTERNET CONSORTIUM HAS announced the publication of the Industrial Internet of Things Distributed Computing in the Edge Technical Report. Designed for IoT system architects and implementers, the report describes a distributed computing framework that moves the capabilities of data center-based cloud computing closer to intelligent IoT devices at the edge.

"In edge computing, data, networking, storage, and computing are distributed throughout layers of edge computing nodes from IoT devices to the data center – distributing the economies of scale of cloud capabilities throughout the system," Chuck Byers, Co-Chair, IIC Distributed Computing Task Group, and Associate CTO of IIC said.

"The migration of cloud capabilities into the edge allows data, storage, and computation to gravitate to where it can be handled most efficiently, whether in a data center or the edge."

The technical report includes:

- A structural and functional framework for distributing computing in the edge
- Definitions of key architectural concepts employed in distributed edge computing
- Essential capabilities of an edge system's elements
- Security and management functions
- Essential interfaces for these elements



SOURCE: IIC

Report describes a framework moves cloud computing closer to intelligent IoT devices at the edge.

System architects can use the framework as a template to derive a concrete distributed computing architecture. Operations technologists, information technologists, and managers can use the report to learn more about the elements and advantages of distributed computing in the edge.

"Distributed computing, and the nodes and edge systems that form its key components are essential to the success of organization's critical IoT systems and digital transformation plans," said John Zao, Co-Chair, IIC Distributed Computing Task Group. "By moving to a distributed edge computing architecture, organizations across industries can reduce costs and meet critical performance, trustworthiness, and efficiency requirements for their IoT applications."

*News from **Industrial Internet Consortium**.*

International Initiative to Define OPC UA Cloud Library

THE OPC FOUNDATION, IN COLLABORATION with CESMII, has announced the launch of a OPC UA Cloud Library Joint Working Group (JWG).

The goal of the JWG is to specify how OPC UA information models of machines, SCADA and Manufacturing Execution Systems will be stored in and accessed from a cloud-based database. The database will enable manufacturers to draw from a wide range of OPC UA information models and profiles for use in their pre-built shopfloor and business digitalization applications.

Collaboration between the OPC Foundation and the Smart Manufacturing Institute is a natural fit given their complementary efforts. On one hand, the US government-backed Smart Manufacturing Institute sets out to help accelerate the adoption of Smart Manufacturing by businesses of all sizes by enabling frictionless movement of information (data and context) between real-time operations and the people and systems that create value in their organizations.

On the other hand, the OPC Foundation created a globally adopted open data interoperability standard via its OPC UA specification. The specification's information modeling capabilities and secure, scalable communications made it a cornerstone of Industrie 4.0 and other national Industrial IoT initiatives.

By working together, CESMII and the OPC Foundation aim to enable the broadest range of US manufacturers and beyond to innovate and go-to-market in their digital transformation using the right data modeling foundation.

John Dyck, CEO of CESMII, explained: "This joint working group validates our core, overarching strategy and commitment to interoperability and an open ecosystem, enabling the digitization and reuse of standard, templatized data structures that will dramatically reduce the cost and complexities of implementing Smart Manufacturing."

"Crowdsourcing the domain expertise required to create these reusable device, machine and process profiles will dramatically lower the barrier of entry for innovation and value creation in manufacturing, and ensure that Smart Manufacturing is accessible not just to the large manufacturers, but to the small and medium manufacturers as well," Dyck added.

*News report by **OPC Foundation.***

The C7015: bringing multi-core in IP 65/67 directly to the machine

www.beckhoff.com/c7015

Up to four cores in IP 65/67: with its extremely robust, fanless C7015 ultra-compact Industrial PC, Beckhoff as a specialist in PC-based control technology offers the possibility to install a high-performance Industrial PC in a highly compact design directly at the machine. Versatile on-board interfaces enable connection to the cloud or to other networks. The integrated Intel Atom® CPU with up to four cores allows simultaneous automation, visualization, and communication in demanding industrial IP 65/67 applications. In addition to classic control tasks, the C7015 is ideally suited for use as a gateway to connect machines and plant sections – and can even handle complex preprocessing of large data volumes thanks to its high processing power.

3 x LAN, 2 x USB, Mini DisplayPort and integrated EtherCAT P port

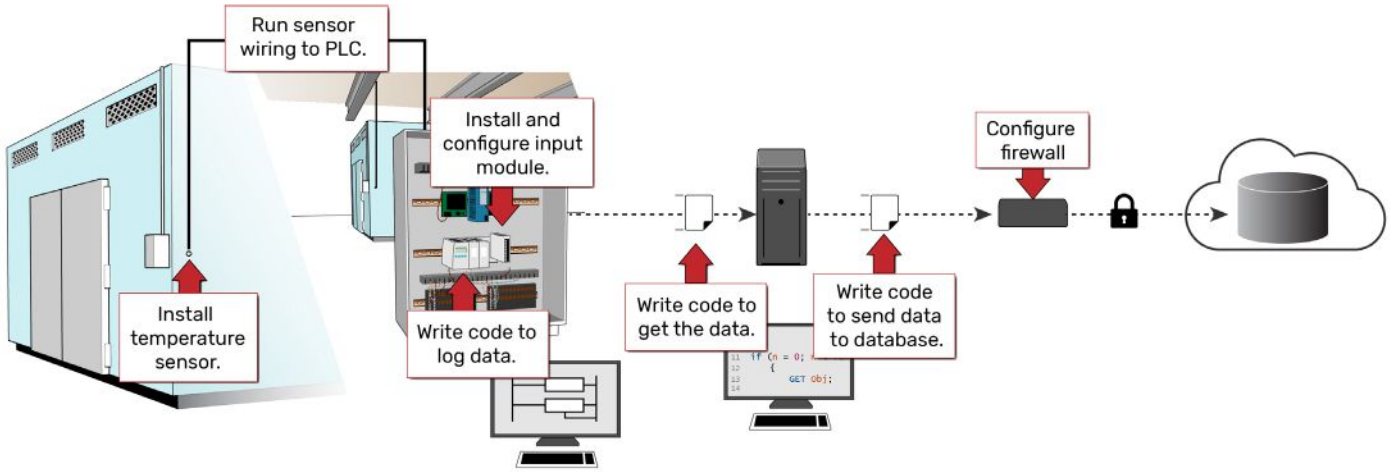
sps connect
The digital automation hub

Connect with the Beckhoff experts:
www.beckhoff.com/sps

New Automation Technology **BECKHOFF**

Distributed I/O and control build IIoT from edge to cloud

Next generation digital I/O and more distributed global architectures are enabling connectivity to the cloud for sensors and actuators, and for the I/O systems and controllers linked to them. These edge-to-cloud architectures depend on options at the edge for acquiring, securing, storing and processing field data.



SOURCE: OPTO 22

Traditional data acquisition methods require configuring and maintaining many layers in a hierarchy of hardware and software.

DIGITAL TRANSFORMATION ALONG WITH THE Internet of Things (IoT) or Industrial IoT (IIoT), are familiar concepts to almost anyone working in a role involving industrial automation. These initiatives involve ever smarter devices communicating progressively closer to the "edge," perhaps connected to an internet "cloud," or even through some kind of intermediate "fog." Even if we consolidate these terms under the umbrella of IIoT, for most folks a simple question remains: what is the goal of the IIoT?

Simply put, end users would like the IIoT to 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. Sharing process data has long been a goal of industrial automation, but traditional operational technology (OT) architectures are poor at scaling, priced prohibitively, and demand complex configuration and support. So what is changing to achieve this more ambitious goal?

Much as consumer hardware and software technologies have shifted to improve ease-of-use and connectivity, industrial products and methods are following the same trend. By adopting information technology (IT) capabilities, they are making it easier to connect industrial equipment with computer networks, software, and services, both on premises and in the cloud.

Up and down the architecture

Industrial automation architectures generally address data processing from a hierarchical perspective, as with the classic Purdue model. One good feature of this hierarchy is the clarity it provides with regard to where data can originate, be stored, undergo processing, and be delivered.

However, the task of transporting data and processing it in context is often quite difficult, because so many layers of equipment are required to connect devices and applications.

For example, the illustration above shows a traditional method of acquiring temperature data from facility equipment and moving it to a back-end client, like a database.

The lowest level of the automation architecture is made up of the physical devices residing on process and machinery equipment: sensors, valve actuators, motor starters, and so on. These are connected to the I/O points of control system programmable logic controllers (PLCs) and human-machine interfaces (HMIs), both of which are well suited for local control but less useful for advanced calculations and data processing.

However, using industrial communications protocols, these low-level devices can respond to data requests from upstream supervisory control and data acquisition (SCADA) systems where it might be historized or made available to corporate-level analytical software. Sharing data within multi-vendor systems, however, often requires additional middleware, such as OPC device drivers, to translate the various industrial protocols.

More advanced site manufacturing execution system (MES) and overall enterprise resource planning (ERP) software also reside at higher levels of the architecture, hosted on PCs or servers on site or in the cloud, where the cloud is defined as large-scale, internet-based, shared computing and storage.

Information generally flows up to higher levels to be analyzed and used to optimize operations, but the middle layers are required in order to interpret, translate, filter, and format the raw data produced by low-level devices and protocols.

Since these low-level devices typically lack protection against cyber-intrusion, a clear division must also be maintained between high-level systems exposed to external networks and low-level systems. Developments over the past decade are significantly altering this traditional hierarchy, flattening and simplifying it to a great extent.

Spanning edge, fog and cloud

A hierarchical approach was necessary when computing capability, network bandwidth, and security features were much less available. Each step up the hierarchy from a basic hardwired sensor to cloud computing systems was required to access greater computing and networking resources. It also clearly

delineated the security measures networks required around unsecured field equipment.

Today, the relationship has changed because sensors and other edge devices are far more capable, with some of them including processing and communications abilities similar to a PC. Security protections like embedded firewalls are also becoming a standard feature, allowing each device to act as a peer on the network instead of passively listening and responding to high-level systems.

The architecture is evolving to become flatter and more distributed, as in the image below, which illustrates the same data acquisition scenario but replaces several layers with a low-level device capable of sending data directly to its destination.

The edge, made up of low-level networks, is still a critical source of data, and the cloud is still a valuable resource for heavyweight computing. However, the resources in between, especially at the site level, are becoming a blend of data-generating devices and data-processing infrastructure.

This fuzzy middle ground earns the name fog, because it is akin to a widespread, pervasive, and middleweight cloud.

Many other factors besides advancing technology are driving this shift to a flatter architecture. The most straightforward motivation is to balance computing and networking demands between the edge and higher-level systems. Edge computing offloads central processing, preserves data fidelity, improves local responsiveness and security, and increases data transfer efficiency to the cloud.

Ultimately, however, this edge-to-cloud architecture depends on having new options at the edge for acquiring, securing, storing, and processing field data.

Distributed I/O evolution

Field data can be raw I/O points connected at the edge or derived calculation values. Either way, the problem with traditional architectures is the amount of work it takes to design, physically connect, configure, digitally map, communicate, and then maintain these data points.

Adding even one point at a later date may require revisiting all these steps.

To create more scalable, distributed systems, some vendors are making it possible to bypass these layers between the real world and intermediate or top-level analytics systems.

With enough computing power, all the necessary software for enabling communications can be embedded directly in an I/O device. Instead of requiring a controller to configure, poll, and communicate I/O data to higher levels, I/O devices can transmit information on their own.

This kind of edge data processing is becoming possible also due to a proliferation of IIoT tools, for example:

- *MQTT with Sparkplug B*: A secure, lightweight, open-source publish-subscribe communications protocol designed for machine-to-machine communications, with a data payload designed for mission-critical industrial applications
- *OPC UA*: A platform-independent OPC specification, useful for machine-to-machine communication with legacy devices
- *Node-RED*: A low-code, open-source IoT programming language for managing data transfer across many devices, protocols, web services, and databases

Today's smart remote I/O, also known as edge I/O, takes advantage of these technologies and combines them with standard IT protocols like TLS (transport layer security) encryption, VPN (virtual private networking) for secure remote connection, and DHCP (dynamic host configuration protocol) for automatic addressing.

Rather than requiring layers of supporting middleware, edge I/O devices are first-class participants in distributed systems.

Another obstacle to scalability for IIoT

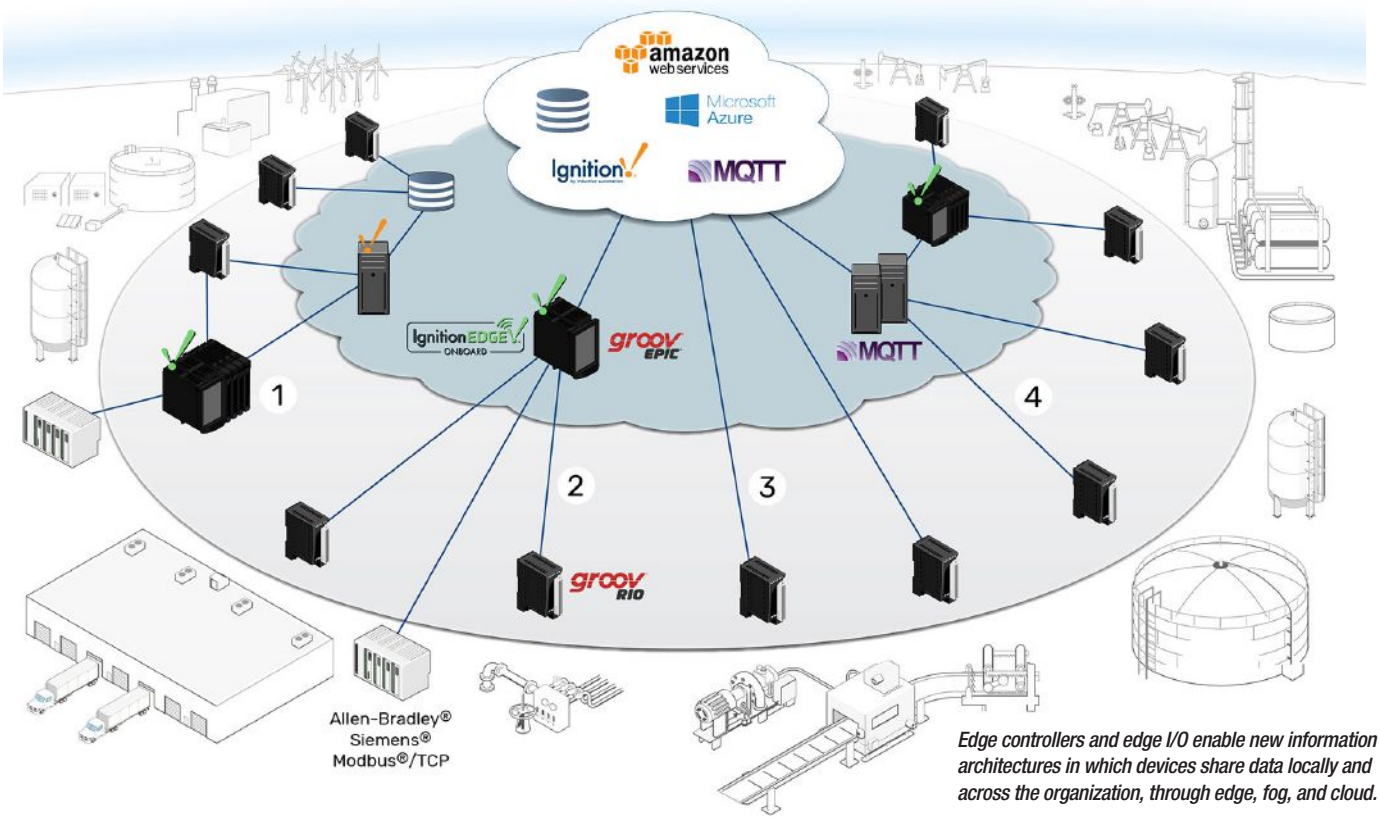
Robust Ethernet Networks

Complete your automation network with CTRLink's wide range of cost-effective wired and wireless 24 VAC/VDC powered Ethernet connectivity products with panel or DIN-rail mounting

- Managed and unmanaged 10/100/1000 Mbps Ethernet switches
- Single mode and multimode fiber optic switches and media converters
- Wired and wireless IP routers for easy machine integration and secure remote access
- PoE switches, mid-span splitters and injectors
- Diagnostic switches for network troubleshooting
- Custom configurations and outdoor-rated options available

CONTEMPORARY CONTROLS®

Learn more at www.ccontrols.com/ctrlink



SOURCE: OPTO 22

Edge controllers and edge I/O enable new information architectures in which devices share data locally and across the organization, through edge, fog, and cloud.

systems based on classic I/O hardware is the work required to provide power, network connections, and the right I/O module types. To address these issues, vendors are taking advantage of new technologies to make distributed I/O more feasible and flexible.

Power plus networking

One example is power over Ethernet (PoE) capability, which uses an Ethernet network cable to simultaneously supply low-voltage power and network connectivity.

When PoE is embedded into an edge I/O device, it can even supply I/O power, simplifying electrical panel design and saving money on additional components and labor.

Flexible I/O

To make it easier for designers to specify the right I/O interface types, some new I/O devices also offer more flexible configuration, like mixed and multi-function I/O channels. These provide extensive options to mix and match I/O signal types as needed on one device, reducing front-end engineering work and spares management.

The combination of these features within edge I/O devices makes it possible for implementers to easily add I/O points anywhere they are needed, starting with a few points and scaling up as much as necessary at any time. Wiring needs are minimized, so long as networking infrastructure is accessible.

For more comprehensive integration, control, and calculation, any number of edge controllers can also be integrated.

Edge controllers bring it together

As with traditional I/O hardware, traditional industrial controllers are limited in scope and require intermediary systems in order to connect process data to the rest of the organization. Like edge I/O, modern edge programmable industrial controllers (EPICs) leverage new technologies to assimilate more automation functions than previous generations could.

With industrially hardened components, secure networking options, multi-language programming, and multi-core processing, edge controllers can deliver traditional real-time I/O control while also hosting communications, visualization, and even database servers.

In the case of IIoT applications, edge controllers can use this flexibility to communicate with an array of data producers, transform their data in meaningful ways, and deliver it securely to data consumers.

Edge controllers combine sensing and control of traditional I/O, intelligent device fieldbus protocols, and modern edge I/O. They can also host OPC UA servers like Ignition Edge to communicate with a variety of networked devices, making them uniquely efficient at bridging disparate automation networks.

Then, with support for IT-compatible MQTT and REST interfaces and a variety of networking options, EPICs can securely connect OT networks to IT systems while reducing the layers of middleware required to do so.

The combination of edge I/O and edge control leads to a new distributed data architecture.

New system architecture options

So what new architectural possibilities are available to industrial automation designers using modern edge I/O and edge controllers? With edge devices making local data available to computing resources at the edge and at higher organizational levels, the logical hierarchy can be flattened even as the geographical distribution is expanded.

Here you can see some examples of new information architectures that are becoming possible for use in places like remote equipment installations, commercial facilities, campuses, laboratories, and industrial plants.

Shared infrastructure processing

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.

For example, area 1 in the image above shows edge I/O (groov RIO) placed at multiple remote sites with an edge controller (groov EPIC) at another site integrating data from existing PLCs. Two of the edge I/O modules are sourcing, processing, and communicating field data directly into a central corporate database, using Node-RED. The EPIC and other edge I/O exchange data for local control while also transmitting data to a central SCADA over MQTT. Data processing is distributed throughout the edge network, allowing central systems to ingest data more efficiently.

The combination of smart hardware and software closes the gap between OT and IT systems, creating a unified data network that is scalable and centrally managed.

Legacy device integration

Edge I/O can form a basic data processing fabric for existing equipment I/O in brownfield sites and work in combination with more powerful edge controllers and gateways using OPC UA to integrate data from legacy RTUs, PLCs, and PACs. This approach improves security and connectivity without interfering with existing control systems.

The example in area 2 demonstrates this. An edge controller acts as a secure gateway for legacy devices, allowing them to interact with cloud-hosted IoT platforms, SCADA, or MQTT clients while protecting them against unauthorized access from external networks. At the same time, edge I/O is used to integrate facility equipment (pumps, blowers, temperature sensors) and new equipment skids into the same network. The groov EPIC may control the groov RIO modules, aggregate and buffer their data in an embedded database, or simply transmit data to external systems.

Direct-to-cloud I/O network

Engineers can also design simple, flat, data processing networks using only edge I/O devices (without controllers or gateways), expanding as needed to monitor additional field signals. A distributed I/O system like this can process and report data directly to cloud-based supervisory systems, predictive maintenance databases, or MQTT brokers.

Area 3 shows groov RIO modules reporting data from the factory directly to the cloud, via Node-RED or MQTT. There's no need for intermediary control hardware, because each module provides configurable firewall and data encryption settings as well as a data processing engine to combine, filter, and format data. Since each edge I/O module is independent, the network can grow incrementally, reducing capital project expenditures required to integrate new equipment.

Many-to-many MQTT infrastructure

Edge devices with embedded MQTT clients can publish field data directly to a shared MQTT broker/server or redundant MQTT server group located anywhere the network reaches: on premises, in the cloud, or as part of regional fog computing resources. The broker can then manage subscribers to that data—any number of interested network clients across the organization, including control systems, web services, and other edge devices.

Area 4 shows this architecture. Both groov RIO and groov EPIC have embedded MQTT clients, allowing any of the other architectures to be combined into an efficient data-sharing network. Two edge I/O modules in this example are publishing to a regional server group.

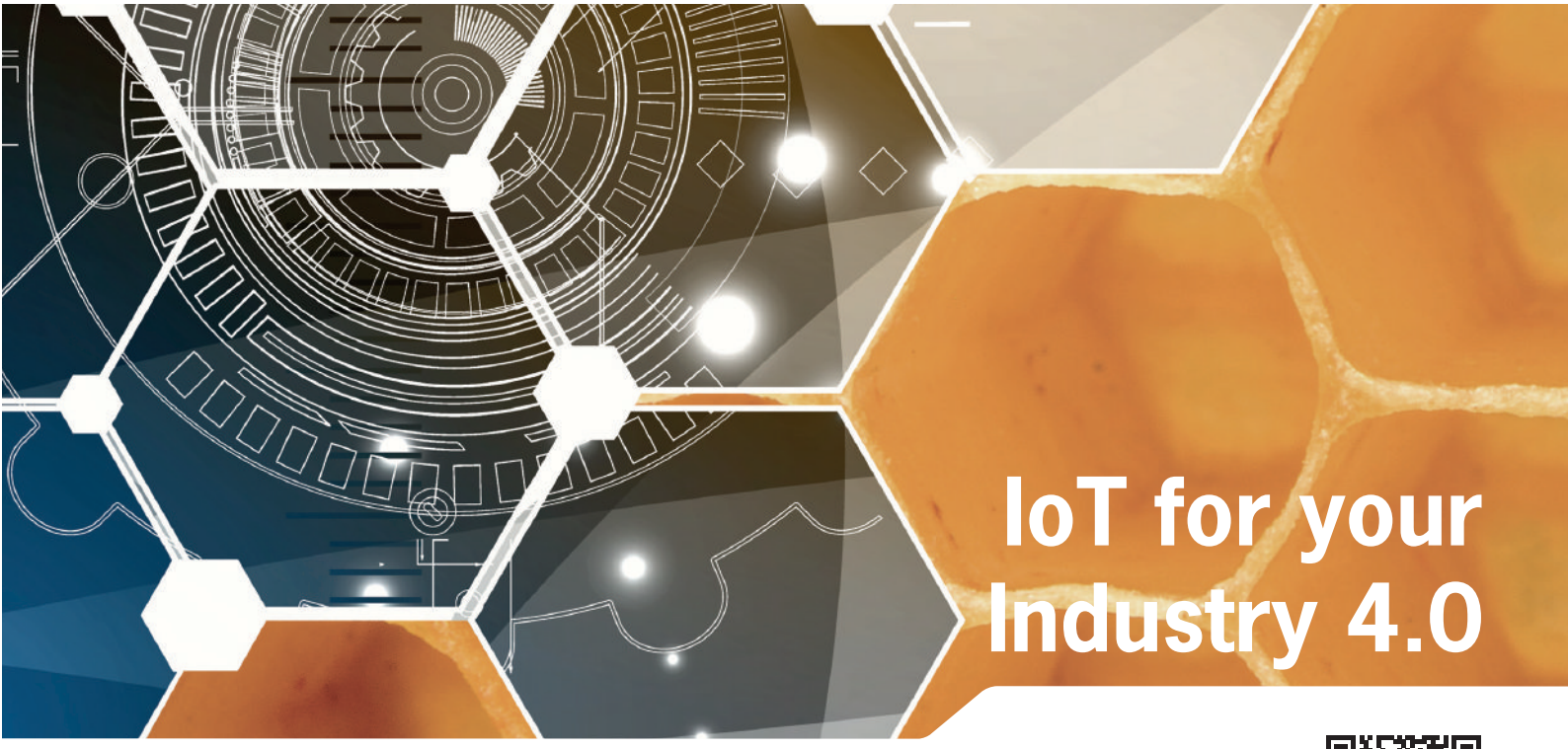
The other two are communicating with an edge controller at another site, which is using the edge modules as distributed I/O and publishing their data into the MQTT network. Once data is published to the broker, devices and services that need that data can subscribe to it from wherever they are on the network.

Seamless connectivity

Seamless connectivity is now a reality, thanks to technologies that make ubiquitous data exchange possible. New hardware and software products enable interconnectivity among physical locations in the field, at the local control room, in the front office, across geographic regions, and up to global data centers.

Distributed edge I/O, edge controllers, and associated networking technologies support data transfer through the edge, fog, and cloud portions of an industrial architecture. Using this approach, you can erase the former boundaries between IT and OT domains and get the data you need to optimize operations.

Josh Eastburn, Director of Technical Marketing, ***Opto 22.***



The IoT Enablement Company

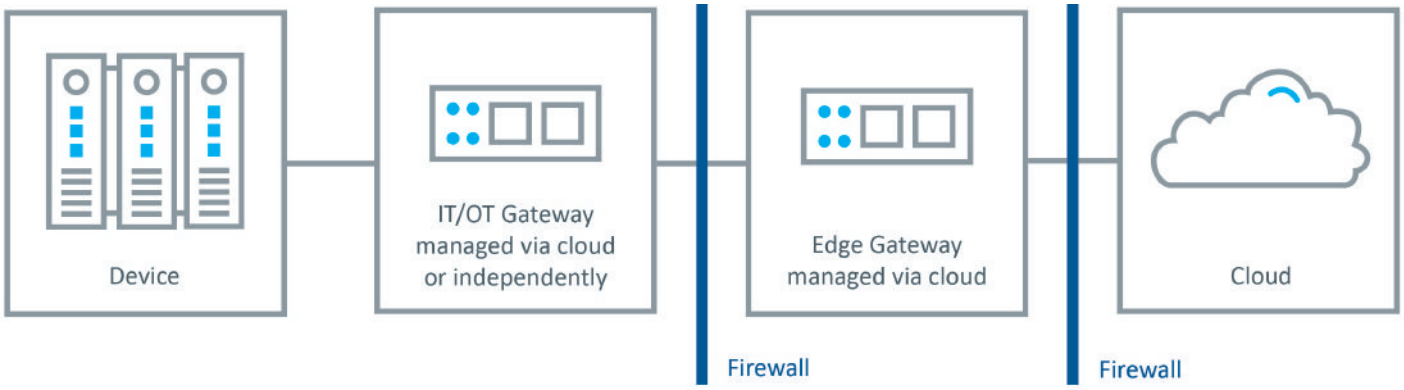
As a pioneer in connected applications, Eurotech provides best-in-class, proven building blocks for open, standard-based Internet of Things solutions for your Industry 4.0.

www.eurotech.com

EUROTECH
Imagine. Build. Succeed.

Data integration for the Industrial Internet of Things

IT architectures need to play a vital role in IIoT system architectures, with gateways evolving to provide more flexible, innovative and efficient software solutions. A key question is how network solutions can be deployed to exploit software, IT and innovative algorithms and make production more efficient.



SOURCE: SOFTING

In a typical IoT application topology, two gateway layers include one in the automation network and a second in the 'demilitarized zone' between two firewalls.

WHEN IT COMES TO EXPANDING AND OPERATING innovative IoT solutions, IT architectures have a key role to play. What questions need to be answered about the architecture that interfaces IT with OT, and what relevance does this interface have for edge and cloud? In this era of digitalization, how are traditional gateways evolving into flexible and efficient software solutions for data integration?

A question of IT architecture

Whether we are talking about digitalization, Industrie 4.0 or the Industrial Internet of Things (IIoT), these rather overworked terms refer to much the same thing: how we can exploit software, IT, and innovative algorithms to make production more efficient.

Many companies and users have gotten their first look at these ideas in test installations and proof-of-concept projects. But there are major challenges to address before a successful transition to broad-based usage in production environments.

Questions about architecture or more accurately, the IT architecture, play an important role here. Which standards and technologies are utilized in an Industrial IoT solution – and how do cloud platforms fit in here? How is IT security guaranteed?

Where are open interfaces needed in the overall system to ensure the easy integration of different makes of component? Which standards are relevant here? The answers to these and other architectural questions will decide how successfully users can then handle the kinds of challenges posed by the inherent potential of their software and IT systems.

ROI for Industrial IoT applications and innovative software solutions is often unclear for a new project. While the underlying potential offered by AI, machine learning, and Big Data analytics is hardly in doubt, the real-world benefits are often difficult to assess before a project begins.

This is where a good architecture ensures that providers keep costs manageable at project start while simultaneously offering reusability, future-proofing, and expandability for the solution.

Industrial IoT typically refers to the use of a centralized platform that enables applications to be deployed at any site and in any plant situation, despite any actual differences between the various sites in terms of installed equipment and available interfaces. A well-chosen architecture will ensure the efficient operation of this centralized platform while reducing the extent to which investments in IIoT depend on the specific circumstances of these sites and plants.

The pace of innovation in IT remains high: While plant systems and installed equipment are still likely to have a multi-year or even multi-decade lifecycle, the cycles of innovation in IT tend to be short. As a result, architectural decision-making, especially at the OT/IT interface, will greatly affect whether, and at what cost, operators are able to exploit the plant's potential for innovation over its lifetime and the expected improvements offered by innovative software solutions.

Efficient use of IT: As more money is invested in IT and IT costs rise, general questions about the overall efficiency of IT systems become more important. Accordingly, decisions about architecture and IT infrastructure in particular are of fundamental importance for the Total Cost of Ownership (TCO) of an IIoT solution.

The role of major IT providers

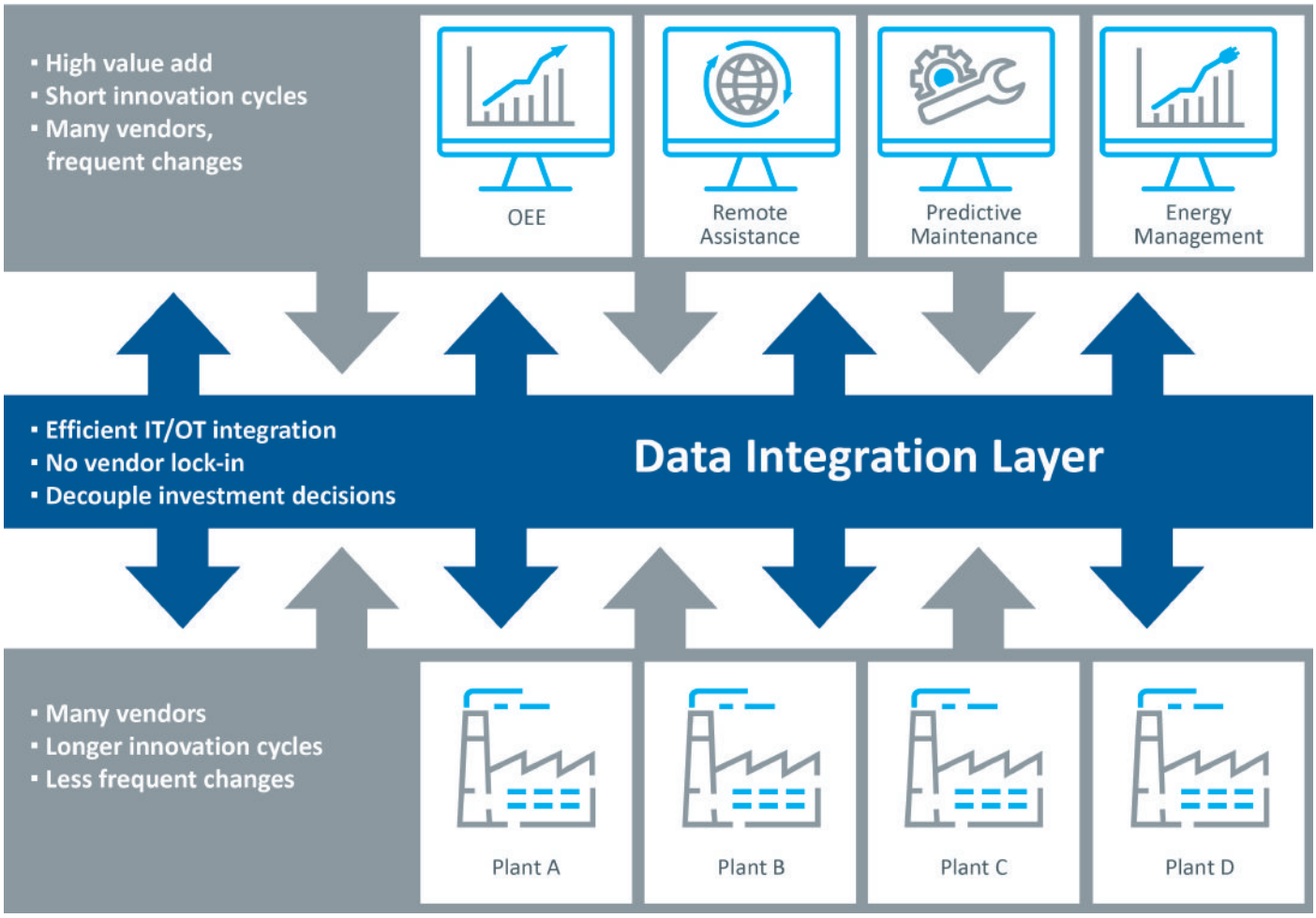
As the importance of software and IT continues to grow, it goes without saying that the major traditional IT infrastructure providers will also have a key role to play in industrial production systems.

In the vanguard are the Big Three in cloud platforms: Amazon, Microsoft, and Google (also known as 'hyperscale' providers). For manufacturers, these companies are relevant for several reasons.

Cloud platforms typically offer general advantages for software usage in terms of costs and flexibility, which goes a long way to explaining their resounding success in enterprise IT. Unlike enterprise IT, however, the Internet of Things needs processing power near these 'things' and not just in the cloud. So for a while now, cloud providers have been supplementing their main platform with services for the 'edge' – a term referring to local data storage and processing.

In recent years, cloud platform functionality has also been extended to include specialized services for IIoT applications. Alongside their infrastructure and base services for cloud, edge, and IIoT, these providers have also been busy developing innovative algorithms for machine learning and artificial intelligence that can also be used easily by application developers and system integrators.

SOURCE: SOFTING



Data integration for innovative IoT solutions must fulfill a series of complex requirements, while architectural issues have a key role to play in implementation.

Power of software virtualization

Turning to look at the reference architectures used by IIoT cloud providers, we can see that they have 'standardized' at least in the sense that they all support the use of virtualization technology for edge computing. Let us first take a closer look at virtualization before we consider the needs of our industrial users.

Virtualization, which uses integration mechanisms to reduce the dependencies between the software layer and the hardware layer, has been one of IT's megatrends during the last ten years.

Virtualization allows software to be deployed simply and flexibly to a wide range of hardware and system environments: users enjoy a range of benefits that include lower costs for software development and maintenance.

One specific example of virtualization is 'containerization', which, with the introduction of services from Docker, has become increasingly widespread over the last five years or so. This technology is now predominantly used in IoT reference architectures for edge and cloud computing.

However, virtualization technology is by no means limited to cloud platform interactivity. Even if users decide not to utilize a cloud platform, there are still many good reasons to make use of virtualization when designing the implementation of an innovative and efficient software solution such as a solution for the Industrial Internet of Things.

Automation networking

So, what do the typical plant systems and automation networks look like? What are the requirements of the users who operate these systems? And how do these match up to the architecture questions discussed earlier?

IT security and network topology are core issues here. An automation network is usually operated behind a multi-layered setup with two firewalls. A 'demilitarized zone' (DMZ) is located between these two firewalls. There is no direct connection between the automation network and the company network (or Internet), and communication between the DMZ and automation network must also be secure.

As a result, most IIoT use cases therefore make it necessary to work with at least two gateway layers. One layer includes all of the edge gateways within the DMZ, which have connectivity to the Internet or to a cloud platform (as required), plus a second layer of IT/OT gateways within the automation network, which can communicate directly with the edge gateways but not the company network or a cloud platform.

Apart from these specific network requirements, as derived from the network topology, other (functional) requirements for data integration and for the OT/IT interface also need to be considered.

In a nutshell, this means that installed plant/equipment as well as brownfield projects will remain relevant and dominant for many years. While newer devices might increasingly offer standardized interfaces, especially ones based on the OPC UA standard, most of the installed base of equipment will not.

As part of IIoT solutions, data integration also needs to do much more than simply translate proprietary interfaces into standardized protocols.

Some of these more complex requirements include the efficient handling of what can be a potentially large number of data sources (data aggregation) as well as the above-mentioned need to abstract plant- or device-specific interfaces to achieve the multi-site deployment of a uniform set of software applications.

Users also need to be able to respond flexibly to IT security requirements – not only to maximize security but also to ensure the costs involved stay at an acceptable level.

IT/OT gateway architecture

Let us now look at the architectural nuts and bolts of an IT/OT gateway. Traditionally, this gateway 'belongs to OT': It is installed and operated locally at one site, with the aim of providing an HMI system or database with data from the automation network, for example. These traditional applications change very little over the lifetime of the plant system. As a result, the use case here requires a low-maintenance product that can be operated for many years with barely any changes to its configuration. Innovative IIoT solutions will place very different demands on such a gateway or data integration, however. These requirements include the following

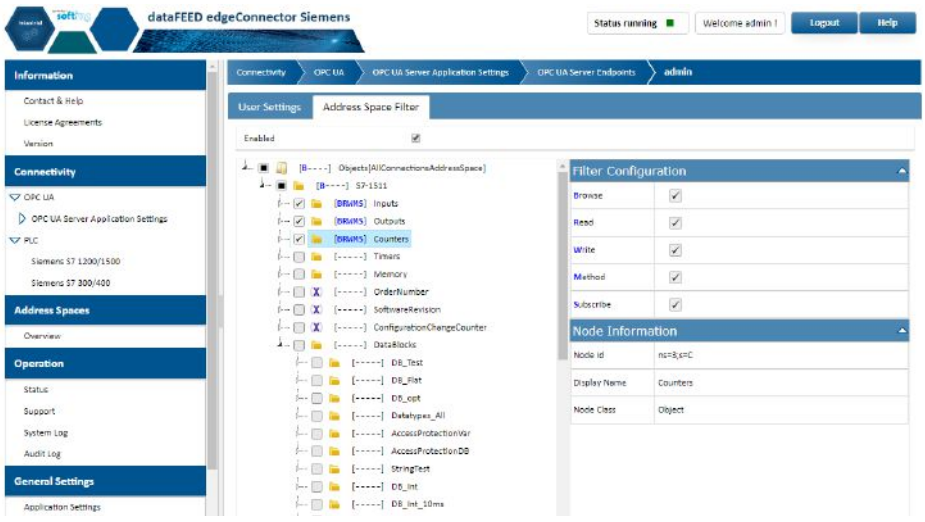
Dynamic and flexible payload configuration. In many cases, it is not advisable or even technically possible to simply send all data generated to an edge gateway sitting in the DMZ. Users need options for easy configuration of the payload as well as the efficient modification of this configuration over the lifetime of the plant system – such as when a new software application needs access to data that have not been provided to date.

Flexible expandability: Very few users will be able to say which new pieces of software or IIoT applications might be of interest in a couple of years. Accordingly, a data integration solution must also be flexible enough to support later applications without data integration needing to be redone from scratch.

Flexible data normalization even at the lowest level: The IT/OT gateway supplies the relevant OT-facing interface for software applications and so it should abstract out the actual equipment installed and other details of the plant system. A corresponding configuration will, in all likelihood, also change over the lifetime of the plant system, whether due to changing requirements for the interface stemming from IT or because changes also occur now and then in the plant system itself but the outward-facing (OT/IT) interface needs to stay the same.

Use of edge analytics and machine learning: Some applications need to have complex computations executed as near as possible to the data source. This requires IT/OT gateways capable of acting as platforms for the corresponding software modules.

Summing up, we can conclude that data integration on an IT/OT gateway has a more complex set of functional requirements than mere 'protocol translator' gateways. The software architecture used by a gateway of this kind should support innovative IT technologies like virtualization in particular, since the associated benefits are also relevant for this layer in an innovative and efficient IIoT solution. By transforming themselves from a merely static component within OT into a dynamic software solution manageable from IT and via cloud platforms, gateways are becoming part of an 'industrial edge' that runs on standard hardware.



SOURCE: SOFTING

Web interface for local configuration of the edgeConnector Siemens. Configurable settings include the granting of separate and independent sets of access privileges for different IT applications.

Evolution of dataFEED technology

These were the reasons why Softing set itself the goal of redeveloping its trusted dataFEED product family into a modular, open software platform about a couple of years ago.

One focus of this redevelopment work involved providing existing gateway functions and software products as Docker containers. Another aspect was the development of entirely new functions that would enable the dataFEED product family to handle the requirements, as discussed above, for more complex data integration in an IIoT context. This included the cleanest possible implementation of the OPC UA Companion Specifications, to provide straightforward support for corresponding server interfaces.

Ensuring customer choice was another very important factor. This needed to be oriented on the options typically offered by many IoT platforms; dataFEED customers can therefore choose whether they want to operate the software components together with one of the cloud platforms from a major provider (Amazon AWS and Microsoft Azure are currently supported) or as a data integration solution that is independent of any cloud platform.

The recently released edgeConnector Siemens is the first commercially available Softing product to be based on container technology. Connecting to Siemens SIMATIC S7-300/400 and S7-1200/1500 controllers, this product provides access to data via an OPC UA server interface integrated into the connector. As a Docker container, the software module offers flexible deployment options, such as to devices running edge services from major cloud platforms (Azure IoT Edge or AWS IoT Greengrass, for example); it can also be deployed independently of these platforms.

An integrated web interface makes it easy for users to manage local configuration of the edgeConnector Siemens. For remote administration, the module also offers a REST interface that allows the connector to be managed by a cloud-based application (for example). Configuration itself is flexible and includes fine-grained security settings (such as separate and individual role-based access privileges for different OPC UA client applications).

In this way, the edgeConnector Siemens offers industrial users an opportunity to exploit the potential of virtualization and cloud both for data integration as well as the setup and operation of an interface between IT and OT as part of an innovative Industrial IoT solution. Other container-based products will be released over the next few months.

Potential for innovation

Commercial software offering efficient deployment are available for data integration, and fundamental issues about protocols and methods of access to data from automation networks can now be considered to have been solved as part of innovative IIoT solutions.

As a result, standardization bodies and data integration solution providers are now increasingly tackling the question of how best to enrich interfaces with semantics and information models, and to ensure their simple usability by software applications hosted in the cloud. While the OPC UA standard fulfills all of the technical requirements for defining interfaces capable of offering valuable semantic information, the standard itself is silent concerning the question of how the enrichment of an unstructured interface with this relevant semantic data can proceed most efficiently in a real-world brownfield project. This is an area offering further potential for innovation in the years to come.

Technology report by ***Softing.***

CC-Link Partner Association: The future is transparent, convergent and time-sensitive

INDUSTRY 4.0 IS AN ESTABLISHED trend in factory automation, aimed at increasing convergence and transparency. By implementing systems with these capabilities, businesses can gain greater insights into their processes, hence achieving better quality, productivity and reduced costs. The technology that is delivering these benefits is Time-Sensitive Networking (TSN).

John Browett, General Manager of the CC-Link Partner Association (CLPA) – Europe, looks at how TSN supports convergence and transparency and what solutions businesses can adopt.

The Connected Industries of the future will generate a constant stream of data from their production systems. Insights derived from this data will provide a key tool for optimising manufacturing processes and improve the ability to adapt to new or varying demands. To gain these insights, data transparency and convergence will be paramount, as they represent the foundations of data-driven manufacturing.

The ability to implement these capabilities ultimately lies in the ability of industrial networks to deliver them. In particular, the network must be able to transfer high volumes of data from multiple sources across the enterprise. Also, it should share time-critical traffic in a reliable and predictable manner to maintain operational performance and efficiency.

The most promising technology for this is TSN, an extension of industrial Ethernet that supports deterministic communications via accurate time synchronisation and traffic scheduling. These mechanisms provide the foundation of the convergence necessary to provide the required levels of transparency. Hence, we are moving to a future where not only machine control data, such as I/O states, safety and motion control, share the same network in real-time, as it is the case with many current industrial Ethernet protocols, but now we can add almost any other kind of Ethernet traffic too. The benefits are simpler, less expensive and easier to maintain networks that provide unprecedented levels of transparency into manufacturing processes. The associated convergence can not only offer the ability to simplify networks on the shop floor, but can also more tightly bind the shop floor to the enterprise, delivering ever greater integration between the operational technology (OT) and information technology (IT) worlds.

2020 sees the CLPA celebrating its 20th Anniversary. During that time, it has been at the forefront of technology innovation in open automation networks with a proven track record of leading the industry. As part of its goal to provide innovations for the next 20 years, in late 2018, the CLPA launched CC-Link IE TSN. This is the first open industrial Ethernet that combines gigabit bandwidth with TSN functionalities and is designed to provide a gateway to the industrial communications of the future, while supporting current needs. This will help automation vendors develop TSN-driven products as quickly as possible, in turn supporting machine builders and end-users to improve their operations by implementing the technology on the factory floor.

By selecting CC-Link IE TSN open network technology for automation devices, vendors can become the first to offer TSN-based products, gaining a unique competitive edge. Machine builders will benefit from lower cost, simplified system designs and faster time to market. Similarly, manufacturing businesses using these products and systems can improve their current operations while getting ready for the future.

Want to learn more? The CLPA has just produced a white paper that explains the case for action now on TSN. End-users, machine builders and device vendors alike will find this a useful guide to why incorporating TSN into their activities will deliver concrete benefits as we move into this converged future. Download your copy now from https://eu.cc-link.org/en/campaign/2020/tsnwp

If you would like to discuss CC-Link IE TSN with the CLPA directly, they will be participating in SPS Connect. For free access to this on-line event, visit https://eu.cc-link.org/ to claim your complimentary ticket code and get your questions about TSN answered.

Alternatively, contact the CLPA at partners@eu.cc-link.org for Europe, or Info@CCLinkAmerica.org for North America.

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

Expert Insights: The inside view from our industry partners

Contemporary Controls: Benefits and versatility of IP routers

MOST NETWORKS TODAY COMMUNICATE via the Internet Protocol (IP) – the backbone of the Internet. This includes modern machines comprised of complex subsystems with PLCs, HMIs, Barcode Readers, Motors etc. The machine builder pre-defines each subsystem IP address and the range of addresses devoted to each machine along with the application used for controlling these devices. This addressing convention used by the machine builder may conflict with the addressing policies of the customer potentially jeopardizing a speedy integration of the machine or machines at the plant.

Ease of integration

Contemporary Controls' Skorpion series of IP routers eases the integration of new machines into the existing network. Each machine consisting of multiple IP devices connects to the LAN side while keeping the same IP settings for the devices and the application, lowering installation cost and eliminating the troubleshooting associated with changing IP addresses.

The IP address for the WAN port on the IP router is the only setting that requires modification to match the customer network. This allows the reuse of the same configuration across multiple machines that form their own separate network on the LAN side behind an IP router. Having the same setup across all machines makes training maintenance personal easier and reduces maintenance errors. In case of a failure, a device replacement can be achieved quickly as the configuration is the same across all the machines. An IP router cuts down on the number of IP addresses required at the site, as only a single IP address for the WAN port of the IP router is required.

Accessing machine data

IP router features such as Port Forwarding, Port Range Forwarding and NAT allow access to the LAN side devices of the machine from the WAN-side plant network. This access can be used to gather data from the machine for later analyzing it or to update programs on the machine for a different product build from a WAN-side server. An additional benefit of using the IP router is that it restricts multicast and broadcast packets to the LAN side within the machine preventing extra traffic on the plant network that would add extra burden to process and throw away this traffic. The same thing applies for the machine– it is only busy doing its task with the devices that are part of its network and not inundated with extra plant traffic.

Providing extra security

Some older IP devices don't offer the ability to setup the Gateway IP address which prevents them from communicating across different subnets. An IP router with the masquerade feature changes the IP packets to allow communication to occur from the WAN-side to this LAN side device without a Gateway IP address. IP routers provide extra security with the use of an Allowlist where only specified IP address on the WAN-side can access the individual IP devices in the machine. The IP router blocks unauthorized access from the devices not specified in the Allowlist.

Remote access via VPN

IP routers also offer VPN capabilities that allow for secure remote access. A machine builder can securely login to a machine at the customer site from his own location to diagnose, troubleshoot or perform firmware updates without the need to travel to the customer site. IP routers are available with wired (Ethernet), Wi-Fi or cellular options.

These options provide the customers multiple options to meet their application need. Cellular routers allow access to devices at sites where Internet infrastructure doesn't exist – either because they are at remote location or it has just not been put in place yet. With so many advantages, using an IP Router to facilitate network integration is a no brainer.

Harpartap Parmar
Senior Product Manager, ***Contemporary Controls***
www.ccontrols.com

Phoenix Contact: Industrial automation security: Specialized or better integrated?

DIGITIZATION OFFERS MANY opportunities, but also poses risks. For example, the factory network may be subject to unwanted attacks, such as unauthorized access, malware, incorrect operation or malfunction. To address these risks, cyber security includes technical measures designed to prevent or at least contain damage.

Essentially, these are methods to limit access and approaches to protect integrity. The individual measures complement each other in their effects.

Protection against unauthorized access

Regardless of whether a targeted attack or a misuse must be prevented, access protection is probably the most important instrument of cyber security. It begins with physical protection against unauthorized access and continues on the communication level. If the attacker does not gain access to the network, the damage potential is obviously much lower.

Protection at the network level

Firewalls are the first line of defense to prevent unauthorized intrusion via communication links. They filter the communication connections so that only permitted connections can be established. This filtering can either be integrated into a device or implemented by a dedicated firewall component in the network. A built-in firewall is advantageous in terms of cost, but is more vulnerable to attack depending on the quality of the main system implementation. If many different devices with integrated firewall are to be used, all variants must be administered and maintained. If the main system is nevertheless successfully attacked, the firewall can also be infiltrated. In addition, the high-quality setup of a firewall requires own knowledge, which is not always available.

A dedicated firewall as an external device requires a target-oriented investment, but allows a selection independent from the other automation components. In addition, central administration can be realized. The independent security device proves to be robust against weak points in other automation components. It can be patched and updated without affecting the function of the overall system. In the event of a network overload, the firewall provides protection because it can itself take the load and thus shield the automation components located behind it.

Remote connection protection

Remote connections via the Internet should always be encrypted, for example via VPN. The protocols used for this purpose generally not only protect against the interception and tapping of information, but also contain mechanisms to protect against manipulation. For the implementation, it is also true here that integration through software or as an already built-in function opens up cost advantages, while execution as a dedicated component has a positive effect on the quality of the implementation and administration. That's why the functions of a VPN gateway and a firewall are combined in numerous solutions.

Protection at user level

If the communication has been allowed by a firewall or is possible via a local access, it should be protected by a user login. The user management can take place locally, but is then difficult to administer. Central management systems prove to be more practical. If the automation system does not support access control, a dedicated firewall can help. This firewall will only allow pre-defined connections if the user has already logged on to the firewall.

Protection against malware

Many damages are caused by malware whose damaging effect only occurs when it is executed. To prevent the malware from being implemented nevertheless, anti-virus software is available as a classic security product. However, its quality depends on the detection rate and regular updates. Furthermore, the demands on computing power and occasionally observed error detections lead to malfunctions in automation applications. Solutions that directly prevent the execution of unknown software - keyword: whitelisting - as well as automation components with built-in integrity protection are more suitable. An essential element here is a secure patch and update process that only allows the installation of original software or firmware.

Conclusion

The comparison of integrated security functions with specialized security products makes it clear that both concepts have their strengths and should at best complement each other. Built-in functions prove to be particularly useful if, for example, the entire application is operated by a single control unit that is also used to connect to the Internet. More complex systems consisting of several devices are better connected by specialized firewalls and VPN gateways. Simultaneous use of the security functions integrated into the components can further increase the security level.

Dr.-Ing. Lutz Jänicke
Corporate Product & Solution Security Officer,
Phoenix Contact
www.phoenixcontact.com

Omdia: Industrial connectivity – an overview

CONNECTIVITY IS ONE OF THE fundamental pillars upon which the industrial IoT (IIoT) is built. And over the last few decades, industrial connectivity in particular has evolved considerably, especially in response to the ever-changing requirements of the manufacturing industry.

Following the advent of discrete wires to communicate with field devices, the Fieldbus industrial networking technology came into play, introducing the concept of a controller to communicate with field devices. A rival technology, Ethernet, became a household name in the early 1990s and then found gradual adoption by industry starting in the early 2000s.

In many industrial networks today, Ethernet is deployed along with Fieldbus and wireless technologies. Those mechanisms continue to evolve even with the arrival in the industrial manufacturing world of much newer technologies, such as 5G, Time-Sensitive Networking (TSN), and Advanced Physical Layer (APL).

The new technologies form part of a comprehensive examination of the industrial connectivity landscape covered by my recently published study, Industrial Communications Report – 2020.

A number game

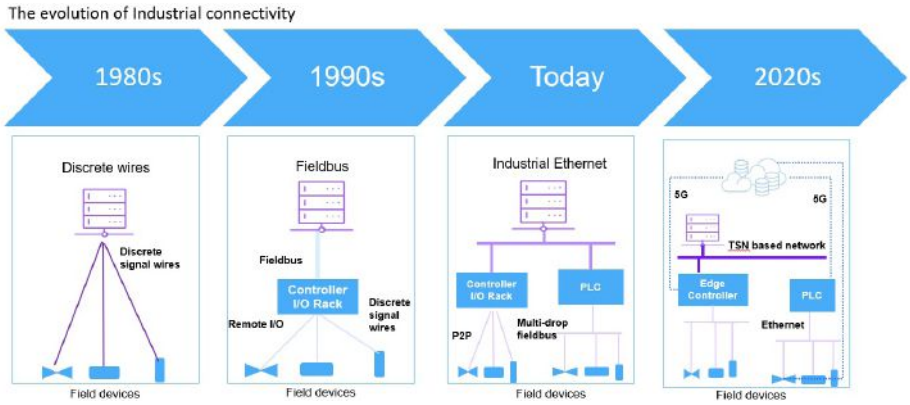
The number of connected nodes being shipped every year continues to increase with an exception of 2020, Omdia estimates. Not only are more devices able to connect to a network, the number of nodes is also on the rise. The market for connected nodes in industrial communications approached 142 million units in 2019 and is forecast to grow to more than 204 million in 2024. The shift to Ethernet has accelerated as Industry 4.0 and IIoT solutions are maturing and becoming more prevalent, with Ethernet seen as the industrial networking technology enabling the solutions. Overall, the number of Ethernet-connected nodes will more than double from 67 million units to 117 million by 2024, translating into a compound annual growth rate (CAGR) of 11.3% for the Ethernet market during the five-year period, Omdia is forecasting.

PROFINET and EtherNet/IP, two industrial Ethernet protocols, account at present for 56.4% of newly connected Ethernet nodes, and both protocols will increase their share of market during the forecast period. By 2024, the two will represent more than 61.4% of all newly connected Ethernet nodes.

For Fieldbus, growth will decline for the same period with a 0.1% CAGR; Fieldbus-connected nodes are forecast to decline from 51.3 million to 50.9 million. Even so, Ethernet technologies have outpaced Fieldbus technologies on new connected nodes in 2019.

PROFIBUS remains the leading Fieldbus protocol at 20.7% market share of the Fieldbus market, but IO-Link is the fastest-growing, with many sensors using IO-Link for Fieldbus.

Wireless use in industrial networks, meanwhile, will grow at a healthy CAGR of 12.1% during the same 2018-23 period, from 1.7 million connected nodes to 3 million. The two leading wireless protocols are WLAN and WirelessHART. Together with cellular these three accounts for 63.5% of total market of the wireless protocol market.



Syed Mohsin Ali
Senior Analyst, Industrial Connectivity, ***Omdia***
www.omdia.com

IEB Media: Networking megatrends shape Automation & Control in 2021

INDUSTRIAL AUTOMATION AND CONTROL is a primary beneficiary of the networking megatrends that have been shaping the future of the Industrial Internet of Things (IIoT) and Industry 4.0 technology initiatives for more than a decade.

Industrial networking is more of a centerpiece for the world of automation and control than ever before because of the far-reaching implications and technological potential that connectivity offers in industrial applications.

As we head into 2021, a series of automation and control megatrends are in a position to make "outsized" impacts on smart manufacturing and factory automation. Industrial innovation and standards development often seems to be moving in slow motion as they move towards the mainstream.

But as we look into at a series of technology megatrends shaping industry, we see big ideas and industry cooperation taking automation and control to new levels of performance.

Edge Computing

The optimal use of data and connectivity between enterprise systems and the plant floor easily, flexibly and securely offers a wide range of benefits for manufacturers. IT technologies need to play a vital role in IIoT system architectures, even as gateways are evolving to provide more flexible, innovative and efficient software solutions.

Cloud Connectivity

While we note above that edge computing is on the move, don't sleep on the continuing impact of the major cloud suppliers including Amazon AWS and Microsoft Azure.

Industrial cloud computing provides the infrastructure for the transmission of data to applications that operators are using on computers or mobile devices, and software programs used in a wide variety of automated processes.

Single Pair Ethernet

One megatrend that is hard to underestimate its future impact is Single Pair Ethernet, a key development and the infrastructure that will make another level of IIoT and Industry 4.0 connectivity possible.

For the reliable establishment of the entire future SPE ecosystem, standards for transmission protocols, cabling and device components are all being jointly developed by a broad coalition of industrial automation and control suppliers.

OPC UA

OPC Unified Architecture (OPC UA) has become a vital, vendor-independent communication protocol for industrial automation applications. Based on the client-server principle, it enables seamless communication from sensors and actuators up to enterprise systems or the cloud.

OPC UA is a global standard for industrial interoperability with common data models. As a framework for industrial interoperability based on data models that can be communicated using modern industrial protocols, Ethernet, cellular, and wireless technologies, it has tremendous room for growth.

Time Sensitive Networking

Time-Sensitive Networking (TSN) is a technology poised to deliver an entirely new level of determinism for standard IEEE 802.1 and IEEE 802.3 Ethernet networks.

We are currently moving into the next phase for TSN, and the ongoing development of the IEC/IEEE 60802 TSN Profile for Industrial Automation expected to be finalized in 2022.

Internet of "Things"

And last but not least, let's not underestimate the impact of smart devices and technology developments adding connectivity to sensors, actuators, motion systems, feedback devices and the wide range of "things" that connect to factory networks.

Looking to 2021

It's an adage that "a system is greater than the sum of its parts". But it's definitely true in industrial automation and control--especially given the complexity of factory automation applications. So as we head in to 2021, let's keep an eye on the big picture, the continuing development of worldwide standards and how we see these megatrends intersect the deployment of real-world solutions.

Al Presher, Editor, ***Industrial Ethernet Book.***
www.iebmedia.com

No edge computing without an appropriate network

With the continuing emergence of the Industrial Edge, the industrial network will play an even more central and vital role, particularly in highly connected manufacturing operations. But also the advantages of end-to-end Ethernet networking can only be fully utilized, if the network is equipped with necessary resources.

EDGE COMPUTING IN ITS VARIOUS FORMS IS considered one of the next big steps not only in automation engineering. What can be easily overlooked is that the communication infrastructure, the network, is becoming more and more important.

Much has happened since Ethernet-based protocols for industrial communication such as EtherNet/IP and PROFINET were introduced in the early 2000s. It is now clear that Ethernet is the key foundation for industrial networking and will probably remain so for some time. This is supported by further developments such as TSN that rely on wide acceptance from automotive applications to system networking, as well as the strong growth rate of Ethernet-based protocols such as PROFINET.

The triumph of Ethernet technology

The big advantage has been flexibility. By utilizing a common technological basis, interoperability and the parallel use of different technologies has become easier.

In terms of communication, this means that it is no problem, for example, to carry out the process communication in an automation cell via PROFINET, while OPC UA is used in parallel to read data from individual devices or to send data directly via an Industrial IoT gateway such as the SIMATIC CC716. Both communication paths can serve completely different applications.

A co-existence is possible. For this to run smoothly, it is important that the industrial network meets the requirements of the applications. Another big trend with a very similar core competence is edge computing.

Industrial edge computing

The basic idea behind edge computing is quite simple; it is the logical development of the "cloud concept." That is the abstraction of hardware in order to be able to handle software functionality more flexibly and with more focus on the solution.

The term "edge" already indicates the crucial difference. In the context of edge computing, the execution layer shifts closer to the actual process again. Economic considerations also play a role here. Data that is processed directly on site does not need to be transferred to higher-level systems, or maybe only in compressed form, which saves bandwidth and consequently money. It gets a bit fuzzy when it comes to determining where the "edge" actually lies. Since the terms allow a lot of leeway, here is a concrete example: Siemens Industrial Edge.

SOURCE: SIEMENS

Edge computing is a next step in the evolution of Ethernet-based automation and machine control networking.

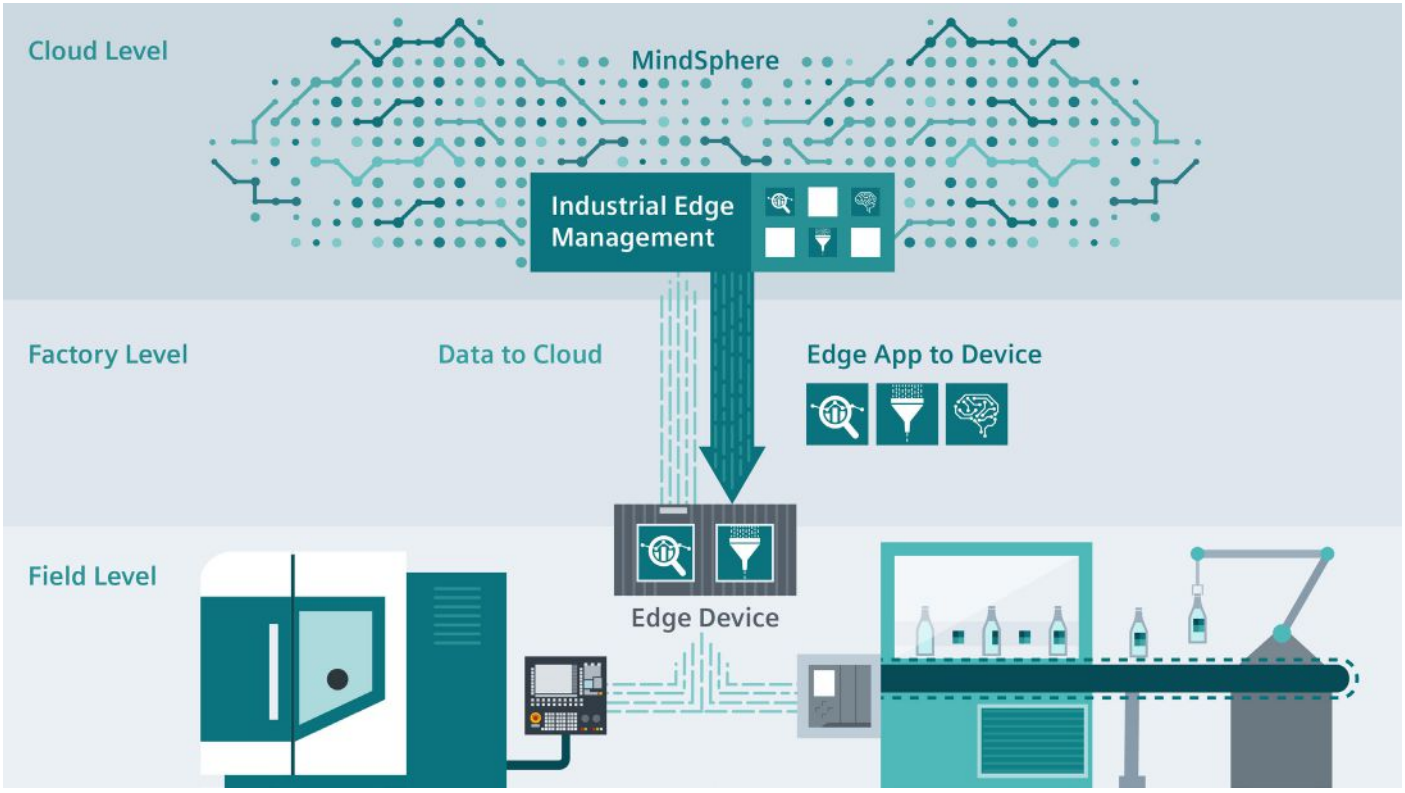
The system consists of multiple elements. For one thing, the "edge devices", devices on which a runtime environment provides services for hosting "industrial edge apps." These "industrial edge apps" are software functions based on container technology such as Docker. Devices and applications are orchestrated by a central "industrial edge management system", either on premise in the factory or perspectively in the cloud depending on customer requirements.

The real highlight is that, in addition to the transparency pertaining to which applications run where with which version and how the devices are doing, the software becomes first and foremost more independent of the underlying hardware. For instance, hardware can be selected to match the framework conditions: Do I need a certain form factor, a certain temperature range, a certain performance class, or do I want integration into certain components – such as the PLC of my automation cell?

But one thing must not be forgotten in edge computing. Behind the logical links shown in many depictions, e.g., "App is loaded from management onto the edge device," there is a real network that enables this functionality in the first place.

Industrial network as key element

The industrial network plays a central role, particularly in highly connected



SOURCE: SIEMENS

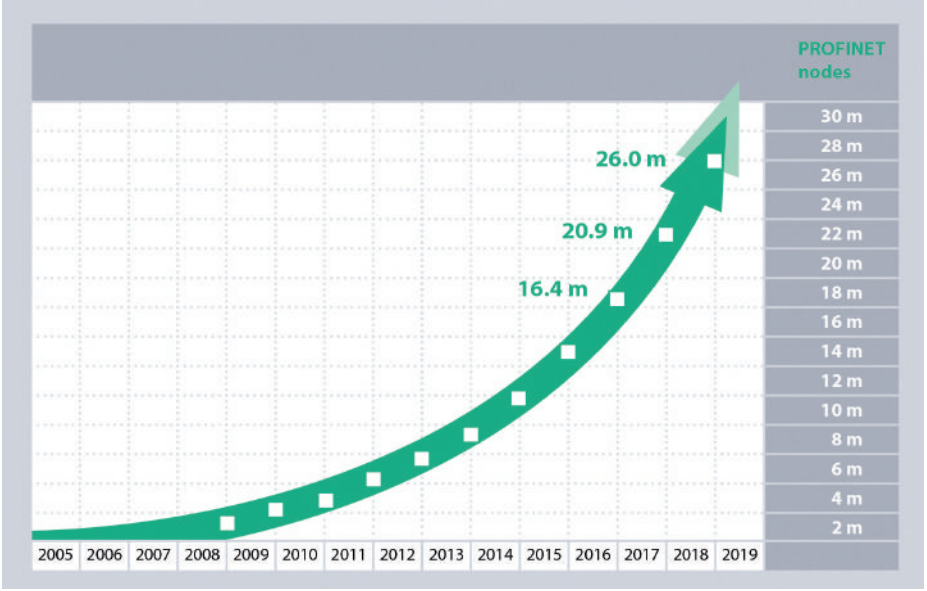
Industrial edge enables flexible management of software and industrial edge devices.

manufacturing, which, for example, makes sense when using Siemens Industrial Edge. But also the advantages of end-to-end Ethernet networking mentioned at the beginning can only be fully utilized, if the network is equipped with the necessary resources.

For one, the bandwidth requirement plays a central role. Specific bandwidth requirements for the automation cell can be calculated based on the configuration. The complexity increases for hierarchically higher networks. It is thus all the more important to be already aware during planning or expansion of a network infrastructure, where known data streams run and what bandwidths are required. Tools or services offered by various suppliers can provide support here. In the operation of the network, network management tools such as SINEC NMS help with the configuration, monitoring and, tracing of errors. Switch and router series such as SCALANCE XC and XR deliver the right performance.

Furthermore, the targeted availability must be taken into account. Are short-term outages of the network tolerable because the individual components are able to continue to work self-sufficiently for a certain time? With a view to the ever-increasing linkage, the highest possible availability is becoming more important. Redundancy mechanisms, at least in the backbone networks, are the means of choice in addition to components intended and suitable for industrial use.

Last but not least, security must always play a central role. A security concept adapted to the character of the network or the production can provide strong protection against unauthorized intrusion by means of access restrictions, network segmentations, etc. Here, too, Siemens and external suppliers assist with the design and building of competence in your house – for example, on the basis of the "defense in depth" concept from Siemens. At the cell level, the requirements are implemented technically with, e.g., SCALANCE S Industrial Security Appliances.



SOURCE: SIEMENS

Ethernet-based protocols, including the arc of PROFINET shown here, are growing rapidly.

How it works out

Due to the implicit demands on the infrastructure from edge computing, the industrial network is becoming more important than ever.

Hence it pays to earmark time and resources to equip it to meet your own requirements because it not only provides a robust communication infrastructure for today's requirements, but also a sustainable basis for the digitalization of tomorrow. Partners like Siemens can support you with the right products and services for planning and implementing your network infrastructure.

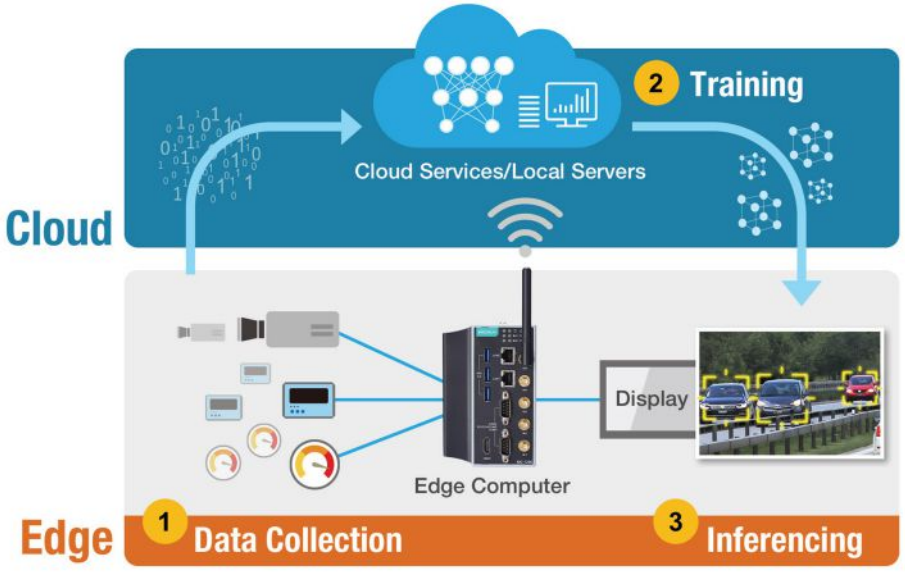
Frederik Nitsche, Product Management of SIMATIC Communication Products, ***Siemens.***

Edge computing and AI create Industrial AIoT applications

Enabling AI capabilities at the edge can improve operational efficiency and reduce risks and costs for industrial applications. Choose the right computing platform for your industrial AIoT application by addressing specific processing requirements during implementation.

IIOT APPLICATIONS ARE GENERATING MORE data than ever before. In many industrial applications, especially highly distributed systems located in remote areas, constantly sending large amounts of raw data to a central server might not be possible. To reduce latency, reduce data communication and storage costs, and increase network availability, businesses are moving AI and machine learning to the edge for real-time decision-making and actions in the field.

These cutting-edge applications that deploy AI capabilities on IoT infrastructures are called the "AIoT." Although users still need to train AI models in the cloud, data collection and inferencing can be performed in the field by deploying trained AI models on edge computers. This article discusses how to choose the right edge computer for industrial AIoT applications and provides several case studies to help get started.



SOURCE: MOXA

There are three phases in building "Artificial Intelligence of Things" applications.

Bringing AI to the IIoT

The advent of the Industrial Internet of Things (IIoT) has allowed a wide range of businesses to collect massive amounts of data from previously untapped sources and explore new avenues for improving productivity. By obtaining performance and environmental data from field equipment and machinery, organizations now have even more information at their disposal to make informed business decisions. Unfortunately, there is far too much IIoT data for humans to process alone so most of this information goes unanalyzed and unused.

Consequently, it is no wonder that businesses and industry experts are turning to artificial intelligence and machine learning solutions for IIoT applications to gain a holistic view and make smarter decisions more quickly.

IIoT data goes unanalyzed

The staggering number of industrial devices being connected to the Internet continues to grow year after year and is expected to reach 41.6 billion endpoints in 2025. What's even more mind-boggling is how much data each device produces.

In fact, manually analyzing the information generated by all the sensors on a manufacturing assembly line could take a lifetime. It's no wonder that "less than half of an organization's structured data is actively used in making decisions, and less than 1% of its unstructured data is analyzed or used at all".

In the case of IP cameras, only 10% of the nearly 1.6 exabytes of video data generated each day gets analyzed. These figures indicate a staggering oversight in data analysis despite our ability to collect more and more information. This inability for humans to analyze all of the data we produce is precisely why businesses are looking for ways to incorporate artificial intelligence and machine learning into their IIoT applications.

Imagine if we relied solely on human vision to manually inspect tiny defects on golf balls on a manufacturing assembly line for 8 hours each day, 5 days a week. Even if companies could afford a whole army of inspectors, each person is still naturally susceptible to fatigue and human error.

Similarly, manual visual inspection of railway track fasteners, which can only be performed in the middle of the night after trains have stopped running, is not only time-consuming but also difficult to do. Likewise, manual inspection of high-voltage power lines and substation equipment also exposes human personnel to additional risks.

Combining AI with IIoT

In each of the previously discussed industrial applications, the AIoT offers the ability to reduce labor costs, reduce human error, and optimize preventive maintenance.

The "Artificial Intelligence of Things" (AIoT) refers to the adoption of AI technologies in Internet of Things (IoT) applications for the purposes of improving operational efficiency, human-machine interactions, and data analytics and management. But what exactly do we mean by AI and how does it fit into the IIoT?

Artificial intelligence (AI) is the general field of science that studies how to construct intelligent programs and machines to solve problems that are traditionally performed through human intelligence. Artificial intelligence also includes machine learning (ML), which is a specific subset of AI that enables systems to automatically learn and improve through experience without being programmed to do so, such as through various algorithms and neural networks. Another related term is "deep learning" (DL), which is a subset of machine learning in which multilayered neural networks learn from vast amounts of data.

Since AI is such a broad discipline, the following discussion focuses on how computer

vision or AI-powered video analytics, other subfields of AI often used in conjunction with ML, are used for classification and recognition in industrial applications.

From data reading in remote monitoring and preventive maintenance, to identifying vehicles for controlling traffic signals in intelligent transportation systems, to agricultural drones and outdoor patrol robots, to automatic optical inspection (AOI) of tiny defects in golf balls and other products, computer vision and video analytics are unleashing greater productivity and efficiency for industrial applications.

Moving AI to the IIoT edge

As previously mentioned, the proliferation of IIoT systems is generating massive amounts of data. For example, the multitude of sensors and devices in a large oil refinery generates one TB of raw data per day.

Immediately sending all this raw data back to a public cloud or private server for storage or processing would require considerable bandwidth, availability, and power consumption. In many industrial applications, especially highly distributed systems located in remote areas, constantly sending large amounts of data to a central server is not possible.

Even if a system had the bandwidth and sufficient infrastructure, which would be incredibly costly to deploy and maintain, there would still be substantial latency in data transmission and analysis. Mission-critical industrial applications must be able to analyze raw data as quickly as possible.

In order to reduce latency, reduce data communication and storage costs, and increase network availability, IIoT applications are moving AI and machine learning capabilities to the edge of the network to enable more powerful preprocessing capabilities directly in the field. More specifically, advances in edge computing processing power have enabled IIoT applications to take advantage of AI decision-making capabilities in remote locations.

Indeed, by connecting field devices to edge computers equipped with powerful local processors and AI, users no longer need to send all of the data to the cloud for analysis. In fact, the data created and processed at the far-edge and near-edge sites is expected to increase from 10% to 75% by 2025, and the overall edge AI hardware market is expected to see a CAGR of 20.64% from 2019 to 2024.

Edge computers for Industrial AIoT

When it comes to bringing artificial intelligence to industrial IoT applications, there are several key issues to consider. Even though most of the work involved with training AI models still takes place in the cloud, eventually there will be a need to deploy trained inferencing models in the field.

AIoT edge computing essentially enables AI inferencing in the field rather than sending raw data to the cloud for processing and analysis. In order to effectively run AI models and algorithms, industrial AIoT applications require a reliable hardware platform at the edge. To choose the right hardware platform for an AIoT application, consider the following factors.

1. Processing Requirements for Different Phases of AI Implementation
2. Edge Computing Levels
3. Development Tools
4. Environmental Concerns

AI processing requirements

Generally speaking, processing requirements for AIoT computing are concerned with how much computing power is needed along with a CPU or accelerator. Since each of the following three phases in building an AI edge computing application uses different algorithms to perform different tasks, each phase has its own set of processing requirements.

Data collection

The goal of this phase is to acquire large amounts of information to train the AI model. Raw, unprocessed data alone is not helpful because the information could contain duplications, errors, and outliers. Preprocessing collected data at the initial phase to identify patterns, outliers, and missing information also allows users to correct errors and biases. Depending on the complexity of the data collected, the computing platforms typically used in data collection are usually based on Arm Cortex or Intel Atom/Core processors. In general, I/O and CPU specifications (rather than the GPU) are more important for performing data collection tasks.

Training

AI models need to be trained on advanced neural networks and resource-hungry machine learning or deep learning algorithms that demand more powerful processing capabilities, such as powerful GPUs, to support parallel computing in order to analyze large amounts of collected and preprocessed training data. Training an AI model involves selecting a machine learning model and training it on collected and preprocessed data. During this process, there is also a need to evaluate and tune the parameters to ensure accuracy. Many training models and tools are available to choose from, including off-the-shelf deep learning design frameworks such as PyTorch, TensorFlow, and Caffe. Training is usually performed on designated AI training machines or cloud computing services, such as AWS Deep Learning AMIs, Amazon SageMaker Autopilot, Google Cloud AI, or Azure Machine Learning, instead of in the field.

Inferencing

The final phase involves deploying the trained AI model on the edge computer so that it can make inferences and predictions based on newly collected and preprocessed data quickly and efficiently. Since the inferencing stage generally consumes fewer computing resources than training, a CPU or lightweight accelerator may be sufficient for the AIoT application.

Nonetheless, users will need a conversion tool to convert the trained model to run on specialized edge processors/accelerators, such as Intel OpenVINO or NVIDIA CUDA. Inferencing also includes several different edge computing levels and requirements.

Edge computing levels

Although AI training is still mainly performed in the cloud or on local servers, data collection and inferencing necessarily take place at the edge of the network. Moreover, since inferencing is where trained AI model does most of the work to accomplish the application objectives (i.e., make decisions or perform actions based on newly collected field data), users need to determine which of the following levels of edge computing are needed in order to choose the appropriate processor.

Low edge computing level

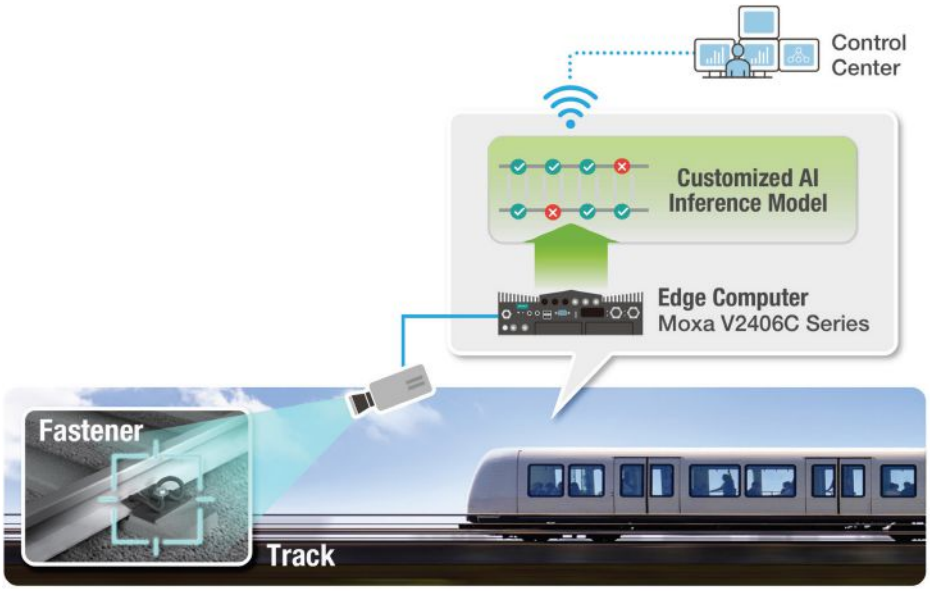
Transferring data between the edge and the cloud is not only expensive, but also time-consuming and results in latency. With low edge computing, applications only send a small amount of useful data to the cloud, which reduces lag time, bandwidth, data transmission fees, power consumption, and hardware costs. An Arm-based platform without accelerators can be used on IIoT devices to collect and analyze data to make quick inferences or decisions.

Medium edge computing level

This level of inference can handle various IP camera streams for computer vision or video analytics with sufficient processing frame rates. Medium edge computing includes a wide range of data complexity based on the AI model and performance requirements of the use case, such as facial recognition applications for an office entry system versus a large-scale public surveillance network. Most industrial edge computing applications also need to factor in a limited power budget or fanless design for heat dissipation. It may be possible to use a high-performance CPU, entry-level GPU, or VPU at this level. For instance, the Intel Core i7 Series CPUs offer an efficient computer vision solution with the OpenVINO toolkit and software based AI/ML accelerators that can perform inference at the edge.

High edge computing level

High edge computing involves processing heavier loads of data for AI expert systems



SOURCE: MOXA

AIoT Track Fastener Inspection System. *Because visual inspection during non-operating hours is time-consuming and human fatigue may lead to data omission, the transit system decided to deploy an AI edge computing solution to accelerate track fastener inspection with computer vision.*

that use more complex pattern recognition, such as behavior analysis for automated video surveillance in public security systems to detect security incidents or potentially threatening events. High Edge Compute Level inferencing generally uses accelerators, including a high-end GPU, VPU, TPU, or FPGA, which consumes more power (200 W or more) and generates excess heat.

Since the necessary power consumption and heat generated may exceed the limits at the far edge of the network, such as aboard a moving train, high edge computing systems are often deployed in near-edge sites, such as in a railway station, to perform tasks.

Several tools are available for various hardware platforms to help speed up the application development process or improve overall performance for AI algorithms and machine learning.

Deep learning frameworks

Consider using a deep learning framework, which is an interface, library, or tool that allows users to build deep learning models more easily and quickly, without getting into the details of the underlying algorithms. Deep learning frameworks provide a clear and concise way for defining models using a collection of pre-built and optimized components.

The three most popular include the following technologies:

- *PyTorch*: Primarily developed by Facebook's AI Research Lab, PyTorch is an open source machine learning library based on the Torch library. It is used for applications such as computer vision and natural language processing, and is a free and open-source software released under the Modified BSD license.
- *TensorFlow*: Enable fast prototyping, research, and production with TensorFlow's user-friendly Keras- based APIs, which are used to define and train neural networks.
- *Caffe*: Caffe provides an expressive architecture that allows users to define and configure models and optimizations without hard-coding. Users can set a single flag to train the model on a GPU machine, and then deploy to commodity clusters or mobile devices.

Hardware-based accelerator toolkits

AI accelerator toolkits are available from hardware vendors and are specially designed to accelerate artificial intelligence applications, such as machine learning and computer vision, on their platforms.

- *Intel OpenVINO*: The Open Visual Inference and Neural Network Optimization (OpenVINO) toolkit from Intel is designed to help developers build robust computer vision applications on Intel platforms. OpenVINO also enables faster inference for deep learning models.
- *NVIDIA CUDA*: The CUDA Toolkit enables high-performance parallel computing for GPU-accelerated applications on embedded systems, data centers, cloud platforms, and supercomputers built on the Compute Unified Device Architecture (CUDA) from NVIDIA.

Environmental considerations

Last but not least, also consider the physical location of where the application will be implemented. Industrial applications deployed outdoors or in harsh environments such as smart city, oil and gas, mining, power, or outdoor patrol robot applications should have a wide operating temperature range and appropriate heat dissipation mechanisms to ensure reliability in blistering hot or freezing cold weather conditions.

Certain applications also require industry-specific certifications or approvals, such as fanless design, explosion proof construction, and vibration resistance. And since many real-world applications are deployed in space-limited cabinets and subject to size limitations, small form factor edge computers are preferred.

Moreover, highly distributed industrial applications in remote sites may also require communications over a reliable cellular or Wi-Fi connection. For instance, an industrial edge computer with integrated cellular LTE connectivity eliminates the need for an additional cellular gateway and saves valuable cabinet space and deployment costs. Another consideration is that redundant wireless connectivity with dual SIM support may also be needed to ensure that data can be transferred if one cellular network signal is weak or goes down.

To see how real-world industrial applications enable and benefit from AIoT edge computing, let's examine the following two examples.

Keeping mass transit on track

All trains, whether in an inter-city railway line or municipal mass transit system, run on metal tracks that need to remain upright and properly spaced according to a standard gauge at all times. If the tracks become uneven, trains could derail.

That's why users always see some sort of support, known as railroad ties or ballasts, laid perpendicularly beneath the tracks. To ensure a smooth ride, railroad tracks need to be securely fastened to the ties by spikes, screws, or bolts.

Due to constant friction and vibration between fast-moving train wheels and the tracks, as well as damage from the natural environment, track fasteners degrade and break over time. Consequently, timely detection and repair of track fasteners is crucial to ensuring the safety of any railway line.

A large metropolitan railway in East Asia needed a more efficient way to inspect the vast number of fasteners used to stabilize thousands of miles of tracks throughout its entire mass transit system. Located in the Ring of Fire where many earthquakes occur, the transit system cannot take any chances on the safety of its infrastructure since constant tremors compound the regular wear and tear from rolling stock and high passenger traffic.

Usually, after train service ends on one of the lines, the railway operator dispatches human maintenance engineers to perform manual visual inspection of the tracks and

check for loose fasteners. If a loose or damaged track fastener is detected, the fastener must be repaired before train service recommences on the railway line.

Since visual inspection of railway tracks during non-operating hours is time-consuming and human fatigue may lead to data omission, the transit system decided to deploy an AI edge computing solution that could accelerate track fastener inspection with computer vision.

More specifically, the transit operator wanted a customized AI inference model with object recognition for track fastening systems that could detect track fastener defects while the trains are moving and perform maintenance between journeys.

AI inferencing for track fastener inspection also requires the edge computer to have powerful computing performance and storage expansion for video data, compact size and fanless design for installation in small cabinets, wide operating temperature range, and EN 50155 compliance for use on rolling stock.

The first step was to install high-resolution cameras underneath the train carriages, which enabled the system operator to capture real-time video of track fasteners as trains run on the tracks during service hours. Video data is then transmitted to an onboard edge computer for image processing and object recognition of track fastener defects.

The train operator selected Moxa's V2406C Series rail computer for its compact-size with an Intel Core i7 processor that provides ample computing power for running the trained AI inferencing model. The V2406C also runs on low power consumption and has a wide operating temperature range of -40 to 70°C.

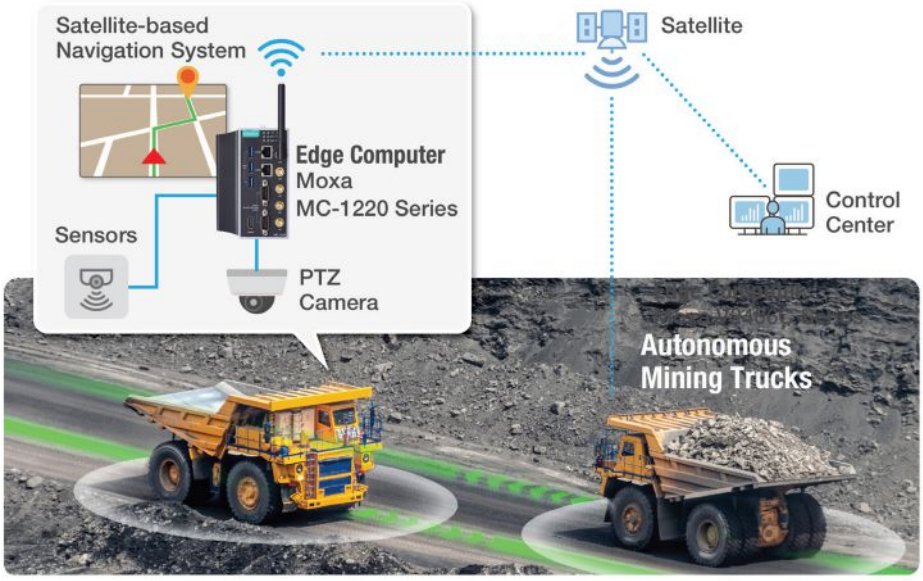
Last but not least, the V2406C supports the Intel OpenVINO toolkit and features two mPCIe slots for Intel Movidius VPU modules to accelerate image recognition computations and edge AI inferencing. By replacing manual visual inspection with real-time AI visual inspection during operating hours, the transit system was able to improve efficiency and reduce maintenance expenses.

Autonomous mining trucks

The growing popularity of autonomous haul trucks in open-pit mining, an application which is expected to triple by 2023, is mainly driven by the ability of autonomous hauling systems to reduce accidents, fuel consumption, and operating costs, while also increasing machine life and overall productivity.

Automating the trucks not only enables mining companies to move human workers to a control room, where they can oversee operations from a safe distance, but also optimizes overall production by shortening truck exchanges and eliminating shift changes.

Surface mining operations depend on heavy-duty dump trucks, called haul trucks, to transport rocks and debris from excavation sites. Due to the heavy weight and large volume of rocks and other materials that need to be moved in mining operations, haul trucks are often massive vehicles in their own right.



SOURCE: MOXA

Autonomous Haulage Systems (AHS). *Systems involve training and deploying AI models to safely traverse rugged terrain and move rocks. They also rely on computer vision and navigation technology to identify obstacles and move into the proper position to collect excavated rocks from excavators and dump the debris in correct locations.*

For example, some of the largest haul trucks used in open-pit mining are designed to carry payloads of 400 tons or more. Traditionally, these giant vehicles are operated by human drivers in quarries located in dangerous, extreme outdoor environments, such as deserts or mountains, where explosives are used to excavate mineral resources and ore from the Earth's surface.

Besides the inherent dangers involved with open-pit mining, human truck drivers often need to work 12-hour shifts or longer, which results in fatigue and a greater risk of human error. In recent years, leading mining companies around the world have been increasingly looking towards autonomous technology and AI to help improve occupational safety and productivity.

As with self-driving commercial vehicles, autonomous hauling systems involve training and deploying AI models to enable haul trucks to safely traverse rugged terrain and move rocks across the excavation site. These autonomous haulage systems (AHS) also rely on computer vision and navigation technology to enable autonomous haul trucks to identify obstacles and move into the proper position to collect excavated rocks from excavators and dump the debris in designated locations.

By installing a high-performance edge computer such as the Moxa MC-1220 series to connect PTZ cameras and sensors on each autonomous haul truck in the fleet, mining companies can obtain real-time video data from the excavation site as well as the exact position of each truck.

The MC-1220 provides high-performance Intel Core i7 processors for video analysis and self-driving systems, as well as Wi-Fi and cellular connectivity to transmit preprocessed field data to the control center.

Since mining trucks need to traverse rugged terrain, solid metal casing and high shock and vibration tolerance are also required. What's more, extreme outdoor quarry environments also necessitate a wide operating temperature range. The MC-1220 is not only Class 1, Div. 2 certified for safe, explosion-proof operation in hazardous mining locations, but also ensures reliable performance from -40 to 70°C.

Conclusion

As the aforementioned case studies illustrate, enabling AI capabilities at the edge allows users to effectively improve operational efficiency and reduce risks and costs for industrial applications.

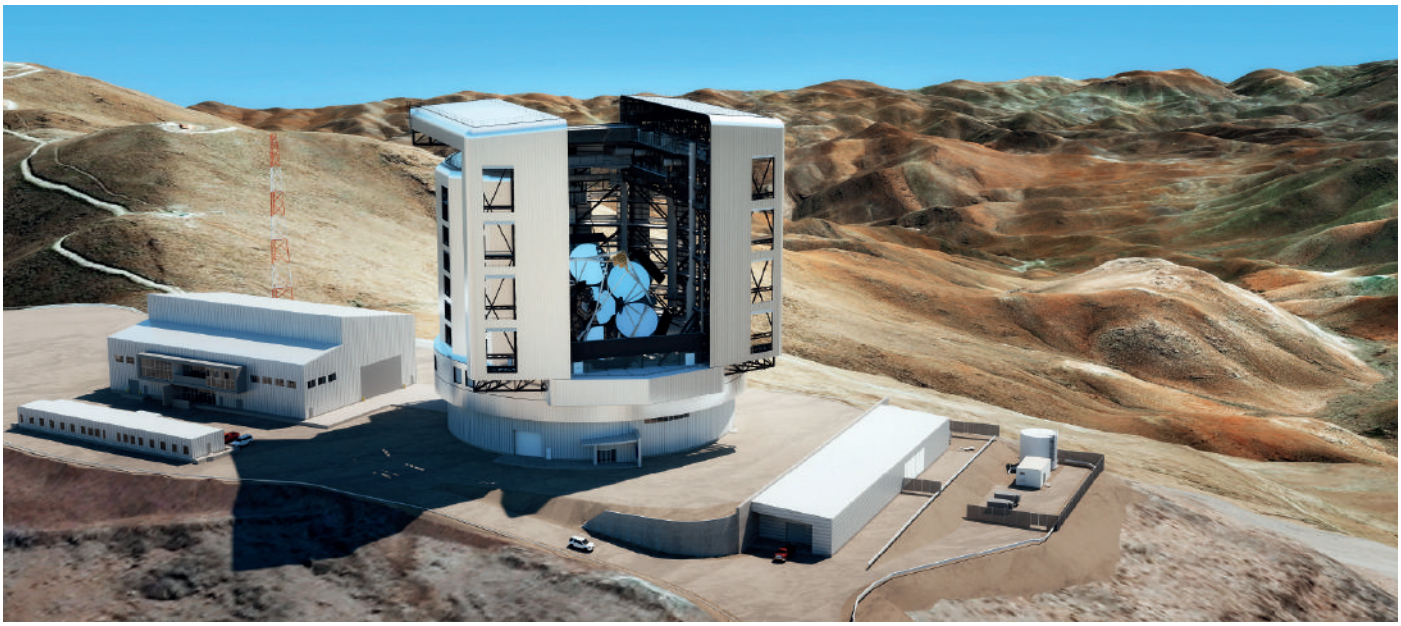
Choosing the right computing platform for an industrial AIoT application should also address the specific processing requirements at the three phases of implementation: (1) data collection, (2) training, and (3) inference. For the inference phase, users also need to determine the edge computing level (low, medium, or high) so they can select the most suitable type of processor.

By carefully evaluating the specific requirements of an AIoT application at each phase, users can choose the best-suited edge computer to sufficiently and reliably perform industrial AI inferencing tasks in the field.

Ethan Chen, Product Manager, Alicia Wang, Product Manager and Angie Lee, Product Marketing Manager, ***Moxa Corporation.***

PC and EtherCAT-based control for next-generation telescope

Giant Magellan Telescope (GMT) combines site-wide, real-time connectivity with 3,000 precisely controlled servo axes. The telescope design boasts a resolution 10 times greater than that afforded by the Hubble Space Telescope, and moved away from building the automation solution using custom control components.



SOURCE: GMTO CORPORATION

With seven mirrors and a combined diameter of 25 meters, the Giant Magellan Telescope will represent the next generation of ground-based telescopes when it goes live at Las Campanas Observatory in Chile in 2029.

THE GIANT MAGELLAN TELESCOPE (GMT) is expected to go live in 2029, after the next-generation telescope completes its long construction and planning period. With seven mirrors and a combined diameter of 25 m, the telescope will enable entirely new resolutions and even allow a look back into the time after the Big Bang.

PC-based control was specified as the future automation equipment. Key factors were the advantages of EtherCAT for site-wide, real-time communication connecting all telescope functions. Various Embedded PCs and AM8000 servomotors were also tested and specified, among other things, to move more than 3,000 motion axes.

Once installed at Las Campanas Observatory, the Giant Magellan Telescope will introduce incredible opportunities for the astrophysics and cosmology research communities. The land-based telescope design boasts a resolution 10 times greater than that afforded by the Hubble Space Telescope by combining seven mirrors into a singular optical system with a total diameter of 25 m.

These advances will enable the GMT to capture images of astronomical objects sharper than currently possible by reducing distortions introduced by the terrestrial atmosphere using adaptive optics systems. Scientists and engineers working on similar telescope projects have traditionally built their own automation solutions using custom control components.

However, the team that is currently planning the infrastructure for the GMT sees this differently, explained GMTO Senior Electronics Engineer José Soto: "We want to change the historical method of treating telescopes as special and totally unlike other automated systems. Future-facing industrial control solutions have the power to solve many problems we face today in astrophysics."

Standards-based automation

Specifying automation and controls components for the GMT also required careful consideration due to the real-time communication and control requirements, especially considering the system will possess more than 3,000 axes of motion. Beyond rotating the telescope's 22-story-tall enclosure, the flexible mirrors must move with utmost precision to implement the complex adaptive optics in order to achieve the highest possible image resolution.

One example is the active optics system, which requires integration of 170 pneumatic actuators per primary mirror to support the mass of each mirror.

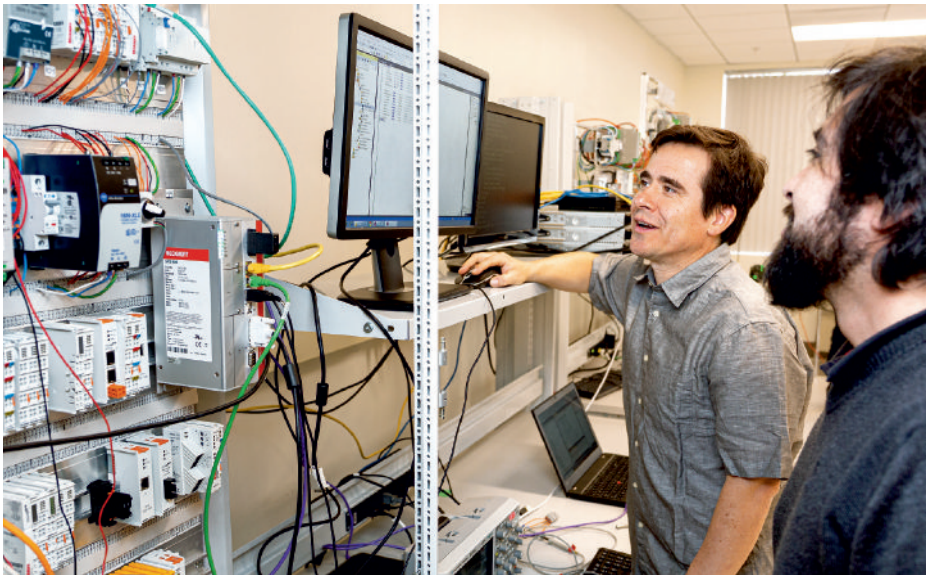
The engineering team identified the need for automation and controls components that were powerful now, but would also support future advances in technology, explains José Soto: "Since these projects take a long time we must account for obsolescence in every aspect. The most effective method of fighting obsolescence is standardizing on proven industrial technologies." These factors led GMTO to base specifications for the control system using industrial standards.

When GMTO engineers began exploring industrial automation and controls, they examined multiple industrial Ethernet networks. They found EtherCAT provided a flexible topology and scalability, along with the ability to incorporate up to 65,535 EtherCAT devices in one network, which matched the system specification of the GMT. "EtherCAT will be embedded in nearly every GMT telescope system — from the primary mirrors to the atmospheric dispersion compensator, the enclosure, mount and even the building automation in the facilities," Soto said.

According to GMTO Engineer Hector Swett, Safety over EtherCAT (FSoE) also offered

impressive functionality for the telescope's interlock and safety systems. FSoE provides GMT with safety-rated, TÜV-certified communication over standard EtherCAT networks, numerous options for distributed TwinSAFE I/O modules and integration with the Beckhoff engineering environment and Industrial PCs.

Certain current GMT specifications recommend multiple PC-based controllers that could be fulfilled by Beckhoff solutions. The interlock and safety system relies on many safety controllers, DIN-rail-mounted CX9020 Embedded PCs working in conjunction with EL6910 TwinSAFE Logic I/O modules. These interface with each other through FSoE via EtherCAT Automation Profile (EAP) to implement safety functions as required by the hazard analysis, Swett says. Beckhoff CX2020 Embedded PCs are used in the GMT Hardware Development Kit, which was built for the project's partners to develop instruments for the telescope.



SOURCE: GMTO CORPORATION

GMTO engineers José Soto (left) and Hector Swett use TwinCAT 3 automation software from Beckhoff to validate various components according to the telescope specifications.

TwinCAT 3 automation software from Beckhoff has offered a key platform to test devices, and it is specified for control of the structures around the telescope. "The PC-based controller for the telescope's enclosure will run TwinCAT directly," Swett said. "It also provides the real-time capability to interface this massive application with the observatory control system via OPC UA."

Exemplifying system openness, TwinCAT can automatically scan and configure third-party devices over ADS and EtherCAT, providing an optimal platform for all tasks from sensing to motion control.

Because the telescope will have thousands of axes of motion, dependable motors and drives will be crucial in the final configuration. José Soto finds the capabilities of Beckhoff AM8000 servomotors impressive and sees them as a serious contender for multiple areas throughout the telescope.

"When our integrator teams begin to commission the telescope, they will very likely use AM8000 Servomotors, for example, in the atmospheric dispersion compensator or the GIR (Gregorian Instrument Rotator) that will move all instruments attached to the Cassegrain focus," Soto said.

New technologies for creative ideas

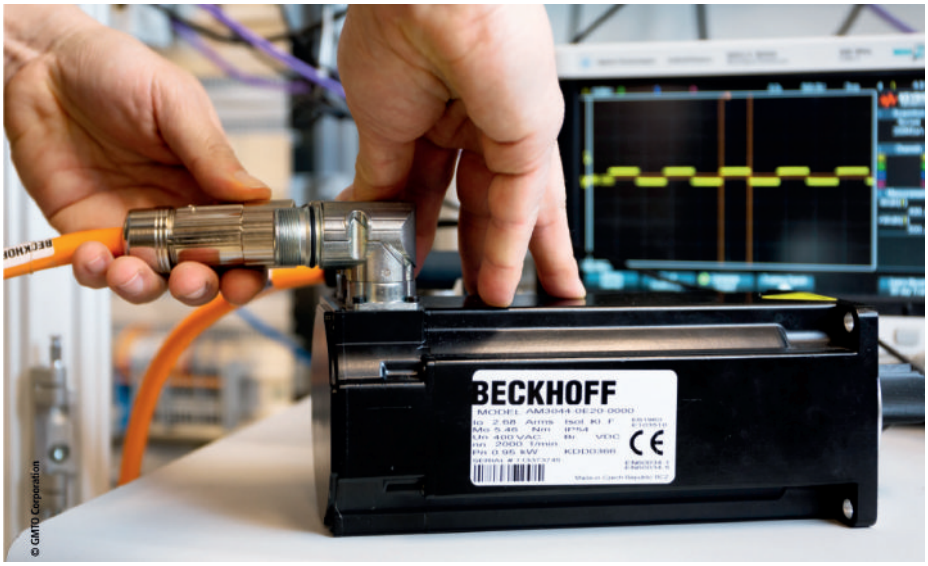
EtherCAT first led the GMTO engineers to Beckhoff, and it remains foundational to the telescope's control architecture design, José Soto explained: "Using EtherCAT as the GMT fieldbus enables real-time communication down to the I/O-level. We have achieved cycle times of 2 ms, which allows enough bandwidth to close the loop on a range of subsystems, expanding our control and networking abilities significantly."

Compact EtherCAT I/O modules and Embedded PCs save space in control cabinets, and because the PC-based controllers can be located at a distance from the I/Os, this reduces heat dissipation.

"Reducing heat is a very big deal for the GMT," Hector Swett added. "Heat makes the air more turbulent inside the enclosure, and turbulence distorts images as the light travels through the air. This distributed I/O architecture helps us prevent that."

In a decade, this process of observation and discovery will not belong to the engineers designing and building the GMT, but to the astrophysicists and cosmologists using it to explore the cosmos.

Researchers will have the flexibility to bring their own creative ideas when using the telescope to make great discoveries that cannot yet even be imagined.



SOURCE: GMTO CORPORATION

Beckhoff AM8000 servomotors are specified throughout the telescope design, which includes more than 3,000 axes of motion.

The Giant Magellan Telescope

The Giant Magellan Telescope project is an international consortium of 12 founding institutions. These include Arizona State University, Astronomy Australia Limited, Australian National University, Carnegie Institution for Science, FAPESP (São Paulo Research Foundation), Harvard University, Korea Astronomy and Space Science Institute, Smithsonian Institution, Texas A&M University, The University of Texas at Austin, University of Arizona and University of Chicago.

By supplying funding for the construction and operation of the telescope, these organizations will receive access for their researchers to use the Giant Magellan Telescope after a peer review process to prioritize projects.

James Figy, Senior Content Specialist, ***Beckhoff Automation USA.***

Industrial automation standard for portability and Industry 4.0

IEC 61499 defines a high-level system design language for distributed information and control. It allows encapsulation of functionality, graphical component-based design, event-driven execution and distribution of automation applications for execution across automation and control, as well as edge computing devices.

SOURCE: SCHNEIDER ELECTRIC

Operating from an open, as opposed to proprietary automation framework, suddenly renders accessible the entire new range of Industry 4.0 benefits.

THE BENEFITS OF INDUSTRY 4.0 AND IIOT use cases for industry are well documented. But, failure to adopt digital age industrial automation standards that are truly open is costly on all fronts: unnecessary expense, delays in rolling out innovative manufacturing plant designs, and lost business opportunity.

The IEC 61499 standard sets a foundation for industrial automation application portability that creates benefits including IT/OT system convergence, improved return-on-investment on software applications that can run independent of any hardware platform, and engineering design efficiency that radically speeds up new product time-to-market.

Global economic and market uncertainties are forcing manufacturers to rapidly adjust to more frequent, high-speed changes in demand and in raw material and energy pricing. Such trends are prompting process manufacturers to rethink the way industrial automation systems need to work. Part of that reassessment involves a need to accommodate increased product variants and shorter sourcing, production, and product delivery lifecycles.

Industrial organizations and their stakeholders also face the challenge of accommodating significant workforce changes as Baby Boomers retire and take their industrial automation systems knowledge with them. The new, Digital Native generation of employees coming in expect that knowledge will be embedded in the systems they will be required to work with.

Many industrial stakeholders are hoping that Industry 4.0 and the Industrial Internet of Things (IIoT) will help to address these new challenges. Early benefits of Industry 4.0 have been well documented—artificial intelligence and machine learning algorithms that greatly improve the quality of operational processes, the prediction of equipment failures before they happen to reduce unplanned downtime, real-time optimization of production based on raw-material spot prices, and real-time optimization of production scheduling to maximize throughput. In fact, industry analysts estimate that the new, more flexible production techniques could boost manufacturer productivity by as much as 30%. However, research has also shown that 60% of enterprises fail to take IIoT projects beyond the pilot stage.

The reasons for this are numerous and linked to people, processes and technology. With regards to technology, the biggest factor that keeps most mainstream manufacturers from attaining such benefits is the closed proprietary nature of the plant systems that support their operations. Operating from a truly open, as opposed to a proprietary industrial automation framework, suddenly renders accessible the entire new range of Industry 4.0 benefits.

This article proposes an approach based on the IEC 61499 standard that not only addresses the shortcomings of proprietary systems, but also facilitates the convergence of operation technology (OT) and information technology (IT) systems.

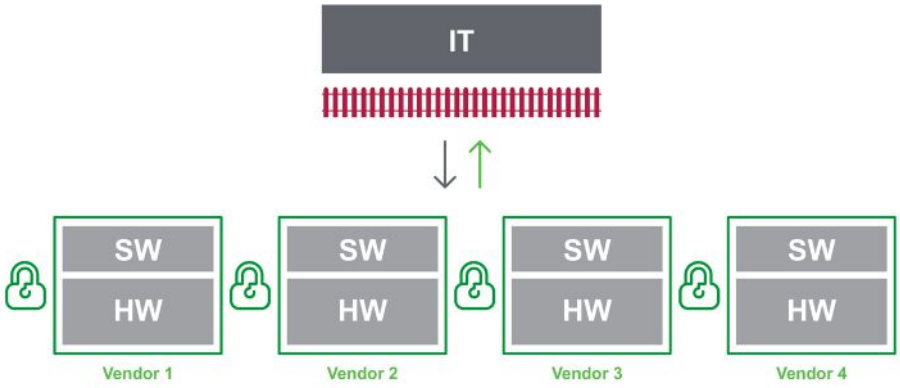
Barriers to overcome

For manufacturers to move forward into the new world of open industrial automation systems, engineering teams need to be cognizant of the barriers that need to be overcome.

Non-digital architecture: Most of today's automation systems are based on principles developed in the 1970s and 80s. Highly optimized for real-time control, the technology has not taken advantage of the recent and rapid changes in IT. It is precisely these technologies (analytics, artificial intelligence/ machine learning, object orientation, service-oriented architectures, etc.) that are required to realize the promise of Industry 4.0.

Hardware-centric business model: Although advancement in hardware can serve to optimize an existing environment, it will not lead to the breakthroughs required to enable the true benefits of the digital transformation. This will require the intelligent application of software-based innovation to OT problems. This will result in a steady shift from hardware-driven to software-driven business value.

Constraints of proprietary systems: Today, automation software applications written for one system will not run on another system. In the IT world, standardized operating systems such as Linux have, for decades, encouraged the rapid expansion of an active third-party



SOURCE: SCHNEIDER ELECTRIC

Proprietary automation cannot leverage advances in IT technologies and lack of application code portability hinders innovation and investment in software.

application development ecosystem. As a result, software of all kinds support IT-related business needs across a wide swath of industries and niches. Unfortunately, in the industrial world, proprietary systems act as a barrier to innovation: Users are unable to improve their production systems at reasonable cost and are unable to mix and match best-of-breed offers from different suppliers. Their rate of innovation is "imposed" by the suppliers of the proprietary platform they use.

Together, these barriers increase total cost of ownership. And since upstream design tools and downstream operations tools cannot be closely coupled with automation systems without a huge investment, the creation of an efficient digital thread covering the full process/machine lifecycle is next to impossible.

Open automation framework

On the engineering side of the equation, value chain members such as machine builders and systems integrators also face their own set of limitations working within the constraint of the current industrial automation infrastructure paradigm.

Machine builders are facing new challenges. On the one hand, there is a trend towards modular machine design using virtual testing capabilities to mix the virtual and physical worlds. On the other hand, increasing the added value of their machines requires services and innovative business models to help differentiate themselves and to help market and grow their business. The current automation construct does not favor their ability to expand into software and services offerings.

For systems integrators, automation systems do not provide the tools to bridge the IT and OT worlds. As a result, they find themselves having to craft solutions that are overly complex and labor-intensive thereby limiting the widespread marketplace acceptance of such services.

On the End User side, organizations such as the Open Process Automation Forum (OPAF) and the User Association of Automation Technology in Process Industries (NAMUR) are advocating for changes to the existing proprietary automation systems paradigm.

For all of these reasons, the time is ripe to move to an open automation framework.

The key that unlocks this new world is the emerging IEC 61499 standard. Technological evolution has finally caught up enough to allow the standard to exercise its full potential. That is, IEC 61499 can now serve as an essential building block for the development of a truly open industrial automation environment where software applications are portable across multi-vendor hardware platforms.

What characteristics of the IEC 61499 standard make it well-suited for exploiting the benefits of Industry 4.0 digitization and for creating a foundation for truly open systems?

Summary

To summarize, IEC 61499 defines a high-level system design language for distributed information and control systems. The standard allows encapsulation of functionality, graphical component-based design, event-driven execution and distribution of automation applications for execution across a broad range of automation & control devices, as well as edge computing devices.

With the emergence of the IEC 61499 standard and the interest of key automation vendors such as Schneider Electric to adopt open automation systems platforms, many of the ingredients are in place to help reshape the industrial automation systems playing field. Early field tests of tools based on the IEC 61499 standard suggest that engineering gains of three to four times can be achieved compared to conventional programming approaches.

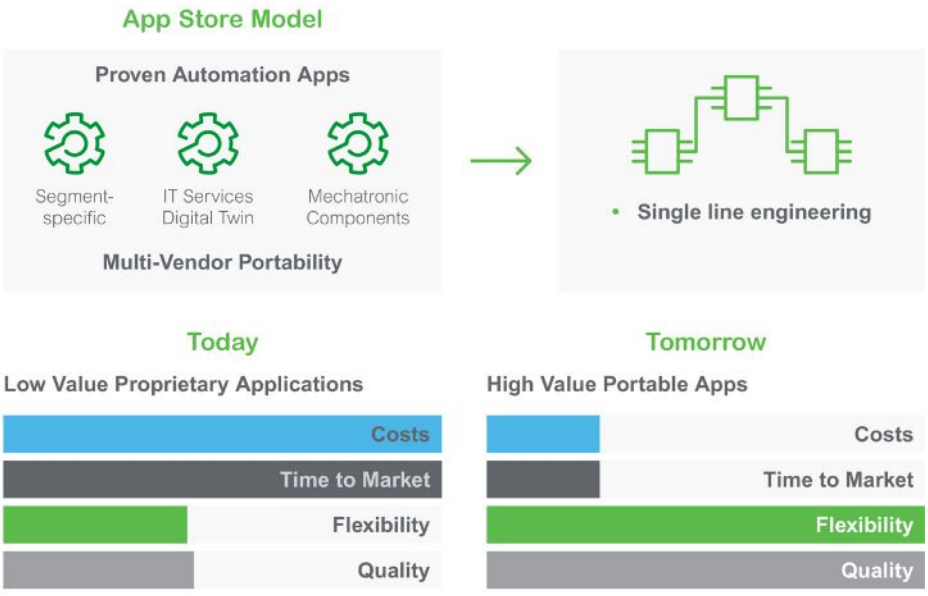
Plug and produce systems

The move to automation systems based on IEC 61499 is more than a simple technology change. It has the potential to fundamentally change the way processes and machines are designed. The technical features described above will drive portability & interoperability of application software across multi-vendor platforms and will enable an app-store model for industrial automation.

This will drive a long-term shift from low-value programming of proprietary controllers to plug & produce automation systems using proven-in-use automation apps developed by a broad Ecosystem. Applications will run on a broad range of multi-vendor devices ranging from embedded SoCs to powerful edge computers.

The reduction in engineering costs and the simplification of the implementation of complex Industry 4.0 use cases will unleash a step-change in productivity, flexibility and speed for industry.

John Conway, ***Schneider Electric.***

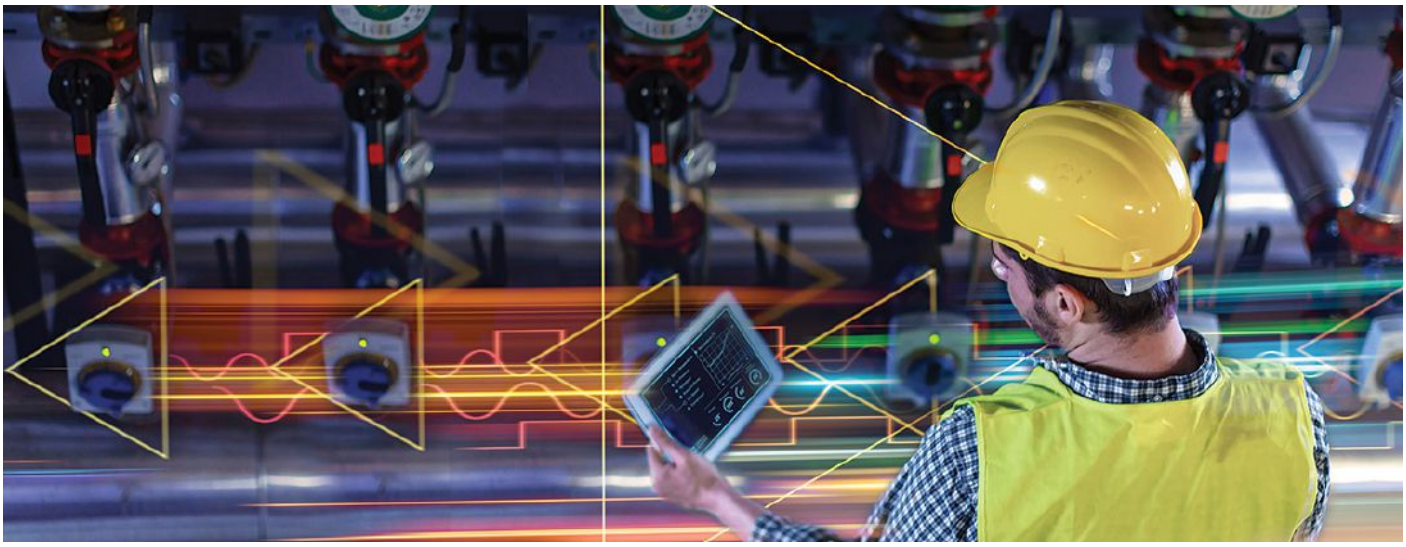


SOURCE: SCHNEIDER ELECTRIC

The move to automation systems based on IEC 61499 is more than a simple technology change. It has the potential to fundamentally change the way processes and machines are designed.

10BASE-T1L extends Big Data analytics to edge of networks

The rapid development of 10BASE-T1L components is enabling industrial equipment manufacturers to start developing new Industrial Ethernet-enabled products. The technology looks set to supplant the 4 mA to 20 mA and HART interfaces, and accelerate the adoption of Industry 4.0.



SOURCE: ANALOG DEVICES

Unlocking rich data streams with 10BASE-T1L for enterprise-level data analytics engines.

THE RATIFICATION OF THE IEEE 802.3CG standard in November 2019 marked the introduction of a new and dramatically different way for factory operators to connect devices at the edge of the network, freeing them from the restrictions of infrastructure based on the legacy 4 mA to 20 mA and HART communications interfaces.

The 802.3cg standard, also known as 10BASE-T1L, is a type of Industrial Ethernet networking physical layer. It provides a way to break down the barriers between the basic operational devices that perform frontline service in the factory or process plant—sensors, valves, actuators, and control—and enterprise data, the vault of bits and bytes where the intelligence of the new smart factory comes to life.

10BASE-T1L networking is set to be an important enabler of the general transformation toward a data and analytics-driven approach to factory operation—the trend known as Industry 4.0 and the Industrial Internet of Things.

Does this mean that industrial engineers should be preparing to replace 4 mA to 20 mA or HART systems with 10BASE-T1L infrastructure now, even though the 802.3cg standard is so new and if so how?

Which key factors will determine whether the transition from 4 mA to 20 mA or HART to 10BASE-T1L will be a success?

Data analytics support

Industry 4.0 implementations are sweeping through every modern factory operation. At Industry 4.0's heart is the desire to profit from the exploitation of big data. New analytics software has begun to transform the way that industry operates and maintains factory equipment and premises. The insights from analytics are often most profound when they uncover patterns in apparently disparate sets of data.

The more data, and the more types of data, that can be reliably captured from devices in the factory, the more opportunities there will be for software to support advanced functions such as condition monitoring and predictive maintenance. And the low data bandwidth of the 4 mA to 20 mA and HART interfaces and the limited scope for integrating them into enterprise computing infrastructures has hampered engineers' efforts to apply analytics to these legacy end points. The 4 mA to 20 mA and HART technologies also restrict the amount of power that can be supplied to an endpoint and the scope to remotely monitor the device's operation.

So, the prize to be won by converting existing 4 mA to 20 mA or HART equipment to 10BASE-T1L is data, and the resulting gains in productivity and efficiency that can be made when the data is put to work. Connected, smart factories typically suffer from less unplanned downtime, waste less energy, achieve better utilization of equipment and other assets, and deploy staff more efficiently. 10BASE-T1L connectivity promises to extend these benefits to the remote corners of factories and process plants, where sensors and other endpoints operate out of reach of the enterprise network.

Data rates and power output

The case for installing 10BASE-T1L equipment today rests on the set of capabilities provided for in the 802.3cg standard. A 10BASE-T1L connection offers:

- A maximum data rate of 10 Mbps over a cable length of up to 1 km.
- Up to 500 mW of power to endpoints in Zone 0 intrinsically safe applications, enabling the operation of a much wider range of more sophisticated endpoints than a 4 mA to 20 mA or HART system can support.
- Potential to reuse existing, installed single twisted pair cabling.
- Rich device management options, including the supply of diagnostic data from the connected device and the provision of software updates to it.
- An IP address for every node, extending IoT capability to the edge of factory network. An IP address enables a node to be monitored and managed remotely.

- Integration with enterprise network infrastructure

From a hardware standpoint, implementation of 10BASE-T1L equipment is normally straightforward. That's because the physical medium for 10BASE-T1L communications is a single twisted pair cable. This might even be the same wiring that already carries 4 mA to 20 mA or HART communications. The 802.3cg standard supports installation in hazardous (explosion-proof) environments.

Early implementations of 10BASE-T1L will likely be hybrid equipment that supports both a legacy interface, such as 4 mA to 20 mA, and the new Industrial Ethernet physical layer.

SOURCE: ANALOG DEVICES

10BASE-T1L enables big data analytics to the edge of the factory network.

Success with 10BASE-T1L

Analog Devices, Inc. (ADI) will play an integral role in many customers' adoption of Industry 4.0 technologies. Our experience suggests that two critical factors will determine whether a 10BASE-T1L project is successful:

- A focus on data
- Network security

Once engaged in the operational details of a 10BASE-T1L roll-out, engineers can easily lose sight of the reason for implementing it to lift the veil on the operation of endpoints, such as sensors, and feed rich streams of data from them to enterprise-level data analytics engines.

It follows that the biggest risk to the success of a 10BASE-T1L project is not at the endpoints themselves, or at the physical infrastructure; the problem is most often at the back end, when inadequate provision is made for handling and using the datasets coming from the newly connected endpoints. So industrial engineers embarking on a 10BASE-T1L installation should have these questions in mind:

- What types of insights do I plan to derive from the data that will be acquired from sensors and other endpoints?
- How will the data be integrated into enterprise-level control systems? Is the format of the data from endpoints compatible or does it need translation?
- How will insights from data analytics lead to process or system improvements?

The second crucial issue for the engineer to face up to is security. The nature of the threat to endpoints changes dramatically as soon as they are connected via a 10BASE-T1L network. Before, when connected via 4 mA to 20 mA, the lack of complex connectivity reduced the risk of attack.

The superior connectivity provided by the 802.3cg standard, including an IP address for every node, makes every endpoint vulnerable to remote attack via the enterprise network. The inherent, physical firewall that isolates 4 mA to 20 mA or HART endpoints from the network disappears as soon as the factory installs 10BASE-T1L.

This means that individual nodes and the network infrastructure itself have to be secured through the implementation of technologies such as:

- Secure authentication of devices via encrypted device IDs
- Encryption of data transmissions
- Firewalls to bar outside entities from gaining access to secure devices

SOURCE: ANALOG DEVICES

ADI Chronous, scalable Ethernet, provides an effective timing mechanism.

Lessons of Industry 4.0 projects

Following the ratification of the 802.3cg standard, the development of 10BASE-T1L-compatible components and equipment has been accelerating. For our part, ADI has been working with industrial equipment manufacturers to ensure that they are able to follow their roadmaps for the introduction of systems that support 10BASE-T1L networking. The expectation in the industry is that products offering 10BASE-T1L capability will be released to the market by mid-2021.

ADI's long experience in supporting customers' implementations of new technology will help make these 10BASE-T1L product introductions successful. The structure of our industrial automation division supports technology implementation, since it combines technology-focused development and support staff with market-oriented staff who focus on the customer's application. This team-based approach marries technical expertise with market insight to produce the right outcome for the customer.

In the case of 10BASE-T1L, this approach will encompass the provision of PHY products and support for the full communications stack. It also takes account of the long commercial lifetimes of industrial products, backed by a roadmap that forecasts production with compatible 10BASE-T1L products to meet the expectations of industrial customers.

The rapid development of 10BASE-T1L components is enabling equipment manufacturers to start developing new Industrial Ethernet-enabled products. Backed by an consortium of industrial companies that support the standard development process, 10BASE-T1L technology looks set to supplant the 4 mA to 20 mA and HART interfaces and accelerate the adoption of Industry 4.0.

Brendan O'Dowd, General Manager Industrial Automation, ***Analog Devices.***

Edge-located HMIs drive new wave of Industry 4.0

Unified HMIs installed at the automation edge effectively connect users to their data by bridging OT plant data with workflows and IT tools. Advances will improve machine performance, reduce downtime, enable greater profitability, and fuel connected enterprises through the Industry 4.0 revolution.

THE RISING TIDE OF INDUSTRY 4.0 IS MARKED by surging data and cloud connectivity demands, as machine builders and manufacturers expect their plant floor process data to be available at all times from anywhere.

While digitalization and connectivity has always been viewed to be competitive advantages in manufacturing, they are now imperatives for achieving profitability, longevity, and responsiveness to rapidly evolving market trends.

Fortunately for machine builders, connected components are in abundance, and it is easier than ever to equip machines with smart sensors, variable frequency drives, and other intelligent components. However, transmitting data effectively from these devices to the cloud remains a challenge.

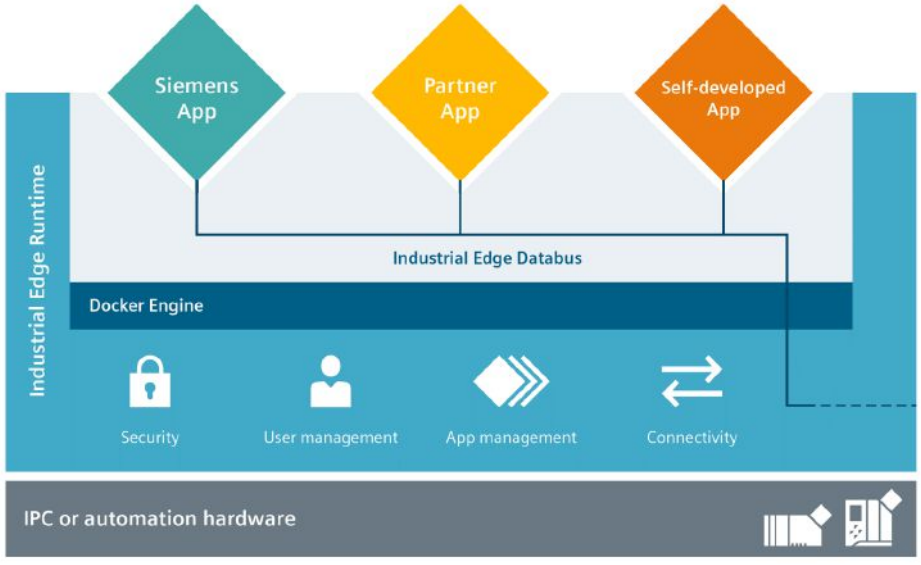
Unified human-machine interfaces (HMIs), located at the automation edge on the plant floor, are positioned to address this issue. Equipped with modern IT capabilities, unified HMIs make it easy to efficiently transfer data, enabling machine builders to deploy apps and centrally monitor one machine or a fleet. Availability of these IT capabilities in the industrial operations technology (OT) space accelerates machine efficiency improvement efforts.

SOURCE: SIEMENS INDUSTRY

A single device offers a wide variety of apps and dashboards for machine visualization and analysis.

Bandwidth and security issues

Internet of things developments are making it possible to connect remotely to numerous smart devices. Direct connection from device to cloud is often favorable in the consumer electronic space or for remote industrial applications where an edge controller is not present. However, in a plant setting with potentially hundreds of devices and sensors, direct connection to the cloud is usually not advisable due to bandwidth constraints and security concerns.



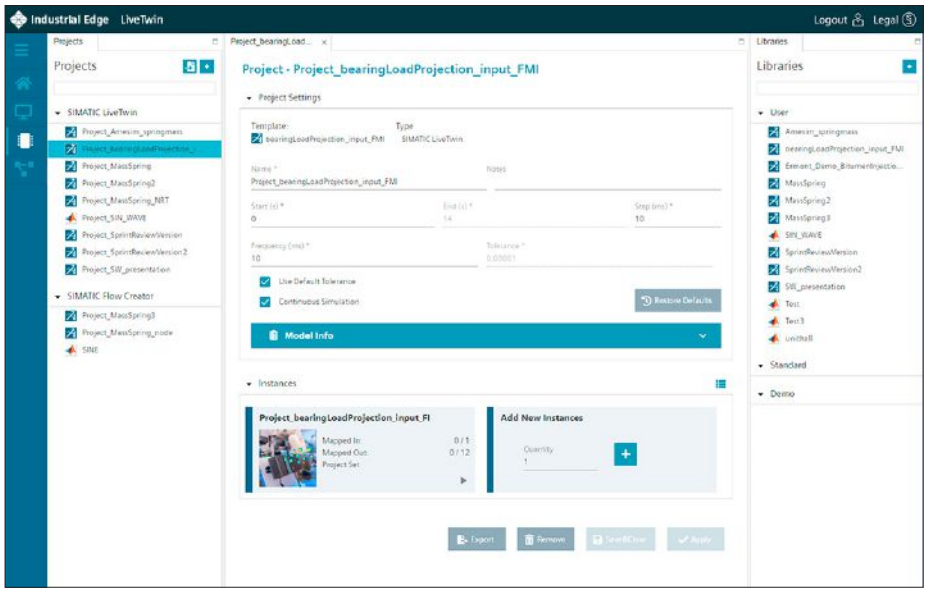
SOURCE: SIEMENS INDUSTRY

Each app has its own container, hosted by a unified HMI's docker.

While a wide array of these devices in the industrial space support direct cloud connectivity, many machine components still require an intermediary device for pre-processing raw sensor data and converting it to cloud-friendly packets. Additionally, hundreds of sensors on a plant floor simultaneously broadcasting their data for external consumption can clog up the network, creating bandwidth and latency issues.

Even if data flows smoothly in both directions between plant floor and cloud, communication must be encrypted to ensure safe operation and protect sensitive information.

Moreover, most modern plants require a PC-based solution to collect, store, and interpret historical performance data for optimizing production. If all sensor data moves directly to the cloud, data aggregation must take place outside the confines of the plant floor, introducing more data integrity risk than is present while the data is closer to its original source.



SOURCE: SIEMENS INDUSTRY

Machine builders can simulate proposed production changes prior to implementation.

Modern HMIs provide solutions

To address these concerns, manufacturers need an edge device on the plant floor to make efficient use of bandwidth in communications outside the plant, and to ensure secure data transactions. By processing data on the plant floor closer to its source, this type of component improves data integrity compared to processing in the cloud.

Though essential, the reliable movement of data from plant floor to cloud is only part of the need. Engineering, operations, and maintenance staff alike must be able to effectively visualize, analyze, and interact with machines to keep the plant running in an efficient manner, and unified HMIs at a network's edge facilitate these functions.

Unified HMIs provide different capabilities than standard edge controllers with built-in apps for managing edge devices and data, and they bring advanced IT capabilities to the machine level in a cost-effective manner. When implemented, they serve as a central repository for data across the plant floor, enabling direct visualization and analysis of machine health and performance through a single interface. Compared to direct cloud connection of individual sensors, unified edge HMIs are less complicated to implement and more feature-rich out of the box, adding capabilities to plant-floor data processing.

Configuration and usage

Acting as a bridge between OT and IT, unified HMIs are automation infrastructure agnostic, and their applications can scale as plant floor layouts evolve. This is largely in part to a wide variety of applications available for managing and interacting with machines. While developers have a host of tools available for custom app creation on unified HMIs, they are also equipped with a wide selection of built-in, scalable edge apps.

In light of the headache-inducing challenge of managing application dependencies and compatibility across devices, unified HMIs use docker and container structure to alleviate this issue, freeing developers to focus on app logic and functionality. This makes unified HMI apps heavily configurable, as opposed to programmable, because the underlying infrastructure is already vetted.

Containerization wraps up all dependencies for an app into a single package, allowing it to be deployed to any device, without the need for a checklist of external resource requirements on the target. It is similar to virtualization of a personal computer (PC)—where an operating system (OS) and its entire file system are stored in a directory, and can be run without extensive external dependencies—though containers require lower overhead than virtual machines (VMs).

A docker engine running on a device's OS enables the storage and execution of multiple containers. As a container is to a VM, so an HMI's docker is to a host PC's hypervisor.

In addition to using pre-built apps, machine builders can develop their own apps utilizing a unified HMI's docker engine. The docker incorporates security intrinsically, another advantage enabling focus on app development and less time spent on building and maintaining infrastructure.

For machine builders and end users short on time, there is likely already 'an app for that'. Native and third-party apps are available for purchase to run on unified HMIs, accomplishing tasks such as:

- Performing advanced production algorithms and calculations
- Connecting to data from multiple sources over multiple protocols
- Visualizing data
- Automating workflows
- Managing inventory
- Analyzing machine and drive health, and calling out predictive maintenance
- Analyzing performance and creating insights
- Creating notification pipelines and sending alerts
- Simulating production with digital twin

Furthermore, unified HMIs are repositories for data collection, analysis, storage, and forwarding. With the right apps, users can connect to automation controllers, drives, OPC UA devices, and other edge devices. Using the MQTT protocol, these devices can efficiently publish data to the cloud, consuming minimal network resources.

Due to their multilingual properties, unified HMIs perform well as interfaces for establishing key performance indicators (KPIs) and measuring actual production output from multiple machines. Unified HMIs also eliminate the need for PCs in many applications because they can execute many of the IT functions performed by PCs within their industrially-hardened HMI housing.

Device and app management

Adding another IT characteristic increasingly making its presence known in OT, unified HMIs include enterprise management. Machine builders and manufacturers can centrally manage devices and apps from on or off premise through a web-based interface independent of the HMI automation project file. This can be done from any device capable of hosting a web browser, such as a laptop, smartphone, or tablet.

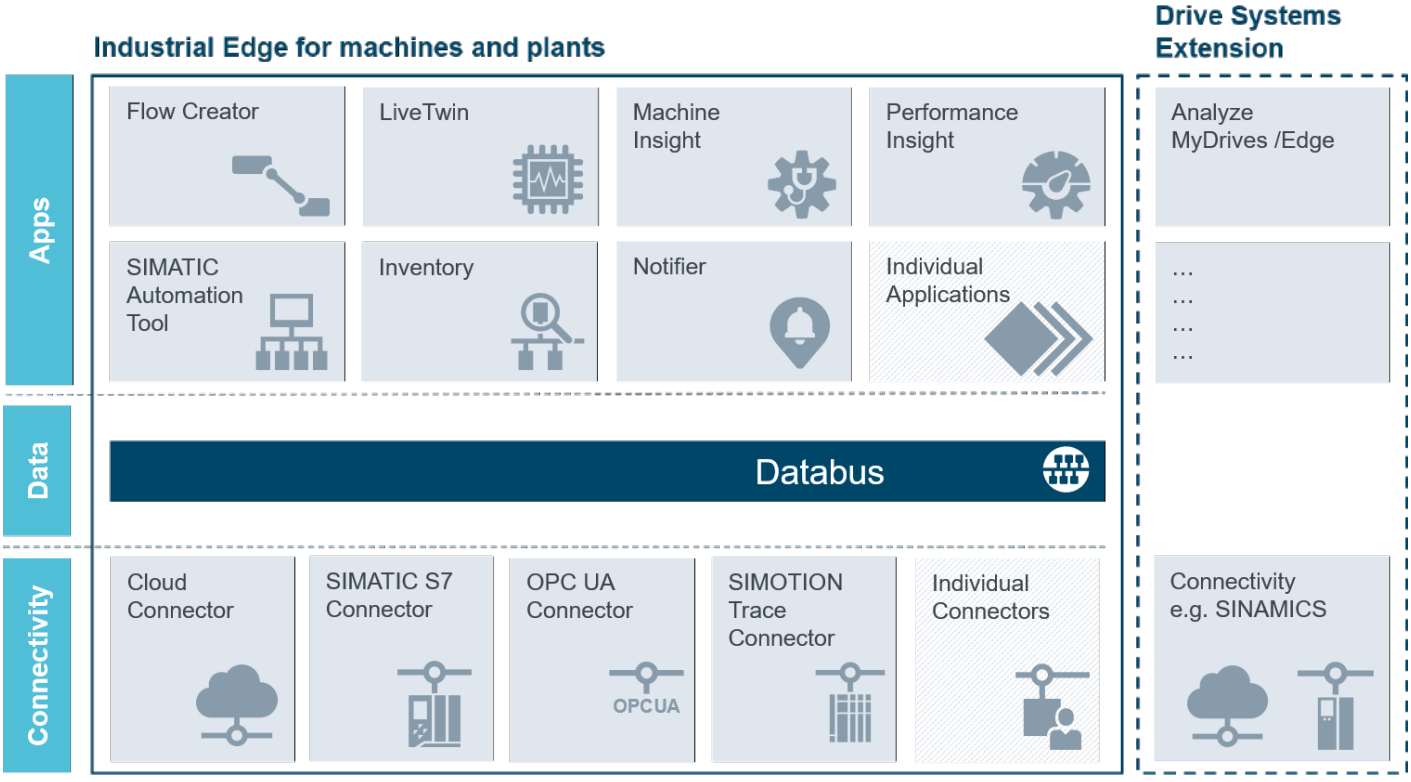
This model provides the flexibility to store apps and licenses on servers, remotely deploy or update apps without modifying machine-level functionality, apply security patches, and manage content of all unified HMIs across the enterprise. Communication among devices is encrypted, and HMIs can be configured for automatic system backup to prevent data loss.

Apps run in the background fulltime with their hooks in the docker—independently of the OS running the classical HMI automation project also present on a unified HMI—so a change in app configuration does not impact HMI runtime execution. This provides the flexibility to update apps on a regular basis without concern of modifying the automation program file.

Results

For an industrial heater manufacturer, struggling to keep up with growing demands from its stakeholders, implementing Siemens WinCC Unified HMI software and panels enabled it to deliver greater functionality and performance to its users.

This empowered the manufacturer to develop its own apps for machine and performance



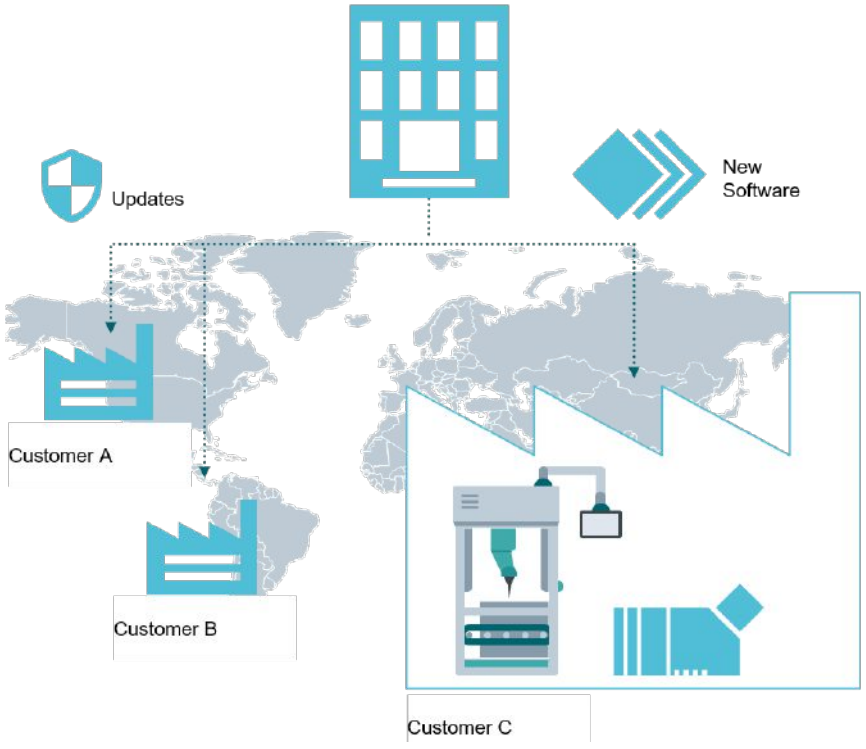
SOURCE: SIEMENS INDUSTRY

The right industrial apps ease connectivity between the cloud and plant-floor devices.

analysis, and for maintenance support. The HMI's docker ensured app security, and it saved development time because the pre-built container infrastructure allowed attention to be placed on app functionality.

Using unified HMIs' remote management capabilities, the machine builder was able to remotely push updates to machines around the world whenever they released a new revision, comparable to app updates on a smartphone or patches on a PC.

Unified HMIs' native support for MQTT made cloud connectivity possible, while OPC UA protocol support enabled users to connect their new machine with other machines in their facilities, and with intelligent devices.



SOURCE: SIEMENS INDUSTRY

Machine builders can remotely push software updates to machines around the world.

Continually improving

While industry grows more agile and geographically dispersed, machine builders are pursuing always-on access to data. Unified HMIs installed at the automation edge effectively connect users to their data by bridging OT plant data with workflows and IT tools, phasing out the need for industrial PCs in many applications.

This consolidation of functionality is already driving Industry 4.0 as machine builders are empowered to:

- Connect to their data from anywhere
- Consolidate traditionally separated OT and IT devices for data processing and access into a unified HMI
- Integrate machine performance data directly with business process workflows
- Deploy out-of-the-box or customized apps for interaction with their data
- Utilize app containers to streamline functionality and security, and alleviate OS and firmware compatibility issues

As unified HMIs evolve and continue to simplify hardware infrastructure, more and more manufacturers are relying on these devices to branch out further, supporting an increased breadth of factory-floor communication protocols.

These advances will improve machine performance, reduce downtime, enable greater profitability, and fuel connected enterprises through the Industry 4.0 revolution.

Ramey Miller, the HMI/Edge product marketing manager, ***Siemens Industry.***

City of Denver transforms traffic control network

The ability to offer a robust, easy-to-use solution that could meet the needs of today and scale to meet the challenges of tomorrow solidified Denver's decision to modernizing its TCN infrastructure. Highly configurable offerings also helped them achieve a holistic view and better management of its massive network.

TO ADDRESS ITS POPULATION AND infrastructure growth, the City and County of Denver, Colorado's largest municipality, underwent an upgrade to its traffic control network. Despite the size and operational complexities of the Denver area, city officials can now confidently manage its current and future traffic control needs with reliable, high-performing next-generation technology.

SOURCE: BELDEN

Increasing gridlock challenges in Denver were reduced through large-scale operating system upgrades.

Project overview

Traffic control systems have a lot at stake, promoting the orderly movement of vehicular and pedestrian traffic to not only encourage the steady flow of activity, but to preserve public safety. Traffic lights, cameras, sensors and other connections have become an integral part of society. Despite the public's reliance on the organizational structure and uptime of roadway signals, many are unaware of the resources necessary to effectively manage these systems.

For any traffic control network (TCN), signal management consists of many moving parts. Aside from maintaining outages, teams are tasked with geographic configuration, proportioning population to the number of signals, congestion mitigation, signal timing and more.

The increasing number of high-throughput devices such as cameras have only made this more complex. While traffic divisions rely on the active prioritization and collection of information to expedite critical data transfer, higher bandwidth requirements have created issues for legacy systems. As one of the transportation industry's most visible services, officials must prioritize traffic engineering and operations.

Sitting among the top 20 most populated cities in the United States, this has been no small feat for the City and County of Denver, which began its journey to modernization after its primary devices were discontinued by its long-standing vendor. Denver's network had already experienced dozens of failures with its existing technology, and with its main technician retiring, they had to act fast. City planners reasonably began to worry there was only a matter of time before bottlenecks and outages—or worst-case scenario, a complete crash of the system— would cause detrimental effects.

As Denver continued to experience rapid population growth, its TCN currently consisting of more than 6,000 devices, legacy systems wouldn't cut it. Continued network expansion was inevitable for this large-scale project. Its massive size and complexities required a highly configurable, reliable and comprehensible solution that could grow along with its network.

Project needs and challenges

City engineers sought a solution that could expand enough to meet the needs of Denver's quickly—and constantly—changing infrastructure. Reliability, ease of use and defensibility were primary considerations during vendor selection, but also top- of-mind for Denver engineers was timelessness.

For this transformation, a future-proof infrastructure meant:

- *Attention to design*: There was little need for redundancy capabilities and segmentation of Denver's old layout, meaning they needed to redesign their network from the ground up, restructuring based on the City and County's rapidly evolving IoT device installations.
- *Configuration with legacy devices for minimal downtime*: To ensure continuity and avoid a major malfunction of its traffic network, the City needed next-generation technology that would comply to the load and security specifications required in today's increasingly connected IoT traffic devices, without disrupting functions directing current traffic operations.
- *Higher bandwidth and scalability*: Denver's previous iterations were extremely limited in terms of performance. And lagging, or prolonged delays, are not feasible for traffic signal operations. The system required higher throughput with the opportunity to expand the network without another device replacement.
- *User-friendly maintenance*: Traffic operations are mission-critical to any city and downtime must be resolved as quickly as possible.

Systems that were too complicated to configure were not practical in this environment. Knowledge of network design and maintenance needed to exist outside of those involved with maintenance and upkeep. "From CV technology to UPS systems, the current traffic operations field equipment is increasingly reliant on IP networked devices. So, we needed a field hardened, reliable, high bandwidth network switch that could meet our rapidly changing transportation systems equipment. Our decision to go with Belden has allowed us to have the proper edge deployed equipment in place, so we can continue to modernize our transportation system safely and effectively," said Michael Finochio, engineering manager for the City and County of Denver.

Phased approach

As part of the planning process, officials and the engineering team worked together in the

field to identify issues that would likely become problematic down the road and mapped out a customized plan.

A network as large and complex as Denver's city-wide traffic system physically could not be converted to a new platform in a single instance. This large-scale conversion continues to be conducted in stages to ensure performance and uptime, while building safeguards and redundancies on the backend.

Phase One: test drive

To meet the City and County's performance and uptime requirements, as well as provide the evidence the team needed to continue modernization, a combination of existing and Hirschmann devices were suggested for the first phase of the migration.

In 2013, Belden field application engineers joined City and County engineers out in the field for testing, making sure the suggested plans and recommendations were ideally suited for the network's environment. Approximately 20 MACH1040 switches were installed to match the redundancy requirements of Denver's TCN and the migration project was in full swing.

Phase Two: getting the green light

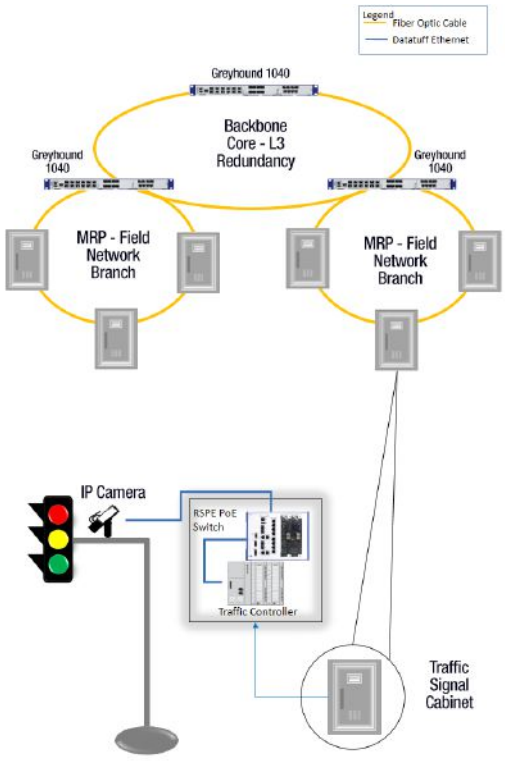
The second phase centered on the annual replacement of legacy equipment with Hirschmann devices. These gradual upgrades involve the migration from switches with underperforming redundancy capabilities, to the faster, more dependable performance of new switches.

Although Belden's engineers are not always actively on-site to address network gaps as they arise, the graphical interface of the Industrial HiVision management software and seamless configuration capabilities has enabled Denver's technicians to complete tasks that once seemed impossible.

Phase Three: no more roadblocks

Considering the constant replacement of lights and installation of other devices to improve Denver's TCN, it's no surprise the project is still underway. Complemented by the dedicated, day-to-day technical and design support of Belden's engineers and the graphical features of Industrial HiVision, a slow—but steady—transformation has allowed Denver to maintain system integrity without compromising comprehensibility.

"The demands presented by the City and County of Denver were unique in that there were multiple layers of complexity that needed to be accounted for. This was truly a case of a zero-fail standard. When working with government agencies the importance of not only designing a network that operates as intended, but is also highly secure, cannot be overstated. The City and County of Denver was a great partner and together, we built a traffic control network that can serve as a model for municipalities all over the world," said Scott Kornblue, field application engineer at Belden.



Traffic network system architecture.

Why redundancy matters

At the heart of this network solution is a core redundant ring topology which facilitates multiple subrings that provide redundant network connectivity and robustness to Denver's TCN.

By using this technology, as opposed to integrating other redundancy techniques, Belden significantly increased the availability and resiliency of the network—providing multiple paths for communication. Apart from the industrial-grade equipment recommended, Belden has the advantage of a fault-tolerant network that can handle multiple consecutive failures happening in a very short period.

The design integrated robustness and contingencies that allow the TCN to operate transparently, regardless of the disruptions that arise—whether it be a network failure, disconnection of copper or fiber cables, or another unexpected circumstance. Essentially, the industrial ring topology makes transition more seamless and comprehensive for engineers with little or no experience in design or upkeep.

Technology Details

The City and County of Denver used the following networking technology to transform its TCN operations.

RSPE Switches: Designed for networks that require 100% availability for data communications, the compact and extremely robust RSPE switches comprise a basic device with eight twisted pair ports and four combination ports that support Fast Ethernet or Gigabit Ethernet. The device can be extended to provide up to 28 ports by adding two media modules.

- Future-proof network design and best-possible investment protection
- Maximum productivity for machines and systems
- All-around protection against network attacks and operating errors

Full Gigabit Ethernet Switches: Designed specifically for use in the power industry, they can be connected to form sub-networks, which in turn can be linked up to each other.

- Designed for harsh environments with a fanless cooling system, high vibration resistance and an operating temperature range of -40°C to +70°C
- Comprehensive management and redundancy methods for configuration and diagnostics
- Redundant power supply system and fast functionality with non-blocking architecture

Network Management Software: Industrial HiVision technology safely and automatically identifies network devices and helps you configure and monitor them. The result is all-around network protection and high performance network management, all while making engineering teams more efficient.

- Highly graphical user interface for instant vision of key performance indicators
- Remediation through expedited faults detection to improve uptime and security
- Syncs to all network infrastructure, allowing easy identification, mapping and configuration across the network in real time

Conclusion

The ability to offer a robust, easy-to-use solution that could both meet the needs of today and scale to meet the challenges of tomorrow solidified Denver's decision to partner with Belden in modernizing its TCN infrastructure. The increasing benefits of the migration, however, are not solely reliant on the consultancy and conversion of Denver's devices to Hirschmann switches.

Highly configurable offerings were introduced to Denver to help them achieve a holistic view and better management of its massive network. Together, these solutions will provide virtually foolproof detection of behavioral anomalies, as well as maximize efficiency at every point of the network.

Application article by ***Belden Corporation.***

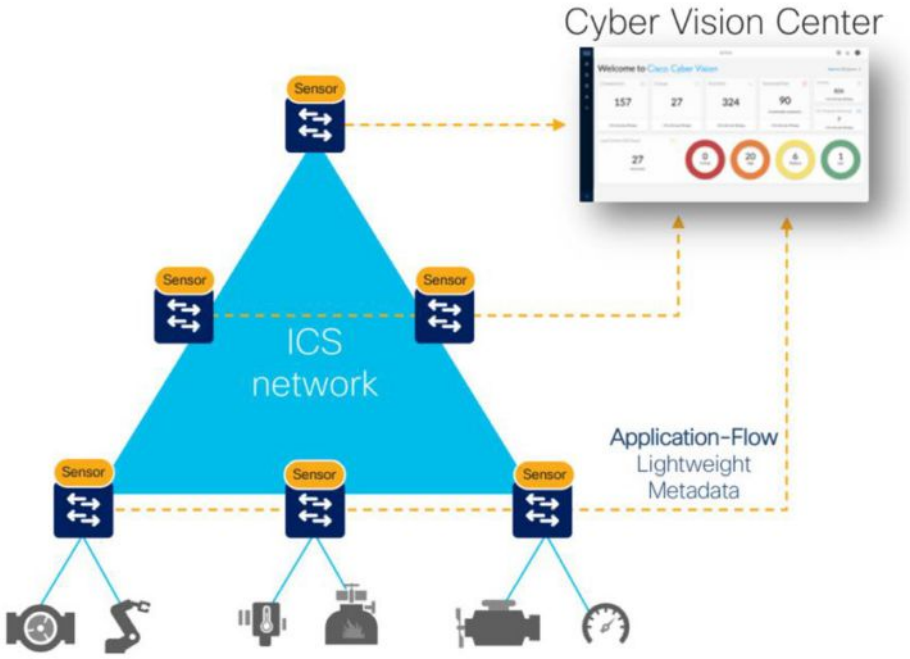
Secure collaboration spaces in manufacturing workflows

The combination of security and collaboration platforms paves the way to accelerate engagement of a "community of experts" to address anomalies in industrial control networks. These communities can react rapidly to security and operational issues within the manufacturing environments.

BASED ON OUR EXPERIENCE VISITING AND touring multiple customer plants, we can safely say that whether you are building an airplane or making a chocolate-chip cookie, the processes (with slight modifications) are similar, the safety and compliance challenges are almost the same.

In addition, the network and security challenges are almost identical. Security at the manufacturing zone has always been a tough equation to solve. It requires a delicate balance among performance (with automation), compliance (and visibility), internal polices (traffic movement), and the various "personas" that operate the environment (process ownership).

In this article, we introduce a security and collaboration model that utilizes Cyber Vision technology for monitoring on industrial networks and subsequently uses the power of WebEx Teams to create "virtual spaces" or communities of interest to react to a certain reported event. Cyber Vision provides full visibility into the Industrial Network that includes asset inventory, real-time monitoring, and threat intelligence.

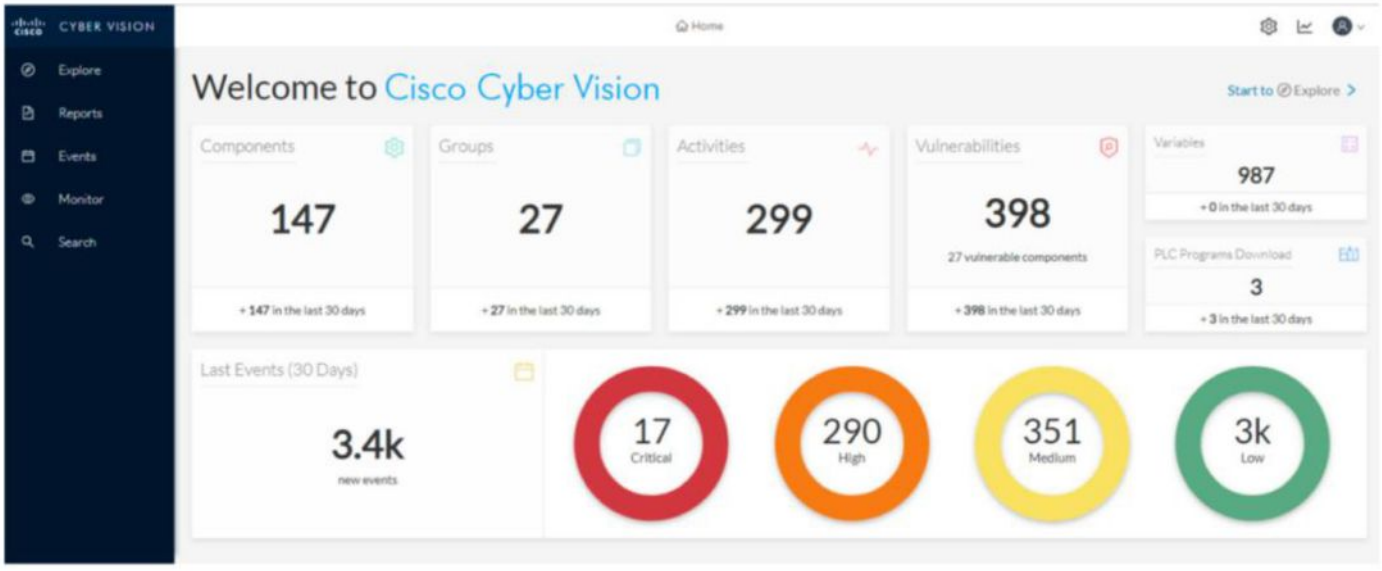


SOURCE: CISCO

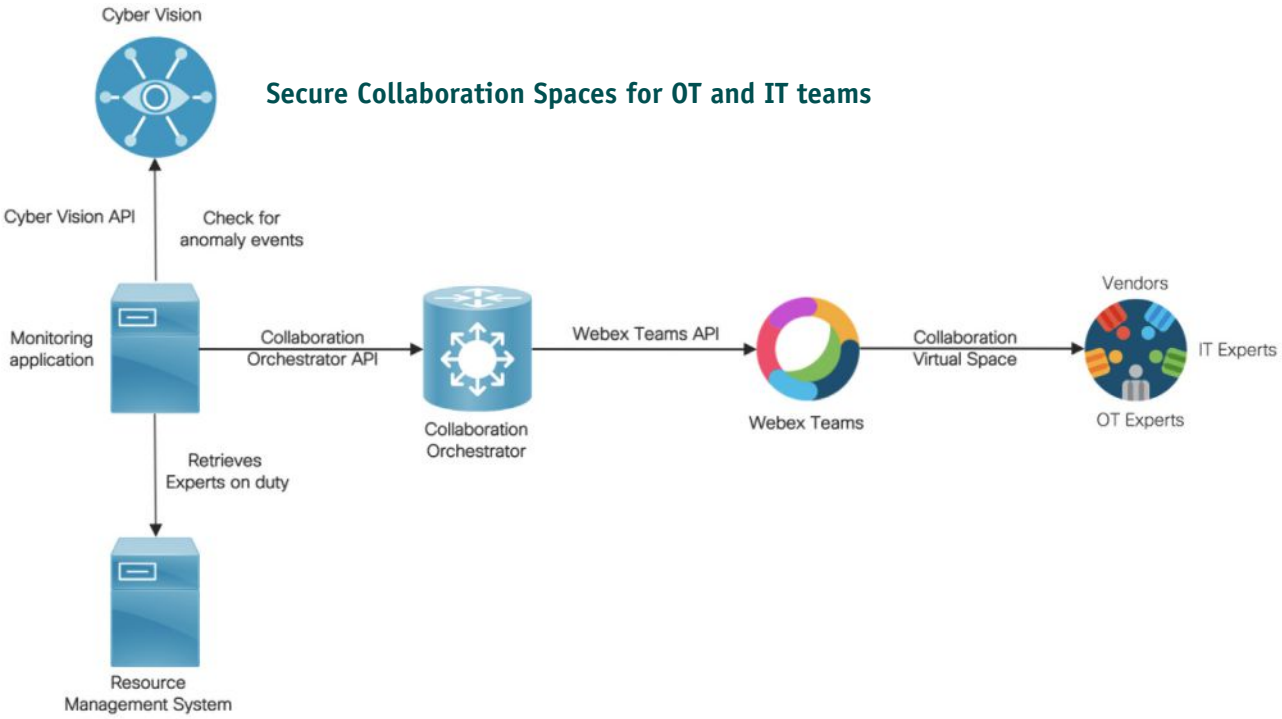
Cyber Vision deployment in manufacturing plants.

Problem Statement

Manufacturers need to protect plants from external threats and protect employees from accidents due to unplanned events. The introduction of Ethernet based protocols within Industrial control networks has brought tremendous operational efficiency by allowing control devices like Programmable Logic Controllers (PLCs) and field devices like Robots to be automatically upgraded, continuously monitored to predict future failures and proactively schedule maintenance to avoid unnecessary downtimes. The efficiency is made possible due to the ability to communicate with the control devices through remote network connections and to stream telemetry events from field devices in the plant to the Robotics vendor. This network connectivity also increases the potential threat vectors and poses a serious security challenge to manufacturers. The challenge is exacerbated by rich ecosystem of control and field



SOURCE: CISCO



Secure Collaboration Spaces for OT and IT teams

SOURCE: CISCO

devices from different vendors, talking different protocols and running different software versions. The key question is how to detect, manage and mitigate a security threat in a multi-vendor industrial control network?

Detect and inform

Cyber Vision provides a unique solution to this security challenge by providing real-time insights into communication flows within an industrial control network. The network switches such as Cisco IE3400 and Cisco Catalyst 9300 series run a Sensor application which captures the traffic from OT components such as PLCs, Supervisory Control and Data Acquisition systems (SCADA), decodes the packets, analyzes the communication exchanges and sends metadata to Cyber Vision.

The network sensors automatically discover the type, software version, vendor details of the device through deep inspection of the packets and are able to understand protocol message flows that correspond to activities such as reading a variable value from a PLC, writing a variable value to a PLC, file transfers and upgrade processes. The flow metadata sent to Cyber Vision enables it to form an understanding of the normal operation of the industrial control network in a given plant.

Cyber Vision continuously analyzes the traffic streams from sensor applications and compares the identified activities against known communication patterns and detects anomalies in the network as and when an unexpected known or unknown event happens in the network. These anomalies are brought to OT (operational technology) admin's attention through critical, high, medium and low events in Cyber Vision Center web-based dashboard.

The detection of an anomaly event doesn't necessarily mean that it is a security threat. Some of these events could be triggered by an unplanned change by process control engineers working in the plant while some of them could be real threats triggered by malware running in the OT and IT devices. The next key question that arises is how do we differentiate between unplanned change management events and security threat events and take swift action to mitigate the risks and protect the control network?

It is essential to inform plant experts about anomaly events and facilitate collaboration among the experts to discuss and determine next steps such as acknowledge and ignore the event, invoke an emergency safety procedure etc. The event notifications displayed in a Cyber Vision center dashboard may get unnoticed due to the sheer volume of events.

Supervisors and Experts who are responsible for a particular event (also called as Community of interest) need to engage with their peers manually through out of band communication channels such as email, push-to-talk, walkie-talkie, phone call or call for a meeting. The API based integration between Cisco Cyber Vision and Webex Teams platforms automate the engagement of the "community of interest" through secure collaboration virtual spaces.

An example deployment illustrates how the Monitoring application periodically checks for anomaly events using the Cyber Vision APIs. When events of interest such as critical, high severity event types happen, the monitoring application determines the list of resource roles to be engaged based on an Event category to Resource roles mapping table. It then retrieves information about plant employees with the identified role and who is currently on duty/shift.

The application requests Collaboration Orchestrator to create a secure collaboration space and adds the on-shift OT experts as participants. IT experts and external vendors are added as required depending on the type and criticality of the event. The monitoring application also posts relevant information of the event to the collaboration space for expert's review. The application could also add bots to the space to augment the review process. The bots can be used by experts to get quick information about control devices and machines right within the collaboration space instead of manually retrieving information from multiple systems.

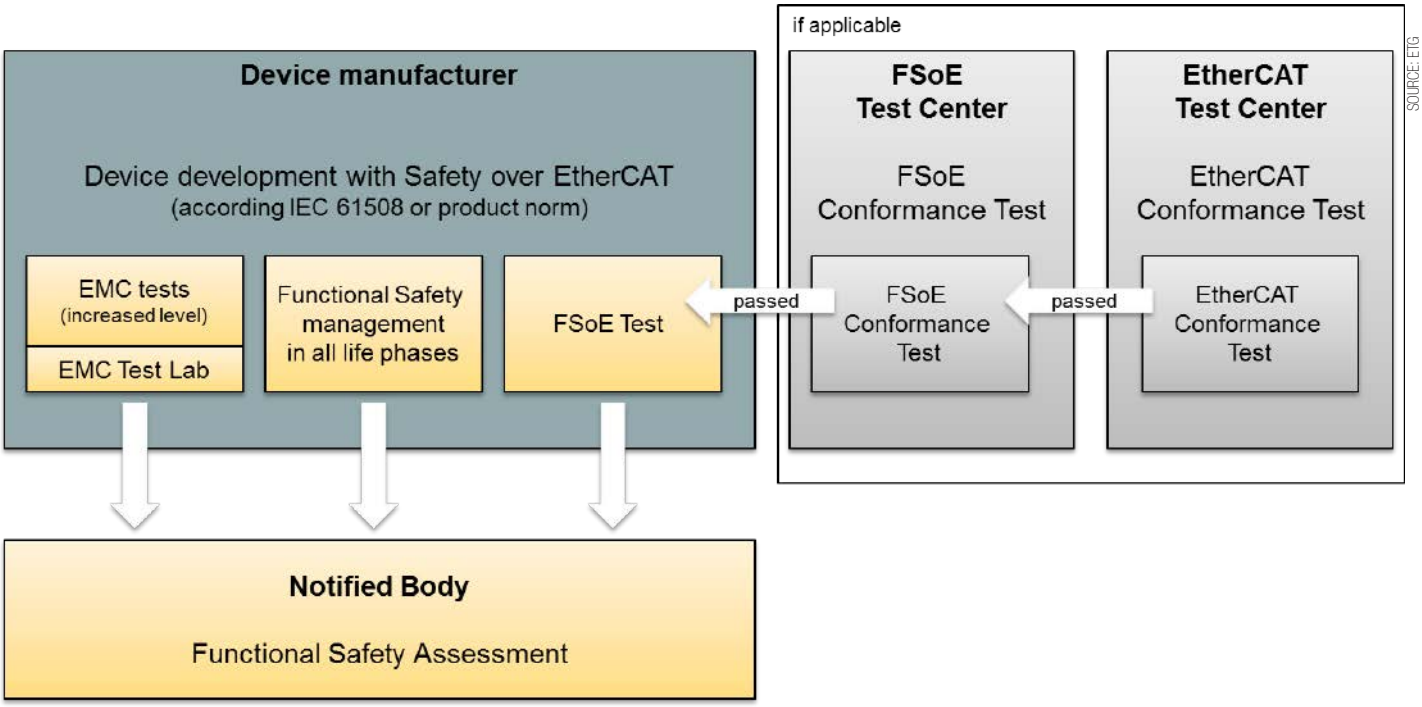
Supervisors and process control experts get notified through their mobile, desktop based Webex Teams clients and start to review the event. They collaborate and decide on next steps swiftly. They could even use the bot participant to execute administrative next steps such as acknowledge and mark the event as an unplanned, no harm event. In other scenarios, they could invoke safety procedures to protect the industrial control network from the identified threat or trigger troubleshooting processes to isolate the source of the issue, execute a task to mitigate the impact and perform root cause analysis in order to prevent future threats.

The combination of security and collaboration platforms paves the way to accelerate engagement of "community of experts" to address anomalies in an industrial control network of a manufacturing plant faster and more effectively.

Chidambaram Arunachalam, Principal Engineer and Hazim Dahir, Distinguished Engineer, ***Cisco Systems.***

Safety over EtherCAT conformance testing

To formally confirm a high level of safety, the manufacturers of EtherCAT devices must meet requirements during development, testing and implementation to ensure the safe operation of products. A wide range of support services are available including tools, tests, documents and consultation.



SOURCE: ETG

Acceptance process for Safety over EtherCAT (FSoE): Development of functional safety devices requires a rigorous formal process to verify the performance of high quality safety hardware and software. Proof must also be provided for the reliable and standard-compliant implementation of the Safety over EtherCAT protocol. The goal is to ncreases the reliability, freedom from errors and interoperability of secure communication and ultimately customer satisfaction.

IN APPLICATIONS WHERE LIFE AND LIMB are at stake, or where valuable machines and manufactured goods require protection, safety devices ensure the necessary safety measures in the field.

In the event of a fault, they trigger mechanisms at lightning speed, which for example force an emergency stop of a machine to reliably ensure the safety of the application and above all of the operator.

To formally confirm this high level of safety, the manufacturers of such devices are subject to official requirements during development, testing and implementation to ensure the safe operation of products.

The EtherCAT Technology Group (ETG) therefore offers manufacturers of Safety over EtherCAT (FSoE) devices an ecosystem with a wide range of technical and engineering support services such as tools, tests, documents and consultation.

The central component of these support services is the official FSoE Conformance Test, which is mandatory for manufacturers.

FSoE conformance test

The development of functional safety devices is associated with a rigorous formal effort, which on the one hand results in high quality hardware and software, and on the other hand also ensures verifiability.

Finally, before the market launch of a new product, a recognized test center must prove that the entire implementation meets the requirements of the desired Safety Integrity Level (SIL).

In addition to the actual safety-relevant function of the application (e.g. safe emergency stop or safely limited speed for a drive), proof must also be provided for the reliable and standard-compliant implementation of the Safety over EtherCAT protocol. One of the means of choice for this is the so-called FSoE Conformance Test, which is carried out by an officially recognized FSoE test service provider in the EtherCAT Test Center.

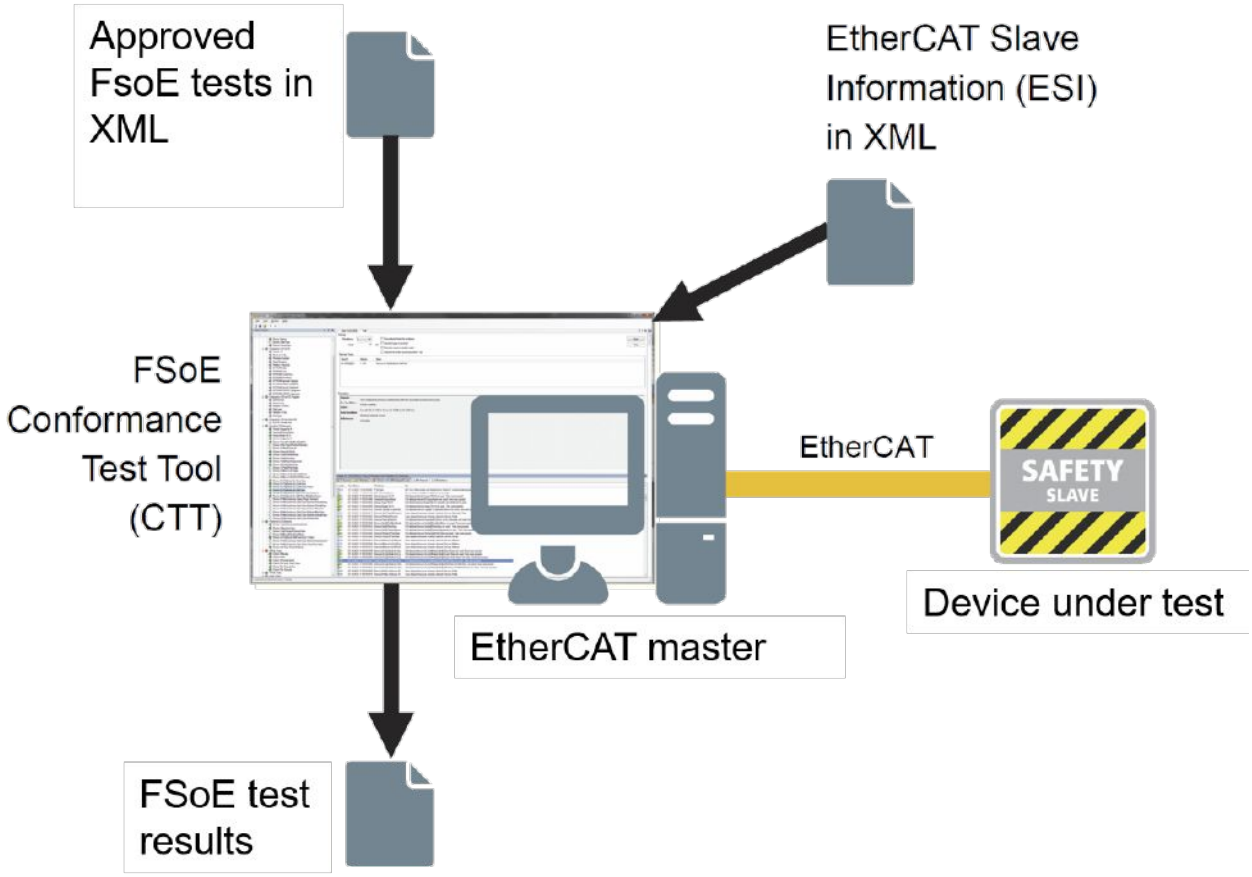
According to the FSoE Policy, each manufacturer is obliged to perform this test, which in itself already constitutes a subset of the formally required proof overall.

And even if the official FSoE Conformance Test only represents a relatively small part of the obligation to prove the safety of a device, it nevertheless provides great added value for the manufacturer – especially in connection with the other test options offered by ETG.

In concrete terms, the official FSoE Conformance Test significantly increases the reliability, freedom from errors and interoperability of secure communication and ultimately customer satisfaction.

What actually happens

The prerequisite for the FSoE Conformance Test is the EtherCAT Conformance Test, which checks whether the basic EtherCAT implementation works reliably. If this is not the case, and if errors already occur in the underlying communication, the safety function is constantly triggered in a machine, which makes it a supposedly safe machine, but drastically reduces its availability and



SOURCE: ETG

FSoE Conformance Test Tool (CTT) for automatic verification and conformance test.

throughput. If the device passes the test for the EtherCAT protocol, the FSoE conformance test checks the implementation and integration of the FSoE protocol.

Conformance test in safe hands

In Germany, the FSoE Conformance Test is carried out by TÜV Süd Rail, which is recognized as one of the world's leading institutions in industrial device testing and verification.

The test is therefore usually also internationally recognized by other test facilities commissioned by the manufacturer for the overall verification, such as TÜV Nord or TÜV Rheinland. In addition, the FSoE Conformance Test itself is based on a world of specifications that have already been confirmed by TÜV Süd: The FSoE specification ETG.5100 was officially certified in 2005 and has been part of the international standard IEC 61784-3 FSCP 12 (Functional Safety Communication Profile) since 2010.

The ETG.7100 test definition in the form of a test table has also been approved by TÜV and completely covers the tests for FSoE slave devices as well as masters, enabling every device manufacturer to implement it in their own test environment.

Through the integration of these tests into the EtherCAT Conformance Test Tool (CTT), the tests can also be automated and performed in a repeatable manner. This is also done during the official FSoE Conformance Test and serves device manufacturers during the development and integration of the FSoE stack into their devices and, of course, in preparation for acceptance in the EtherCAT Test Center.

Manufacturers not alone

In addition to the FSoE Conformance Test as a central element, the EtherCAT Technology Group offers manufacturers further assistance in the planning, development and testing of FSoE devices.

An important document is the Safety over EtherCAT Implementation Guide, which provides relevant information for implementation best practices. It contains all references to specifications and documents as well as the available facilities for training, support, development products and services and testing.

In addition, developers have the opportunity to participate in EtherCAT Plug Fests, which are considered a pragmatic approach to test the functionality and interoperability of their own devices and stacks with those of other manufacturers.

In addition to the general EtherCAT Plug Fests, where tests specific to both EtherCAT and FSoE protocol can be performed and questions can be answered, there is a special Plug Fest once a year where only FSoE device manufacturers come together. Here the interoperability of FSoE slaves, masters and configuration tools is tested. The Plug Fests are a good opportunity for manufacturers to validate their own implementation in the prototype stage and are useful as part of the preparation for the official EtherCAT and FSoE Conformance Test.

As with the EtherCAT base protocol, the EtherCAT Technology Group offers a comprehensive ecosystem around FSoE implementation, testing and release. The organization's goal is to support manufacturers of FSoE devices in realizing their implementation as quickly and successfully as possible and to go through the official acceptance process as smoothly as possible.

Final steps in FSoE testing

The FSoE conformance test is carried out by TÜV Süd Rail at the ETG-accredited EtherCAT Test Center in Nuremberg, Germany. In a so-called one-stop-shop procedure, the device manufacturer can have the EtherCAT Conformance Test, which is mandatory as a basis for general EtherCAT implementation, carried out in one day. If this test is passed, the FSoE Conformance Test is usually performed on the following day.

Christiane Hammel, ***EtherCAT Technology Group.***

Industrial Control Systems: CIP Security and IEC 62443-4-2

CIP Security meets a significant number of IEC 62443-4-2 requirements and implements robust and ubiquitous security technologies to achieve protection of the control system device. These technologies can be part of an IEC 62443-4-2 security certification, and apply to the system level through IEC 62443-3-3.

ISA/IEC 62443 IS A STANDARD FOCUSING on cyber security in industrial control systems. It is comprised of a suite of specifications including policies, procedures, and requirements for system-level installations as well as industrial control systems and devices.

One part of ISA/IEC 62443, specifically ISA/IEC 62443-4- 2, contains detailed technical requirement for industrial control systems and devices.

Security requirements/levels

IEC 62443 utilizes the concept of Security Requirements as well as Security Levels to classify the security features and security functionality for industrial control systems and devices. Devices fulfilling those Security Requirements and Security Levels may achieve a security certificate if reviewed by an accredited auditor.

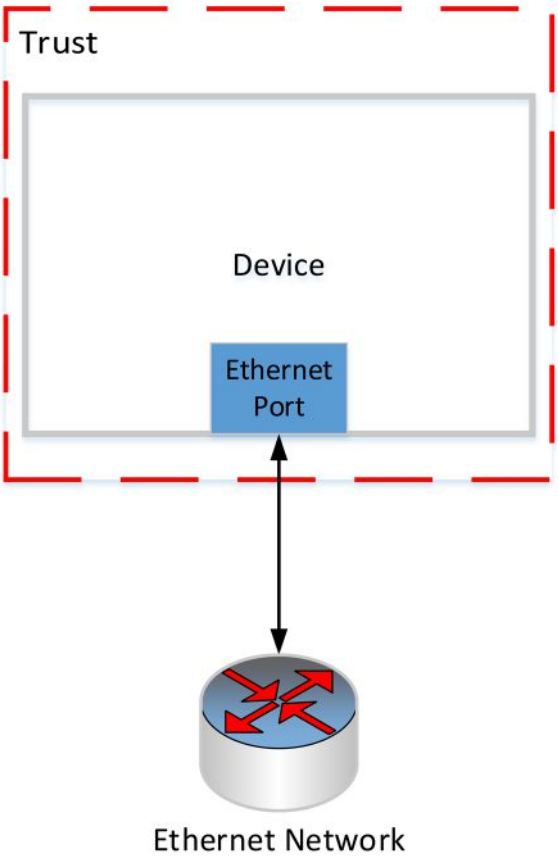
In this article we will look at how the feature set of CIP Security, both the existing CIP Security EtherNet/IP Confidentiality Profile as well as the in-development CIP Security User Authentication Profile, maps to and fulfills requirements defined in IEC 62443-4-2. The Security Requirements in IEC 62443-4-2 have been reviewed and we can present an investigation on which security requirements are fulfilled by CIP Security, and which are out of scope and need to be fulfilled by other means.

A company developing products intended to be certified against a security level in IEC 62443-4-2 can leverage the information in this paper to facilitate their investigation and design. The investigation done in this paper can reduce the effort needed to achieve a certification. Beyond IEC 62443-4-2, this analysis can also aid in vendors seeking IEC 62443-3-3 certification, as that is a certified system rather than a single product. For IEC 62443-3-3, this analysis can show what capabilities a CIP Security enabled product can provide to the system, which can help in constructing an IEC 62443-3-3 argument.

Introduction

IEC 62443 is an international standard around the security of industrial control systems. Over the last several years this standard has grown in prominence to become a highly recognized, ascendant standard for industrial control system security. The standard itself contains several parts, with part 4-2 focused specifically on the security requirements an individual product must satisfy in order to be certified. CIP Security is the ODVA standard for securing CIP and EtherNet/IP, with reliance on widespread and robust technologies such as TLS, DTLS, OpenID Connect, and OAuth 2.0. This article analyses CIP Security and the IEC 62443 requirements to determine which requirements are satisfied, either partially or fully by CIP Security.

It is important to keep in mind that certification of a product to IEC 624434-2 is an intensive process that requires formal threat modeling and analysis of the product. Given this, it is not possible to make claims that CIP Security will satisfy IEC 62443 requirements in all possible cases and all possible implementations. This article is intended to be a guide for those seeking IEC 62443-4-2 certification and leveraging CIP Security for meeting some of the requirements. Necessarily, some assumptions must be made for this analysis, and those assumptions do not necessarily apply in all scenarios.



SOURCE: ODVA

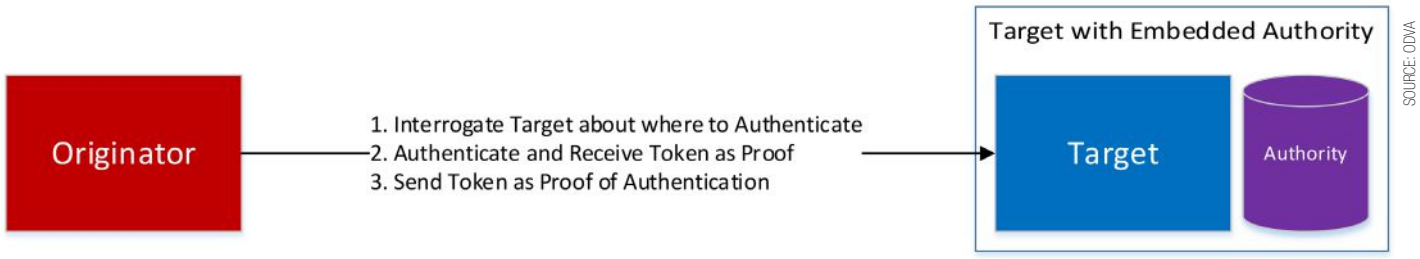
Concept of trust boundary is part of CIP Security.

For the purpose of this article, the product under consideration is assumed to be a simple device with one physical Ethernet port. That port allows for EtherNet/IP and CIP communications (other communication protocols are not considered). CIP Security has been implemented, which includes the EtherNet/IP Confidentiality Profile and the User Authentication Profile. That is, the trust boundary is drawn around the device, with the data coming in from or going out to the Ethernet port crossing the trust boundary. Many devices that will be certified to IEC 62443-4-2 will have other ports and more complex trust boundaries, however the device and trust is assumed to be this simple, illustrative case.

CIP Security overview

CIP Security has two main profiles: the EtherNet/IP Confidentiality Profile and the User Authentication Profile. The former is focused on transport level security for EtherNet/IP, and the latter is focused on providing user authentication and basic authorization. A brief description of these two profiles is given, for more information please see Volume 8 of the CIP networks specification.

The EtherNet/IP Confidentiality Profile makes use of the IETF-standard TLS (RFC 5246) and DTLS (RFC 6347) protocols in order to provide a secure transport for EtherNet/IP traffic. TLS is used for the TCP- based communications (including encapsulation layer, unconnected messaging, transport class 3), and DTLS for the UDP-based transport class 0/1 communications. This approach is analogous to the way that HTTP uses TLS for HTTPS. Certificate management is also provided by this profile. Certificates can be managed over the standard EST protocol, or over CIP via defined attributes and services.



Local Authentication.

Profile provides these security attributes:

- *Authentication of the endpoints:* ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.
- *Message integrity and authentication*: ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS/DTLS hashed message authentication code (HMAC).
- *Message encryption*: optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS/DTLS handshake.

The CIP Security User Authentication Profile provides mechanisms to authenticate users and to limit access to the least privilege appropriate for a given role. The User Authentication Profile again takes advantage of IETF standard technology, such as JWTs, OAuth 2.0 and OpenID Connect to authenticate the user and grant the appropriate level of access to protected resources. This profile allows for a CIP target to act as an identity authority itself, containing a database of users and their associated claims, or allows devices to integrate into a third-party identity management system.

This integration is achieved through the standard OpenID Connect technology, commonly leveraged throughout the Internet and in enterprise systems and IT systems. A basic level of authorization is also defined by the User Authentication Profile, although for most actions it is up to the vendor to determine what roles have appropriate privilege.

IEC 62443

The IEC 62443 series have been developed to address the need for cyber security and robustness in industrial control systems. Some general background information will be given here on the IEC 62443 specification, and especially the IEC 62443-4-2 specification. However, the IEC documents remain the authoritative reference; understanding of the IEC documents is necessary for a full interpretation of the information presented.

The family of the IEC 62443 standards is divided into 4 parts, General, Policies & Procedures, System, and Components. Within each part there are several elements that address specific topics related to the specific part of the standard. The standard in the series have the name of IEC 62443-X-Y. Figure 4 shows the groups and the individual elements of IEC 62443.

Each part deals with information related to the focus of that part and its intended audience. The parts refer to the X in the naming of the standard and the four are:

- *General*: this group provides elements that discuss items that are common and general for the whole series.
- *Policies & Procedures*: items address policies and procedures to implement a cybersecurity management system.
- *System*: elements describe requirements and management of systems.
- *Components*: requirements for components used in industrial systems.

IEC 62443-4-1

IEC 62443-4-1 introduces an established secure development process, and this is the basis for developing products that comply to IEC 62443-4-2. For the purposes of this article, IEC 62443-4-1 and the associated processes are outside of scope.

IEC 62443-4-2

In IEC 62443-4-2 functional requirements for components that are to be used in industrial control systems are defined. Although the term component is quite general, it can naturally be applied to a singular product or device. The document defines requirements for different types of components: software applications, embedded devices, host devices, and network devices.

Each component type has its individual set of requirements defined, however most of the requirements that are defined within IEC- 62443-4-2 are generic for all types of components.

The cyber security requirements that are defined in the specification for the different components are derived from the industrial control system requirements defined within IEC 62443-3-3. This is derived from the intention of the IEC 62443 series to provide a flexible framework that assists in addressing existing and future cyber security vulnerabilities in industrial automation control systems by applying necessary mitigations for defense. IEC 62443-3-3 defines the concept of system requirements which IEC 62443-4-2 then expands into a series of component-level requirements; these two portions of the IEC 62443 specification align with one another.

The component-level requirements are a technical description of the cyber security requirements in an industrial control system device. Those descriptions give the implementor an understanding about the requirements and what they are intended to protect against. It does not give any direct guidance on how to implement and apply the specific requirement in a product; this is left to the discretion of the implementer.

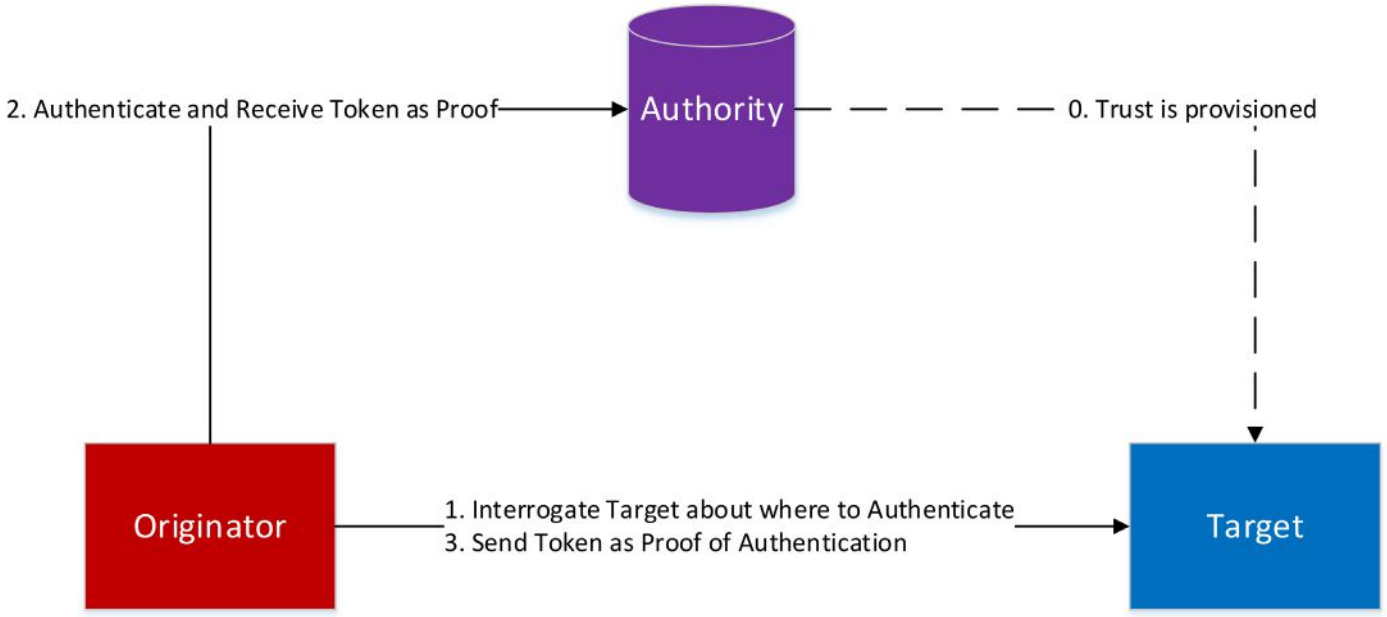
The component-level requirements are derived from foundational requirements in IEC 62443-1-1; there are a total of seven foundational requirements. Within each foundational requirement group there are a set of component-level requirements. The foundational requirements are used for grouping the component-level requirements as follows:

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

Each component-level requirement has a defined component security level, described with a value of 0 through 4. The value of 0 for a component-level requirement indicates that it is not defined as a requirement. A higher value denotes a higher and more stringent requirement. A brief description of the different security levels is:

- SL 1 – Focused on actors who unintentionally cause security events
- SL 2 – Focused on motivated attackers with basic skills and resources
- SL 3 – Focused on advanced attackers with moderate resources
- SL 4 – Focused on the highest level of attackers with significant skills and resources

The evaluation done is targeting an SL 3 level attacker; therefore SL 4 capabilities are outside the scope of this evaluation.



SOURCE: ODVA

Central Authentication.

CIP Security map to requirements

This section details how CIP Security maps to and fulfills the individual component-level requirements. Each IEC 62443-4-2 component-level requirement is listed, along with the relevant CIP Security functionality that covers the requirement.

CR 1.1 Human user identification and authentication: Devices that implement the CIP Security User Authentication Profile will be able to identify and authenticate human users requesting access to the device using CIP Security. CIP Security User Authentication Profile makes use of OpenID Connect when integrating with an external authority. Beyond OpenID Connect integration, the User Authentication Profile also provides the option for the device to store the user account information locally, in which case no authority external to the device is needed. In either case JWTs are used for identification of the users.

CR 1.1 RE-1 Unique identification and authentication: The User Authentication Profile allows for unique identification and authentication through tokens (JWTs). Each JWT is unique and provides proof of authentication, either via a central mechanism like OpenID Connect, or locally to the device's database of users.

CR 1.1 RE-2 Multifactor authentication for all interfaces: The User Authentication Profile supports integration into a third-party identity provider via OpenID Connect and OAuth 2.0, which can support multifactor authentication. CIP Security devices will not support multifactor authentication within the device itself, although they will fully integrate into third-party systems supporting OpenID Connect, which can support multifactor authentication. However, it is also possible for a vendor to extend the User Authentication Profile to support multifactor authentication locally within the device if they wish to do so.

CR 1.2 Software process and device identification and authentication: Devices implementing CIP Security use either X.509 certificates or pre-shared keys as a proof of their identity. The X.509 certificates or pre-shared keys are also used when devices authenticate themselves within a system, via the CIP Security User Authentication Profile. In the User Authentication Profile, JWTs are used as proof of authentication and allow integration into central identity management solutions. JWTs can be utilized by software processes, devices, and human users.

CR 1.2 RE-1 Unique identification and authentication: JWTs and X.509 certificates both provide unique identification for components. PSKs do not, and should not be selected as the authentication mechanism for users wishing to meet this requirement.

CR 1.3 Account management: CIP Security User Authentication profile defines the functionality for CIP Security devices to manage accounts either locally using username and password or certificates or integrate in an OAuth 2.0/OpenID Connect system for a centralized account management.

CR 1.4 Identifier management: For locally stored users in the CIP Security Authentication profile the device must keep a list of all usernames and to be able to identify the account via a unique username. In the case where the CIP Security device integrates with an OAuth 2.0/OpenID Connect system, the system identity provider ensures that the user identifier is unique.

CR 1.5 Authenticator management: The CIP Security User Authentication Profile allows for optional implementation of initial authenticators. This is meant to bootstrap the system for trust provisioning of the user's preferred authenticators; the user is prevented from using the default authenticator for any activity outside of provisioning user-controlled authenticators. The User Authentication Profile also allows for updates of the authenticators, whether stored locally or managed externally via OpenID Connect/OAuth 2.0.

When used with EtherNet/IP the authenticators are required to be transmitted over TLS/DTLS with a confidentiality-based cipher suite, ensuring protection from disclosure and modification. Storage of the authenticators internally is not specified by CIP Security, although the specification notes that best practices should be followed to prevent any vulnerabilities that may compromise the authenticator. Other than the internal storage of authenticators, which is outside of scope of the specification, this requirement is met by the User Authentication Profile.

CR 1.7 Strength of password-based authentication: For locally authenticated users, the CIP Security User Authentication Profile provides functionality to enforce the length and complexity of the password. In the case when integrating with an OAuth 2.0/OpenID Connect system it is up to the system to enforce this requirement; many OpenID Connect systems provide support for this.

CR 1.7 RE-1 Lifetime Restrictions for Human Users: For this requirement again OpenID Connect/OAuth 2.0 servers can be configured for this. For locally stored passwords the CIP Security User Authentication Profile provides the option to prevent previously used passwords for a configurable number of generations.

CR 1.7 RE-2 Password Lifetime Restrictions for all Users: CIP does not differentiate between human users and

non-human users; this requirement is met using the same rationale as CR 1.7 RE-1.

CR 1.8 Public key infrastructure certificates: The CIP Security public key infrastructure integration is based on EST (Enrolment over Secure Transport) which is an established standard from the IETF. EST relies on X.509 certificates which represent the industry standard defining digital certificates. Using EST a number of workflows and processes can be used to deploy certificates; some of the most common are described in the Pull Model paper presented at the ODVA 2018 Industry Conference. Certificates may also be managed over CIP, through which integration with a PKI can be achieved using CIP client software that can manage certificates on CIP endpoints and can be designed to interact with the PKI.

CR 1.9 Strength of public key-based authentication: This requirement has a number of sub requirements:

- Validate certificates by checking the validity of the signature of a given certificate.
- Validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued.
- Validate certificates by checking a given certificate's revocation status;
- Establish user (human, software process or device) control of the corresponding private key.
- Map the authenticated identity to a user (human, software process or device).
- Ensure that the algorithms and keys used for the public key authentication conform to CR 4.3 Use of Cryptography.

CR 1.11 Unsuccessful login attempts: When using the centralized authentication scheme of the CIP Security User Authentication Profile this is covered by using an OpenID Connect Authority which enforces limits on unsuccessful login attempts. When using local authentication this is achieved via setting an attribute in the Password Authenticator Object to enforce the number of allowed unsuccessful login attempts.

CR 2.1 Authorization enforcement: CIP Security User Authentication Profile mandates authorization enforcement based on roles. CIP Security specifies role assignments that are required to perform specific security-related operations. For other operations, general guidance is provided by the in the CIP Security Specification as to what is appropriate for a given role.

Due to the wide variety of functions a product which implements CIP can perform it is ultimately up to the vendor to decide what roles can perform what operations on a given product, although CIP Security requires that these decisions be made and enforced via the product's access policy.

CR 2.1 RE-1 Authorization enforcement for all users: CIP Security User Authentication Profile does not differentiate between humans, software processes, and devices. All of these types of users are subject to authorization controls.

CR 2.1 RE-2 Permission mapping to roles: CIP Security User Authentication Profile provides well-defined roles, with the possibility for a vendor to add more. The roles are not strictly hierarchical and apply to humans as well as software processes and devices.

CR 2.1 RE-3 Supervisor Override: CIP Security User Authentication Profile provides a service allowing for a temporary escalation of privilege. This escalation lasts for a configurable amount of time.

CR 2.4 Mobile code: Given the assumption that only CIP and EtherNet/IP is used for data communication, then mobile code is transmitted using CIP Security. Therefore, mobile code is protected in transit via TLS or DTLS, and only an authorized user via the User Authentication Profile can transmit Mobile Code (Engineer or Administrator). This requirement is met via CIP Security.

CR 2.6 Remote session termination: Remote sessions are terminated automatically after inactivity time. This applies to TLS sessions, DTLS sessions, and User Authentication sessions, each having its own configurable inactivity time.

CR 2.7 Concurrent session control: CIP Security devices support and Electronic Data Sheet (EDS) file which includes information on connection capacity. This defines limits on number of CIP sessions as well as I/O sessions.

CR 3.1 Communication integrity: Integrity of communications is provided by HMAC on TLS/DTLS sessions, using SHA-2 family algorithms. This provides best-in-class integrity protections for data in transit via internationally recognized and well-vetted cryptography and security protocols.

CR 3.1 RE-1 Communication authentication: Authenticity of communications is provided by HMAC on TLS/DTLS sessions, using SHA-2 family algorithms. This provides best-in-class integrity protections for data in transit via internationally recognized and well-vetted cryptography and security protocols.

CR 3.7 Error handling: Generally, CIP provides a rich set of error handling and feedback in order to allow integrators and users to commission a device within a system. However, this information is application related information. CIP Security has specifically been designed not to disclose or reveal any information that can be used to exploit the device or system; the error codes defined do not leak sensitive information.

CR 3.8 Session integrity: This requirement has a number of sub requirements:

- The capability to invalidate session identifiers upon user logout or other session termination;
- The capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and
- The capability to generate unique session identifiers with commonly accepted sources of randomness.

CR 3.12 Provisioning product supplier roots of trust: CIP Security defines the use of vendor certificates, which includes a root of trust managed by the vendor. Those certificates and associated root of trust can be used as the key to perform the integrity check and offer a way to prove it is a genuine device that has not been tampered with. However, it is up to the vendor to securely store the vendor certificate and provide means to use the vendor certificates.

CR 3.13 Provisioning asset owner roots of trust: CIP Security provides interfaces to commission user-defined certificates used for secure communication between devices in a system. Besides this the User Authentication Profile adds interfaces and capabilities to authenticate users that have access to the device or system as a whole.

CR 4.1 Information confidentiality: Protecting the data at rest is out of the scope for CIP Security as this is not related to the communication protocol. However, for data in transit CIP Security fully covers this requirement via the CIP Security EtherNet/IP Confidentiality Profile. This profile is built on TLS and DTLS which has the capability to provide confidentiality to the data in transit. The protection of data is done via TLS and DTLS confidentiality-based cipher suites.

CR 4.3 Use of cryptography: As noted before data at rest is out of scope for CIP Security. To protect data in transit CIP Security is built using standards such as TLS and DTLS, OpenID Connect, X.509, OAuth 2.0, RSA, ECC, AES, SHA-2, which represent widely accepted and widely used, well-vetted and well- tested algorithms and technologies.

CR 7.6 Network and security configuration settings: CIP Security provides the ability to configure a device according to recommendations provided by documents such as The Converged Plant-Wide Ethernet guide.

CR 7.6 RE-1 Machine-readable reporting of current security settings: The Get Attributes service of the CIP Security Objects allow for security settings to be read out of a device in a machine-readable format.

CR 7.7 Least functionality: CIP Security includes options to close TCP and UDP ports not in use, the same option is provided to close down IANA protocols such as ICMP.

Jack Visoky, Security Architect and Sr. Project Engineer, ***Rockwell Automation*** *and Joakim Wiberg, Manager Technology and Platforms,* ***HMS Networks.***

Connectivity in the changing robot industry

Changes in the robotic industry, especially trends toward connectivity, miniaturization and Industry 4.0, led to a partnership between HARTING and Kuka. Responding to these megatrends put the focus on detailed application knowledge, a common view of holistic customer benefits and concrete new product solutions.

QUALITY, COMPETENCE AND TRUST FORM the foundations and guarantee for a good partnership. With this in place, convincing performance and high standards can be achieved. With the willingness and know-how to innovate, companies can always master new challenges, weather competition and shape the future.

Digital transformation

More than ever before, today's world is characterised by digitalisation both in the consumer and industrial sectors. With a look to industry, it is clear that this cannot happen without cooperation and partnerships.

Specialists with a wide range of competencies and skills are needed everywhere to offer suitable holistic solutions. This is already clearly demonstrated by the large number of platforms and exchange formats that exist for IoT and IIoT systems today.

This understanding of the bundling of competencies and requirements has shaped the cooperation between KUKA and HARTING from a very early stage. Some examples from this partnership show the path from the jointly developed specific solution through to the resulting standard.

Since embarking on cooperation more than 20 years ago, HARTING and KUKA have always created new solutions with a view to market requirements. One example is the constantly increasing EMC requirements which led to special EMC housing designs for connectors, and which have meanwhile become a standard today.

Also in the field of robotics production, it is essential to reduce the installed number of parts so as to keep complexity low and reduce the number of production steps. Here, the two companies worked together and joined forces and took a look at the processes and created a specific component, the so-called multifunctional housing, which optimally combines the connector function and IP67 sealed electronics housing.

This approach is now being offered as a system solutions in various application areas: whether data cabling in the controller, power cabling to the robot itself or solutions which take mechanical requirements into account, such as specific transition elements for a PROFINET infrastructure on axis 3.

SOURCE: KUKA

Han-Yellock connector system on KR AGILUS robot system from KUKA.

Miniaturization trend

In recent years, a major trend for the robotics industry has been an increasing need trend twoard miniaturization. The KR AGILUS robot system, for example, is a new line of compact robotic systems which are specifically designed for use in increasingly flexible production environments.

The requirement for plug-in connections requires fast and intuitive handling, in which the design aspect also plays an important role at the same time.

With Han-Yellock, a new innovative connector system featuring completely new locking technology, a technology solution was found for this new robot series.

Finally, the intensification of cooperation was particularly evident in the extension of the technologies and solutions to all the so-called "lifelines" of an application. In addition to the normal connectivity such as plug connections at the robot base or data interfaces at the transfer points, both upward integrations such as system solutions and products such as switches were used.

Here the demand for flexibility and adaptability to the communication systems used by the customer in automation was relevant. Quality switches became the central communication element, as they were able to process various automation systems in a very open manner.

Thanks to this consistency of the power-data-signal infrastructure on the robot, system designers were able to achieve a holistic approach to three infrastructure elements: customer-oriented, application-neutral and flexible.

SOURCE: KUKA

KUKA KRC 5 control cabinet (left) and KR C5 micro controller with the two new har-motion interfaces (right).

Industry 4.0 developments

In the field of Industry 4.0 developments, both companies again worked on joint solutions at a very early stage. For example, KUKA equipped the I4.0 demonstrator, the "HAII4YOU Factory", with new LBR iiwa type sensor-based robots. The system became the stage for an integrated Industry 4.0 approach for individual and cooperative production systems all the way through to quantity.

Flexibility, miniaturisation and also modularity are highly significant trends that are driving joint developments today. While around the middle of 2000 years, the robot control cabinet was as large as a control cabinet, today's solutions are no larger than a desktop PC. Especially application areas for small robotics call for solutions that are adapted to resources.

In addition to the smaller robot, the controller must also be more compact in the future, as there will hardly be any space envisaged for it. In response to this situation, KUKA launched the KR C5 micro onto the market, which is tailored precisely to these application areas. Connectivity must also adapt in line with these developments.

For this reason, HARTING KUKA is also providing a new solution for this new controller family in the form of the "har-motion connector", which is particularly suitable for use in compact robotics. Adapted both to the power requirements and to the space available, it can be used flexibly for transferring the lifelines of the robot.

Even the larger robots, however, are also subject the miniaturization trend. This is particularly evident in the new KR C5 control system. This system offers customers the option of operating up to three machines on one control cabinet in the same space as a previous control system. A performance adjustment can also be easily and flexibly accommodated by selecting different controllers. This is enabled by a completely new modular and scalable structure of the cabinet system.

A docking solution was developed for this purpose, which makes adaptation to customer requirements very easy: The control systems are inserted into the cabinet like drawers. In order to enable the transfer of the so-called lifelines for such a flexible coupling, a special docking connector solution was developed in close cooperation.

Following the requirements of the protection class applicable in the cabinet and the reduced space conditions, the new Han Board connector proved an optimal solution, allowing for the mechanical plugging necessary for this case. Special mechanical guides, as well as the design structure of the connector solution, ensure the necessary tolerance compensation.

SOURCE: KUKA

Han Board connector system.

Conclusion

Responding to megatrends, long-term partnerships characterised by mutual understanding, detailed application knowledge and a common view of holistic customer benefits will be capable of developing the necessary technologies and concrete new product solutions. The connectivity and infrastructure solutions incorporated in the new KR C5 generation of control cabinets demonstrate this to a particular degree.

Guido Selhorst, Head of Marketing Services, ***HARTING Technology Group.***

Autonomous forklift guided by swarm intelligence

By using swarm intelligence, new forklifts are able to navigate a production facility or warehouse in a truly autonomous fashion. Programming or "teaching" the vehicles is easier, while central software programs including maintenance and updates are rendered obsolete using advanced communications technology.

NEW LINE OF INTELLIGENT GUIDED VEHICLES, operating using swarm intelligence, includes an autonomous, omnidirectional counterbalanced forklift. With this introduction, AGILOX has entered a new area of application: classic intralogistics in inbound/outbound warehousing and storage.

With the "ONE", AGILOX's ultralight, high-efficiency forklift product line, the company is reshaping the concept of AGVs. The fleets operate without a central control system, meaning the vehicles navigate the production facility or warehouse in a truly autonomous fashion.

The compact AGILOX IGVs organize their routes according to the decentralized principles of swarm intelligence, making them much more flexible than traditional AGVs. Additionally, programming or "teaching" the vehicles becomes significantly easier, while central software programs including maintenance, updates, etc. are rendered obsolete—an innovation that lowers operating costs.

AGILOX is also expanding its range of IGVs to include the OCF—an abbreviation for "Omnidirectional Counterbalanced Forklift". While the ONE is equipped with a scissor lift to function as a load handling device (and thus transports the load within the vehicle contour), the OCF is designed according to the principles of the counterbalanced forklift. Hence, it can pick up pallets, lattice boxes, and other load carriers with a maximum weight of 1500 kg (3300 lbs), transport them to the destination, and set them down at a height of up to 1600 mm (63 in).

AGILOX's intelligent and cost-saving IGV concept opens up new application areas. While the ONE vehicles are mainly used for material supply in production, the OCF enables classic intralogistics tasks in incoming and outgoing goods, order picking and storage, as well as in production—provided that the transport is pallet-bound.

Just like the ONE, the OCF uses an omnidirectional drive concept. It can therefore also drive sideways through narrow aisles, turn on the spot, and maneuver in the tightest of spaces. The same lithium-ion (LiFePO4) battery technology ensures short charging and long operating times; just three minutes of charging allows for up to one hour of operating time.

SOURCE: AGILOX

Autonomous counterbalanced forklift navigates factory by using swarm intelligence.

The IGV fleets can be connected to customer software systems (LVR, ERP, WMS, MES) via an open API interface. An optional IO box enables the integration of external infrastructure, such as rolling gates and stationary conveyor systems, in the intelligent control system. An analytics module provides the user with all relevant operating data and KPIs.

Dipl.-Ing. Franz Humer, M.A. Co-Founder and CEO of AGILOX, noted that "the OCF is a logical addition to round out our product portfolio. With it, we open up opportunities in storage and order picking technology, and thus, a large market in which the IGVs can showcase their advantages over both AGVs and man-operated forklifts."

The combined operation of the ONE and OCF in a "swarm" also provides a great advantage. For instance, while the smaller vehicles carry out delivery services to assembly workstations or tend to e-Kanban shelves, the OCF can, using the same control system and WiFi infrastructure, take over pallet transport.

The OCF pilot series has already been successfully tested in Vorchdorf, Austria. Series production will begin shortly, with the first OCFs set to be delivered to customers in the first quarter of 2021.

All of the company's intelligent logistics robots (AGV's, AGC's, AMR's) use "swarm intelligence" to intelligently navigate through warehouses and factories, delivering pallets and totes where they are needed.

All aspects are developed in-house, from mechanical design, electrical engineering, navigation, and related software. This allows for faster reactions to changing requirements and customization depending on the customer's requirements.

Application story by ***Agilox.***

E800 TSN enabled inverter

Mitsubishi Electric: The new E800 compact inverter family offers CC-Link IE TSN connectivity, allowing TCP/IP and inverter control traffic (including safety) to share the same network. This reduces costs, troubleshooting and time to market due to simpler system designs.

Fast, Secure IP Routers

Contemporary Controls: Simplify device commissioning and troubleshooting with Contemporary Controls' IP routers. Easy set-up and advanced features including PAT, NAT, port forwarding and stateful firewall. Gigabit, cellular and secure remote access also available.

Modular all-in-one industrial PCs

Phoenix Contact: With its all-in-one solutions (AIO), Phoenix Contact offers industrial PCs with a completely closed die-cast aluminum housing (IP65), which are ideally suited for modern operating concepts due to their powerful technology, modular extendibility, and integrated PROFIsafe functionality.

Edge computing

WAGO: Edge devices can take over data mining from controllers that require low latency and a high level of determinism. Collected data can be evaluated directly, displayed graphically and made available to the cloud. WAGO introduced two new edge devices that are designed for these applications: the edge controller and the edge computer.

The new Edge Controller (752-8303/8000-0002) utilizes an ARM Cortex-A9 quad-core processor and offers an extensive selection of interfaces including two ETHERNET ports, one CANopen port and two USB ports. It also has a serial interface and four digital inputs/outputs for connecting local devices or sensors. Project design for the Edge Controller can occur in the familiar e!COCKPIT environment, so it fits seamlessly within WAGO's automation solution ecosystem.

The new Edge Computers feature a 1.91 GHz quad-core Atom processor and are equipped with standard Debian Linux. An SSD disk can be installed to expand the existing 64 GByte flash memory for very large data volumes. Despite their extended temperature range from –20°C to +60°C, the edge computers do without a fan and are very compact, simplifying integration. Standard software, such as Node-Red, can be used on all edge devices. These devices communicate via all common protocols, both on the factory floor and with the cloud.

Functional Safety over EtherCAT

Renesas Electronics: An extension of the company's RX Functional Safety solution is complete with the release of a Functional Safety over EtherCAT (FSoE) Application Software Kit, the first software offering that supports functional safety on EtherCAT from a semiconductor manufacturer. This solution for industrial automation applications reduces the complexity of IEC 61508 SIL3 certification, an international standard for functional safety.

New FSoE software is based on the FSoE standard published by the EtherCAT Technology Group. Developers can obtain an FSoE protocol stack in addition to an RX microcontroller (MCU) with functional safety support and the software all in a single package, speeding up the development of industrial equipment incorporating FSoE. This allows the quick implementation of communication functions needed to support functional safety, such as essential alarms indicating danger or emergency stop signals using an RX MCU.

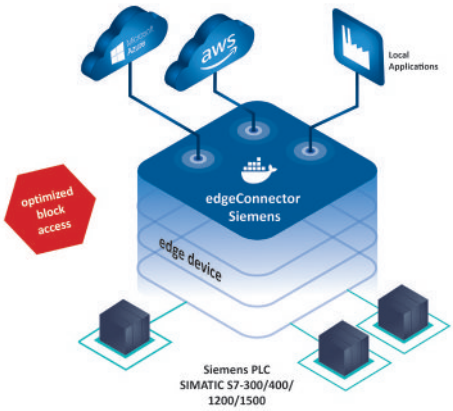
Stepper motor controller and driver

Optimal Engineering Systems: ICAD Series of integrated motion controllers and drivers are now available for two-phase stepper motors.

Available as 1, 2, 3, and 4 axes modules they are designed for NEMA 8 to NEMA 42 stepper motors. These compact 6.000 in. x 8.000 in. plug-and-play, integrated controllers incorporate high resolution micro-stepping drivers for precise positioning.

Other features include home and limit switches per axis, joystick interface, TTL/CMOS inputs and outputs, quadrature encoder feedback, USB and optional Ethernet interfaces permits each module to be customized for specific applications.

Edge controller software module



Softing: A new software module based on container technology connects Siemens controllers with industrial IoT applications. In addition to SIMATIC S7-1200 and S7-1500, the

new version also supports SIMATIC S7-300/400 controllers.

Use of edgeConnector Siemens enables access to S7-1200 and S7-1500 data including optimized data blocks. Version v1.20 additionally supports SIMATIC S7-300/400 controllers. Client applications have access to data via the interoperability standard OPC UA. The product can be configured locally via a built-in web interface, or remotely via a REST interface. It integrates with Azure IoT Edge and AWS IoT Greengrass, and is made available via online repositories such as Docker Hub.

Users benefit from flexible deployment and ease of use which comes with virtualization and container technology.

Low power CPU for PLCs

IDEC Corporation: With the addition three new 12V DC CPUs, the MicroSmart FC6A PLC family now offers users more options for automating battery-backed systems, traffic controls, and mobile equipment.

Many applications require 12V DC power. Smaller smart relays may support too few I/O points and lack enough programmability, while more full-featured PLCs are too expensive and don't provide the necessary I/O voltages. The new 16 I/O FC6A All-in-One CPUs with 12V DC offer the right balance, enabling these PLCs to handle over 100 I/O points in an economical and expandable form factor.

Users can configure and monitor the PLC using the WindEdit app for iOS and Android over Bluetooth and Ethernet. The popular Modbus TCP and RTU industrial protocols are built-in, as are data logging and web server functions.

Rackmount appliance

Lanner: The new NCA-4220 appliance is designed for network traffic security, cloud computing and data centers.

The NCA-4220 features the brand new LGA 1151 socket, up to 32GB of dual-channel DDR4 memory capacity at 2666MHz, comprehensive Intel C246/Q370/H310 series chipset, either eight or six GbE LAN configuration and three pairs of Gen3 bypass. For expansions, the NCA-4220 does come with 1 Ethernet NIC module socket (PCIe*8 default, 2x PCIe*4.

IIoT monitoring and automation

Quantum Automation: New hardware platforms can be used individually or together to enable IIoT monitoring and automation.

The Quantum Remote Telemetry Unit (QRTU) and QSolarBattery provide standardized yet customizable hardware platforms. They are part of a growing array of Q-Line products which are enabling end users and systems integrators (SIs) to deploy industrial internet of things (IIoT) and automation solutions anywhere, regardless of whether internet connectivity or power are readily available.

The QRTU is a complete edge hardware solution for all remote commercial, industrial, and utility/infrastructure data collection and control applications. Numerous options are available to incorporate PLCs from major suppliers such as AutomationDirect, IDEC, and Allen Bradley.

Studio 5000 software updates

Rockwell Automation: A new Simulation Interface tool can transform how users design, test, validate and commission systems using digital engineering. The tool connects a system's real or virtual controller to advanced simulation and modeling tools. Users can then simulate how products or processes with dynamic properties will behave in production.

By virtually designing, proving and adjusting systems, users can realize significant time and cost savings compared to physically building, testing and re-engineering systems. They can also test and push systems in ways that aren't physically or financially feasible in a typical physical design environment.

The Application Code Manager (ACM) tool has also been updated to expand on its existing productivity benefits.

A new document template editor can save users time by automatically generating documentation for their projects. Users only need to create a template and placeholders for data, and ACM will then auto-populate the data when a project is completed.

Edge controller firmware update

Opto 22: Enhancements that are part of the groov EPIC Version 3.0 firmware include central user management, lower-cost licensing, and better remote troubleshooting.

Version 3.0 focuses on enhancing the scalability of industrial internet of things (IIoT) and automation projects. It introduces centralized user management via LDAP (lightweight directory access protocol), the option of lower-cost Ignition Edge licensing, and improved maintenance and troubleshooting capabilities for remote installations.

Rather than defining user access profiles repeatedly for individual network devices—creating potential gaps in security—with LDAP, IT administrators can define permissions once and manage them centrally across an organization.

Digital I/Os for the Raspberry Pi

STV Electronic: A smart digital I/O expansion module is available for its Raspberry Pi 3 B+ based DIN rail PC. The new I/O Module 16, which can be operated remotely from the system via RS-485, provides 4 digital inputs, 4 digital outputs, and 8 flexible interfaces, configurable either as digital input or digital output. The Smart Manager 4.0 can control up

to 8 of these expansion modules via RS-485, making it possible to provide a total of 16 to 128 flexibly configurable digital I/Os. The I/Os are galvanically isolated according to IEC 61131 2 and support up to a maximum of 2,500 Vrms according to DIN VDE V 0884-11:2017 01.

The digital I/Os, which can be controlled conform to IEC 61131-3 using free CoDeSys libraries, are desigmed for digitalization and edge computing applications in mechanical and plant engineering, as well as industrial and building automation solutions in small flush-mounted distribution boxes.

Bluetooth module

u-blox: The NORA-B1 Bluetooth module is the newest member of its short range radio portfolio. Based on Nordic Semiconductor's nRF5340 Bluetooth low energy chipset, it is designed to meet the needs of performance-oriented applications in areas such as industrial, medical, and smart building and smart city markets.

NORA-B1 helps engineers get maximum value out of a single component. Taking advantage of the chipset's dual core MCU, NORA-B1 can handle performance-oriented applications and even drive a display without requiring an external host processer. With one low-power-optimized core dedicated to managing network connectivity and a second high performance core exclusively running the device application, NORA-B1 enables smooth and uninterrupted operation with minimal processing latency.

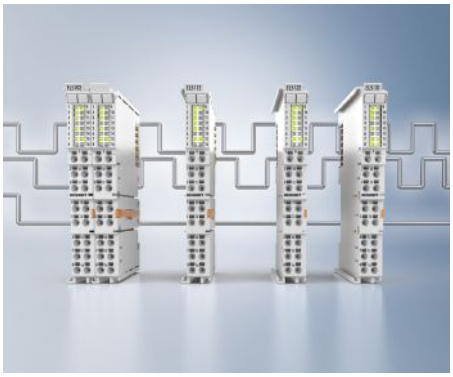
Embedded wireless connectivity

Emerson: New automatic recovery module enables easy valve system commissioning and configuration. New module (ARM) for its AVENTICS G3 electronic fieldbus platform makes it easy for technicians to perform pneumatic valve system commissioning and diagnostics from a mobile phone, tablet or laptop computer.

The wireless ARM module provides easy access to the AVENTICS G3 fieldbus platform's diagnostic and commissioning capabilities via an internal Wi-Fi access point and mobile website even when the valve system is located inside a machine or on a ceiling. It offers the visual benefits of a hard-wired human machine interface (HMI) at lower cost and with higher flexibility.

The module generates error notification for alarms, voltage levels, short circuits, module errors, open load errors and distribution errors to reduce system downtime.

Enhanced signal analysis



Beckhoff: New EL51xx EtherCAT terminals provide built-in incremental signal analysis functionality. Incremental encoders have become indispensable in many applications due to their compactness and low price points. Beckhoff meets this important need with the comprehensive EL51xx series for analysis of 5 V incremental encoders via RS422 and TTL signals. These four new high-performance I/Os feature eXtreme Fast Control (XFC) technology and enable analysis of incremental signals in the controller in a space-saving and cost-effective manner.

The new EtherCAT Terminals acquire incremental signals with high frequencies up to 5 MHz and feature many parameterization options and integrated functions that enable optimum adaptation to control tasks. Each terminal offers an integrated sensor supply, which is parameterizable to 5, 12 or 24 V. Users can easily connect encoders with differential RS422, 5 V TTL or open collector interfaces.

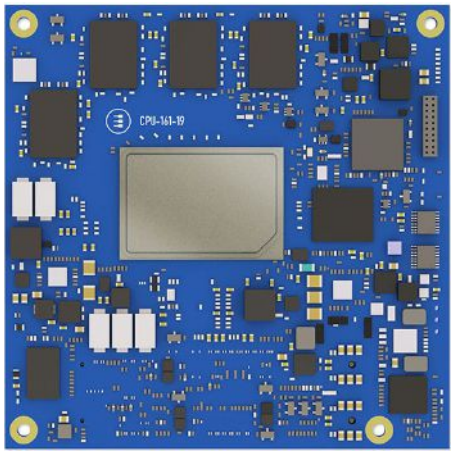
AC Drives

SIGMATEK: An extensive, coordinated motion control system include new AC drives of the FDD 3000 series that compliment the drive portfolio in the low voltage range. Economic asynchronous motors can be precisely controlled with the low-voltage AC drives. The motion application is thereby more efficient and at the same time, saves energy.

The compact units are available in nine sizes. The single- or three-phase AC drives (200/240 VAC or 380/480 VAC) cover a power range of 0.37 to 132 kW.

These units are an effective solution for motion applications that must be cost-effective. In industrial production, a continuously regulatable rotation speed that is adapted to the application enables an optimal manufacturing process. At the same time, energy-efficient operation can be achieved with exact rotation speed control. Functions such as dynamic R/f control or standby mode also minimize energy consumption, which helps reduce operating cost.

COM Express module



Eurotech: Powered by lntel Atom x6000 Series and featuring the COM Express Type 6 Compact standard, the CPU-161-19 enables soft real time and simplifies the development of edge systems.

The CPU-161-19 comes in two variants. One is 100% COM Express Type 6 compliant, and the other has proprietary extensions. The proprietary extensions provide additional features that are mapped on unused pins and delivers a range of novel interfaces that can greatly simplify the design of the carrier board and reduce its cost.

Designed for fanless applications in harsh environments where long term reliability is a must, the CPU-161-19 delivers up to 4 CPU cores and up to 32 graphic execution units and in-band ECC RAM. It features an all-soldered down design to improve resilience and thermal coupling, and comes with a -40 to +85°C operating temperature range.

Security cells against cyber threats

B&R: Security cells provide effective protection against hacker attacks and cyber threats. To achieve maximum protection, the manufacturing system must first be divided into autonomously functioning process cells. These consist of production-relevant zones, sections, sub-areas or subsystems. One or more of these process cells are then combined into security cells. The flexible client/server architecture of APROL allows up to 64 of these security cells.

The advanced multi-runtime server architecture of the APROL process control system ensures that all required systems operate independently. Each multi-runtime server includes its own LDAP server (389 Directory Server) that provides cybersecurity, allowing systems and subsystems within a safety cell to be operated even without an external network connection.

SafeMotion solution

Bosch Rexroth: New scalable system can be used as required, from the drive-integrated SafeMotion solution in ctrlX DRIVE to the complete ctrlX SAFETY control. In addition to the flexible use, the advantages include a very high level of safety thanks to the fastest reaction times and efficient engineering through graphical programming of the safety PLC.

ctrlX SAFETY is based on two components that can be used independently or as an overall system: SafeMotion and SafeLogic. The hardware is extremely compact and, as a safety control, its graphical programming allows the required programs to be created quickly and easily without extensive training. The intuitive engineering interface, a documentation-supported user guidance and ready-made dialogs for the acquisition of acceptance-relevant information enable significantly faster engineering than conventional solutions.

Monitor remote equipment

Red Lion Controls: A next-generation remote access solution meets the most demanding security requirements of modern industrial applications. Red Lion's Secure Remote Access Platform centralizes the management of routers, allowing customers to quickly respond to and act on their most crucial assets from anywhere, at any time.

The ability to remotely access, monitor and manage diverse equipment helps to lower operational costs and downtime by reducing site visits and dramatically improving response times.

To simplify deployment, remote access routers offer Simply.Connect technology. This enables the setup of routers in under two minutes, facilitating small or large deployments using only a smartphone. Once configured, routers can be deployed anywhere, providing real-time, secure, and seamless connectivity to remote assets or sites. The foundation of Red Lion's remote access platform is RLConnect24, a remote service portal that provides a simple centralized site to monitor and manage deployed assets and users.

Faster E-motor production

Siemens: New application for optimally controlling wire tension is designed for linear winding, and minimizes fluctuations in force. The Wire Brake software application for automated winding of rectangular coil former controls the tension of the copper wire. In comparison to passive systems, this enables higher winding speeds and a higher winding quality to be achieved. The functionality can be integrated directly into the machine project using the standard library "Simotion Wire Brake" which shortens engineering and commissioning costs.

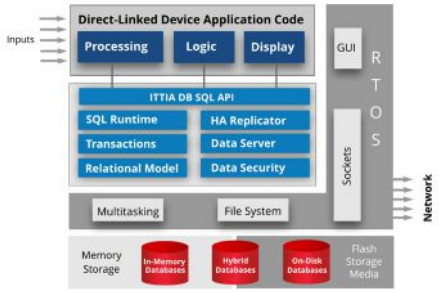
It contains algorithms which include the rectangular geometry of the coil former as well as the "TensionControl" components to control the wire tension brake axis and "CamGeneration" to calculate cams using reference values.

AI-at-the-Edge design tools

Microchip: Cartesiam, Edge Impulse and Motion Gestures have integrated their machine-learning (ML) offerings into Microchip's MPLAB X Development Environment.

Integration will simplify machine learning implementations at the edge by using the company's ARM Cortex based 32-bit micro-controllers and microprocessors, and projects including data gathering, training the models and inference implementation.

Edge data management



ITTIA: DB SQL sotwre tools extend data management automation capabilities to FlexCtrl software, and helps significantly improve system data storage and processing performance.

Automation enables always-on systems to enhance the delivery of goods and provide seamless continuity for maximum profit and productivity. Automation systems generally include sensors and devices that collect, and are required to make sense of, a large quantity of data, then utilize that data to automate and manage industrial processes. Connected sensors are required to understand the collected data as the volume increases exponentially.

In architecting IIoT solutions to collect, store and act, device data management requires new approach. In a continuous effort to accelerate the collection and understanding of a large flow of data, BitCtrl has solutions for the process industry, smart factory and control markets.

Can wearables help the fight against Covid-19?

Whether you want to get physically more active or train for sports, tracking your fitness is going to be easier with a fitness tracker. These wearable devices help you lead a fitter and healthier life, as they easily track your fitness level, and they might even add protection against Covid-19.

"FITNESS TRACKERS ARE A GREAT tool for your heart health," says Johns Hopkins cardiologist Seth Martin. Recent research suggests that these wearables can do even more. A paper published in Nature Medicine reports that fitness trackers are capable of identifying cases of COVID-19 by evaluating changes in heart rate, sleep and activity levels. This approach may identify cases with greater success than looking at symptoms alone.

Good reasons to wear a fitness tracker, but which device is right for you? It depends on what you are looking for.

In-depth metrics

PICTURE: GARMIN

The Garmin Vivoactive 3 packs a surprising number of features into a compact timepiece.

It includes fitness monitoring, such as VO2 max and fitness age estimate, as well as all-day stress tracking and relaxation-based breathing timer. Sports apps include yoga, cardio, strength training, running, swimming and many more.

Using the Garmin Connect app, you can even enable Abnormal Heart Rate Alerts, so it will notify you if your heart rate is unusually high or low.

The Vivoactive features a color touch screen with a durable Corning Gorilla Glass cover, a fiber-reinforced polymer case, a stainless steel bezel, and is rated 5ATM for water resistance.

www.garmin.com

Tracker/smartwatch hybrid

The Fitbit Versa 3 offers more smartwatch features than any other fitness tracker. It has a built-in microphone and support for Google Assistant and Amazon Alexa, so you can use voice control to set alarms, ask questions, or check the weather forecast. In addition to this smartwatch functionality, the Versa 3 offers the usual fitness features, such as activity and sleep tracking, heart-rate monitoring, and automatic workout detection. It also offers integrated GPS for distance tracking and a blood oxygen sensor.

www.fitbit.com

Smartphone integration

The Samsung Galaxy Fit is a sleek tracker wristband with an easy-to-use interface and a long battery life. The 240 by 120 pixels color AMOLED display is large enough to show multiple stats at once.

PICTURE: SAMSUNG

It accurately measures workouts, heart rate, and sleep. You pair the tracker to your phone via Bluetooth with the dedicated Galaxy Fit app. You can also connect it with the Samsung Health app, which will then show a variety of different metrics including fitness goals, steps, heart rate, weight, and more on its dashboard.

www.samsung.com

Win a Samsung Galaxy Fit

The Samsung Galaxy Fit is a fitness tracker with always-on, full-color display, swim-ready design and military-grade durability

For a chance to win one, enter our contest at:
www.iebmedia.com/quiz
The winner will be announced December 20.

Contest sponsored by:

CC-Link CLPA PARTNER ASSOCIATION
OPEN AUTOMATION NETWORKS
CC-Link IE TSN

CC-Link Partner Association (CLPA) – Europe
https://eu.cc-link.org/

Function meets elegance

The Withings Steel HR is different in that it combines smartwatch features with the classic look of an analog watch. It has a round face with hour marks around the edges, two hands, and a button on the side.

PICTURE: WHITHINGS

Inside this housing it packs a heart rate infrared sensor, motion sensor, and a three-axis accelerometer. The Steel HR doesn't have its own GPS, but connects to your phone to tell the distance you've gone. The watch automatically recognizes and records certain workout types, and you can manually select 30 more exercises. In the companion smartphone app you can get a post-workout summary, showing a map of your activities and heart rate zones.

www.withings.com

Leopold Ploner