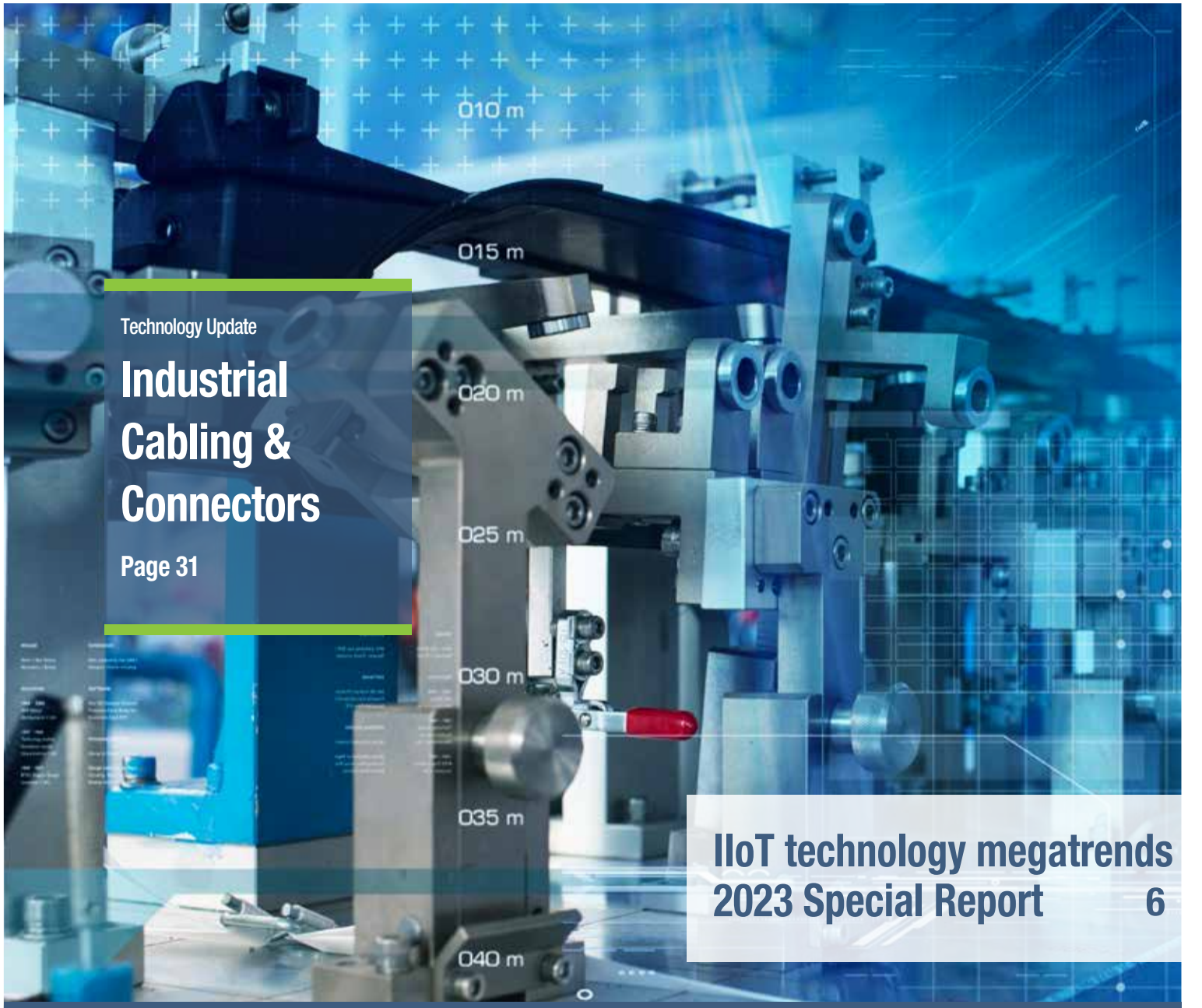
January/February 2023 134
ISSN 1470-5745

industrial ethernet book

Industrial Ethernet Automation Networking & IIoT



Technology Update

Industrial Cabling & Connectors

Page 31

IIoT technology megatrends 2023 Special Report 6

groov RIO

Remote, Ethernet I/O with built-in OPC UA Server

Another first from Opto 22!
A universal Ethernet I/O module with an embedded OPC UA server. Now connect your favorite OPC UA-compatible SCADA or HMI software directly to your multi-signal, multifunction Ethernet I/O system. Easy-peasy!

Learn more and watch a video at:
op22.co/groovrio-opcua

OPC UA

MADE IN THE USA

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

OPTO 22
Your Edge in Automation.™

GET CONNECTED…

Visit our new website at: www.iebmedia.com

IIoT Insights from AWS

Industrial IoT solutions have not emerged as fast as many were predicting but we are still on the path. I can remember attending a press dinner at the Hannover Messe more than 10 years ago, listening to the CEO of Siemens providing insights into this fourth industrial "revolution".

It was easy at that point to assume that the pace of innovation would be brisker and the key would be effective data collection (which didn't seem revolutionary at the time) resulting in "actionable insights" (a much bigger goal).

One way to gauge the success of any market segment is to learn about the leaders in the field, so I decided to visit the Amazon in Manufacturing website to see what this market leader has been doing in the area of IIoT solutions. I would invite you to do the same: https://aws.amazon.com/iot/solutions/industrial-iot/

The result is what I consider an outline and overview of where the IIoT is making inroads when it comes to use cases, applications focus and IIoT software services aimed at industrial and manufacturing needs.

Use cases highlighted focus on three areas with massive potential for smart manufacturing: Predictive Quality, Asset Condition Monitoring and Predictive Maintenance. All of them focus on capturing IoT data and extracting actionable insights from industrial data sources such as manufacturing equipment, environmental conditions, and human observations to optimize the quality of factory output.

A group of case studies provides insights into major customer successes.

- Volkswagen Group uses AWS IoT to increase plant efficiency and uptime, improve production flexibility, and increase vehicle quality.
- Pentair uses AWS IoT to improve beer filtration processes and boost performance by 10%.
- Woodside Energy leverages AWS IoT to expedite delivery of new analytics algorithms from 3-6 months to a matter of weeks and sometimes even days.
- Deutsche Bahn uses AWS IoT to gain new insights to achieve operational efficiency for their rail fleet.

And finally, the breadth of available IoT Services for Industrial Applications spans as one might suspect across areas including Data Management, Device Connectivity and Control – along with Analytics and Event Detection.

The IIoT is here to stay; there is no doubt about that. But it will be interesting to see how the next ten years plays out in terms of new solutions for smart manufacturing.

Al Presher

Contents

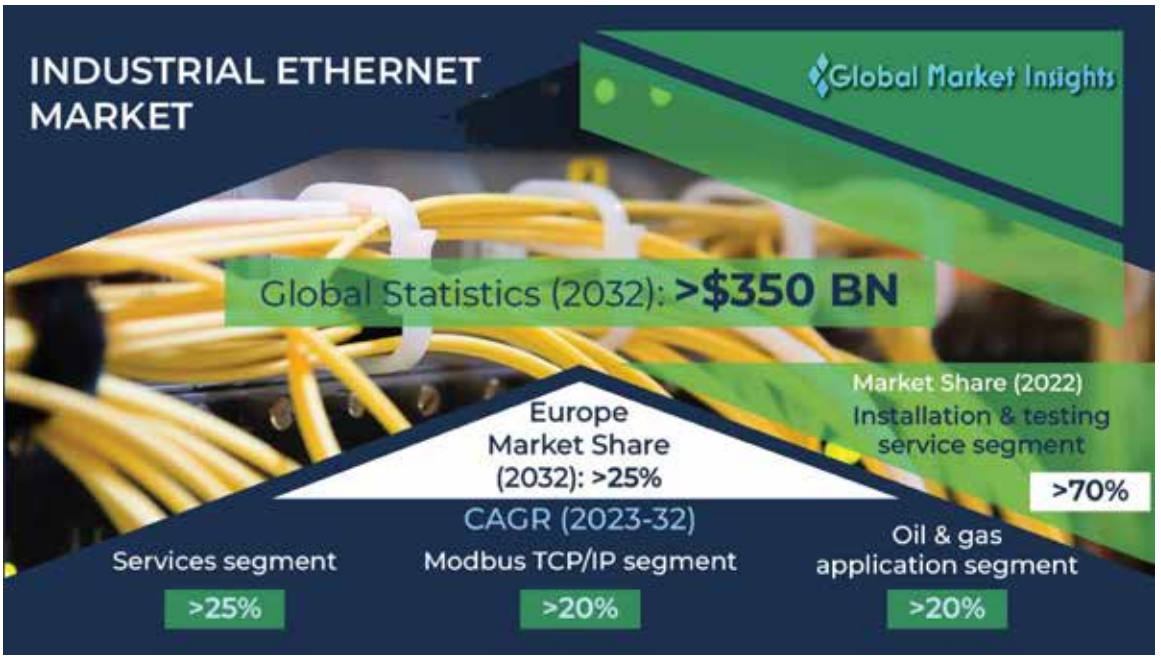
Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2023.**
Deadline for editorial: March 14, 2023 **Advertising deadline:** March 14, 2023

Editor: Al Presher, editor@iebmedia.com
Advertising: info@iebmedia.com
Tel.: +1 585-598-4768
Free Subscription: iebmedia.com/subscribe
Published by IEB Media Corp., Box 1221, Fairport, NY, 14450 USA ISSN 1470-5745

Industrial Ethernet market to cross $350 Billion USD by 2032

The Industrial Ethernet market is expected to amass substantial gains in the next decade, in part due to the emergence of 5G technology across global industries.



SOURCE: GLOBAL MARKET INSIGHTS

The Industrial Ethernet maintenance service segment is foreseen to expand at over 30% CAGR between 2023-2032 as Ethernet services aid firms in reducing failures that occur due to maintenance issues such as cable failures.

INDUSTRIAL ETHERNET as a marketplace is set to grow from its current market value of more than $50 billion to over $350 billion by 2032, as reported in the latest study by Global Market Insights, Inc.

The Industrial Ethernet market is speculated to amass substantial gains by 2032 owing to the emergence of 5G technology across global industries. In addition, the burgeoning demand for industry 4.0 and automation in the manufacturing industry, along with the surging awareness regarding economic industrial solutions, is likely to propel the market growth over the forecast period.

The COVID-19 pandemic created exponential opportunities for the industrial ethernet industry as many firms witnessed a shift in working trends and adopted advanced automation solutions. Industrial Ethernet emerged as an efficient choice for implementing an Industry 4.0 approach throughout the industrial segments.

For instance, the food and beverage industry witnessed a lag in connectivity during the pandemic due to food contamination concerns. Later, the FDA clearance on guidelines related to installing industrial switches encouraged many F&B industry players to implement industrial ethernet switches.

Moreover, the major players in the industry have been focusing on rigorous R&D initiatives to enhance their business outreach, thereby fostering overall market dynamics. For instance, in July 2022, Ethernet Alliance, a global ethernet consortium, approved the UL Solutions for Ethernet Alliance Gen 2 Power over Ethernet Certification Testing in Taiwan, extending new features to manufacturers. This certification makes products safer, secure, and sustainable.

The Industrial Ethernet market has also become bifurcated based on component, protocol, application, and region.

Segment breakdown

Based on component, the industrial ethernet market has been divided into hardware, software, and service. The services segment has been further classified into integration & testing service and maintenance service.

The Industrial Ethernet maintenance service segment is foreseen to expand at over 30% CAGR between 2023-2032 as Ethernet services aid firms in reducing failures that occurred due to cable breakdowns. The surging use of predictive maintenance in Industrial Ethernet applications aids in receiving a failure analysis through Industry 4.0 equipped networks, enabling the failed cable to be replaced.

With respect to protocol, the Industrial Ethernet market has been classified into Ethernet TCP/IP, gigabit, PROFINET, EtherCAT, Ethernet/IP, Modbus TCP/IP, Powerlink, Sercos III, and HSE.

Ethernet TCP/IP held over 40% market share in 2022 due to the mounting popularity of Ethernet TCP/IP protocol to manage the connection between automated devices & technologies such as CNCs, PLCs, sensors, robots, and other industrial equipment.

On the basis of application, the Industrial Ethernet market has been classified into aerospace & defense, oil & gas, electrical & electronics, energy & power, automotive & transport, chemical, and others. The electrical & electronics segment amassed over 20% of the market share in 2022 as a result of technological advancements in electrical and electronic products. Furthermore, electronics products such as routers, firewalls, gateways, hubs, and switches enable the implementation of Industrial Ethernet, helping to drive segment growth.

In the regional context, the Latin America Industrial Ethernet market is poised to showcase over 15% CAGR through 2032. The government initiatives towards improving and expanding power generation capacity and transmission infrastructure are contributing to market growth in the LATAM region. Also, swelling demand for setting up renewable energy generation plants in the region is anticipated to encourage power cable installations over the next 10 years.

*News report by **Global Market Insights**.*

Visit Website

Vision: Complete and system-integrated

- industry-standard, real-time image processing solution complete with integrated software and hardware
- full synchronization with all EtherCAT-based machine processes
- reduced wiring work thanks to the EtherCAT P single-cable solution
- cameras with 2.5 Gbit/s for rapid image transfer
- C-mount lenses with assembly-oriented design
- future-proof lenses designed with 2 µm pixel structure
- correction of chromatic aberration into the near-infrared range
- wide range of EtherCAT-compatible, precisely synchronizable, multicolor LED illumination options
- maximum flexibility afforded by image contrast adjustment during runtime and high pulse power
- Vision Unit Illuminated is a compact unit comprising of a camera, illumination, and focusable optics

Scan to learn more about Beckhoff Vision

New Automation Technology **BECKHOFF**

IIoT technology megatrends: 2023 special report

Industry experts provide their perspective on the megatrends and technology shaping the Industrial Internet of Things (IIoT). Automation and control system manufacturers are leveraging IT tools and security solutions, and focusing on edge computing to increase the scalability and manageability of IIoT solutions.

SOURCE: ISTOCKPHOTO

"IIoT is evolving but it has not seen the quantum leap that many predicted. Instead, it has taken a decade to become mainstream because automation users are conservative about change, particularly concerning security." -- Phil Marshall, CEO at Hilscher North America.

IIOT TECHNOLOGY IS MOVING AHEAD WITH new solutions for smart manufacturing, even if it hasn't been fulfilling the loftiest predictions of explosive growth.

In this special report, the Industrial Ethernet Book reached out to industry experts to gain their insights into the technology megatrends driving IIoT networking, new applications and the challenges for automation engineers.

IIoT data & security

Focus on quality communications utilizing MQTT and OPC UA technologies.

According to Phil Marshall, CEO at Hilscher North America, the Industrial Internet of Things (IIoT) requires quality communications, making both message queuing telemetry support (MQTT) and Open Platform Communications Unified Architecture™ (OPC UA) key technologies.

"These technologies enable future IIoT developments and allow other technology solutions to work. MQTT is a communications protocol with very low overhead, which makes transferring massive amounts of information into cloud-based systems manageable. OPC UA is a universal way to exchange data between systems, supporting that flexibility on a system-to-system basis," Marshall told IEB recently.

Marshall said that MQTT and OPC UA must also go hand in hand with security. Cybercriminals will continuously find attack vectors and so to block threats, a collective effort is required. This means that embedded, layered security spanning every link in the communications chain — from the component manufacturer to the end user — is essential. This is where IEC 62443 comes in. With over 30 years of communications experience, Hilscher has long-supported security through products such as its netX 90 communications controller.

netX 90 technology

Hilscher's netX 90 technology enables security functions to be embedded into automation products, and protects CPU activity with "root of trust" techniques and isolates communications from applications to ensure that neither can be affected by the other. Its successors will be similarly enabled in order to match network security requirements as they evolve. The company recently announced that the netX 90 supports Common Industrial Protocol™ (CIP) Security, an important next step for North American automation vendors.

Hilscher recently announced the netX 90 supports Common Industrial Protocol (CIP) Security.

"IIoT is evolving but it has not seen the quantum leap that many predicted. Instead, it has taken a decade to become mainstream because automation users are conservative about change, particularly concerning security," Marshall said. "In addition to that hesitation, early IIoT implementations were cumbersome and extremely expensive. These issues led many users, such as small machine builders, to be disinclined with their involvement. Today, powerful IIoT solutions are both far less expensive and far more flexible."

He added that the reality is that automation users have always pushed for better and more effective ways to operate and manage assets. Today, they recognize that they cannot compete unless they start offering IIoT features with their equipment. The latest products on the market today offer plenty of opportunity to deploy cost-effective solutions in innovative ways."

Challenges for smart manufacturers

Marshall said that, as of now, IIoT spans the entire manufacturing hierarchy. At the highest levels, global interaction of systems allows companies to manage their enterprises better and more effectively across global markets. And at the lowest levels, processing the data

HARTING

Pushing Performance
Since 1945

INDUSTRIAL ETHERNET.WEEK

VISIONS OF IIOT AND SENSOR2CLOUD

With contributors from

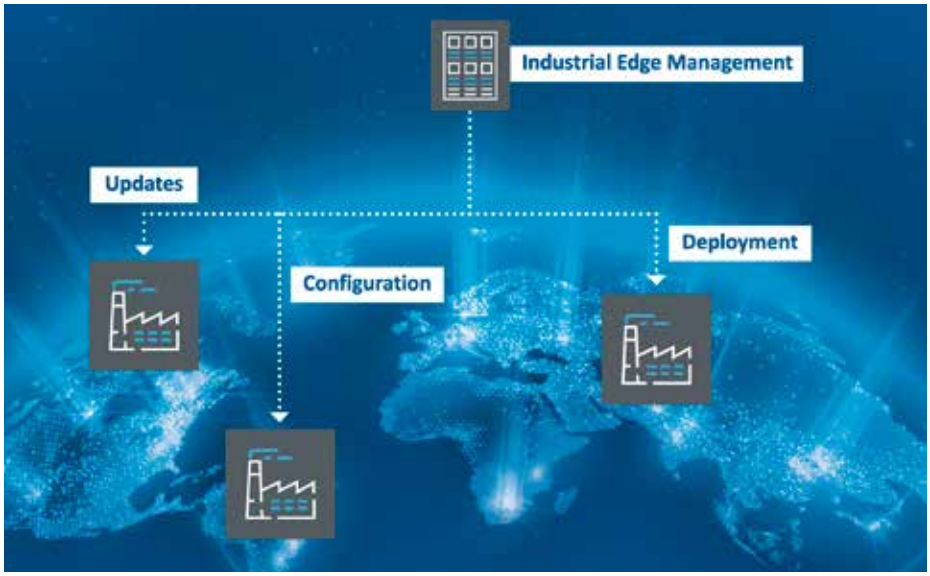
SCHAEFFLER · Microsoft · IOT USE CASE · FLUKE networks · EPLAN · ANALOG DEVICES · sparkfun ELECTRONICS · Supplyframe · BECKHOFF

Digital event

FEBRUARY 21 - 23, 2023

Live broadcast from the HARTING Forum

Register now



SOURCE: SOFTING

"Edge computing in combination with machine connectivity enables applications to work with relevant (and possibly a huge amount of) machine data, and with low latency. This is a precondition for many innovative algorithms and applications, such machine learning and predictive maintenance." -- Dr. Christopher Anhalt, VP Product Marketing, Softing Industrial Automation.

from sensors mounted on machines can help manage equipment more efficiently and send this data to where it can most effectively be used — locally or globally.

"Gathering sensor-level data via smart IO-Link modules delivers continuous access to machine condition and performance. From a performance perspective, this opens up exciting opportunities to improve processes such as enhancing work flows, increasing product quality and boosting manufacturing flexibility," he said. "Better monitoring can also uncover potential failure mechanisms that may be addressed before the failures cause downtime. Additionally, the "digital twin" version of a machine becomes a reality, enabling off-line diagnosis, process improvement and system design."

These technologies also allow vendors to monitor their machines from anywhere in the world. This presents new business opportunities because vendors can take greater responsibility for their equipment, wherever it may be. Machine rental, rather than purchase, becomes an option that is paid for on a per-use basis — which is an attractive option as staffing levels decrease and skills and experience are lost. Machine providers can also support continuous quality improvement and online upgrades.

Looking ahead

Given that the IIoT is already more than ten years in the making, his assessment of the progress and overall impact of the IIoT on industrial automation and smart manufacturing is that it is a work in progress.

"So far, IIoT has moved forward at a pace that I would expect. But now, I see it accelerating as the possible added value of new solutions become clearer," Marshall said. "For a product vendor like ourselves it offers exciting new opportunities too. Our netX family, especially the netX 90 system on a chip (SoC), has become the foundation of a new range of Hilscher IIoT solutions called netFIELD."

He added that 30 years of communications experience plus the security offered by netX allows Hilscher to broaden its product range to include a variety of processing solutions that deliver fast results at the point of greatest need. These can be edge or cloud-based solutions and they are suitable for virtually any class of user. Furthermore, all of this can be delivered at a far lower cost than before.

In effect, products like netX and netFIELD are typical of a new generation of IIoT solutions that are less costly, more versatile and easier to deploy. And, these solutions operate without compromising performance or security. Huge IT infrastructure is no longer needed to implement IIoT since solutions can now be tailored to exact needs and budgets. Fewer IT skills are required, existing software can often be reused, and users can focus on what they know best – their own processes – by utilizing solutions that are user-friendly and less expensive than any previous offering.

Development of IIoT applications

Marshall said that semiconductor developments will continue to drive IIoT forward as always. "Solutions will become better and more secure while added value will continue to grow as users become more and more familiar with the options. It is certain that with the type of scalable and cost-effective IIoT solutions on the market now, users will become smarter in the ways they utilize the features. Innovation will play its usual role and the manufacturing world is likely to find plenty of new opportunities to exploit," he concluded.

Edge computing

Adoption of standard IT tools and edge computing increases scalability and manageability of IIoT solutions.

Dr. Christopher Anhalt, VP Product Marketing for Softing Industrial Automation, said that one of the technology megatrends that will be shaping and enabling development of the IIoT in 2023 is edge computing, i.e. a system of computing nodes which reside near machines and devices on the shopfloor, and which can be managed centrally.

"Edge computing in an industrial context is increasingly based on standard IT technologies and tools. Customers use edge computing in combination with cloud, but limit or eliminate cloud-vendor lock-in," Dr. Anhalt said. "Key technologies are Docker container, Kubernetes based management platforms, and the communication protocols MQTT and Kafka. Machine- and device connectivity can be implemented based on these technologies, and fully integrated into edge computing."

Technology benefits

Edge computing provides specific technical benefits that will enable new IIoT application successes, versus what is possible with typical applications today.

Anhalt said that edge computing in combination with machine connectivity enables applications to work with relevant (and possibly a huge amount of) machine data, and with low latency. This is a precondition for many innovative algorithms and applications, such machine learning and predictive maintenance.

"The integration with cloud platforms means that relevant data can also be made available to surrounding business processes, for example improving energy efficiency of production sites," he said. "And the increasing adoption of standard IT and central platforms for operation means that these systems can managed efficiently by personnel with standard IT skills, and that the solution scales more easily."

Looking to the future

Anhalt added that the adoption of IIoT at scale has probably been slower than most people in the industry expected ten years ago. Reasons include organizational challenges, the different speed of innovation cycles in IT- and traditional automation industries, and sometimes difficult ROI estimates which imply a "start-small-and-grow-as-you-learn-more" approach. On the other hand, the pressure to operate production sites more flexibly, more efficiently and in sustainable way is only

increasing, and the IIoT can obviously help to address these challenges.

"On a technology level, the adoption of standard IT and edge computing will increase scalability and manageability of IIoT solutions. Top level management attention is required to overcome organizational challenges, and to change business processes as needed to take full advantage of the IIoT," he concluded.

Effective network management

Harmonizing data semantics and secure communication between IT and OT networks.

According to a joint statement by Dr. Frank Possel-Dölken, Chief Digital Officer and Member of the Group Executive Board and Dr. Christoph Kelzenberg, Director Digital Innovations, for Phoenix Contact, cyber crime currently poses the greatest threat to manufacturing companies in terms of IIoT.

"The barriers to entry for cyber criminals are low because factories contain a variety of network-enabled devices from different manufacturers. There is little holistic overview in terms of asset management; furthermore, there is no assurance that all security vulnerabilities have been addressed through software updates. Besides the lack of knowledge regarding assets, the common process of update and patch management does not master the threat not in the least," Possel-Dölken stated.

"It goes like this: go to web page of device manufacturer, search device via article number, check notification for bug fixes and software updates, download software and patch the device, make sure the device works properly – that needs to be executed for each and every device at least once a day! This is neither practical nor manageable. The options for hackers to access factory networks are numerous – at every industrial enterprise," Kelzenberg added.

Managing network-enabled devices

Thus, one major topic of IIoT in 2023 and beyond will be finding solutions for a scalable, automated and fast update and patch management of network-enabled devices. The basis for this solution is seamless and barrier-free data logistics between different industrial companies and their software systems. The Asset Administration Shell (AAS) as a standardized technology for developing digital twins plays an essential role.

Additional areas of focus are specific technical benefits that new technologies can provide that will enable new IIoT application successes, versus what is possible with typical applications today.

The goal is that through seamless and barrier-free data logistics, the current process of data transmission – which requires high amounts of time and money, and a lot of resources – will be revolutionized! Now, establishing new data connections requires more than generation costs of almost zero! (In business administration and economics, "generation costs" refers to the costs generated by the production of one additional unit.) For data transmission from one system to another, the data needs to be unpacked, checked, reorganized, and packed again – in fact, before it is even sent and also after it has been received. This process includes many activities and thus is extremely prone to errors. Consequently, comprehensive testing is necessary to ensure operability.

SOURCE: ISTOCKPHOTO

"One major topic of IIoT in 2023 and beyond will be finding solutions for a scalable, automated and fast update and patch management of network-enabled devices. The basis for this solution is seamless and barrier-free data logistics between different industrial companies and their software systems. -- Dr. Frank Possel-Dölken, Chief Digital Officer and Member of the Group Executive Board and Dr. Christoph Kelzenberg, Director Digital Innovations, Phoenix Contact.

"The big advantage of the Asset Administration Shell: it is standardized! The AAS operates as a standardized data container and enables the standardized data transmission via common sub models, structure and security requirements." Possel-Dölken and Kelzenberg said.

"The chances that AAS is becoming at least one or even the standard for digital twins is high as a big consortium of international key players – under the umbrella of the Industrial Digital Twin Association (IDTA) – are continuously working on the development of the AAS and its implementation with their internal processes."

Challenges for automation and control engineers

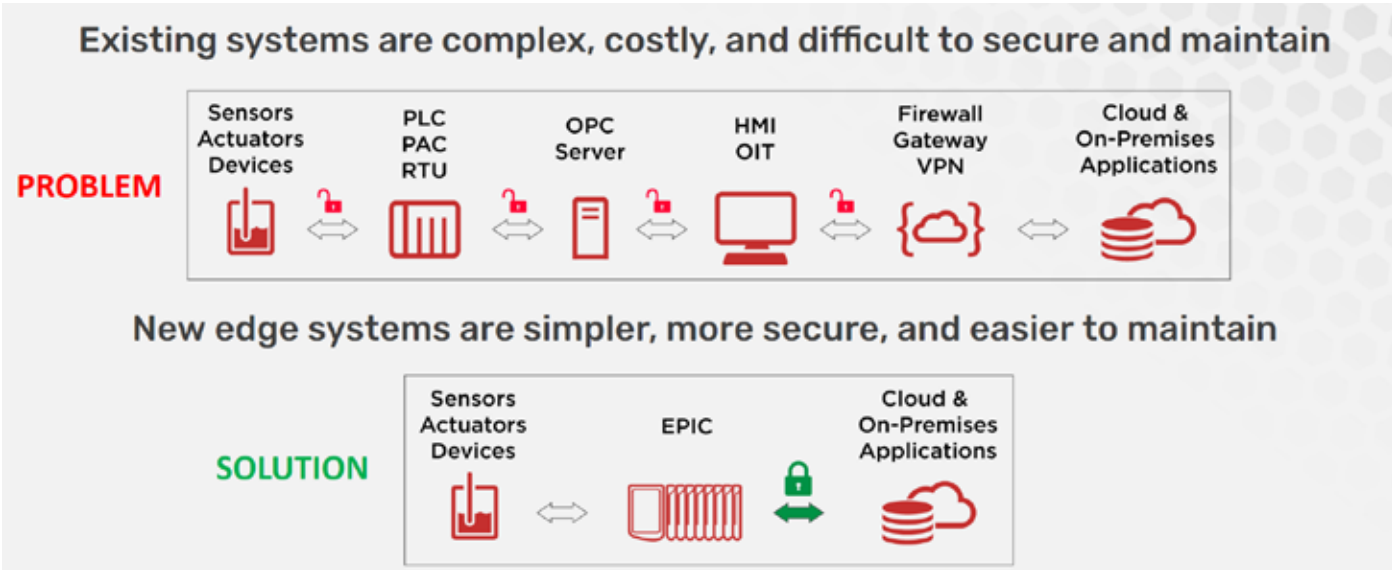
The topics/technologies mentioned before address the currently missing interoperability of software systems within one company as well as between different companies. The consistency of data is not only required from customers (e.g. digital twin of products with regards of traceability), it is furthermore required by law (e.g. burden of proof for raw materials and components alongside the entire supply chain – supply chain act in Germany).

One exemplary benefit for customers of automation and equipment industry: the end customer receives an "As-Is" bill of material! Currently, the end customer receives an "As-Built" bill of material – but this is not the exact (digital) representation of the physical good! Why is that? Alongside the different value creation steps – for example of a cabinet – different entities add, configure and adjust components.

They do parameter adjustments, apply software updates and execute other customizations that the customer does not know about – because he receives the "As-Built" bill of material. While consistently using the Asset Administration Shell among other technologies – for example saving the configuration of a power supply within a cabinet – the "real" digital twin of the physical good is developed along the different value creation steps and displayed within the "As-Is" bill of material.

Overall IIoT impact

"With regards to IIoT, we often hear statements like 'data is the modern oil'. However, the 'new oil boom' has so far failed to materialize – looking through economic statistics for evidence of the predicted efficiency or productivity potentials seems to be in vain," Possel-Dölken and Kelzenberg said. "All in all, the progress and the impact of IIoT is way lower than expected. The reasons behind have been illustrated in the questions before – it is because the current processes for data transmission within one and between



SOURCE: OPTO 22

"The most important new tools are cybersecurity features that resemble those of a Linux computer, server, or IT system. Built-in cybersecurity features are vital for IIoT applications to scale in 2023." -- Arun Sinha, engineer, Opto 22.

several companies are very time-consuming and costly."

They added that developments in freight logistics – especially the introduction and establishment of the standardized ISO container that led to tectonic changes within the global economy – are an excellent analogy for the current situation in data logistics. They should serve as an inspiration to us when it comes to Industry 4.0 – because they have allowed the costs of global freight transportation to either decrease significantly or even become negligibly small. This holds true equally for the standardization of goods transport itself (in the form of containers, load carriers) and for the many year's process of developing the standards through the participation of various entities (such as ports, shipping companies, freight forwarders, etc.).

Key next steps and/or technologies are important to enable rapid development of IIoT applications. Possel-Dölken and Kelzenberg said that, as stated before, industrial enterprises are well advised to participate in the development and usage of the Asset Administration Shell for efficient data logistics and digital twins. A close collaboration between the Industrial Digital Twin Association and its members is highly recommended. Development and use of this standardized technology especially facilitates projects and activities with other industrial enterprises (that use the Asset Administration Shell).

They added one last remark to the development of industry-wide use of IIoT applications and solutions:

"With regards to completed and current (research) activities in the field of IIoT, we often see that highly complex use cases are addressed. These use cases will always be use cases and not real cases – because they usually do not solve day-to-day problems in industrial enterprises!"

"Our advice is to focus on solving those day-to-day problems – as "easy" as they seem. If you take a closer look and speak to other companies, you will immediately see that (standardized) solutions for the majority of these so-called 'low hanging fruits' do not exist…so please start with simple cases that could run within a year and directly raises the efficiency within your own processes. This approach will furthermore contribute to scalable solutions and industry-wide roll-outs."

Leverage IT tools & security

Automation and control system manufacturers leverage IT tools and security solutions.

Arun Sinha, an engineer at Opto 22, told IEB that a key technology trend that will enable IIoT development is the new IT functionality that automation and control system manufacturers are adding into their products, including new tools and applications onboard the controller itself.

"The most important new tools are cybersecurity features that resemble those of a Linux computer, server, or IT system. Built-in cybersecurity features are vital for IIoT applications to scale in 2023," Sinha said.

"Onboard applications beyond PLC programming that facilitate edge computing will shape the future of IIoT, too. Examples include higher-level programming languages, secure access to the operating system to run custom or third-party applications, and even open-source tools geared towards IIoT, like Node-RED."

In addition, automation platforms will support next-generation communication methods. A fundamental premise of IIoT is for OT data to be shared with IT systems easily and securely. Forward-thinking automation vendors will directly support APIs, MQTT, SparkplugB, JSON, and OPC. This trend will continue as additional PLC manufacturers come on board with these IIoT-enabling technologies.

IIoT successes versus typical applications today

Sinha said that traditional PLCs have been the workhorses for industrial automation applications since the early 1980s, playing an essential role in what we now call Industry 3.0. The technology advanced incrementally with modular I/O replacing fixed I/O, increased processor memory and speed, and serial communications. A paradigm shift occurred (albeit gradually at first) with the implementation of Ethernet and TCP/IP as a control network on board PLCs in the late 1990s, which paved the way for where the industry is today—poised for Industry 4.0, digital transformation, and IIoT.

Typical PLCs today are still purpose-built for traditional plant-level and machine control. Edge computing, data cleansing, and interfacing with higher-level software and IT systems often require protocol translation, middleware, or custom code. Next-generation automation platforms and communication methods will enable IIoT success by being more like a smartphone, with apps installed to do the required tasks.

"You pick the app or software you need based on the task you want to perform, and that choice is based on how familiar you are with a given app or the app's suitability for the given task," Sinha said.

He added that, as automation and control engineers set out to address their applications and projects in IIoT, they typically end up with a mixed bag of technologies stitched together to achieve the desired result. With

this patchwork of components, engineers have to deal with multiple vendors, software licensing, Windows updates, IT integration, cloud connectivity, and much more. Over time, these systems become brittle, complex, expensive, and difficult to maintain. This approach not only presents scalability problems, but also the often overlooked side-effect of cybersecurity issues. There are too many security vulnerabilities and so-called "attack vectors" between these components.

New automation products like Opto 22's groov EPIC (Edge Programmable Industrial Controller) combine the functionality of a PLC, cyber-secure edge computer, communications gateway, and HMI into one platform. This technology helps reduce or eliminate extraneous pieces, parts, and components while adding security to build maintainable IIoT applications over the long term.

IIoT progress report

According to Sinha, significant progress has been made in IIoT for industrial automation and smart manufacturing. Perhaps most importantly, OT/IT convergence is an accepted idea. Most stakeholders on both sides in large and small organizations are less resistant to working together than they were a decade ago. Engineers from both disciplines realize that IIoT, smart manufacturing, Industry 4.0, and digital transformation initiatives fundamentally require a confluence of people, strategy, and technology. Regarding technology, a few automation vendors have released new platforms that are more IT and IIoT friendly, and others are sure to follow suit. As a result, OT systems using these platforms are already sharing data with IT systems much more easily.

"Future IIoT progress will depend on how this newly democratized OT data is used effectively for business outcomes such as efficiency improvements, quality, cost reduction, and sustainability," he said. "The challenge of unlocking siloed process, plant floor, and machine data—and securely sharing it with IT systems and software quickly and inexpensively—has largely been solved. But the tangible examples (in the public domain) of how this data has generated positive business outcomes have just started to emerge. These will be exciting to watch."

Sinha said that one key technology that will enable IIoT to help reach its full potential is artificial intelligence and its subset, machine learning. The promise of the IIoT is ultimately to use OT data to achieve positive business outcomes. A lot is being written about ML and AI in the automation sector, often in the context of predictive maintenance—yet at this time there aren't a lot of tangible examples of it in practice. For case studies and tech notes that are publicly available, most present the results but not the mechanics of how they were achieved.

"ML has challenges in the industrial and manufacturing space. Process, plant, and machine data is not homogeneous like data in banking or even healthcare might be. Every process, manufacturing line, and machine is different and more importantly, requires domain expertise from someone with hands-on experience to train the models," Sinha said.

"I am concerned that we may be approaching a "trough of disillusionment" for IIoT if this is not somehow addressed. The key next step is to find ways to approach these challenges with ML and AI in the manufacturing space, enabling more rapid development of IIoT applications and helping them deliver actual value to the operation or business."

Focus on IT/OT harmonization

Harmonizing data semantics and secure communication between IT and OT networks.

Raymond Kok, Senior Vice President, Cloud Application Solutions for Siemens Digital Industries Software said technology and software solutions are poised to continue the pace of IIoT innovation 2023.

"We see the convergence of information

SOURCE: ISTOCKPHOTO

"We see the convergence of information technology (IT) and operational technology (OT) being a decisive factor: combining the field and automation level of production with the enterprise and management level – as seamless and complete as possible. Harmonizing data semantics and secure communication between IT and OT networks is key." -- Raymond Kok, Senior Vice President, Cloud Application Solutions, Siemens Digital Industries Software.

technology (IT) and operational technology (OT) being a decisive factor: combining the field and automation level of production with the enterprise and management level – as seamless and complete as possible. Harmonizing data semantics and secure communication between IT and OT networks is key," Kok told IEB recently.

Kok said that another trend that is increasing is low-coding.

"Rather than using codeful customization, low-code enables model-driven, drag-and-drop UI and application development. All development skill levels — professional developers, novice developers, subject matter experts, business stakeholders, and decision makers — can use low-code to build value-driven IT and OT end user applications. Consequently, application development is more accessible to users without deep software development expertise," he added.

He also added that, last but not least, AI applications that e.g. enhance quality assurance or predict and optimize scheduling service and maintenance windows, will more and more shift from POC status to productive industrial usage. Development and especially deployment is becoming easier to handle through complementary software-based micro-services / apps.

Emphasis on technology benefits

Kok said that IIoT applications already today simplify operations within a business; data can be accessed anytime and anywhere, and learnings out of it can be re-implemented to improve engineering and production processes. Combining IT with OT now enables industrial enterprises to meaningfully use the data generated across disciplines within and beyond company borders. Breaking up information silos help companies significantly and lead to higher production efficiency due to faster decisions and reduced manual efforts, secure data-supported decisions, maximum transparency, and greater sustainability.

Addressing automation challenges

"Global trends and rapidly changing challenges require quick and confident decisions," Kok said. "The greater transparency provided by the constantly available analysis of enterprise data creates knowledge, which leads in turn to better decisions and more concrete actions with continuous improvements. The question is how to access and process field data for further evaluation especially thinking about scaling in an industrial context."

He also added that there are significant challenges in a number of key areas.

- *Data security/ cyber security:* The growing connection between production networks and office networks as part of IT/OT integration and the utilization of the Internet of Things have many benefits – at the same time know-how and plants need to be protected at all times.
- *Sustainability of enterprises* needs to be enhanced by identifying energy or cost hogs and optimizing the availability of materials.
- *Real-time analysis of workflows and processes* enhances transparency in all areas and boosts efficiency throughout the enterprise and throughout the entire value chain: material flows, procurement processes, production, inventory levels, disposition of goods.

Progress and impact of the IIoT

Kok said that "reservations about storing and processing data in the cloud have decreased significantly and we see a growing importance of digital transformation and becoming a digital enterprise.

Purpose-built applications with low-code technologies are accelerating the data-driven insights for manufacturing organizations. With recent global political insecurity and supply chain issues arising, companies need to make their production more flexible and decentralized in order to avoid one-sided dependencies. To maintain efficiency, among other things due to different wage cost levels, IIoT applications are the means of choice to increase productivity and to optimize global networking."

He concluded by stating that key next steps and/or that will enable more rapid development of IIoT applications involve a series of potential technology solutions.

Low Code

Low-code application development is the fastest and easiest way to build IoT software and applications. Visual model-driven approach enables both pro and less technical developers to consume IoT services from best-in-class IoT platforms to build data driven purpose-built applications.

The low-code approach helps organizations to build rich experiences on top of connected devices to transform their operations, products and business models. With low-code technology the IT – OT convergence and user engagement is realized at an accelerated pace, making edge to cloud and cloud to edge data transparency a reality.

Industrial 5G

Thanks to 5G technologies, IIoT is becoming significantly more flexible, as companies can process large volumes of data many times faster and in real time. The new mobile communications standard is providing an additional boost to edge computing in particular.

AI

Artificial intelligence (AI) and machine learning are technologies that enable engineers and data scientists to structure, analyze and evaluate the vast amounts of data. Use cases span the lifecycle: intelligent recommendations, generative design, anomaly detection, and predictive maintenance optimize the way and speed with which products are designed and produced. To use industrial AI in a trustworthy and value-adding way, they must interact seamlessly with software and automation, as well as the corresponding IT infrastructure.

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

OPC UA enabling technology for IIoT communications

OPC UA easily connects the shop floor to the top floor in a semantic and standardized way. It provides proven technology that is essential to Industrial Internet of Things (IIoT) and enterprise connectivity, and can possibly be standardized for a whole industry segment or company via companion specifications.

OPC UA TECHNOLOGY IS MAKING AN ONGOING impact with its ability to enhance factory and network communications. Check out our Q&A with Oliver Jöhnßen of Siemens on the value of this technology in manufacturing.

SOURCE: SIEMENS

There is an urgent need to improve cyber security for OT that must start with education and research.

What key technical trends are driving the adoption of OPC UA automation, control and networking solutions? How does OPC UA fit into the broader Industrial Ethernet ecosystem?

OPC UA can easily be used on any industrial automation or HMI device and so is an ideal possibility of integrating special components, such as measuring applications, or innovating existing machines, vendor independent. OPC UA fits perfectly into new or existing industrial ethernet systems as it runs convergent to many other standardized protocols.

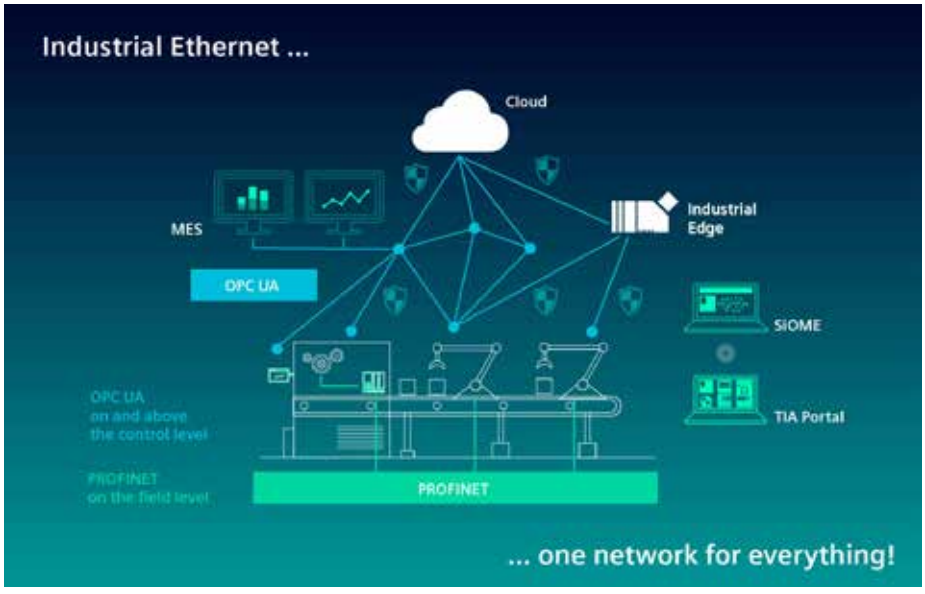
What are the key technical advantages of automation systems that utilize OPC UA technology solutions? What are its primary technology benefits for automation and control networking?

Automation systems, utilizing OPC UA have the key technical advantage that they still communicate in their proven way, e. g. via PROFINET and PROFIsafe and additionally integrate third-party applications via OPC UA in horizontal and vertical direction up to Industrial Edge and Cloud systems. Via OPC UA information model, production data are converted into comprehensive information, containing values, units and accompanying information.

What is the impact of OPC UA on the types of network architectures that are possible? What are the advantages of these new approaches?

OPC UA extends existing networks especially towards Industrial Edge or cloud applications and easily exchanges information with these Apps. This enables customers to integrate essential solutions such as predictive maintenance, performance optimization and determination of KPIs. Thanks to "security by design" in OPC UA, cloud connectivity enjoys maximum data privacy.

OPC UA easily connects the shop floor to the top floor in a semantic and standardized way and so contributes essentially to IoT and enterprise connectivity, possibly standardized for a whole industry segment or company via companion specifications. This increases productivity in the production, ensures secure data connection via OPC UA GDS and speeds up trouble shooting with OPC UA A&C.



What are the engineering challenges that the newest OPC UA systems and architectures are designed to address, and how is OPC UA evolving to provide more comprehensive solutions?

With OPC UA, I/O data become "comprehensive information" including 'value' and 'unit'. So, previous errors in interconnecting metric values and imperial values are avoided. Thanks to efficient engineering in SiOME via drag&drop, production data from the field are quickly mapped to an OPC UA information model. The companion specification guarantees easy integration of machines throughout an entire industry segment, e. g. OMAC PackML for packaging industry.

Oliver Jöhnßen, Senior Marketing Manager, Digital Industries, ***Siemens.***

Visit Website

Role of IIoT sensors and cloud in data-driven maintenance

Smart condition monitoring uses artificial intelligence to make mechanical plant components fit into data-driven maintenance models. In these systems, IIoT sensors monitor and gather vibration and temperature data which is sent via Bluetooth to gateways, and from there to a cloud application for analysis.

SOURCE: SIEMENS

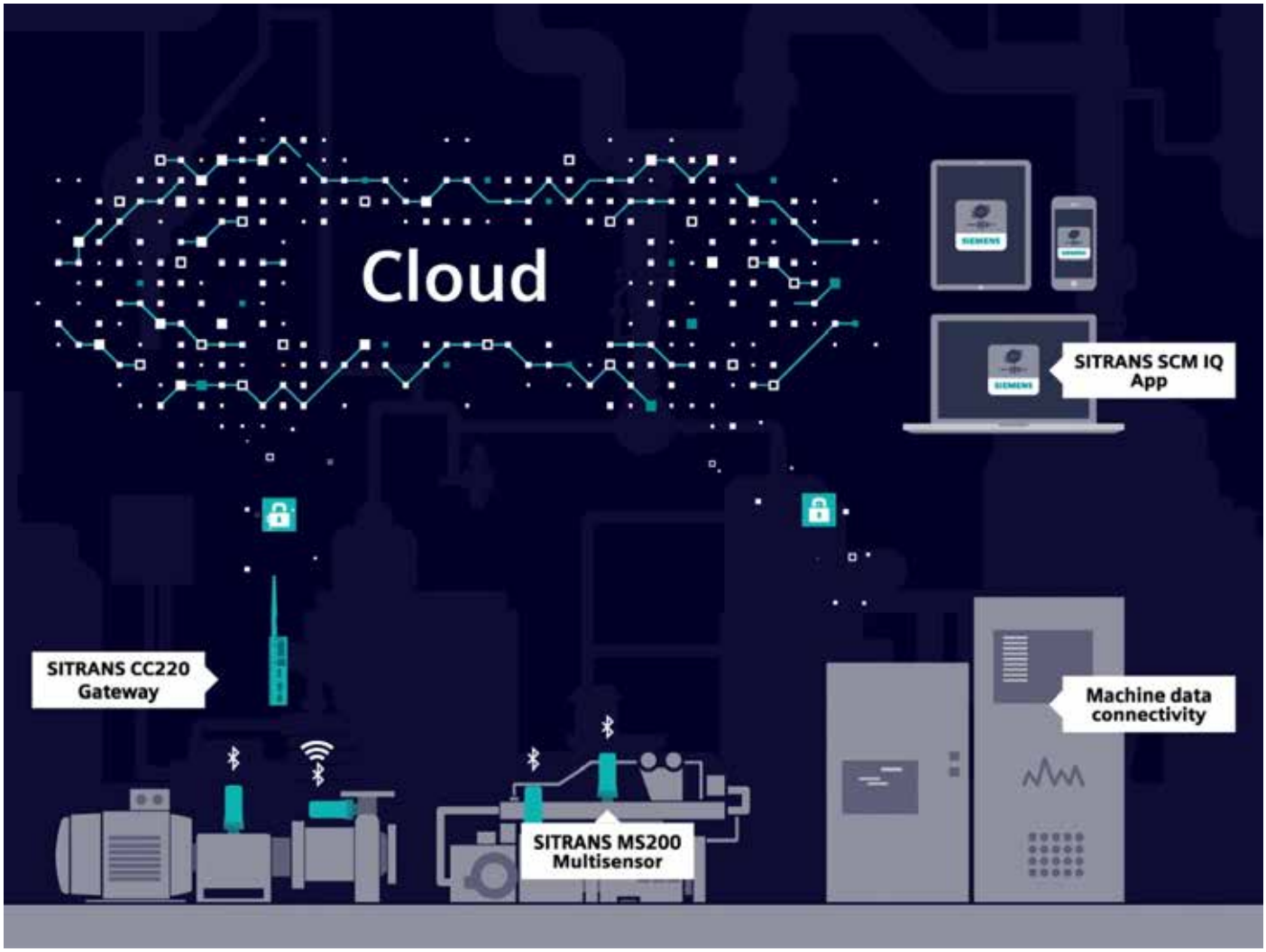
The lack of data, communication options, computing capacity and visualization options prevents the integration into a monitoring or even predictive maintenance system. But new technology options are opening up ways to retrofit mechanical subsystems into the league of IIoT devices.

IN TERMS OF IIOT, SMART FACTORY OR digitalization in general, the lack of actual implementation is often due to many unresolved questions: Where to start? With the supply chain? In production? Or with distribution? What is the resource commitment required for this? And what is the goal to be achieved? Discover an application yielding quick results.

Just as other process industries, production facilities in the food industry have matured and heterogeneous infrastructures. Ultra-modern and networked plant components stand alongside closed production units that have been operating reliably for many years. The degree of automation of individual lines differs, etc. All in all, the lines are integrated into systems ensuring stable production performance and high product quality.

In any case, this includes maintenance and repair management. However, traditional maintenance models based on experience, legal requirements and fixed maintenance intervals quickly become cost-intensive for extensively automated lines with many integrated units and are outdated today. Modern plant components monitor their health

SOURCE: SIEMENS



Making mechanical plant components fit for the future: Enabled by an intelligent combination of IIoT sensors, gateways and cloud services - easily retrofittable.

status independently and provide the basis for so-called condition-based maintenance. In this monitoring maintenance, measures are taken based on the current state of wear and not according to fixed schedules.

But what about machines that don't have built-in self-diagnostics? For such mechanical components still largely lacking automation and communication capabilities, Siemens has developed a system that propels these plant elements into the league of IIoT devices in just a few steps.

IIoT for retrofitting

The system is autonomous and does not influence the process operation to any extent. This circumstance, coupled with very simple installation, makes Sitrans SCM IQ a partner for the move into digitalization and thus opens up ways to significantly more efficient maintenance strategies and higher plant availability.

Sitrans SCM IQ from Siemens AG is a smart condition monitoring system using artificial intelligence to make mechanical plant components fit for data-driven maintenance models. For this purpose, IIoT sensors are screwed onto the machines to be monitored and gather vibration and temperature data which is sent via Bluetooth to gateways, and from there to a cloud application for analysis. Artificial neural networks constantly monitor vibration characteristics, and event-based warnings are issued in case of deviations that indicate an impending asset failure.

Example: Pumps in the cloud

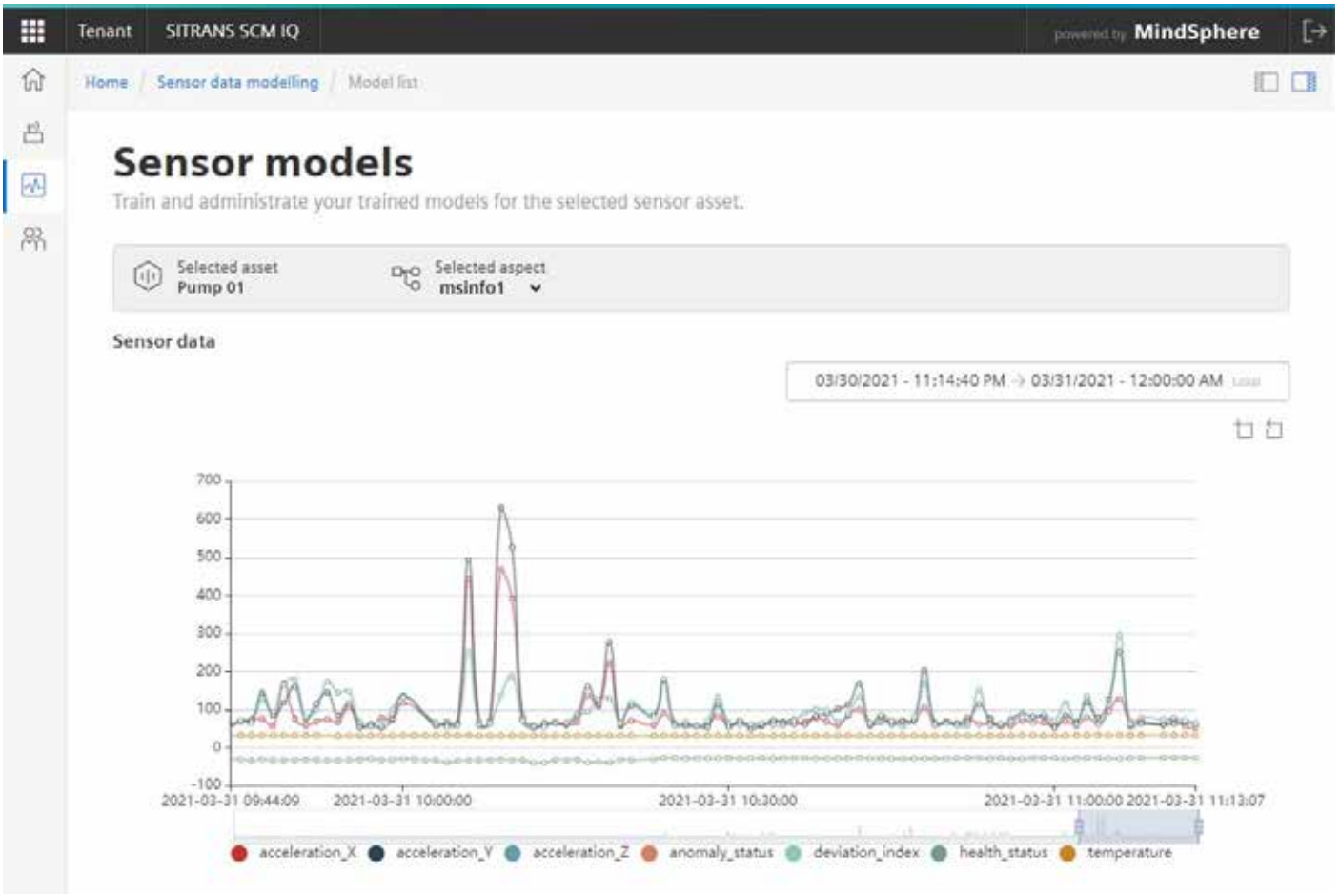
Food production involves a lot of movement. This process requires, for example, pumps that are subjected to high loads. Normally, these aggregates are embedded in a rigid maintenance plan and are additionally serviced on the basis of experience and trained observation.

The lack of data, communication options, computing capacity and visualization options prevents the integration into a monitoring or even predictive maintenance system.

It is precisely along this signal chain that Siemens has bundled products and services in Sitrans SCM IQ. To start with, the pump is equipped with one or several Sitrans MS 200 multisensors, depending on the scope of the monitoring. The IIoT sensors are housed in a robust industrial enclosure with IP 68 protection, which is screwed directly onto the plant component using a stud bolt or grub screw. In principle, the multisensors work with all assets that vibrate or rotate and that are within the range of the sensor's specification.

The battery-powered sensors do not need to be wired. The vibration and temperature data are sent via Bluetooth Low Energy (BLE) to the next link in the chain, the decentralized data processing in cloud gateways. A Sitrans CC220 gateway can receive the transmitted information from several multisensors and transfer it from there to the cloud - the industrial IoT-as-a-service solution MindSphere.

All paths are fully encrypted from the sensor, to the gateway and from there to the cloud and the apps. In the cloud application, the delivered data is analyzed and monitored for anomalies. Finally, the last link in the chain is visualization. Via the Sitrans SCM IQ app, the user is always informed about the status of his monitored plant components.



SOURCE: SIEMENS

Is everything running smoothly? Vibration and other data from machines such as pumps or fans are clearly visualized in dashboards. Automatic notification is sent in the event of anomalies.

Turning data into added value

Once the battery is installed, the sensor initializes and is reported to the corresponding Sitrans CC220. After configuring the gateways, everything is ready on the machine side. As soon as the connection with the cloud application is established, vibration and temperature data are transferred to it and the learning phase begins:

Over a period of approximately two weeks, the system learns about different operating states of an asset.

Using statistic methods and explorative data analysis, the application detects patterns in the data streams and selectively assigns them to the good state. During this time, the user does not have to document the operating states or explicitly report them to the system.

Obviously, the system will likewise recognize a condition not yet learned as an anomaly at first, for example a load condition or CIP operation that has not occurred before. The good state can be conveniently extended by re-learning the corresponding time periods. The application does not only allow to evaluate the vibration and temperature data of the multisensors.

In fact, the methods can also be applied to other machine data available in the cloud, such as speed or counter values. Thus, already built-in aggregates can be very easily and conveniently integrated into a condition-based predictive maintenance strategy.

Once the training phase is over, Sitrans SCM IQ reliably detects deviations: If an anomaly occurs due to increased vibration, the system reports that a machine part is on its way to bad condition. The maintenance specialists are informed by SMS or e-mail.

After checking the corresponding machine part and determining the cause, the app feeds back the results to the system, e.g. signs of incipient bearing or seal damage, an imbalance, etc. In addition, the maintenance steps performed on the machine can also be documented. If the same characteristic deviation occurs at any time, Sitrans SCM IQ reports that it is very likely the same incipient fault and how it can be resolved.

Quick wins and long-term successes

On this basis, condition-based predictive maintenance is possible, resulting in far greater plant performance than corrective and preventive approaches.

Sitrans SCM IQ allows users to retrofit individual aggregates or entire machine parks with a condition monitoring system in a very cost-effective way and with little installation effort.

To get started, a clear use case is recommended, such as a pump used in a problematic process step. Valuable insights can be expected here within a short time due to the retrofitted condition monitoring. The system can then be easily extended to other assets or entire lines or plant sections by installing additional sensors and gateways. Sitrans SCM IQ was partly developed as a co-creation project between Siemens and Coca-Cola Hellenic Bottling (Coca-Cola HBC) Company's plant in Edelstal, Austria. The customer's feedback was directly used to improve the products.

Within six months after the system was installed, managers at Coca-Cola HBC saw a demonstrable reduction in downtime. Four unplanned line shutdowns were averted during this period thanks to timely maintenance measures. At the same time, plant performance improved because maintenance measures could be planned and combined over the long term.

Johannes Burchardt and Melanie Marke, Product management - SITRANS SCM IQ, ***Siemens.***

Visit Website

Digital twin technology boosts operational efficiency

Digital twins can improve operational efficiency and commissioning process for industrial machinery by reducing lead times and costs. By using an automation platform, integrators can boost connectivity further to ensure that their industrial machinery will meet their operational needs.

THE WORLD ECONOMIC FORUM (WEF) STATES that leveraging the digital twin to support Industry 4.0 business models could increase operational efficiency by ten percent. This allows manufacturers to simulate the behaviour of real machines for operational gains. leveraging the benefits of a digital twin that is controlled by automation software.

Digital twin for the win

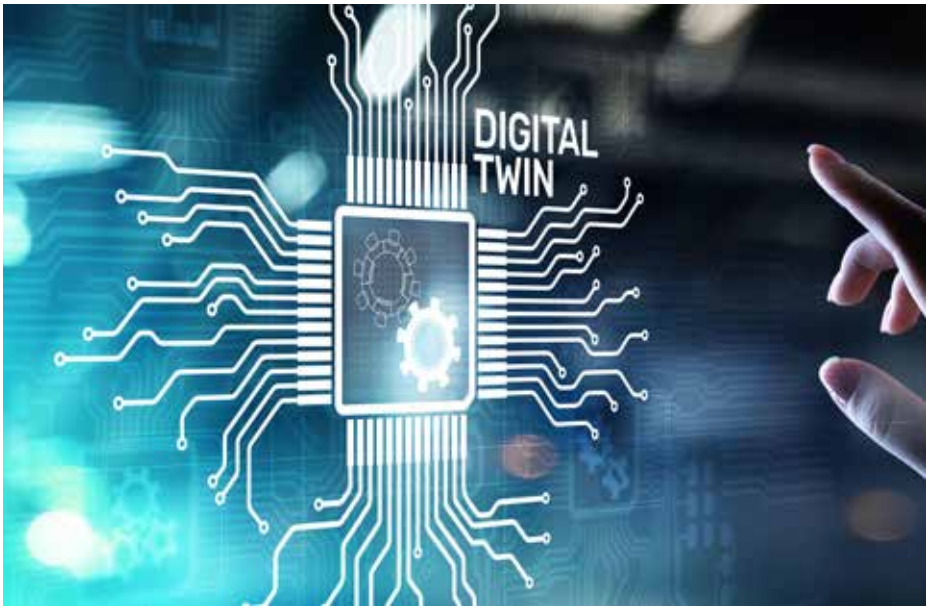
The idea behind using a digital twin is to take the place of a real machine for testing and development scenarios. They can be used for prototyping, product design, user training and testing. Machine builders and operators need to conduct extensive tests on systems and control software, and using a digital twin offers a safer and more cost-effective way to do this.

Good performance and safe operation are essential in industrial machinery. Equipment is often expensive, and failures or breakdowns can incur even larger costs. Industrial operations require high quality and reliability even in challenging processes, and their machines are often operated 24/7. To ensure that they can withstand operating conditions and to evaluate the risk of applying a software patch which is due to a security vulnerability, testing is required.

These testing processes, while essential, can be time consuming and costly. This adds additional time to the commissioning and manufacturing process and complicates matters further when a machine isn't available, or where testing under extreme conditions can be dangerous. This is where digital twins come in.

COPA-DATA and the Vorarlberg company Eberle Automatische Systeme, together with the Salzburg and Vorarlberg Universities of Applied Sciences, have pioneered a way to simulate machine behaviour using a digital twin to take the place of a machine for testing purposes. This can be run with COPA-DATA's automation platform zenon.

Based on physics principles, the simulation is as real as possible, from the mass of the elements to be tested down to the friction levels on machine surfaces. Users can add actuators, sensors and other elements to the virtual machine using a library before running realistic simulation scenarios with minimal additional programming.



SOURCE: COPA-DATA

Using a digital twin, engineers can begin to implement and test automation systems more efficiently.

When developing new machines, developers depend on having access to the machine and programmable logic controller (PLC) to develop the Human-Machine Interface (HMI) and the supervisory control and data acquisition (SCADA) software. Using a digital twin, engineers can begin to implement and test these systems more efficiently, and these tests won't need to be repeated, as the twin is operated based on 'real' sensors and actuators.

Implementing a digital twin is also quite straightforward with effective planning and mathematical modelling. Using models to describe the behaviour of robots or machinery components and defining interactions between them can create a simulation of even complex systems, and this can then be used for further testing and analysis based on the twin.

Using a digital twin can boost production and improve the timescales and efficiency of equipment commissioning processes. Some processes can be carried out in parallel, for example the development of HMI and SCADA systems without the final PLC. If zenon is used in conjunction with the digital twin software design programme digifai, the two platforms can communicate out of the box, for easy integration and strategy planning for systems integrators.

Engineers can take different approaches when it comes to developing a digital twin. One way is through using an automation platform like zenon, which can support the development and evaluation of the models needed for an effective digital twin. zenon provides real-time data from existing machinery components, allowing the engineers and integrators creating the models to receive instant feedback on their developments. This method even has the potential to facilitate automatic development and training of digital twins in future.

On the other side of the process, zenon could use the information generated by a digital twin to automatically create content such as alarms, tag lists and navigation patterns based on the algorithms.

Digital twins offer a convenient way to improve the operational efficiency and commissioning process for industrial machinery by reducing lead times and costs, as well as reducing risks associated with training or testing. By using an automation platform, integrators can boost connectivity further for a quicker, safer and more cost-effective testing process to ensure that their industrial machinery will meet their operational needs.

Reinhard Mayr, head of information security and research operations, ***COPA-DATA.***

Visit Website

Top 5 edge computing and IIoT predictions for 2023

Edge computing and Industrial IoT expert Jim White, IOTech's CTO, provides his Top Five predictions and honorable mentions for the coming year, including forecasts related to security, hyperscalers, artificial intelligence and machine learning.

SOURCE: ISTOCKPHOTO

Building edge/IoT solutions requires planning and execution, and the ability to adjust according as edge technology inevitably changes.

PLAY TIME FOR EDGE COMPUTING IS OVER—full scale deployments in 2023, predicts IOTech. Edge computing and Industrial IoT expert Jim White, CTO at IOTech, provides his top 5 predictions and honorable mentions for the coming year including forecasts related to security, hyperscalers, and AI/ML.

1. Edge play time is over

Companies that are wanting to put edge/IoT solutions in place are making things clear to providers: research and play time is over.

These companies are done "trying" things. Edge solutions have to work "now," they have to work at scale, and they have to work such that IT and OT teams can use them effectively.

Companies are growing impatient with solution providers that are not able to provide solutions that are already working at scale and immediately demonstratable. Edge elements must be fully integrated into their choice of technology (hardware, sensors, devices, network, cloud providers, data visualization, analytics, security, management, etc.). Companies want edge solutions that are easily installed and even easier to own and operate.

2. OT Edge Security becomes a thing

Threats at the edge are becoming more publicized and known. Companies are reading about various attacks on the edge and they are becoming educated on what they want for solutions. Requirements are becoming clearer and more specific.

Companies are no longer under the illusion that closed loop networks are truly closed, that obfuscation is good enough protection because "this stuff is complicated," or that "no one would bother to want to get access to this type of data."

Organizations want to know how to protect all parts of the edge solution, from sensor to cloud. They also want to know how to detect when something seamy or unexpected seems to be going on. Progress is being made with edge/IoT security capability, but much of that is related to protecting cloud native environments and doesn't integrate well at the edge. Edge/IoT and security industries are starting to recognize this.

3. Reinvention and disruption of hyperscalers

Cloud providers and the hyperscalers have tried to lure all that precious edge data into the cloud where AI/ML and other analytics were to operate on it.

The challenge is that the vast transfer, storage, and compute charges associated with moving all that edge data to the cloud is significantly expensive. Trying to sift through all that data for nuggets of commercial value doesn't always show an ROI – at least not yet. Companies are beginning to wake up to this reality.

Hyperscalers know how to do scale. They

SOURCE: IO TECH

Jim's 2022 Predictions	Result	Grade
Pervasive adoption of AI/ML at the edge	Partially true. We've seen more organizations trying to apply AI/ML in their overall edge solution. Not all of it has worked its way to running at the edge yet.	B
Hybrid edge-cloud architectures will be the norm	Part of almost every "edge" solution also has elements in the cloud. Per this year's predictions, we have seen cloud providers and hyperscalers let us down in some ways, but that will change.	A
The industrial sector emerges from edge/IOT research mode	Play time is definitely over for the industrial sector. Make it hum, make it simple, make it scale is now the order of business.	A
Customers will demand solutions rather than pieces/parts	True, but admittedly I did not foresee just how fast organizations would require the entire edge/IoT solution to include everything – hardware, sensors, visualization, network, etc.	B
Realization that K8s is not enough edge management	A full realization is something organizations are still working on. Admittedly, bigger "edge" (more resources) also allows for more K8s in some cases. I don't think we are all the way there yet and I think, per this year's predictions, the K8s community is going to start to approach edge management in a way that is more supportive and with better solutions than shrunk down K8s.	C
Traditional IT hardware OEMs will need to develop edge/IOT strategies	They are trying in some cases (look at Dell's recent announcement on Project Frontier). Others are EOL their efforts (HP). I suggested they "risk becoming irrelevant". I think this is still a risk in some cases. My prediction was correct but not all the OEMs are developing to compete.	B
Digital twin standards are needed to ensure pace of innovation	I thought we'd be much further along. My biggest prediction fail and regret for the industry. Also part of the reason I suggest hyperscalers need to do more this year.	F
The use of digital ledger technology (i.e., block chain) will start to grow	Another fail. I still think this is coming but we aren't there yet. Organizations are still collecting the data and making use of it. Providence of the data still to come.	F
Noise level for edge and 5G will continue	Nailed this one and it remains the same story.	A
COVID sped up challenges that were already exhibiting	Per my last prediction this year, this is just one part of the need to do more with less that is driving edge innovation.	A

Jim's 2022 score card.

just need to do edge at scale and in a way that adds value and lowers cost. They can and will figure this out, but they are going to require help from organizations, people and projects that know the edge. Watch for an increase in new product announcements, new partnerships and acquisitions as the hyperscalers finally take on "edge native."

4. Not everything requires AI/ML

AI/ML is revolutionizing numerous industries and spaces. But as with any supposed magical balm, it can be overapplied. There is a lot of edge processing going on – some of it might even require some sophisticated calculations and algorithms – but not all of it needs costly ML models and AI engines.

Simple rules engines and scripting engines can provide a lot of value at the edge – saving operational costs, improving safety and even generating new revenue. Edge solutions don't always require advanced/complex skill sets to produce, nor do they require all sorts of compute power to operate.

There is still a lot of low hanging fruit (aka money to be found) by measuring a few edge values and automatically actuating when things get out of range. Edge solution providers that help keep it simple and harvest that fruit, might become the new darlings of investors and companies looking to improve their company bottom lines.

5. Kubernetes still not the full answer, but...

Everyone's edge is different, so Kubernetes can be used to deploy, orchestrate and manage containerized workloads at some edges. But Kubernetes does not solve all the issues around management at the edge and it struggles in resource constrained environments or environments that aren't going to support containerized workloads.

There have been and continue to be more CNCF efforts to extend cloud native – call them Kubernetes light – to the edge. Many of these have been attempts focused on shrinking Kubernetes at the cost of functionality. microK8s, KubeEdge, K3s are all options that have been traversing this path.

There is growing recognition on the part of the CNCF community that Kubernetes-light isn't enough. Therefore, 2023 will experience an emergence of new approaches and architectures to help address edge management.

Honorable Mention Predictions

A. Consolidation

There are numerous edge and Industrial IoT platforms, software, tools, etc. (proprietary and open source). These have emerged over the past 5-10 years of the hype cycle associated to edge and IoT computing.

The industry has reached a point (through the trough of disillusionment and onto the plain of productivity) where consolidation is inevitable. Companies want to accelerate their edge/IoT solutions. Over the past few years, companies were buying AI/ML companies to gain control of the IP and the people in that space. They will do the same to consolidate more of their holding on the edge solution space.

B. Use Case Demand Changes

Within the industrials sectors, suppliers of solutions in the edge/IoT space have been addressing use cases for several years. Now, other verticals are starting to become important consumers of edge/IoT solutions.

Climate change, energy shortages, health and environment concerns, people / staff shortages – all areas of need stemming from immediate global economic and geopolitical circumstances – are driving more use cases.

*Technology report by Jim White, CTO at **IO Tech**.*

Visit Website

Technical approaches to defend and protect IoT nodes

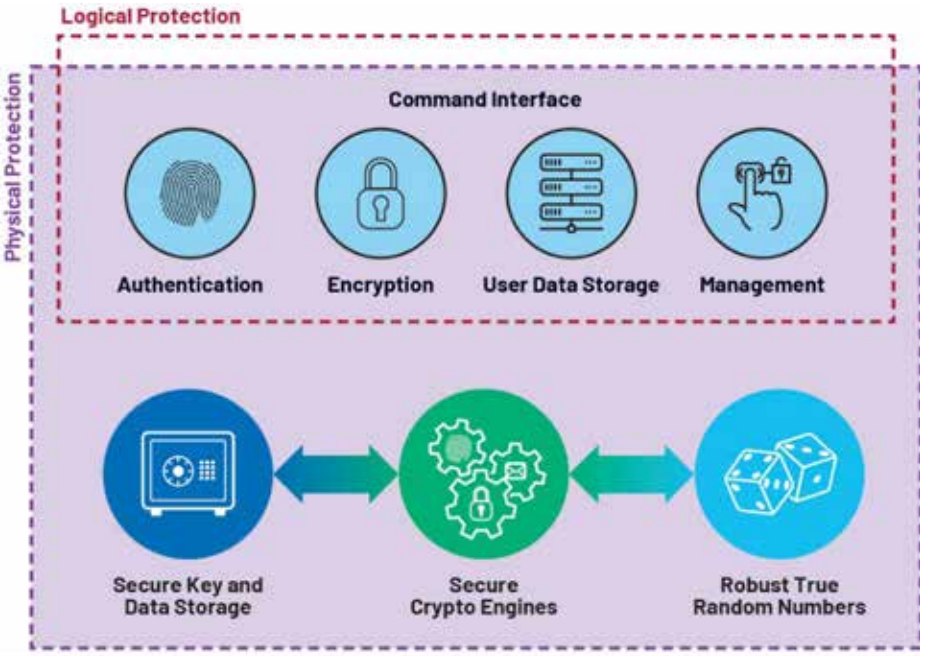
Creating a secure IoT node begins with a "root of trust", a small affordable integrated circuit designed to offer security-related services to the node. Examples are data encryption for preserving confidentiality and digital signatures to ensure authenticity and integrity of information.

TEN BILLION IOT NODES ARE CONNECTED today, ten times more than just a decade ago, and the trend is continuing unabated. With this growth comes an equal growth of opportunities for attackers of industrial and manufacturing facilities.

The estimated annual cost of cyber attacks ranges from tens of billions of dollars to over a trillion, and it too keeps rising. Therefore, security considerations are now essential to continue the successful scaling of the IoT. IoT security begins with the security of the IoT nodes.

No company wants to see its name in the same sentence as "breached, and customer data was stolen." What's more, connected devices are also subject to government regulations, such as FDA rules for medical devices, US/EU cybersecurity requirements for Industry 4.0 critical infrastructures, and several new emerging standards for the automotive industry.

Those requirements push for high-level security while not explicitly mandating the use of hardware-based security. However, IoT nodes are often large-volume, cost-optimized appliances, creating challenges to balance security and cost.



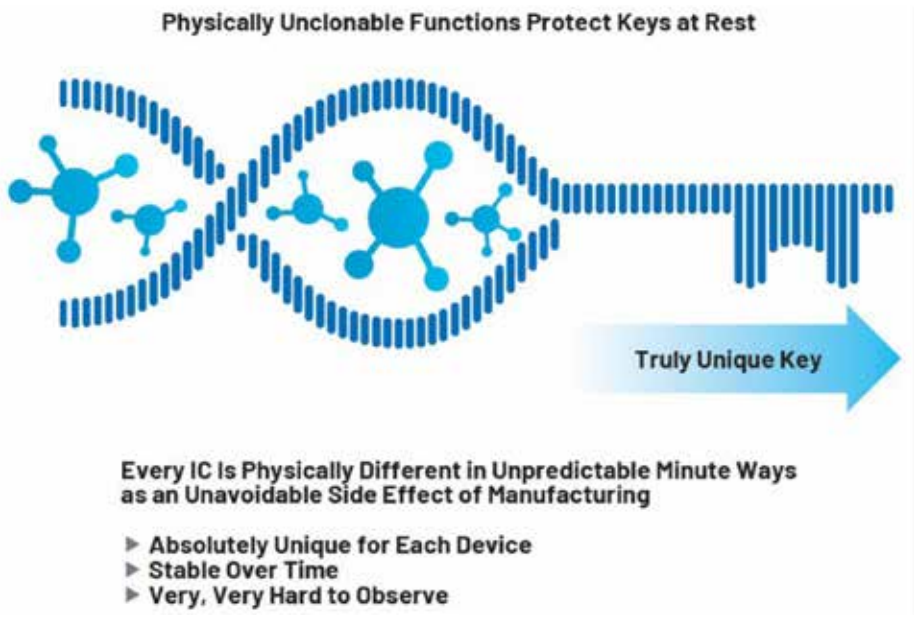
SOURCE: ANALOG DEVICES

Figure 1. The "Root of Trust" concept ensures authenticity and integrity for security-related services.

Secure nodes Using "Roof of Trust"

How can we design a cost-efficient yet secure IoT node? Creating a secure IoT node begins with a "root of trust" (also known as "Secure Element"), a small affordable integrated circuit designed to offer security-related services to the node.

Examples of these functions are data encryption for preserving confidentiality and digital signatures to ensure authenticity and the integrity of information. The ultimate goal of the root of trust is to ensure that the secret keys used for data encryption or digital signatures are protected against disclosure. The biggest challenge for "root of trust" security ICs is resistance against physical attacks, such as direct probing and so-called side-channel attacks.



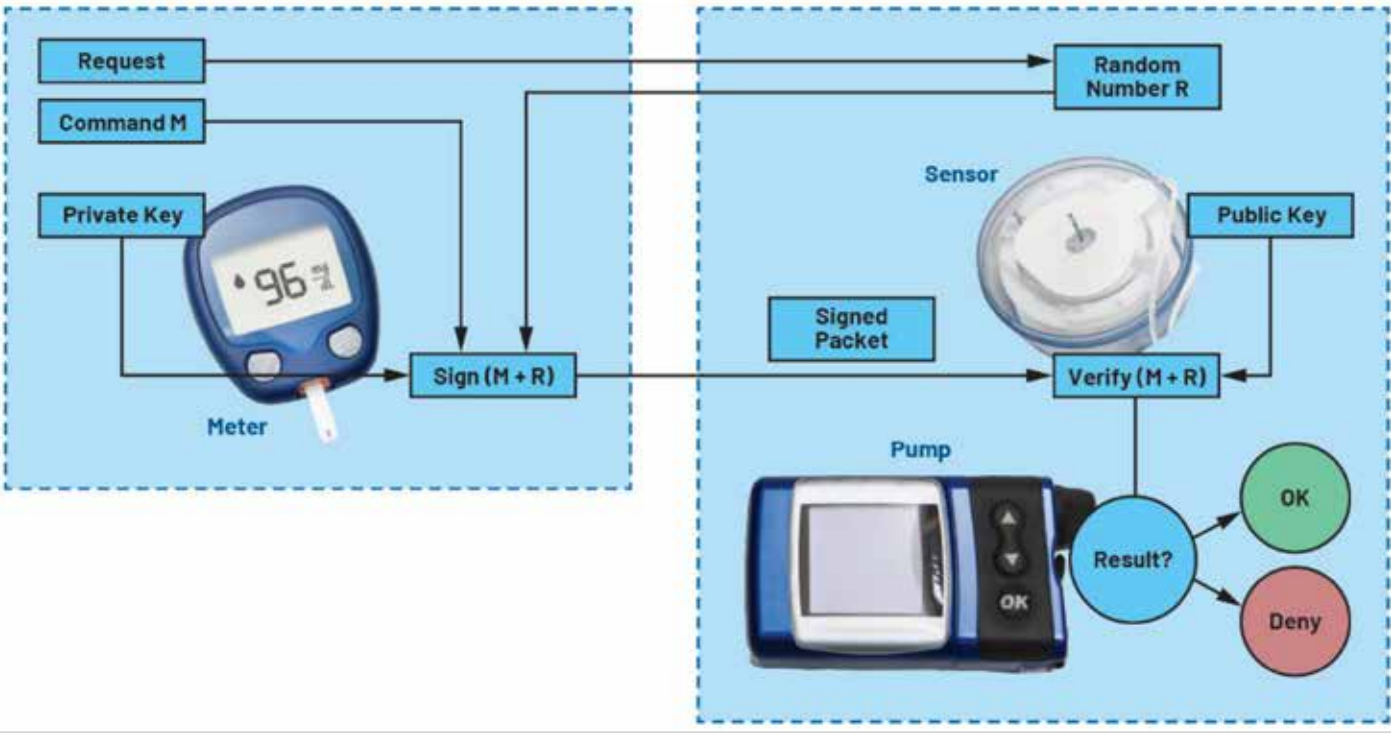
SOURCE: ANALOG DEVICES

Figure 2. PUF technology mitigates the risk from direct probing of microcircuits.

Physically unclonable function (PUF)

Unfortunately, because direct probing attempts to observe internals of microcircuits, memory technologies typically used in general-purpose microcontrollers (i.e., EEPROM or Flash) are not secure.

An attacker can directly observe the memory contents at a relatively modest cost using Scanning Electron Microscopy (SEM). The semiconductor industry has developed the "physically unclonable function" (PUF)



SOURCE: ANALOG DEVICES

Figure 3. Insulin pump authentication is a simplified example of root of trust.

technology to mitigate this risk. The PUF is used to derive a unique key from the intrinsic physical properties of the chip. Those properties are far more difficult to probe directly, making it impractical to extract the resulting key via direct probing. In some instances, the PUF-derived key encrypts the rest of the internal memory of the root of trust and, therefore, protects all other keys and credentials stored on the device.

Side-channel attacks are even cheaper and less intrusive. They leverage the fact that electronic circuits tend to leak a signature of the data they are manipulating, for example, over the power supply, radio, or thermal emissions.

The subtle correlation between measured signals and the processed data can lead to successfully guessing the value of a secret key after a moderately complex statistical analysis when the circuit uses that key, for example, to decrypt data. A root of trust is explicitly designed to prevent such data leakage using various countermeasures.

Application Example Using a Security IC

The benefits of a hardware-based "root of trust" become evident in the type of secure applications depicted in Figure 3. The protocol used is a simple challenge/response authentication protocol:

1. The meter requests a challenge from the pump in preparation for sending a command.
2. The pump challenges the requestor with a random number R.
3. The meter uses its private key to sign the command, the random number R, and some fixed padding. This operation is deferred to the "root of trust" of the meter.
4. The pump verifies that the signature is correct and that the random number is the same number it sent out earlier to avoid the trivial re-sending of a valid command. This operation is deferred to the "root of trust" IC of the pump.

In addition to the fact that every new attempt at sending a command requires a new random number, the security of this protocol relies on the secrecy of the private key used to authorize commands and the integrity of the public key used to verify the authorizations. If these keys were stored inside common microcontrollers, they could be extracted or manipulated, and fake meters or pumps could be manufactured, potentially endangering the patients' safety.

In this case, "root of trust" ICs make it much more difficult to counterfeit meters or pumps, manipulate the credentials, or tamper with the communication protocol.

Benefits of dedicated security ICs

Overall, a sound node device design will cause the cost of breaking a device to be much higher than the potential rewards for the attacker. The benefits of an architecture relying on a dedicated security IC are numerous:

IoT security is an endless battle. Attack techniques keep improving but, at the same time, security IC vendors continue to enhance their countermeasures so that security ICs remain extremely costly to attack. The security of a connected device can be increased by upgrading the security IC with little impact on the overall device design and cost.

Concentrating the critical functions in a strong, tamper-proof physical environment separated from the application processor allows for an easier "proof of security" when evaluating regulatory compliance. Isolation also makes it harder to leverage weaknesses in the device's application processor, which are very difficult to detect and remove entirely.

Ensuring the security of an IoT node across all its life cycle is easier when the security IC is commissioned early by the security IC vendor. This approach eliminates the need for sharing critical information with contract manufacturers, and a secure personalization flow and secure OTA updates are made possible. Overbuilding and cloning become much harder as well.

Conclusion

There are many components in a typical connected system, and security must be designed in from the beginning. While securing IoT nodes is not the only step, it is a necessary step.

Stephane di Vito, Senior Principal MTS, Robert Muchsel, Fellow and Don Loomis, Vice President, ***Micros, Security & Software, Analog Devices.***

Visit Website

Basis for an end-to-end security strategy

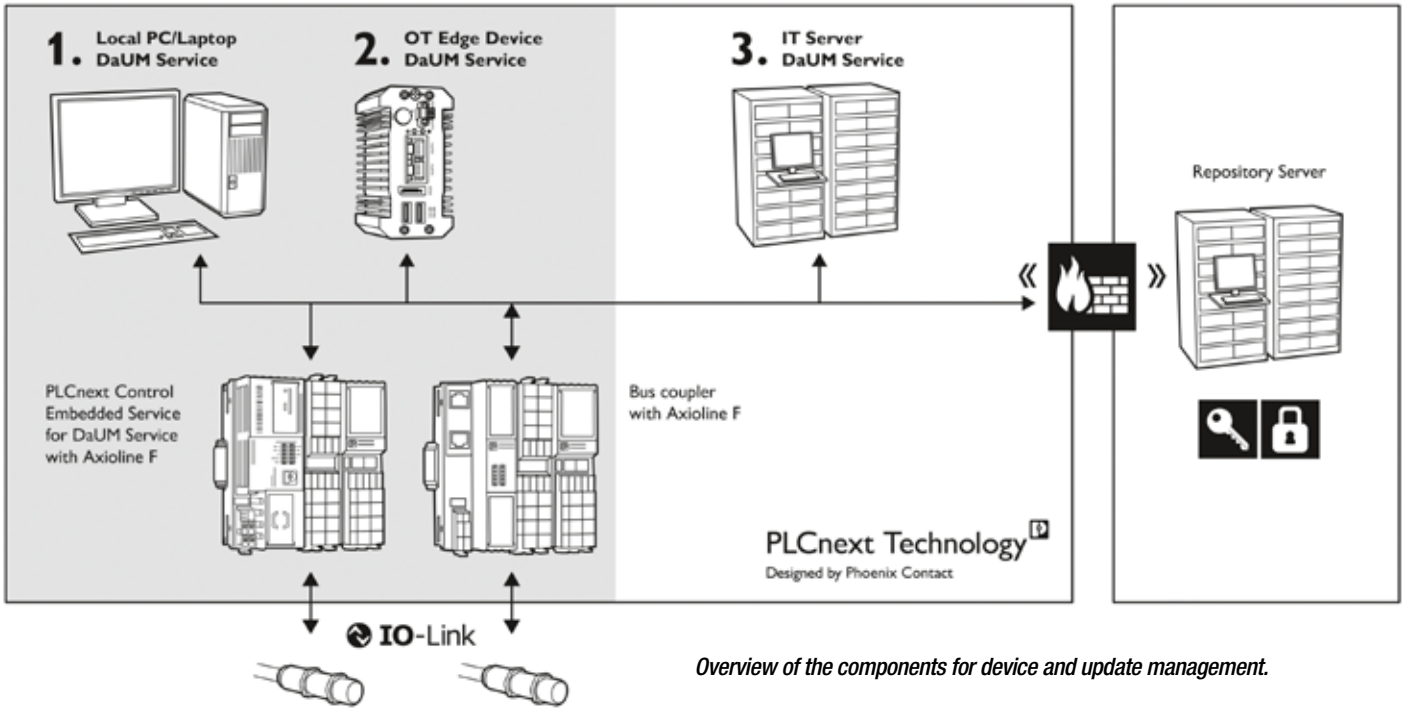
Managing assets as part of device and update management. Due to the development of automated tools for identifying resources and threats, industrial asset management plays a vital role in many industries where security operations are required. Asset management is not just crucial for software and IT companies.

SOURCE: PHOENIX CONTACT

IN THE WORLD OF CYBERSECURITY, THE ONLY things that can be protected are those that are known to exist. This is why managing industrial assets has proven to be important for protecting all kinds of companies from unauthorized access.

In this context, device and update management is an essential building block for a proactive, end-to-end security strategy. It provides security teams with an inventory of OT resources and the associated components.

Industrial asset management is a process



SOURCE: PHOENIX CONTACT

Overview of the components for device and update management.

that involves constantly checking the accessible components to ensure that they are up to date. This makes it possible to identify and immediately eliminate their potential security risks and vulnerabilities. The assets can come in different forms. Traditionally, assets are a control system or industrial PC. However, special IoT or automation devices and software-defined resources such as control apps or reloadable apps are also listed as assets.

In the OT area, any device, resource, or service can pose risks or possess vulnerabilities that could result in a breach of the particular resource and in turn, of the network as a whole, if hackers use the compromised resource as the gateway for a full-scale attack.

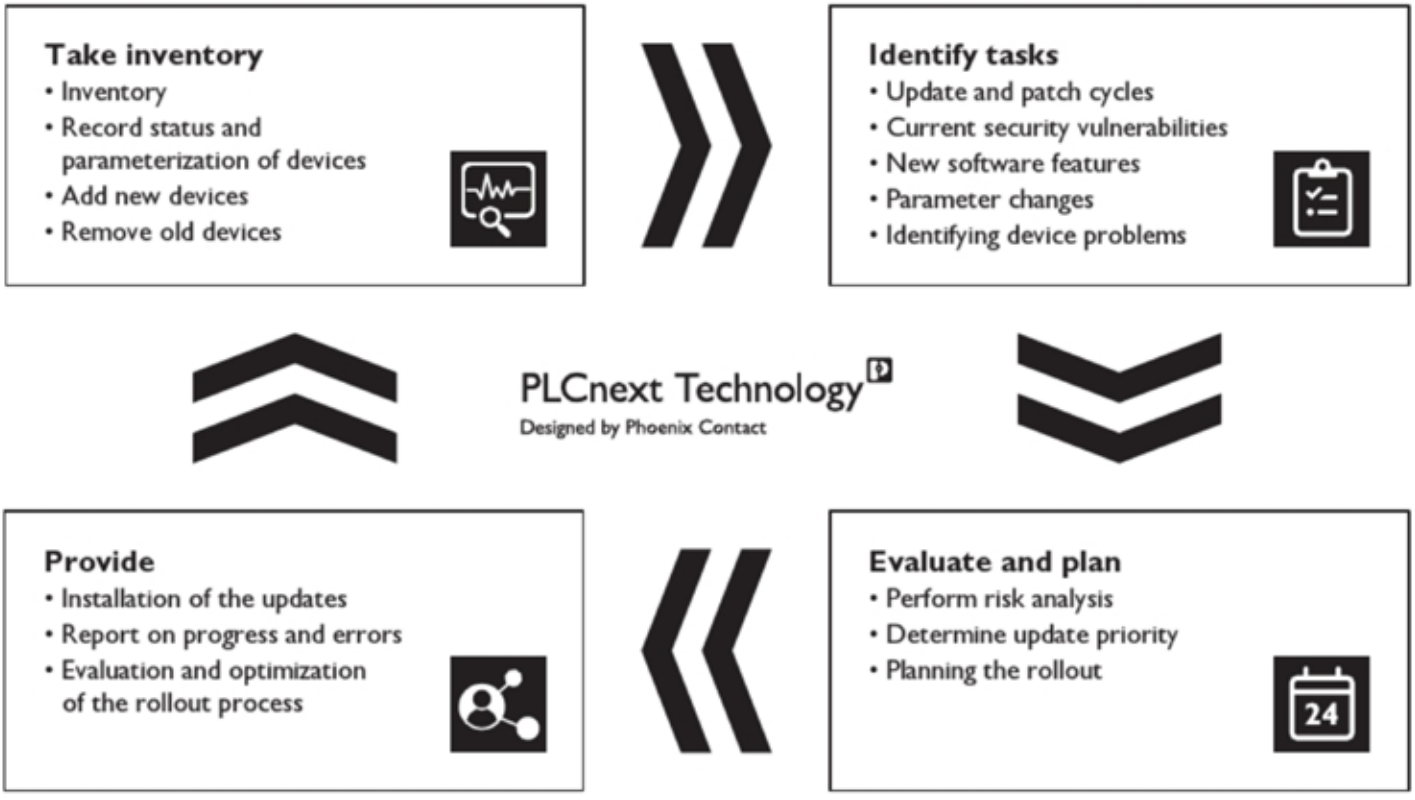
The advantages at a glance

Managing industrial assets gives the entire company the visibility it needs to develop a long-range security strategy that can be used as a basis for keeping assets up to date and helping to defend against threats quickly and proactively. This type of approach offers several key advantages:

- *Taking inventory:* When a solid process for managing assets is in place, new OT services and resources can be identified and applied without compromising the security of the company.
- *Interoperability:* Companies use OT services and components from different manufacturers. It must be possible to manage these assets in the interests of cybersecurity, preferably through a central service. Device and update management using OPC UA ensures that it is possible to manage industrial assets regardless of the manufacturer.
- *Consistent updates:* Device and update management is capable of implementing both security-critical and functional updates for all directly accessible assets. This also applies to the underlying assets connected to the main assets.
- *Easy and secure receipt of updates:* Those responsible for assets or security teams must be informed about updates from the asset manufacturers in good time. For this purpose, device and update management can connect to the update repository provided by the manufacturer

SOURCE: PHOENIX CONTACT

Risks in the context of protection against unauthorized access.



SOURCE: PHOENIX CONTACT

Diagram of the software update process

and search it for new versions of the deployed assets at regularly defined intervals. If an update is available, it can be obtained directly and without loss of integrity and used in device and update management.

- *Flexible use:* Device and update management can be deployed in a range of environments. Depending on the application, it can be used as an app on an industrial PC, software on a PC, or an IT container. Depending on the application, it can be used with the identical functionality.

In the ways described above, device and update management puts companies in a better position to detect and react to security risks. Although industrial asset management is only one component of an effective cybersecurity strategy, in most cases it is impossible to implement proactive security measures without central asset management.

Consequences of inadequate management or no management at all

Poorly implemented device and update management or the complete lack of industrial asset management complicates more than just security procedures. It also creates critical risks for the entire company, including a higher risk of business interruption.

If key data or systems are no longer available due to a security breach, the company might not be able to operate any longer. Such interruptions damage a company's reputation and also lead to serious financial consequences. Inadequate device and update management also interferes with a continuous and accurate inventory of OT resources.

If operators do not know where each asset is located in their company, they can never really know the areas that pose the greatest risks. This lack of certainty makes it difficult to apply security resources efficiently when risks occur.

Similarly, ineffective industrial asset management erodes the ability of security teams to operate effectively. Security operations are difficult to automate if operators do not have an accurate list of existing resources and risks.

Instead, their security teams have to rely on locating and securing devices manually, which is an inefficient use of time and money.

Numerous continuous activities

Since there are many forms of OT resources and security risks, device and update management is a process that involves numerous activities. The industrial asset management approach varies from company to company, depending on the kinds of resources at risk. The pillars of the process for a typical company are presented below:

- *Identifying devices:* By identifying and assessing each critical point in the network for security vulnerability, teams can take immediate action to fix problems.
- *Identifying tasks:* Industrial asset management provides support for identifying tasks in order to close security gaps or roll out new features.
- *Planning implementation:* As updates can have different levels of urgency, device and update management offers the option of starting an update immediately or at a specific time.
- *Installing updates:* After the tasks have been scheduled and prioritized in the industrial asset management system, the update is installed on the assets. In this context, the security team can choose whether the update should be applied immediately after the transfer or later.

It is important to remember that many of the resources described above constantly change. Network devices can come and go. This is why industrial asset management processes must be executed on an ongoing basis to keep pace with rapidly evolving environments.

Conclusion

In the past, industrial asset management was not a high priority for companies. This is because there were no suitable tools for automating industrial asset management processes. Manual continuous inventory management was not practical. Today, due to the development of automated tools for identifying resources and threats, industrial asset management now plays a vital role in many industries where security operations are required.

Asset management is not just crucial for software and IT companies. It is also key to any company that relies on software and hardware to keep operations running. This is true for almost every company right now.

Arno Martin Fast, B.Eng., Senior Specialist Digital Services, ***Phoenix Contact Electronics.***

Visit Website

Updating Software with OPC UA

SOURCE: PHOENIX CONTACT

Using OPC UA in the process industry

The software update model defined in the OPC UA 10000-100 specification is used to manage the software of an industrial asset. This can involve installing new software, updating existing software, updating firmware, and performing a limited backup and recovery of parameters and firmware as needed for the update.

The OPC UA standard can be used for the following applications, among others, regardless of which manufacturer is involved:

- Updating devices by using software update client software. To address domain-specific constraints, this may involve domain-specific client software. For example, this software stops a machine from updating in the production area while a redundant device needs to be activated in the process area.
- The software update can be applied to any device or software component that is exposed in the address space of the server.
- If multiple connected devices are to be updated in a machine or plant, they must first be switched to a specific mode in which they wait for the update to start and do not resume operation.
- Backup and restore for fast (re-)commissioning after a possible system failure or device replacement: The data that was backed up beforehand is transferred to the (new) device, and the original state is restored.

IIoT and automation saves time and enhances control

Farm Data Systems and Azcal Management reduce pump management time by up to 90%. FDS Ignition client app for Water Informatics can be used on phones to power up pumps within seconds, along with an ability to see pressures and flows continuously and make adjustments without visiting any of the sites directly.

AZCAL MANAGEMENT FARMS 8,700 ACRES IN Kings County, California, in the heart of the San Joaquin Valley. They farm a diverse range of crops including pistachios, wine grapes, alfalfa, and row crops like onions, garlic, and tomatoes.

The Customer

Pioneers in precision agriculture technology, Azcal focuses on increasing production, on efficiency, and on improving crop quality.

In drought-prone California, farmers walk a fine line on water use. Water costs, government regulations, and concern for future water availability all mean they must start focusing much more on providing just enough water for crops, not too much or too little.

One of the Azcal ranches has 12 deep-well pumps, all with VFDs (variable frequency drives), feeding a single mainline serving a 4,000 acre ranch just south of Lemoore, California.

Monitoring and controlling these pumps used to be a full-time job for farm managers Jake Sheely and Marty Rhoads. It took six to seven hours throughout each day to drive around the ranch and make the needed micro adjustments to pumping and irrigation systems.

Their monitoring was vital, ensuring that system pressures and flows were within range and that pumps were operating efficiently. With four or five well pumps running at the same time, Jake and Marty had to be extremely diligent to avoid both low and high pressure events and often had to switch wells based on farming needs.

The wells must be kept in operation but not overdrawn. A drop in the flow rate would mean the well was overdrawn, and if air was sucked into the pump, the well could require thousands of dollars to repair.

In addition, like many growers, they also suffered from power failures and incoming voltage spikes. It could be several hours before they realized a pump was no longer running or had burned up.

The time involved in manual monitoring and control was just too much. Azcal looked for a simple way to automate their water management and track pumping events for monthly water accounting.

SOURCE: OPTO 22

All Azcal wells and irrigation filter stations are equipped with VFDs and flow meters.

Azcal interviewed several Ag Tech providers about their need for remote pump monitoring and control. They tried proprietary tools designed for pump control, but although these tools worked for one pump and 40 acres, none of them could integrate everything at scale. And there was limited support for remote control or sophisticated PID loop control.

Discouraged, Azcal was dubious when Farm Data Systems (FDS) in Madera, California, approached them with some new technology. However, FDS owner and president John Williamson had worked on projects for them with a previous company, so they were willing to listen.

"No one has been able to deliver what we needed," said Jake.

As John notes, agricultural customers are trying to solve fairly simple problems, but there are so many difficulties that it becomes complex. Assets are spread out over wide distances. You can't run Ethernet wiring; the system has to be wireless. And cost is a huge factor, as farms don't usually have big budgets.

But the engineers at FDS have spent the last 20 years figuring out how to make technology in the field both relevant and cost-effective to growers. In the early years they used their own technology for monitoring, but customers began asking for more and more features. So FDS standardized on Opto 22 hardware and Ignition software from Inductive Automation®, bringing agriculture into the internet of things.

"Five years from now I don't know how anyone will be able to farm efficiently without this IoT technology," says John.

Using the Opto 22 hardware and Ignition software, FDS has developed an end-to-end field monitoring and automation solution for crop irrigation management.

Opto 22 groov EPIC controllers and groov RIO modules connect to sensors and equipment in the field to gather data and automate control.

FDS' Water Informatics platform, an Ignition project hosted on FDS' private cloud, provides

SOURCE: OPTO 22

Azcal well pumps all feed the same mainline pipe, leading to complex pressure management requirements.

the control and data that farmers need in a way that they understand and can easily use. Each customer has a private view based on their login that shows just the assets and information for their ranch.

By avoiding expensive custom hardware that can be time consuming to build and maintain, FDS can keep prices affordable while also limiting downtime if something needs to be replaced or upgraded. With off-the-shelf controllers, sensors already widely used in many other industries, and their own easy-to-use software, FDS' systems are very affordable for farmers.

Not only has the company significantly improved irrigation management at over 500 farms covering more than 50 crops, they also farm their own 200-acre technology lab to test system improvements.

The Solution

What Azcal needed was a controller at each well pump, fully integrated with their existing VFDs, that would allow them to remotely start and stop pumps as well as make micro-adjustments to either the speed or the pressure setpoints. They also needed reliable monitoring of flow meters and incoming voltage.

FDS met Azcal's needs with an integrated, modular architecture that can be easily adapted to meet the unique requirements of each customer.

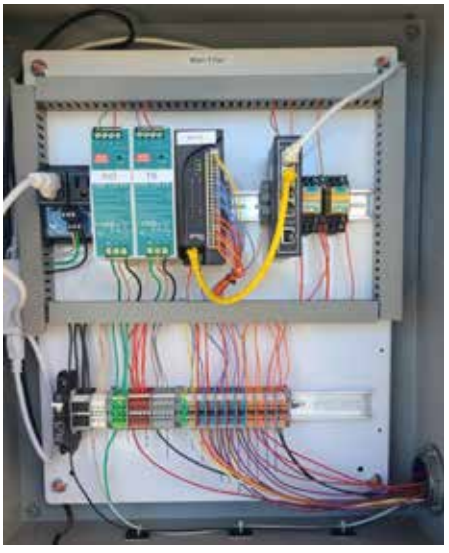
The Hardware

Farm Data Systems began using Opto 22 controllers and I/O several years ago. They had used Allen-Bradley® products for pump control, but the systems were too expensive for most farms.

When they discovered that new IoT products from Opto 22 could do the same things more efficiently, John says, "Opto opened the door into Ag for us."

Initially they chose the Ethernet-based, rack-mounted SNAP PAC R-series controllers and I/O for field installations. When Opto 22 released groov EPIC and groov RIO, however, they saw an opportunity to reduce costs further.

"There are 60,000 irrigation pumps in California, and 60-70% have only got four to six I/Os," says John. "It doesn't make sense to put a full controller in there." Instead, FDS uses a groov RIO universal I/O module, a small unit that offers a broad range of software-configurable signal types, plus built-in security and IoT communications.



SOURCE: OPTO 22

The groov RIO with 10 universal I/O channels is well suited to Ag pumps.

For system control, FDS uses the sturdy groov EPIC edge programmable industrial controller. Designed for industrial automation and the internet of things, the EPIC offers security features including a configurable device firewall, user accounts and authentication, data encryption, security certificate management, VPN client, and dual independent Ethernet ports. With control programming options and the ability to run Ignition software, EPIC is a step ahead of other industrial controllers on the market.

Both groov EPIC and groov RIO include Node-RED and MQTT communications, which FDS is increasingly using to streamline data capture. A groov RIO at a remote location, for example, can send data via MQTT directly to an MQTT broker on the Ignition server.

The Software

A key part of Farm Data Systems' installations is their Ignition project software, Water Informatics. With a UDT library of all the features they provide—pumps, flow meters, moisture probes, every physical device—new assets can be easily copied and pasted to build out a new project in minutes. Once added, every feature can be expanded to other customers.

Because the architecture is hosted, FDS just needs to turn on the customer's access to their individual pages. Adding a new client is "super fast," as John notes. "The software part can be completed in a few days. Installing hardware is the bulk of the work."

Using industry-standard controller hardware and SCADA software, FDS offers almost 30

SOURCE: OPTO 22

Azcal filter stations typically serve multiple crops in fields of various sizes.

different modules hosted on a secure web server, from soil moisture monitoring to full irrigation automation. And they constantly add new modules based on customers' needs.

For Azcal, FDS began by installing Opto 22 SNAP PAC I/O units at five well pumps. As soon as groov RIO was available, they installed groov RIO modules at an additional seven well pumps. The well pump I/O reports data on voltage transducers, virtual speed potentiometers, remote setpoints, current switches, VFDs, and flow meters at each location, sending that data over WiFi via an Ethernet switch and a Ubiquiti bridge to the main tower location.

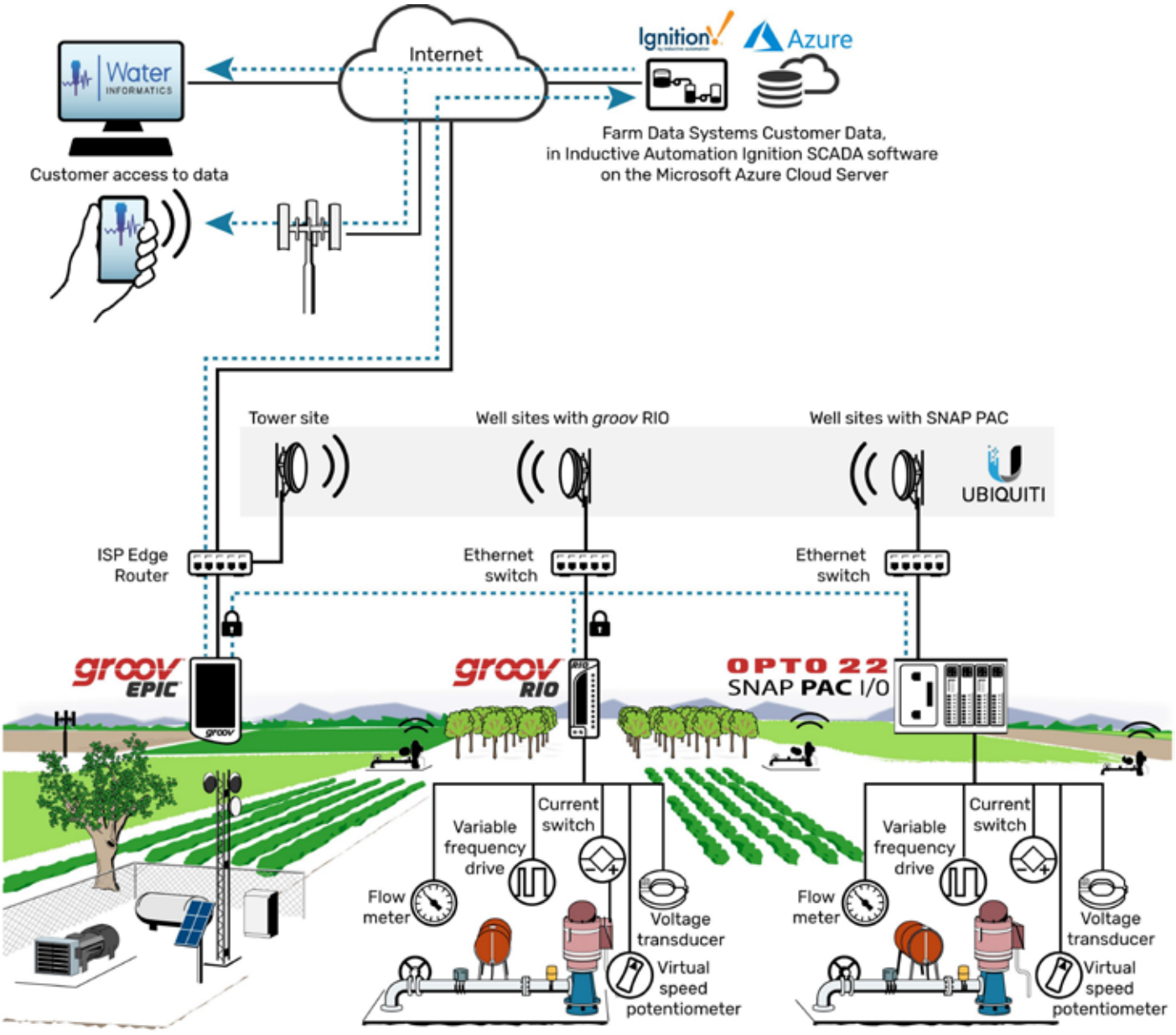
At the tower location a groov EPIC acts as the central controller, running an Opto 22 PAC Control strategy. From a dedicated network at the tower site, data is shared over a VPN from the EPIC, through the internet. The customer data lives in Inductive Automation's Ignition SCADA software on the Microsoft Azure Cloud Server.

The Water Informatics software gives Azcal the ability to access their system via mobile devices. From their phones or other devices with a web browser, Azcal can:

- Remotely start and stop pumps
- Control VFD frequency on four pumps using a virtual speed pot

SOURCE: OPTO 22

Farm Data Systems' software, Water Informatics, gives customers like Azcal data and control from PCs and mobile devices.



SOURCE: OPTO 22

Azcal M&S Ranch system architecture

- Control pressure setpoint virtually on the remaining eight VFDs
- Continuously monitor pump pressure & flow rate
- Track VFD frequency, voltage, current, and power
- Monitor incoming line voltage and well health
- Receive alerts on critical operational issues and general pump activity
- Receive reports on pump activity and water usage

The Result

The manual monitoring and adjustments that used to take Azcal six or seven hours per day now take just a few minutes a day.

"We are thrilled with the FDS solution. I am on top of pump management first thing in the morning before the day gets going. It just works!" says Jake Sheely.

From day one, Jake and Marty have been able to use the FDS Ignition client app for Water Informatics on their phones to power up any of their pumps within seconds. Moreover, they can see the pressures and flows continuously changing and make adjustments without having to jump into their truck to visit any of the sites directly. They also have visibility into their incoming voltage for the first time and receive text alerts any time the system loses power.

And as John notes, every part of the platform, from the Opto 22 I/O, to the Ubiquiti communications, and finally to the Inductive Automation SCADA, can be trusted to be secure and reliable.

The Future

"The combination of Opto and Ignition is very flexible," John says. "I can just keep adding features all day. We've already proposed to come back to add cascading PID control so they don't have to do the remote control themselves. It will do it for them."

Each addition builds Farm Data Systems' ability to help existing and new customers. Says John, "Every time we do something for them, we just add more features for all our customers."

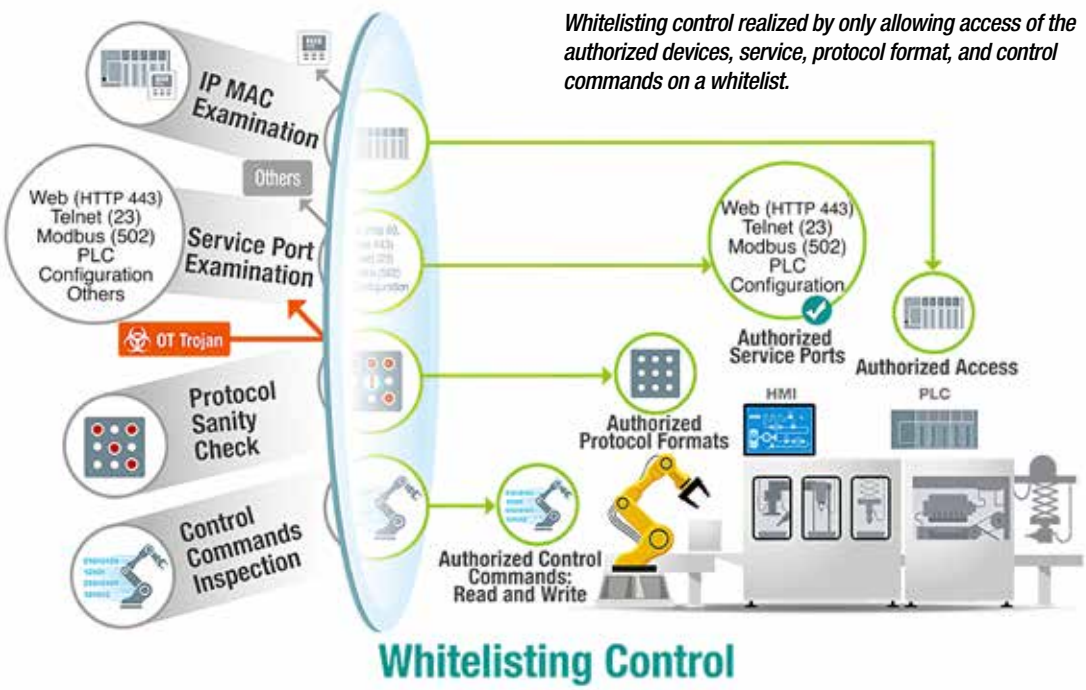
Azcal has exactly the solution they needed at an affordable price. The latest industrial control technologies adapt well to an agricultural setting and start delivering ROI immediately. As a result, Azcal is already rolling out the same technology across their other ranches, with additional features including valve control and irrigation scheduling.

Application and technical article provided by ***Opto 22.***

Visit Website

How to proactively protect your industrial networks

Creating a zone-basis, industrial network architecture can reduce network damage but cybersecurity experts are proposing more proactive actions to protect industrial networks. An industrial intrusion prevention system (IPS) can effectively counteract intrusions and reduce their impacts on industrial systems.



Whitelisting control realized by only allowing access of the authorized devices, service, protocol format, and control commands on a whitelist.

SOURCE: MOXA

INCREASED CYBERSECURITY INCIDENTS HAVE been crippling critical infrastructure and harming businesses. Some are targeted attacks, such as ransomware attacks; however, some are nontargeted incidents, such as contamination through malware that gains access to an unauthorized computer and spreads to the whole industrial control network.

Taking the approach of creating zone-basis industrial network architecture can reduce the damage. In the meantime, cybersecurity experts are also proposing more proactive actions to protect industrial networks. These actions can be realized by an industrial intrusion prevention system (IPS), which can effectively counteract intrusions and reduce their impacts on industrial systems.

What is an IPS?

An IPS is a form of network security designed to detect and block identified threats by constantly monitoring networks, looking for possible malicious cyberincidents and logging information about them. It features deep packet inspection (DPI) technology, enhancing network security visibility, and ultimately helps mitigate risks and protect industrial networks from security threats.

IPS tailored for industrial networks

Although IPS technology has worked very well on IT networks for a while, it is difficult to directly deploy an IPS in OT networks because the first priority of OT networks is availability and performance, while the first priority of IT cybersecurity is confidentiality. Implementing an IPS in OT networks without considering the daily operations requirements of OT engineers could possibly block control commands that are important to production, consequently disrupting operations.

To fulfill the OT cybersecurity requirements, it is essential to empower OT-centric DPI technology. OT-centric DPI can identify multiple industrial protocols and allow or block specific functions, such as read or write access. Based on the identified protocol, an industrial IPS can then prevent any unauthorized protocols or functions. This ensures that the traffic on industrial networks is trusted and non-malicious.

Whitelisting control defines granular access control

Whitelisting control is an approve-and-go mechanism realized by only allowing access of the authorized devices, service, protocol format and control commands on a whitelist. The mechanism ensures that all network activity on industrial networks is authorized and network operators can define granular access controls at different levels depending on operational requirements.

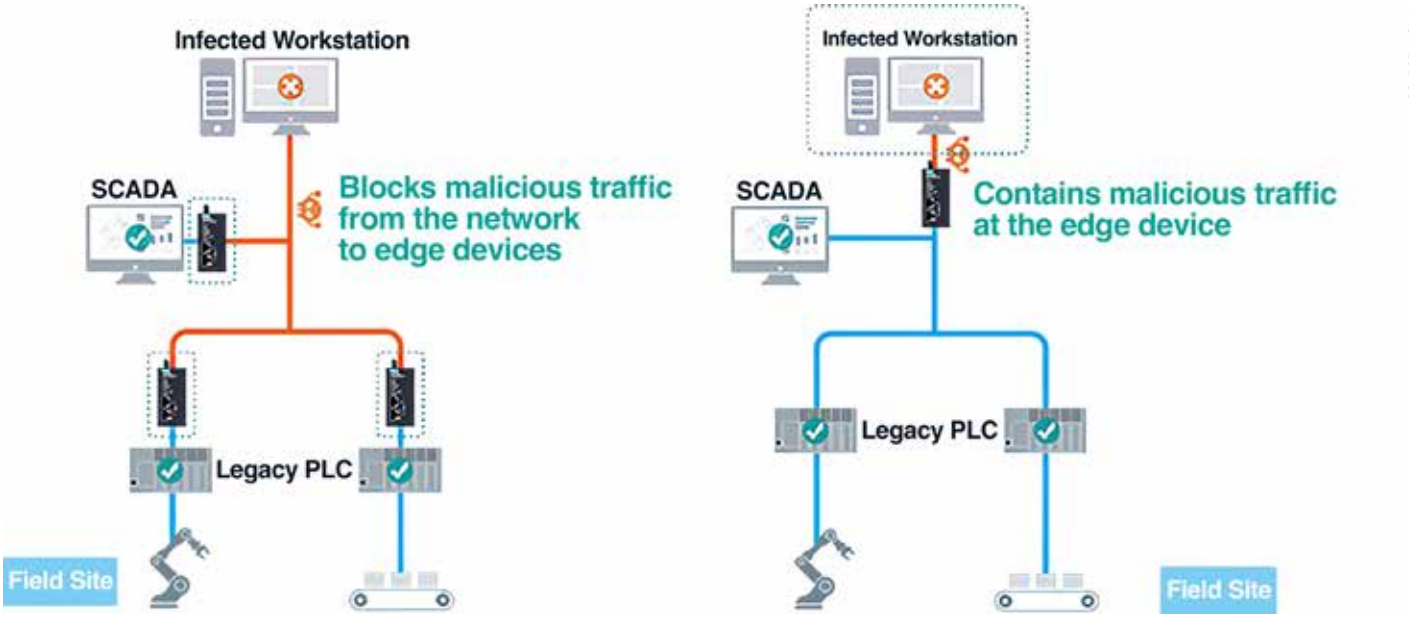
For instance, OT engineers can define a whitelist of devices and services or IP ports that are allowed to access all or part of the entire network. In addition, it is also feasible to define the authorized protocol format to prevent unauthorized commands from passing through networks.

What's more, OT engineers can even define which control commands can pass through the network to reduce human error associated with sending a wrong control command. With whitelisting control, the likelihood of a DoS attack by OT Trojans can be significantly reduced.

Protection Scenarios

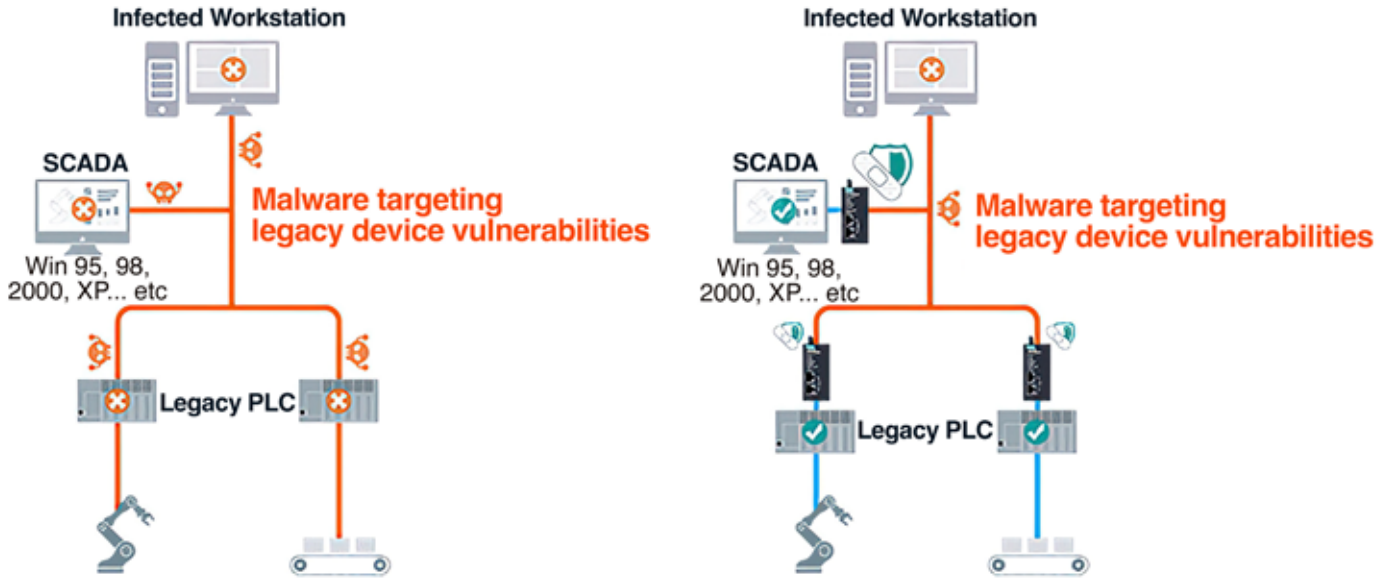
1. Block and Contain Malicious Traffic

An industrial IPS is designed to protect industrial networks by blocking malicious traffic from the network to edge devices and by containing malicious traffic at edge devices. It can be placed in front of critical assets such as PLCs and HMIs to enhance network security



SOURCE: MOXA

Secure Industrial IPS can block malicious traffic from the network to edge devices.



Virtual patching can help OT engineers quickly remedy the vulnerabilities of legacy devices.

and ensure network availability while protecting critical assets from being manipulated by malicious actors. For instance, when there is a workstation being infected with malware, the malware often would find its way to spread to as many devices and networks as possible. It could have probably spread to most of the devices on the networks by the time an OT engineer or network operator notice it.

Therefore, both proactive actions are important to mitigate the risks. One action is to block malicious traffic at the first place when the network is contaminated; the other is to contain it to a manageable degree if it unfortunately occurs.

2. Virtual Patching to Reduce a System's Exposure to Cyberthreats

Frequent patching significantly reduces a system's exposure to cyberthreats. However, it continues to be a critical challenge in OT environments. Devices on industrial control systems are not always available for updates when vulnerabilities are identified. For instance, a production operation keep up and running for a period of time before its next maintenance schedule.

Sometimes, updates are probably not feasible because devices on industrial control systems may have already passed their long life cycle and vendors are not providing updates anymore. Virtual patching technology can help complement existing patch management processes by shielding against vulnerabilities. Virtual patching acts as an agentless emergency security tool that OT administrators and operators can use to quickly remedy vulnerabilities on affected OT equipment.

In order to pursue operational efficiency and availability, it is always important to take cybersecurity into consideration. The thought that OT networks are isolated and secure has been cut down to size by several cybersecurity incidents in manufacturing plants. Two different directions can be taken to enhance network security. One is to ensure that your industrial networks have a secure foundation–secure network infrastructure, which allows authorized traffic to flow to the correct places.

Alternatively, you can identify critical assets and give them layered, proactive protection such as an industrial IPS and whitelisting control.

Roger Chen, Manager of Cybersecurity Market Development, ***Moxa.***

Visit Website

2023 Special Report: industrial automation cables & connectors

Single Pair Ethernet is leading the way by enabling new possibilities for smart factory digitalization. But industry experts point to CAT7 cable innovations, along with application-specific and hybrid solutions, as catalysts for achieving IT/OT convergence and long lasting impact on factory automation applications.

SOURCE: STOCK

Cables and connectors, enabled by Single Pair Ethernet technology, are set to play an important role in IIoT and smart factory connectivity solutions.

INDUSTRIAL CABLING AND CONNECTOR technology solutions have moved center stage with potential game-changers for smart factory applications.

In this special report, the Industrial Ethernet Book has reached out to industry experts to gain their insights into Single Pair Ethernet, along with innovations in cabling and connectors, that are ushering in new levels of factory and IIoT connectivity.

Potent connectivity solutions

CAT7, SPE, Application-Specific Solutions, IP67 and Hybrid Installations.

According to Ralf Moebus, Head of Product Management Industrial Communication at Lapp, the key technical trends influencing the development of the latest generation of Industrial Ethernet cables and connectors are found in five areas.

1. *Cat. 7 for 10 Gbit/s date rates:* Higher data rates are becoming more and more the standard in the factory.
2. *SPE:* Single Pair Ethernet enables Ethernet communication via one single twisted copper pair instead of 2 or 4 pairs.
3. *Application-specific Ethernet cabling:* For use in applications such as Robotics, including the new Type R standard for PROFINET which defines application specific test for use of ETHERNET cables.
4. *IP67 protected Ethernet connectors:* M12D and M12 X for installation of Ethernet devices in the field without cabinet.
5. *Hybrid Installations:* with data and power in the same cable.

Key technology benefits

Moebus explained that these technology solutions offer a series of key technical benefits that are providing solutions for specific applications.

Cat.7 for industrial Ethernet cabling enables higher data rates and higher safety margin for future enhancements of the factory.

Single Pair Ethernet reduces installation effort, saves space and has cost saving potential for the components. Therefore, it makes Ethernet installations for the lowest field levels more cost effective and enables an economical integration of sensors and actuators in the network infrastructure. So it is an important technology to make data from the field accessible for the smart factory.

Application-specific Ethernet Cabling makes Ethernet installations in industrial machinery more endurance since the specific application requirements like mechanical stress or special environmental conditions are considered in the design of the cables.

IP67 protected Ethernet connectors are used for the connection of IP 67 rated Ethernet devices in the field. No cabinet is needed; this reduces cost and saves precious space on the shop floor.

Hybrid installations with data and power in the same cable saves space since only one cable is needed instead of two. The connection and replacement of end devices is quicker since only one connector needs to be connected.

Targeted applications

When asked what specific application areas and networking architectures are these solutions targeting, Moebus noted the following impact on potential applications:

1. Cat. 7 is mainly used for the Backbone of industrial Ethernet Networks, and is the backbone used for Machine to ERP/MES Systems, Machine to Cloud and Machine to Machine communication.

2. Single Pair Ethernet addresses mainly the lowest field level of the factory network. SPE bridges the gap between the sensors and actuators and the automation network or the cloud. By direct SPE integration in these devices they can provide much more information which can be used in other systems like Edge Computers and enable new data driven use cases like predictive maintenance or detailed process surveillance.

3. The new PROFINET Type R Standard is a good example of application-specific Ethernet cabling solutions. The Type R Standard was developed for use in Robotics and ensures that cables work reliably in industrial robotic applications. It describes mechanical test procedures for cables that are used for the PROFINET communication from the robot controller to the end of arm tool on the robot.

4. With IP 67 rated Ethernet connectors the installation of Ethernet devices in the field is possible. Especially directly in the machines, where space is limited, the reduction of boxes and cabinets creates potential to build machines more compact in size. For modern decentralized automation architectures cabinet, less installation is also very supportive.

5. Hybrid Ethernet installations are bringing data communication and also power to the end devices. It is a good solution for applications that need more power than Power over Ethernet can provide. Due to the availability of different cross sections in the cables, it is a scalable solution which can be adopted to the power demand of the individual application. Therefore, hybrid installation is the ideal solution for actuators like smart servo drives.

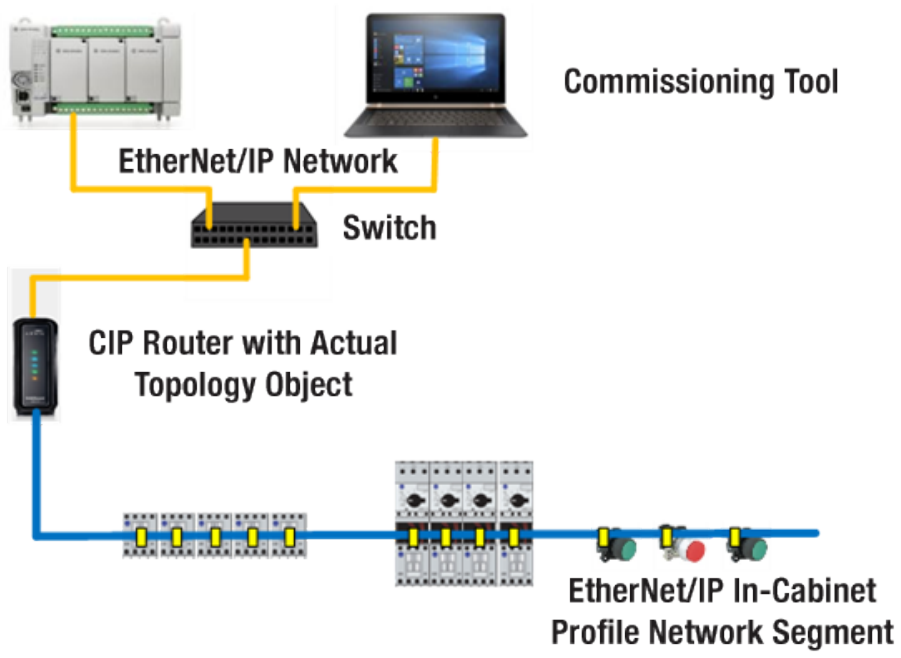
Addressing engineering challenges

These newest solutions are designed to address a series of engineering challenges.

"If powerful factory backbones with up to 10 Gbit/s need to be build up, and the network shall be future proof, than Cat. 7 Industrial Ethernet cables are the right choice," Moebus stated. "If Data from the sensor/actuator Level shall be made available and not very high Data rates are needed than Single Pair Ethernet is a very economical solution."

Moebus said that the movement of robots causes a lot of torsional and bending stresses to cables. In the past the there was no standard that describes these specific mechanical requirements of Cables that are used on robots. With Ethernet cables the fulfill the Type R standard, the Engineer can trust that the PROFINET communication will work reliably.

He added that, for installation of IP67 rated Industrial Ethernet devices outside the cabinet, M12D Coded for up to 100Mbit/s connectors and M12X Coded connectors for up to 10 Gbit/s are a standardized solution. If actuators like servo drives need to be connected to Ethernet than hybrid installation can save space and installation effort.



SOURCE: ODVA

EtherNet/IP In-Cabinet SPE Alternate Topology.

Single Pair Ethernet

Enabling IIoT digital operational technology networks.

"Single Pair Ethernet (SPE) is a crucial enabler of adding the things in IIoT to digital Operational Technology (OT) networks," Dr. Al Beydoun, President and Executive Director of the ODVA, told the Industrial Ethernet Book recently. "These things include contactors, push buttons and motor starters located in cabinets, along with temperature, level, and flow sensors in process plants, and even RFID sensors and gate cylinders in logistics facilities."

"Many of these devices are currently analog with little to no diagnostic or parametrization capabilities. Some of these devices are already on digital fieldbus networks today; however their status and commissioning abilities are oftentimes underutilized leading to a substantial amount of stranded data and untapped operational improvement potential," he said.

Enabling IT/OT Convergence

Beydoun's basic point is that SPE will help enable IT/OT convergence by allowing OT devices to leverage the same underlying Ethernet technologies making it easier to ensure data makes it way up from the field level through gateways and onto SCADA, MES, ERP, and cloud systems.

There are many versions of SPE for different applications with multiple cable lengths and types, speeds, and other factors such as intrinsic safety. SPE encompasses 10BASE-T1L General Purpose SPE applications, 10BASE-T1S in-cabinet applications, and 10BASE-T1L Ethernet-APL applications. Furthermore, there are multiple IEEE SPE standards in addition to those mentioned here.

"The adoption of SPE by both device manufacturers and end users alike is a critical step in unlocking the full potential of IIoT to transform business through more efficient operations. Ethernet-APL is a specialized version of SPE for process automation that includes hazardous area protection, power to field instrumentation, and support for long cable runs of up to 1,000 meters," Beydoun added.

According to ARC's Valentijn de Leeuw, "Felix Hanisch, president of the NAMUR board, mentioned that an Ethernet-APL information highway to the OT systems is critical, and maybe the industry's last chance to enable 'top-to-bottom' digital transformation."

Technology & IIoT benefits

Beydoun said that one of the most clear and important benefits of SPE is the lower cost of cabling relative to standard Ethernet since only a single twisted pair is required. While this may seem small, the difference can add up quickly with factories and plants that have cable runs of hundreds of meters and thousands of communication nodes.

SPE can also reduce the labor and time needed for panel installations with easier to use connectors and fewer wires required. ODVA's in-cabinet resource-constrained device solution is an example as it enables contactors and push buttons to be connected to EtherNet/IP via a SPE multidrop flat cable.

The long cables lengths of up to 1,000 meters, potential reuse of type A fieldbus cable (IEC 61158-2), and up to 10 Mbit/s communication speeds of Ethernet-APL can enable the benefits of Ethernet to be realized at the field level in process plants. One of these advantages is that process instrumentation can easily communicate multiple variables such as temperature, level, and flow from one instrument via the increased bandwidth of Ethernet-APL.

An additional benefit is that SPE minimizes hardware requirements by allowing for usage of smaller physical interfaces, which makes it cost effective to connect to simple devices.

Additional device connectivity opens up possibilities for diagnostics along with development of prognostics. Incentives to utilizing SPE to add devices to Ethernet networks include remote commissioning, digital troubleshooting, and failure prediction via edge and/or cloud enabled analytics.

The cost savings from being able to quickly and easily add a new device to the network and to identify a malfunctioning device without having to physically test for failures adds up quickly between labor savings and downtime reduction. Industrial Ethernet networks, such as EtherNet/IP over SPE can help unlock previously untapped data into insights that can transform operations to increase OEE/ production output, flexibility and quality while also driving down cost.

Impact on Smart Manufacturing

Given that the IIoT is already more than ten years in the making, Beydoun's assessment of the progress and overall impact of the IIoT on industrial automation and smart manufacturing is slow but steady.

"IIoT development progress has been taking place at a steady, yet measured pace over the past decade. The initial steps were organizations working to create a common internal understanding of what IIoT and Industry 4.0 meant and what type of impact they could have on industry," he said. "This was followed by low cost and simple test projects to see what kind of data could be extracted from existing applications and what benefits could be derived from this information by highly trained data scientists.

Further progress was made with IIoT gateways that can consolidate existing operational technology data from the factory floor and then send it to the edge or cloud for analytics and insight development such as operational improvement recommendations."

He said that recent and newer gateway software solutions have been introduced that allow for easier scaling of IIoT gateways across entire facilities. Additionally, easy to use data science software is being made available by companies such as Microsoft to alleviate both the shortage and high cost of data scientists.

Cat7 – The cabling solution for industrial requirements

Cabling technology with a high data rate and a sturdy connection

Future-proof networks are especially required in industrial installations. An important part of this is the use of the correct cabling solution. Industrial cables need to support the high demands of an industrial setting, whether it is a high data rate or a sturdy connection. This is where the new IE FastConnect Cat7 cable from Siemens comes into play.

The new Cat7 cable has been developed for the use in industrial areas. Cat7 performs according to the IEC61156 specifications, ensuring a data rate high enough for industrial purposes (up to 10G Ethernet). Thanks to being designed without an internal cross divider, stripping the cable can be done in a single step with the help of the FastConnect stripping tool. The Cat7 cable also easily connects to the IE FC RJ45 Plug 4x2 and the IE FC M12Plug PRO 4x2. This ensures that all expectations of future-oriented and industrial-grade installation components are met.

To learn more about how to assemble a IE FastConnect Cat7 cable, ***check out the tutorial on YouTube***.

www.siemens.com/fastconnect

The recent trend toward developing solutions that can scale at a reasonable cost is a very encouraging trend that will hopefully transform IIoT from being limited to testing among only a portion of an organization to a critical strategic focus that everyone will play a role in.

Key next steps

"Executives at device manufacturers and end users alike have an opportunity to accelerate the development of IIoT applications by making digital transformation a core part of their operational business strategy." Beydoun said.

"Significant focus, funding, training, and cultural adjustments are necessary to overcome the challenges of developing and adopting new technologies that many current workers aren't familiar with. This approach needs to be undertaken with an understanding that this change will be a long-term shift that will have immense challenges early on and increasing benefits over time."

He concluded that short term results may be limited by the time it will take for full ecosystems to develop, to overcome the learning curve presented by new technology, and to work though the training and inherent cultural resistance to change. Ultimately, a level of risk that organizations don't normally take on will need to be taken on to move from limited IIoT pilot projects to full scale implementations.

"However, the alternative of inaction is to become at a significant disadvantage relative to competitors who do invest in enabling diagnostics, prognostics, and data insights across the entire business, which can help to make business decisions that increase quality, output, and margins over the long run," he said.

SOURCE: HARTING

HARTING T1 Industrial Single Pair Ethernet solutions.

Ethernet Key to Digitalization

Connector and cabling technology will play a major role in digitalization.

"Ethernet is conquering more and more shares of all industrially used communication nodes every year. At the same time, the multitude of different bus protocols is on the retreat." Jonas Diekmann of HARTING told IEB. "All in all, the growing demand for bandwidth down to the lowest field applications can be clearly seen. Connectors and cables play a major role in the development of digitalization. They are the road for all data packets. Without a suitable road, no data traffic."

Diekmann added that, at the same time, the trend of miniaturization can be seen. Devices are shrinking, the infrastructure must also offer smaller solutions than before.

"The last point that must not be ignored, especially in industrial applications: reliability. Interfaces must simply work. This is taken for granted, but unfortunately it is not always the case. And troubleshooting takes a long time and costs money. Transmission rate - miniaturization - reliability: key factors for an IoT-suitable infrastructure," he added.

Industrial RJ45

The well-known RJ45 is the most widely used data connector worldwide both in office applications and in industrial markets. However, the original version of the connection is based on a telecommunications connector that was not very well suited for harsh environments. With its RJ Industrial MultiFeature, HARTING has created a robust and industrially suitable version of the RJ45, which is not only robust and optimally shielded, but can also be easily assembled in the field without special tools.

"User-friendliness is the top priority for the HARTING RJ45, as it is for the preLink cabling system. This separates the formerly fixed connection of cable and connector into a universal, multiple reconnectable connection of cable and connector. A termination block is contacted on the cable, which can then be inserted into all preLink connectors. Whether RJ45 plug, RJ45 socket, M12 plug, soldered PCB socket or coupler," Diekmann stated.

HARTING offers the globally compatible interface in an absolutely reliable version that can transmit high data rates of up to 10Gbit/s, is easy to use and creates absolutely reliable connections.

For smaller applications, the company offers its ix Industrial connector standardized according to IEC 61076-3-124. Diekmann said that it is up to 70% smaller in the device than RJ45 sockets and contributes significantly to the successful miniaturization of devices. It also transmits up to 10Gbit/s with the best possible protection and establishes a secure connection in a space-saving manner.

"In the future, Single Pair Ethernet will fill the last white spots on the Ethernet map. Ethernet via only one pair of copper wires with up to 10Gbit/s transmission speed and with a range of up to 1000 meters. This makes continuous Ethernet communication from the cloud to every sensor a reality," he added.

Focus on applications

All of these robust data interfaces can be used in different market areas. Automation, machinery, transportation, everywhere a strong, reliable und fast connection is demanded.

"The different solutions out of RJ Industrial, ix Industrial and Single Pair Ethernet are working together like a cascade," Diekmann said. "RJ45 is typically used in enterprise and IT level, cabinets and standard applications. ix Industrial is the perfect solution for smaller cabinets, space reduced devices and every application, which needs to be small but connected to standard Industrial or Gigabit Ethernet."

He added that Single Pair Ethernet (SPE) reaches the "last mile". Without a protocol and system break, without gateways ethernet can communicate straight to the edge, if necessary, in real-time. All together, they enable building the infrastructure for IIoT communication.

Engineering challenges

Diekmann said that the I/O interface of a device is often the biggest part of its PCB. If there would be a smaller, but equally powerful and trusty connectivity solution, engineers can reduce the size of housings more effectively. Many parts of an automation concept are using RJ45 interfaces, but in the past, cheap infrastructure caused a lot of interruptions and network issues. One solution is to level up and use a product such as the HARTING RJ Industrial MultiFeature solution.

"You want to upgrade an old machine concept with vision systems, but a bus System does not support necessary data rate? Use SPE and our internationally standardized (IEC 63171-6) interface T1 Industrial. It's compatible with all vendors, using the IEC standard, much smaller stand 4 or 8 wire solutions. Perfect for the field," Diekmann said.

Learn More

If you want to learn more about future industrial communication innovations, sign up for Industrial Ethernet Week 2, held from the 21st to the 23rd of February 2023. Interesting guests and HARTING experts will discuss all of the challenges and opportunities with Industry 4.0.

Visit Website

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

Connected services: autonomous all-in-one laser centres

As one of the world's largest suppliers of machine tools, TRUMPF is focusing on autonomous concepts in the future. The TruLaser Center 7030 model integrates all laser cutting processes in a single machine for the first time, using Single Pair Ethernet as the backbone for IoT data services.

IN ORDER FOR AN ALL-IN-ONE LASER CENTER to work autonomously and also correct errors, it is necessary to combine and evaluate all the necessary data. HARTING and SICK are supporting machine tool supplier Trumpf with intelligent camera sensors and smart single pair Ethernet infrastructure for connected services.

Customer needs in mechanical engineering are changing; batch size 1 is now the expected standard, flexibility is a top priority. Maximising system availability is just as important as making service support evenmore predictive and calculable.

The TruLaser Center 7030 from TRUMPF handles the entire process - from the drawing to the sorted part: loading, cutting, removing, sorting, stacking. Ideally, it will do this completely autonomously in the future.

SOURCE: HARTING

Intelligent camera sensors and smart Single Pair Ethernet infrastructure helps enable connected services.

The challenge: machine downtime due to accompanying processes

Even on a completely tested machine, there will be problems sooner or later due to upstream and downstream processes in real operation at the customer. Manufacturers need all sensor, machine, system and camera data in order to find the causes of errors.

The first step towards this form of autonomy is to understand where unknown problems come from in real operation. This requires a lot of cameras to film the machine and detect the fault remotely. This monitoring often does not yet take place to that extent.

The solution: seamless communication between field level and IoT services

Sensor manufacturers rethink sensor data

In addition to TRUMPF's own sensors, manufacturers such as SICK supply the appropriate camera technology. The experts at SICK are aware that they have to rethink sensor data: no longer in isolated process data, but in systems where the IoT world has to be supplied with high-quality data.

The image data must be linked to all machine data for correct evaluation in real time. The infrastructure required for this must be able to withstand the data volumes, even for medium-sized customers.

Cross-manufacturer data transfer in real time must be possible

For real-time data availability, the extension of OPC UA to include Time-Sensitive Networking (TSN) is being developed as part of the OPC Field Level Communication Initiative. TSN takes over the control of priorities of the individual data packets and provides procedures for queue handling. Sensor data thus become available at the required data rates - the field level can be integrated without hurdles.

Single Pair Ethernet

Being able to sell an autonomous machine economically involves sensor technology, infrastructure and also the necessary connectors and cabling.

HARTING, a specialist in connection technology, offers Single Pair Ethernet (SPE) as a cabling solution. SPE is a robust and material-saving Ethernet cabling that is intended to replace the fieldbuses commonly used to date in the long term. The new industrial standard allows a data transmission rate of up to 1GBit/s with only one pair of wires.

SPE makes the barrier-free connection of devices up to the field level possible and for the first time allows the cost-effective use of Ethernet in the entire industrial automation. SPE is thus the necessary backbone for continuous networks from the sensor to the cloud.

Industrial Ethernet Week 2: February 21-23, 2023

Many industrial companies today are facing the transition to the Industrial Internet of Things (IIoT). Design engineers, factory installers and other professionals are facing new challenges in their day-to-day business due to new technologies, new use cases and new business models. They need to keep up to date with trends and solutions to develop ideas and find next steps in the transformation for their own business.

As one of the key players in the global market for Industrial Ethernet connectivity solutions, HARTING aims to support precisely this target group with the INDUSTRIAL ETHERNET WEEK. Participants in the event will learn about ideas and perspectives from pioneers and thought leaders, and get an update on the latest technologies, solutions and trends.

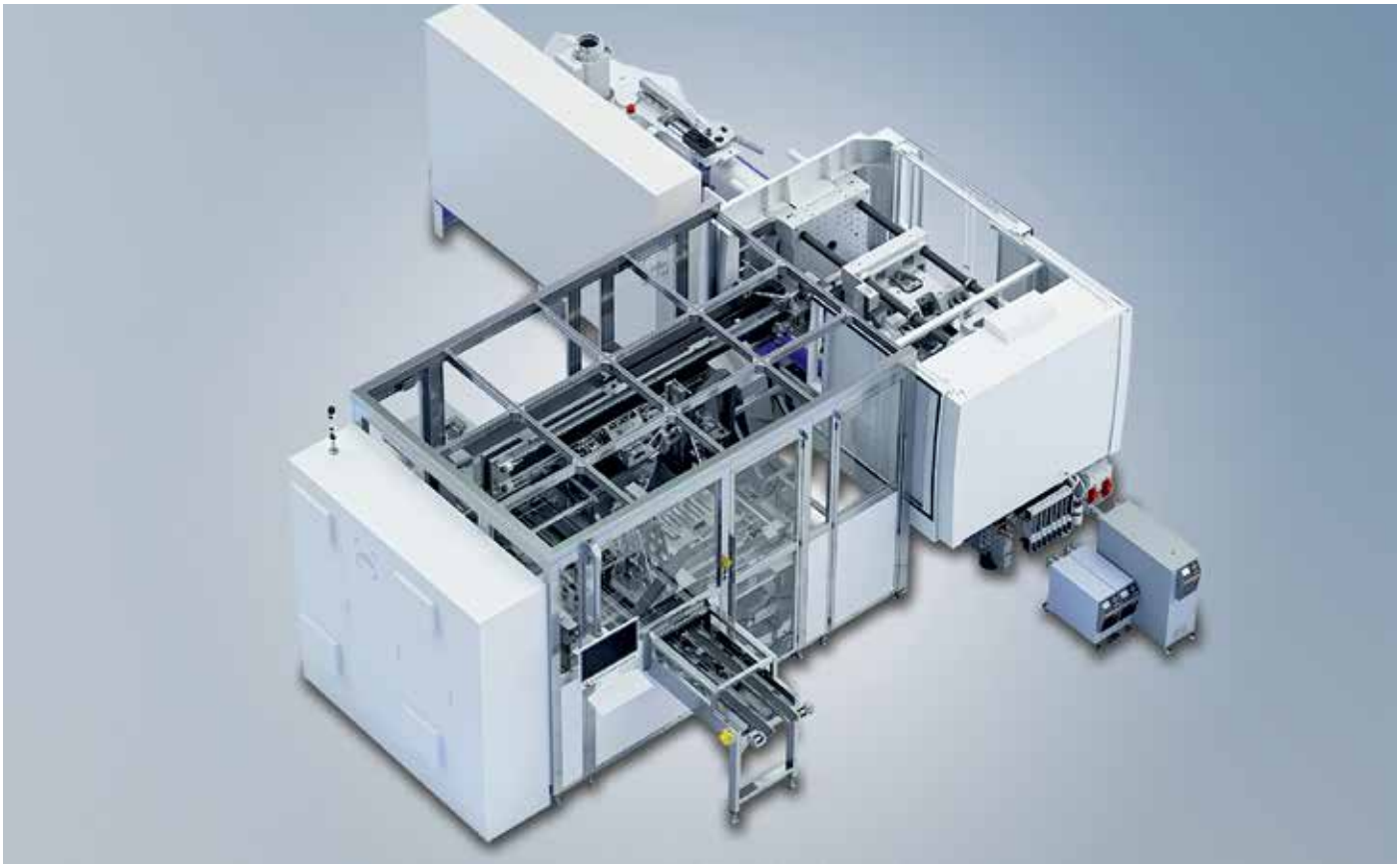
Registration: https://www.harting.com/DE/en-gb/harting-industrial-ethernet-week-2023?source=iebmedia

*Application article provided by **HARTING**.*

Visit Website

One-cable solution: efficiency for modular machine building

One cable technology and EtherCAT P minimize system cabling for a medical equipment manufacturer, and ensure significant increases in efficiency. A major benefit is standardization on OCT for drives and EtherCAT P at the I/O level, significantly reduced the wiring effort and improving decentralized power distribution.



SOURCE: MA MICRO AUTOMATION

With its modular machine concepts, MA micro automation benefits from PC-based control as a flexible automation platform, as well as from the equally flexible installation concepts with EtherCAT P and One Cable Technology (OCT). Picture: © MA micro automation

SPECIAL MACHINE BUILDER MA MICRO automation GmbH designs custom systems for medical technology from basic configurations and a wide variety of modules. Not only does this require a system concept that is consistently modularized at every stage of its core tasks, it also requires control technology and system cabling that can be flexibly configured. Beckhoff provides this with PC-based control, One Cable Technology (OCT) and EtherCAT P, ensuring significant increases in production efficiency.

Based in the German town of Sankt Leon-Rot, MA micro automation manufactures assembly, adjustment and testing systems for medical technology and visual inspection. "We aim to rely on standard modules wherever possible and supplement these with specially developed individual components as required," explains Dirk Striebel, Head of Operations at MA micro automation, outlining the basic idea behind modular machine construction.

As a general rule, the systems are based on the company's CENTAURI IVD and CERES POC machine platforms, which can be adapted to suit a project's respective needs and requirements. This explains the wide range of possible applications for the systems. MA micro automation supplies manufacturing, testing and assembly systems for a wide range of applications, including diagnostic consumables, medical injection-molding components, insulin pens and auto injectors, as well as pipette tips and reaction vessels.

To meet market requirements for high precision and accurate assembly, including those for optical assemblies, the special machine builder relies on its own image processing and software systems, as well as its large image processing and software team.

Mass production with maximum precision

A notable solution based on CENTAURI IVD was developed to meet the pandemic-related increase in demand for pipette tips. These are considered both bulk and precision items, as they are used in laboratory diagnostics to draw precisely defined quantities of liquid and transfer them to test containers. The wall thicknesses and openings at the tip measure just a few tenths of a millimeter each, meaning any discrepancy could affect the diagnostic result. As Dirk Striebel explains, "It is essential to watch out for issues like burrs or deformations during the production process, and to reliably eject any pipette tips with visible flaws." This is why MA micro automation often integrates a variety of inspection stations into the production process, enabling the company to call upon

the necessary image processing expertise in-house.

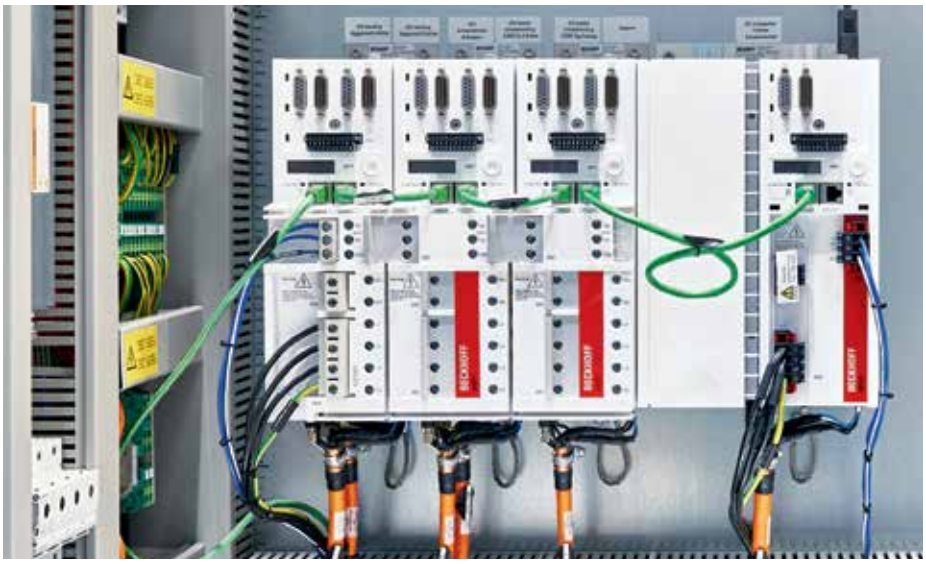
To avoid injection molding machine downtime during 24/7 operation, MA has integrated a buffer storage system between the machine and the downstream processes at the customer's request. "This offers enough capacity to cover 10 minutes, which is long enough to refill labels or filters as needed," explains Dirk Striebel. The faster cycle time of the system compared to the injection molding machine means the buffer storage system empties itself afterwards.

With the second CERES POC platform, MA micro automation has targeted the market for point-of-care (POC) rapid tests in the field of patient-related laboratory diagnostics. These highly flexible production lines cover the entire process chain, from plastic molding to testing and packaging. Systems based on this platform can produce over 30 million tests per year.

If neither of the two machine platforms is suitable for technical reasons, the specialized machine manufacturer also handles the implementation of custom project solutions as a general contractor. According to Dirk Striebel, "With our extensive portfolio of standardized modules and solutions, we provide our customers with the flexibility they need to create the solution they want." From various optical inline inspections, pipette filter assembly, fully automated connectivity with upstream and downstream production processes (rack, aging storage, packaging, etc.), and the fully automated intralogistics process, everything can be defined via the corresponding configurator.

SOURCE: BECKHOFF

With a high density of sensors and actuators in the field, system cabling with the hybrid cables and EtherCAT P saves a lot of wiring time during installation. Picture: © Beckhoff



SOURCE: BECKHOFF

OCT also reduces the wiring effort for the AX5000 Servo Drives. Picture: © Beckhoff

SOURCE: BECKHOFF

No need to pick one or the other: EtherCAT P and EtherCAT can be combined in the field. The IP67-rated EPP9001-0060 Box separates EtherCAT P into EtherCAT and power if required to allow the use of standard EP box modules.

PC-based control in in-vitro diagnostics

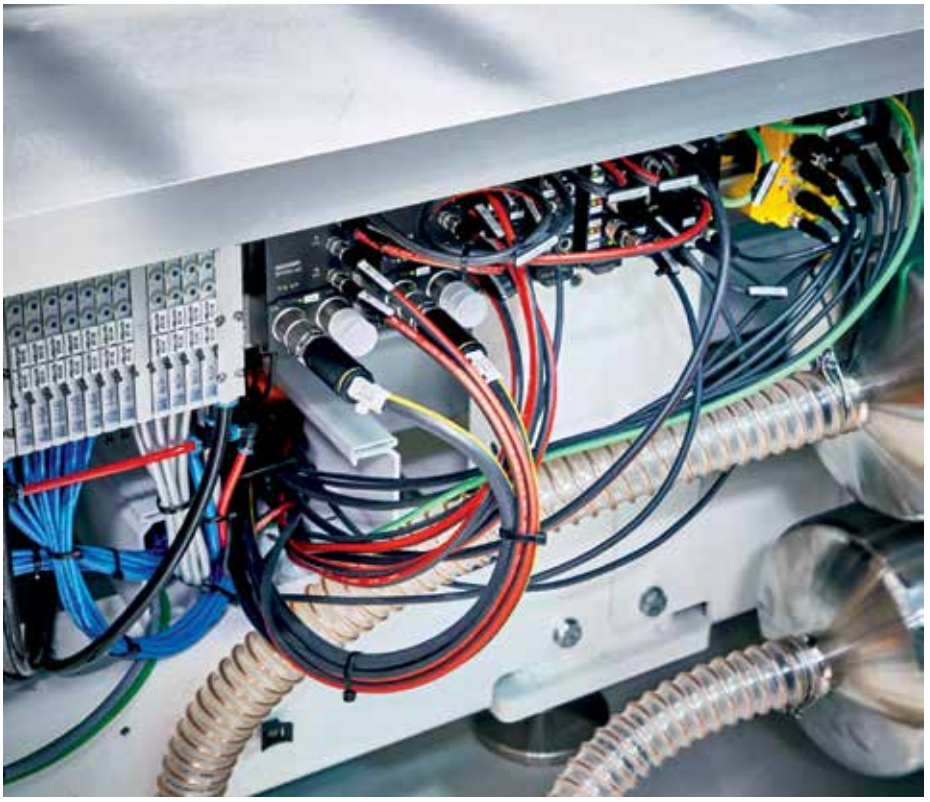
Commissioned as a general contractor, MA micro automation designed a flexible pipette-tip automation solution with an increased output rate for a global player. The brief was to implement a flexible automation solution for production, allowing pipette tips packed in racks to be offered to the in-vitro diagnostics market. To this end, the individual pipette tips had to be fed from the bulk material in a cycle time of less than 0.1 s, separated, inserted automatically into racks and ultimately packed.

The flexibility in terms of pipette variants is based on injection molds with up to 128 cavities, allowing various pipette tips to be produced on the injection molding machines. The pipettes are removed via an axis that can be adapted to the respective number of cavities in just a few steps, making the removal axis universally scalable. The required grid dimension of the final rack is achieved via a special handling strategy so that the pipette tips reach the racks after only a few automation steps before being transported further via the XTS linear transport system, for example.

Scalable automation promotes modularity

The basis of all these system variants is an automation solution in the form of PC-based control. This has been the same approach since 2010, as Dirk Striebel emphasizes: "We use Beckhoff components as standard wherever possible, unless customers request a different control system." As it turns out, this is rarely ever the case.

MA micro automation now relies on the full range of Beckhoff products, including AX5000 and AX8000 Servo Drive systems, XTS for intelligent material transport, EtherCAT and EtherCAT P Box modules, embedded and industrial PCs, and control panels such as the CP3921 in customer-specific designs. According to Dirk Striebel, special machine builders should adhere to proven standards to become more efficient and avoid errors: "Beckhoff system components meet these requirements in every respect, from project planning and development to completion of the systems."



SOURCE: BECKHOFF

Another advantage of EtherCAT P is that the associated IP67 Fieldbus Box modules are so compact that they can be integrated directly into the machine bed. Pictured here in the background is the XTS transport system that connects the individual stations.

Efficient cabling: OCT, ENP & ECP

Dirk Striebel sees a major benefit for the company in the consistent standardization on OCT for the drives and EtherCAT P at the I/O level. Their introduction has significantly reduced the wiring effort and improved the decentralized power distribution by the EP9224-0037 four-channel power distributors from the B17-ENP hybrid connector via EtherCAT P. "In total, these measures have significantly reduced our installation effort and the resulting costs by some 15 to 20%," specifies Dirk Striebel. The pre-assembled cables, which MA micro automation also sources from Beckhoff, also play their part.

Depending on the system size, One Cable Automation (OCA) from Beckhoff saves up to 100 lines with the ENP hybrid lines and EtherCAT P. These no longer have to be assembled, routed and placed in the control cabinet, which in turn reduces potential sources of error. "Typical errors when connecting cables can be reduced further still with the various coding options of EtherCAT P," adds Udo Gruber, head of the Beckhoff sales office in Mannheim.

The I/O box modules and system lines can be coded using different color rings. It is also possible to clearly identify the hybrid connectors with confidence through mechanical coding of the bayonet catches. "We can take all of this into account when ordering our EtherCAT P Box modules and preconfigured cables directly from the factory," says Udo Gruber.

Dirk Striebel adds: "With regard to power distribution, issues such as large cable lengths and the resulting voltage drops virtually take care of themselves with EtherCAT P." Likewise, with the EtherCAT Box modules for power distribution, such as EP9214 and EP9224, various data concepts can be implemented, adapted or completely redesigned. In addition, the extensive diagnostic functions of EtherCAT and the EtherCAT P technology expansion simplify troubleshooting in the event of a fault.

Just about everything has been factored in to ensure that the final assembly can be completed largely without a skilled electrician. "This is definitely the way things seem to be going in the world of 24 V sensor/actuator installation," agrees Dirk Striebel. He is already thinking one step ahead here and striving to simplify the assembly, disassembly and reassembly of the systems: "The aim is to reduce highly cost-intensive activities at the end customer's site, and to shorten system throughput times in the final assembly stage. Here, too, Beckhoff will once again make its contribution as a long-standing, reliable partner and supplier of system components."

SOURCE: BECKHOFF

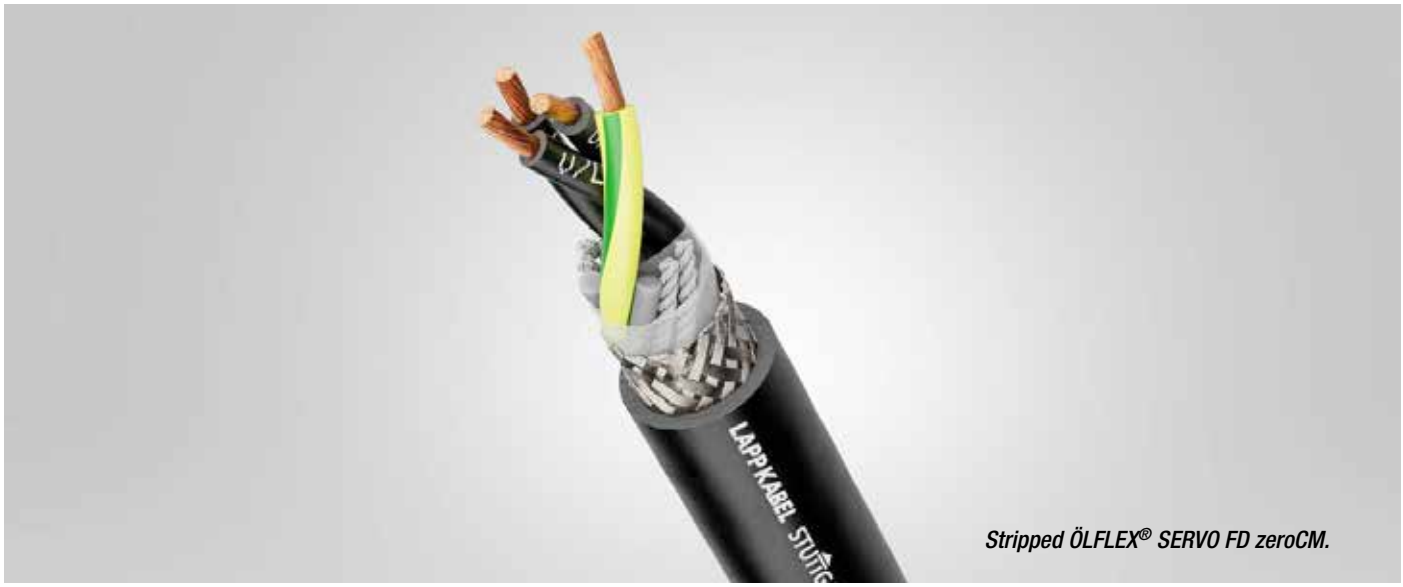
The customized CP3921 Control Panel in conjunction with PC-based control and TwinCAT HMI provides a user-friendly operator interface and short changeover times.

Application article by ***Beckhoff Automation.***

Visit Website

zeroCM® cable technology reduces interference currents

New technology does not eliminate the cause of EMC interference, but it does address significant points at which interference is introduced into a system. A new cable design enables equalization currents to be reduced by up to 80% at the frequency inverter output and on parallel paths such as data lines.



SOURCE LAPP

Stripped ÖLFLEX® SERVO FD zeroCM.

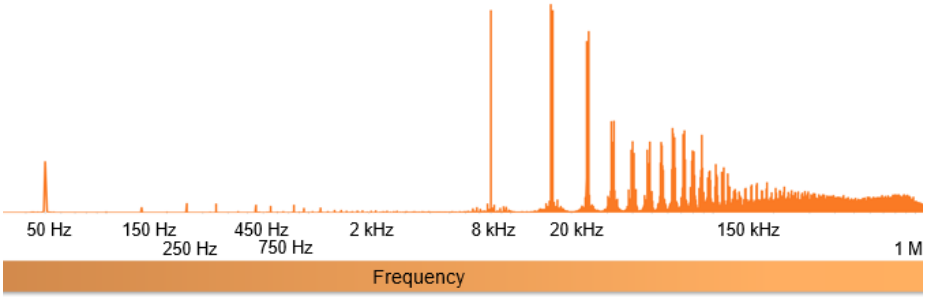
IN THE SMART FACTORY, MACHINES AND systems are increasingly networked. As a result, the topic of electromagnetic compatibility (EMC) is also becoming increasingly important. Especially in industrial plants where frequency converter-controlled motors are used, undesirable currents can increasingly occur on the equipotential bonding (PA) or protective earth (PE) cables. A new, innovative cable design from LAPP reliably reduces leakage currents and makes a decisive contribution to improved EMC in machines and systems.

Nowadays, electric motors in process automation are operated exclusively by means of frequency converters. In addition to the advantage of variable speed, this type of control offers considerable improvements in terms of energy and process efficiency. However, due to the principle of control, undesirable side effects occur and leakage currents are generated. The more components are involved, the greater the risk of such disturbances. At the same time, the installation spaces in machines and systems are becoming smaller and smaller. In order to avoid expensive production downtimes in the smart factory, it is therefore best to consider the topic of EMC during the planning phase.

Cable design rethought

LAPP has demonstrated how interference within connection solutions can be virtually eliminated as part of the "PEPA" research project of the German Federal Ministry of Economics and Climate Protection. In addition to LAPP, SEW-EURODRIVE, BLOCK, Danfoss, MAGNETEC and the Technical University of Darmstadt are involved in the project. Here, LAPP is leading work package 4: Couplings between neighboring cables as well as with plant components. Measurements and optimizations of the cable design. The aim of this work package is to promote cross-company research on a complex topic from the automation/drive world, in which the correct selection of connection components and their professional installation are particularly important.

The subject of the investigation was the question of why undesirable currents very often occur on the potential equalization lines (PA) or protective earth lines (PE) in industrial plants in which frequency converter-controlled motors are used. Due to the clocked control (pulse width modulation), interference currents in the range of about 3 kHz to 1 MHz are excited, which flow off via housing parts, PA/PE conductors/networks and, in the worst case, via the shielding of data lines in the direction of earth potential or to the source. High-frequency equalizing currents with an amplitude of 10 A or more are not uncommon. The consequences are inadmissibly high currents on the protective earth and thus supposedly faulty tripping of residual current circuit breakers (RCD) or impairment of data communication if, for example, the equalizing currents flow over the copper shield of a data line. These faults are difficult to find because they do not follow a systematic approach. LAPP has therefore set itself the goal of investigating the physical coupling mechanisms within motor connection cables and deriving a new type of cable design from this. The result of this development is zeroCM® technology.



Typical spectrum of leakage currents measured on protective earth and equipotential bonding conductors.

Cable technology put to the test

The origin of the innovation was to put the status quo in cable technology to the test: previous designs tended to be trimmed to small outer diameters and optical symmetry. Until then, the problem of EMC was always solved by shielding. LAPP took a different approach with zeroCM technology: the cable is visually asymmetrical, but 100% electromagnetic symmetry is achieved. Ultimately, this means that even less shielding is required.

The secret of zeroCM® technology is a special, innovative stranding technique. Three phase conductors are arranged symmetrically and stranded in an inner layer. In addition, at least one protective conductor is stranded in an outer layer with opposite stranding direction around the three phase conductors in a specific lay length ratio. The insulation of the conductors is capacitance-optimized and consists of polyethylene, polypropylene or a foamed variant. Between the inner layer and the outer layer there is a separating fleece. This design achieves perfect electrical symmetry, which reduces magnetic radiation and greatly reduces internal couplings. The first prototype cable with a new cable design is the ÖLFLEX® SERVO FD zeroCM. It is especially suitable for use in conjunction with frequency converters.

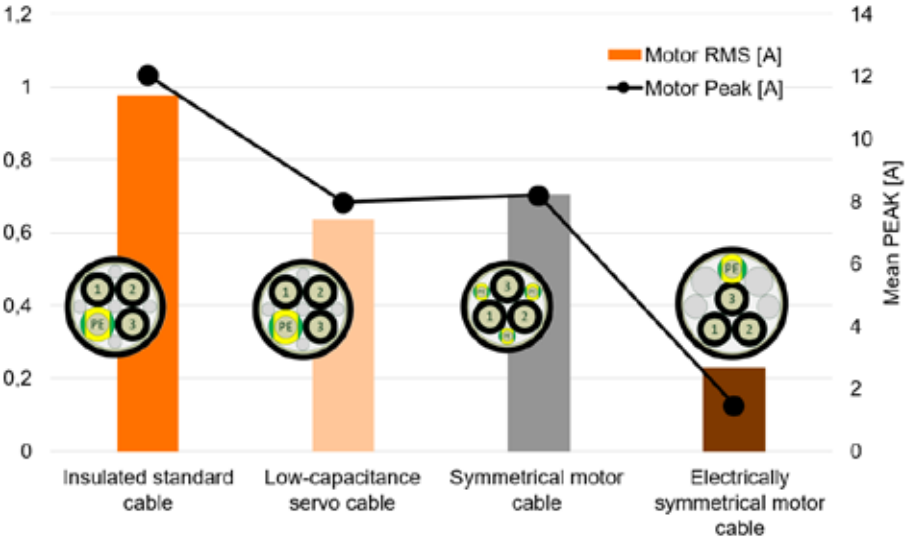
Successful trial

The effectiveness of the new ÖLFLEX® SERVO FD zeroCM cable was confirmed in test setups at the project partners as part of the PEPA research project. In addition to investigating an EMC-optimized installation of components, the role of the output line was evaluated, among other things. For comparison, an identical test setup with a drive system with potential equalization as well as parallel signal line (ProfiNet) were selected.

A shielded PVC-insulated standard cable, a low-capacitance servo cable, a symmetrical motor cable with three protective conductors and the new zeroCM® cable with optimized structure were compared. The results were clear. The best values in terms of leakage current at the converter output were achieved by the low-capacitance design of the zeroCM® cable. The generated leakage currents represent an additional load for the frequency inverter and all components involved and should therefore be kept as low as possible.

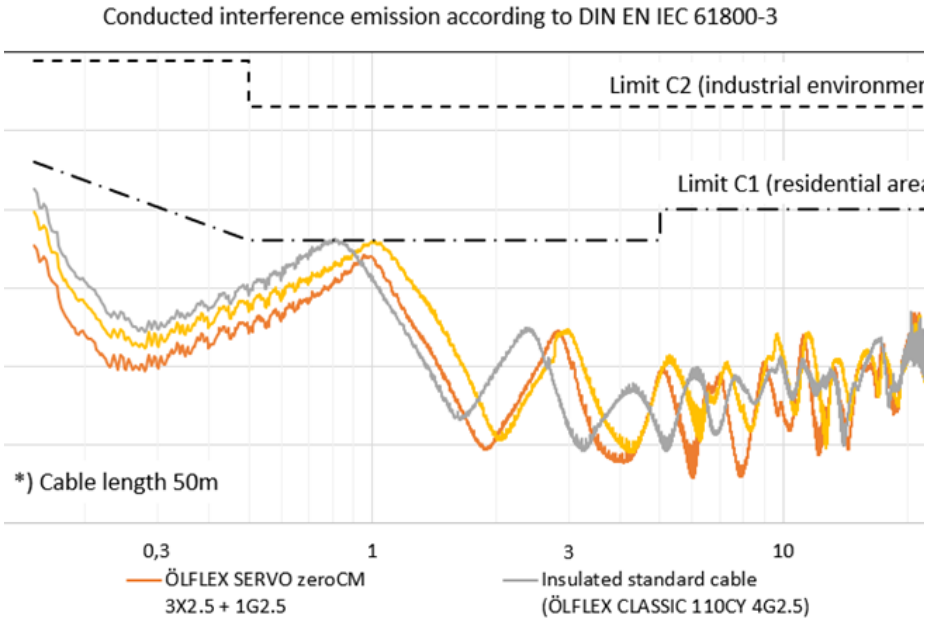
Furthermore, the interference current flowing via a parallel signal line was investigated: Here, too, the use of the zeroCM® cable favors the expression of the lowest possible interference currents. The investigations at the project partners also resulted in clear recommendations for the EMC-optimal installation of frequency converters, such as a low-impedance, RF-compatible and continuous equipotential bonding between the frequency converter and the drive.

The shield connection with EMC-compatible plugs or flat shield connection, such as with the SKINTOP® BRUSH EMC cable glands used, is of major importance here.



SOURCE LAPP

Leakage current (rms and maximum level) measured at the frequency inverter output for a 4 kW drive and 50 m cable length



The measurement curve shows conducted interference emission of a frequency inverter according to DIN EN IEC 61800-3 and the improvement when a zeroCM® servo cable is used.

Longer cable lengths possible

In summary, zeroCM® technology does not eliminate the cause of EMC interference, but it does address precisely one of the significant points at which interference is introduced into the system environment. On the one hand, the new cable design enables equalization currents to be reduced by up to 80% at the frequency inverter output and on parallel paths such as data lines. On the other hand, reduced cable-charging currents ensure reduced load on and in the inverter itself. For example, longer cable lengths can be laid without operating the frequency inverter outside its (EMC) specifications. In addition, zeroCM® technology prevents the occurrence of voltage levels on the ground/earth potential (ground voltage) on the consumer side. This is particularly important when, for example, sensitive sensor technology such as analog encoders are used.

Although the new cable may seem unfamiliar when it is first assembled, the cabling remains as simple as usual, or the effort is even reduced compared to the ground-symmetrical cables with a third of the protective conductor. LAPP's goal is now to equip a portfolio with zeroCM® technology; hybrid lines are next.

Stefan Hilsenbeck, Senior Engineer Advanced Technology, ***Lapp Holding AG.***

Visit Website

Why an IP Rating matters when specifying an industrial switch

Manufacturers of Ethernet switches and other industrial networking devices often make vague claims like "weatherproof" or "dust-resistant" about their products. But how do you know if these claims are legitimate? Are the devices truly safe? Is there a certification that is trusted industry-wide? Fortunately, there is.

1st Digit	Intrusion Protection	2nd Digit	Moisture Protection
0	No protection.	0	No protection.
1	Protected against solid objects over 50 mm, e.g. accidental touch by hands	1	Protected against vertically falling drops of water, e.g. condensation
2	Protected against solid objects over 12 mm, e.g. fingers	2	Protected against direct sprays of water up to 15º from the vertical
3	Protected against solid objects over 2.5 mm, e.g. tools & wires	3	Protected against direct sprays of water up to 60º from the vertical
4	Protected against solid objects over 1 mm, e.g. wires & nails	4	Protected against water splashed from all directions, limited ingress permitted
5	Protected against dust, limited ingress, no harmful deposits	5	Protection against low pressure jets of water from all directions, limited ingress permitted
6	Totally protected against dust	6	Protected against strong jets of water, e.g. on ship's deck, limited ingress permitted

SOURCE: ANTAIRA

THE INGRESS PROTECTION (IP) RATING system was developed in 1976 by the European Committee for Electro Technical Standardization. Basically, an IP rating shows how safe it is to use an electrical or mechanical product in a unique environment or application. The IP rating system is widely adopted by electrical and mechanical engineers, especially in North America, since many consumer products must indicate an IP rating to qualify for UL or CSA's safety standards.

An IP rating is made up of two digits that act as a grading system, such as "IP67" or "IP59," indicating a device's level of protection or resistance against various intrusions. The first digit of an IP rating is a number that describes the object's protection against solids, such as dust and dirt, with 0 yielding no protection and 6 offering the most protection. The second digit of an IP rating describes the level of protection against moisture ingress, including drips, spray or full submersion, again, with 0 symbolizing no protection and 9K providing the most protection.

If a higher IP rating is assigned to a device, it does not automatically imply all lower resistance tests have been passed. For instance, IP67 does not mean the device is resistant to 0-6 in the first digit, and 0-7 in the second digit. Therefore, it is not uncommon for a device to obtain multiple IP certifications. Occasionally, the two digits are followed by a letter denoting other information. Adding a letter is optional and not common, however you should be aware of their meaning. When a manufacturer adds a letter it can signal protection against access to a hazardous part, including back of hand (A), finger (B), tool (C), or wire (D). It can also refer to additional protection, including oil resistant (F), high voltage (H), water testing (M), standing still (S), or weather conditions (W).

You may also see an "X". This indicates that a rating has only been provided for one of the two main ingress types -- foreign body or moisture -- but not for the other. Take, for example, IPX7. Here, a moisture resistance rating of 7 has been assigned to the device, but no rating is provided against foreign body ingress. Alternatively, an IP3X means a 3 rating against foreign body intrusion, but no moisture resistance rating is stated.

It is important to note that manufacturers themselves cannot apply an IP rating to their devices, except in rare cases. All testing must be administered by an independent, certified agency. Not only does a third-party process lend credibility to a manufacturer's claims of protection, but it also clears up vague or ambiguous marketing lingo like "waterproof". Also, it is worth noting that an IP rating indicates how well a device operates when a solid object or water enters its enclosure — it does not infer the enclosure is entirely immune to ingress regardless of the rating.

IP Ratings for Antaira's switches

The physical conditions of the manufacturing floor—from the steamy realms of papermaking to the twisted mazes of hot piping in oil refineries, make it a hostile environment for industrial switches to survive. While some industrial facilities are temperature controlled and clean, the vast majority are not.

Many are continuously very hot and dusty. In other cases, industrial switches can be installed where frequent washdowns occur, particularly in food-handling environments where sanitation and cleanliness are of paramount importance. Others combine intense heat with excessive humidity. Outdoors, challenges are further complicated by adverse weather.

This is bad news for Ethernet switches. Moisture in an Ethernet switch can lead to corrosion, shorts, shock or even fire hazards. Dust ingress will cause irreparable damage. Prolonged exposure to high temperatures will break down an Ethernet switch's circuits.

Certified resistance to moisture and dust is a requirement if you want your Ethernet switch to run optimally with a minimum of network downtime. Antaira builds industrial Ethernet switches hardened against extreme operational conditions. Antaira industrial switches can withstand exposure to dirt and dust, rain, snow and electronic interference. Antaira industrial switches are enclosed in corrosion-resistant metal casings that prevent crushing damage and ingress of contaminates. Many also feature an extended operating range of -40°C to 70°.

Antaira's most rugged Ethernet switches carry the IP67 rating, meaning they are completely dustproof, and making them safe if they end up in the pathway of water projectile and spray. M12 connectors on our IP67 industrial switches ensure a tight, robust connection guarantying reliable operation where they are subject to high vibration and shock in dust, liquid, or gas-laden environments.

Henry Martel, Field Application Engineer, ***Antaira Technologies.***

Visit Website

Communication and safety challenges facing mobile robots

To solve many communication and safety challenges mobile robot manufacturers must establish a wireless connection, send data over different networks, ensure safety, connect to CAN systems, and securely access the robots remotely. Each installation must be re-assessed and adapted to meet the on-site requirements.

MOBILE ROBOTS ARE EVERYWHERE, FROM warehouses to hospitals and even on the street. Their popularity is easy to understand; they're cheaper, safer, easier to find, and more productive than actual workers. They're easy to scale or combine with other machines. As mobile robots collect a lot of real-time data, companies can use mobile robots to start their IIoT journey.

But to work efficiently, mobile robots need safe and reliable communication. This article outlines the main communication and safety challenges facing mobile robot manufacturers and provides an easy way to overcome these challenges to keep mobile robots moving.

SOURCE: HMS NETWORKS

Communication and safety are key goals for mobile robot manufacturers.

What are Mobile Robots?

Before we begin, let's define what we mean by mobile robots. Mobile robots transport materials from one location to another and come in two types, automated guided vehicles (AGVs) and autonomous mobile robots (AMRs). AGVs use guiding infrastructure (wires reflectors, reflectors, or magnetic strips) to follow predetermined routes. If an object blocks an AGV's path, the AGV stops and waits until the object is removed.

AMRs are more dynamic. They navigate via maps and use data from cameras, built-in sensors, or laser scanners to detect their surroundings and choose the most efficient route. If an object blocks an AMR's planned route, it selects another route. As AMRs are not reliant on guiding infrastructure, they're quicker to install and can adapt to logistical changes.

Establish a Wireless Connection

The first challenge for mobile robot manufacturers is to select the most suitable wireless technology. The usual advice is to establish the requirements, evaluate the standards, and choose the best match.

Unfortunately, this isn't always possible for mobile robot manufacturers as often they don't know where the machine will be located or the exact details of the target application.

Sometimes a Bluetooth connection will be ideal as it offers a stable non-congested connection, while other applications will require a high-speed, secure cellular connection. What would be useful for mobile robot manufacturers is to have a networking technology that's easy to change to meet specific requirements.

The second challenge is to ensure that the installation works as planned. Before installing a wireless solution, complete a predictive site survey based on facility drawings to ensure the mobile robots have sufficient signal coverage throughout the location. The site survey should identify the optimal location for the Access Points, the correct antenna type, the optimal antenna angle, and how to mitigate interference. After the installation, use wireless sniffer tools to check the design and adjust APs or antenna as required.

Connecting Mobile Robots to Industrial Networks

Mobile robots need to communicate with controllers at the relevant site even though the mobile robots and controllers are often using different industrial protocols. For example, an AGV might use CANopen while the controller might use PROFINET. Furthermore, mobile robot manufacturers may want to use the same AGV model on a different site where the controller uses another industrial network, such as EtherCAT.

Mobile robot manufacturers also need to ensure that their mobile robots have sufficient capacity to process the required amount of data. The required amount of data will vary depending on the size and type of installation. Large installations may use more data as the routing algorithms need to cover a larger area, more vehicles, and more potential routes. Navigation systems such as vision navigation process images and therefore require more processing power than installations using other navigation systems such as reflectors. As a result, mobile robot manufacturers must solve the following challenges:

1. They need a networking technology that supports all major fieldbus and industrial Ethernet networks.
2. It needs to be easy to change the networking technology to enable the mobile robot to communicate on the same industrial network as the controller without changing the hardware design.
3. They need to ensure that the networking technology has sufficient capacity and functionality to process required data.

Creating a Safe System

Creating a system where mobile robots can safely transport material is a critical but challenging task. Mobile robot manufacturers need to create a system that considers all the diverse types of mobile robots, structures, and people in the environment. They need to ensure that the mobile robots react to outside actions, such as someone opening a safety door or pushing an emergency stop button, and that the networking solution can process different safety protocols and interfaces. They need to consider that AMRs move freely and

manage the risk of collisions accordingly. The technology used in sensors is constantly evolving, and mobile robot manufacturers need to follow the developments to ensure their products remain as efficient as possible.

Safety standards provide guidelines on implementing safety-related components, preparing the environment, and maintaining machines or equipment.

While compliance with the different safety standards (ISO, DIN, IEC, ANSI, etc.) is mostly voluntary, machine builders in the European Union are legally required to follow the safety standards in the machinery directives. Machinery directive 2006/42/EC is always applicable for mobile robot manufacturers, and in some applications, directive 2014/30/EU might also be relevant as it regulates the electromagnetic compatibility of equipment. Machinery directive 2006/42/EC describes the requirements for the design and construction of safe machines introduced into the European market. Manufacturers can only affix a CE label and deliver the machine to their customers if they can prove in the declaration of conformity that they have fulfilled the directive's requirements.

Although the other safety standards are not mandatory, manufacturers should still follow them as they help to fulfill the requirements in machinery directive 2006/42/EC. For example, manufacturers can follow the guidance in ISO 12100 to reduce identified risks to an acceptable residual risk. They can use ISO 13849 or IEC 62061 to find the required safety level for each risk and ensure that the corresponding safety-related function meets the defined requirements.

Mobile robot manufacturers decide how they achieve a certain safety level. For example, they can decrease the speed of the mobile robot to lower the risk of collisions and severity of injuries to an acceptable level. Or they can ensure that mobile robots only operate in separated zones where human access is prohibited (defined as confined zones in ISO 3691-4).

Identifying the correct standards and implementing the requirements is the best way mobile manufacturers can create a safe system. But as this summary suggests, it's a complicated and time-consuming process.

Reliable CAN Communication

A reliable and easy-to-implement standard since the 1980s, communication-based on CAN technology is still growing in popularity, mainly due to its use in various booming industries, such as E-Mobility and Battery Energy Storage Systems (BESS). CAN is simple, energy and cost-efficient. All the devices on the network can access all the information, and it's an open standard, meaning that users can adapt and extend the messages to meet their needs.

Wireless Standard	Advantages	Disadvantages
Bluetooth	Stable	Low bandwidth
Cellular	Secure Easier to control traffic Low latency Offers high or low bandwidth options	Expensive to install Requires expertise to configure the network
Wi-Fi	Cheap to install and scale	Prone to congestion Sensitive to interference

SOURCE: HMS NETWORKS

For mobile robot manufacturers, establishing a CAN connection is becoming even more vital as it enables them to monitor the lithium-ion batteries increasingly used in mobile robot drive systems, either in retrofit systems or in new installations. Mobile robot manufacturers need to do the following:

1. Establish a reliable connection to the CAN or CANopen communication standards to enable them to check their devices, such as monitoring the battery's status and performance.
2. Protect systems from electromagnetic interference (EMI), as EMI can destroy a system's electronics. The risk of EMI is significant in retrofits as adding new components, such as batteries next to the communication cable, results in the introduction of high-frequency electromagnetic disturbances.

Accessing Mobile Robots Remotely

The ability to remotely access a machine's control system can enable mobile robot vendors or engineers to troubleshoot and resolve most problems without traveling to the site.

The challenge is to create a remote access solution that balances the needs of the IT department with the needs of the engineer or vendor. The IT department wants to ensure that the network remains secure, reliable, and retains integrity. As a result, the remote access solution should include the following security measures:

- Use outbound connections rather than inbound connections to keep the impact on the firewall to a minimum.
- Separate the relevant traffic from the rest of the network.
- Encrypt and protect all traffic to ensure its confidentiality and integrity.
- Ensure that vendors work in line with or are certified to relevant security standards such as ISO 27001 Ensure that suppliers complete regular security audits.

The engineer or vendor wants an easy-to-use and dependable system. It should be easy for users to connect to the mobile robots and access the required information. If the installation might change, it should be easy to scale the number of robots as required. If the mobile robots are in a different country from the vendors or engineers, the networking infrastructure must have sufficient coverage and redundancy to guarantee availability worldwide.

Best practices to implement mobile robot communication

Mobile robot manufacturers are rarely communication or safety experts. Subsequently, they can find it time-consuming and expensive to try and develop the required communication technology in-house. Enlisting purpose-built third-party communication solutions not only solves the communication challenges at hand, it also provides other benefits.

Modern communication solutions have a modular design enabling mobile robot manufacturers to remove one networking product designed for one standard or protocol and replace it with a product designed for a different standard or protocol without impacting any other part of the machine. For example, Bluetooth may be the most suitable wireless standard in one installation, while Wi-Fi may provide better coverage in another installation.

Similarly, one site may use the PROFINET and PROFIsafe protocols, while another may use different industrial and safety protocols. In both scenarios, mobile robot manufacturers can use communication products to change the networking technology to meet the local requirements without making any changes to the hardware design.

Conclusion

As we've seen, mobile robot manufacturers must solve many communication and safety challenges. They must establish a wireless connection, send data over different networks, ensure safety, connect to CAN systems, and securely access the robots remotely. And to make it more complicated, each installation must be re-assessed and adapted to meet the on-site requirements.

Mark Crossley, Daniel Heinzler, Fredrik Brynolf and Thomas Carlsson, ***HMS Networks.***

Visit Website

Line speed Ethernet routing for Ethernet/IP control networks

New hardware-assisted Layer 3 switches with router capability use special purpose hardware to route traffic from one Ethernet network to another at Ethernet line speed. They can simultaneously operate as an Ethernet switch or an Ethernet network-to-network router with equal performance forwarding traffic in either role.

SOURCE: REAL TIME AUTOMATION

Long conveyors often between facilities are not uncommon.

FACTORY WIDE CONTROL NETWORKS ARE A mystery to many control engineers and there is a good reason for that. For the longest time, manufacturing cells were small; a simple programmable controller and a group of I/O devices. But today's production systems are massively more complicated than the those from even a few years ago.

Implementing controls for those complex production systems now often means advanced (and more complicated) control systems designs that require the use of advanced Ethernet switch and router technology. It's common now for those designs to include coordinating interaction between automated equipment in widely dispersed areas of the factory where different, asynchronous processes are operating.

Over the years, there weren't many systems of this type and little attention was paid as to how to make them reliable and effective. Historically, when control engineers had to coordinate widely dispersed automation equipment, they deployed long distance control cables and special hardware. These systems were both expensive and cumbersome to maintain. Special, custom PLC programming was often deployed increasing the complexity and maintainability of the control system.

Today, because of the size of factories, the complexity of production systems, the increasing size and sophistication of conveyor systems, there are more applications requiring this type of factory wide control than ever. Some of these applications include coordinating robotic part transfers.

Many of these applications involve controlling the interlocks of long distance conveyor system which sometimes operate in multiple buildings. Another common application is paint shop in automotive plant. The paint system must often coordinate the operation of the paint shop ovens with the incinerator that processes paint fumes. There are now more and more of these types of long distance control applications.

Control engineers can avoid the costs of the special hardware and cabling that were typically used in these systems by using today's more sophisticated switches and routers and the control strategy described in this article.

New technology

Control Engineers today have an advantage over their counterparts from years past. Today, there is a comprehensive Ethernet backbone network covering the entire factory and there is new technology in Ethernet routers that can be applied to these applications. Routers, as you know, route traffic between networks using the layer 3 IP addresses while Ethernet switches route traffic within an Ethernet network using the Layer 2 Ethernet Media Access Control (MAC) address of the destination device.

Historically, routers introduced a communication delay when they performed their traffic forwarding task. While Ethernet switches could switch at Ethernet line speed using specialized custom integrated circuits, routers processed messages in software. The

SOURCE: REAL TIME AUTOMATION

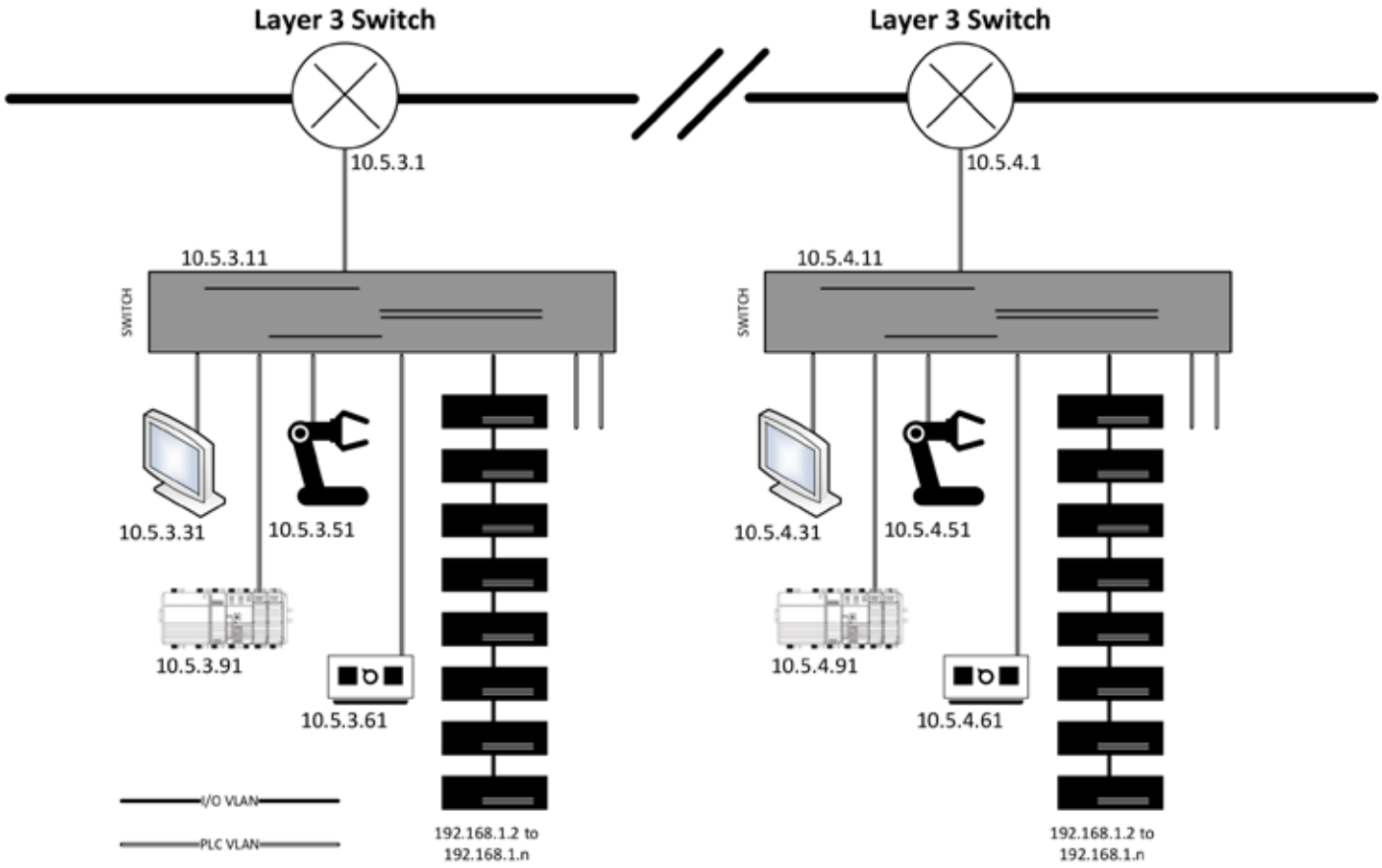


Figure 2 - Two machines cells connected to the Facility Network using Layer 3 Switches.

latency from that software inhibited the ability to use routers as components of factory floor production control systems.

Today, there is a new breed of hardware assisted switches with router capability. These Layer 3 switches use special purpose hardware to route traffic from one Ethernet network to another at Ethernet line speed. They have the capability to simultaneously operate as an Ethernet switch or an Ethernet network to Ethernet network router with equal performance forwarding traffic in either role. They are the ideal device for interconnecting an EtherNet/IP network with other EtherNet/IP networks and/or to the outside world.

EtherNet/IP

Integrating Layer 3 switches with EtherNet/IP is the perfect way to create factory wide control networks. EtherNet/IP has two kinds of traffic: explicit messages for asynchronous traffic and implicit messages for synchronous traffic.

Explicit messages are used for the exchange of information while implicit messages are to exchange control signals and I/O. EtherNet/IP uses standard, UDP and IP to move implicit message traffic , allowing that traffic to be routed through routers. If those routers are layer 3 switches, that prioritized traffic can be routed across the factory with nearly no latency.

In Figure 2, control signal traffic from controllers in separate machine cells can be easily exchanged through a facility-wide backbone network of interconnected layer 3 switches with the same performance as if those controllers were on the same EtherNet/IP network.

And What About Profinet IO

The ability to route unicast control signal traffic is arguably the most significant differentiator between the EtherNet/IP and the Profinet specifications. Profinet is not routable by design. Profinet is designed to optimize I/O traffic by eliminating the processing associated with a TCP/IP stack. I/O traffic is transmitted directly in Ethernet frames.

While I/O traffic in a Profinet IO subnet might be marginally better than the equivalent EtherNet/IP system, Profinet IO is unable to handle the type of facility-wide, interconnection control applications discussed earlier in this article.

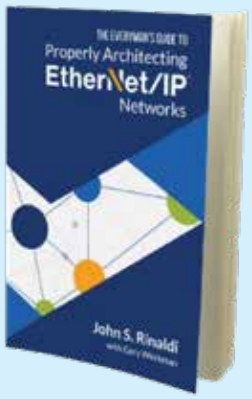
*John Rinaldi, Chief Strategist and Director of WOW!, **Real Time Automation, Inc.** and Gary Workman, retired as the **General Motors** Principal Engineer responsible for plant floor networking in 2017.*

Visit Website

The Everyman's Guide to EtherNet/IP Network Design

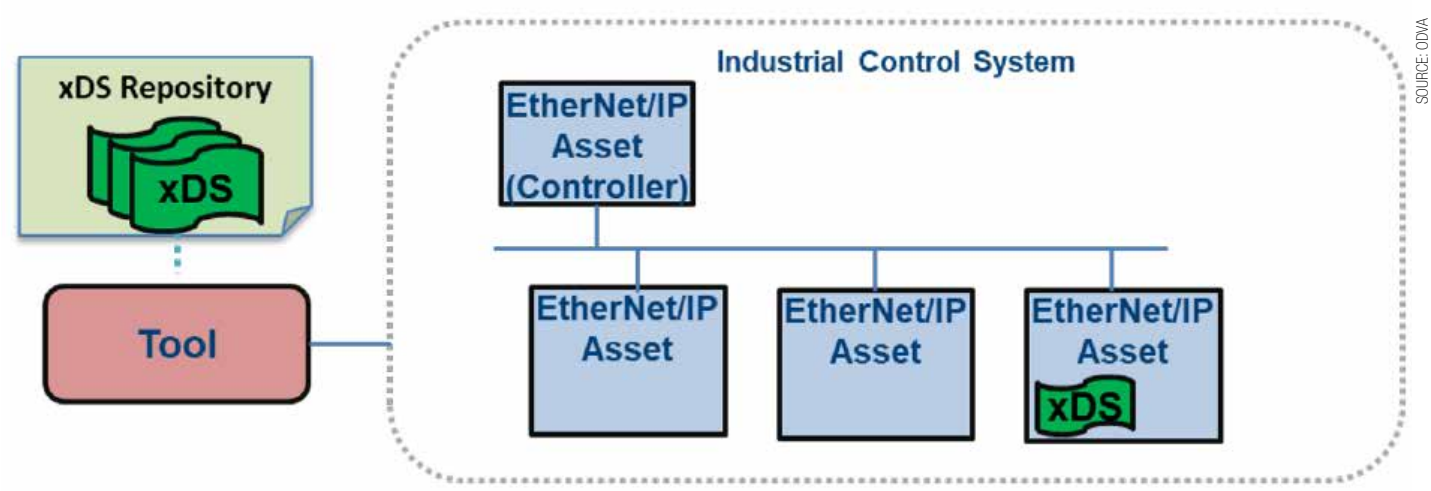
A new book, *The Everyman's Guide to EtherNet/IP Network Design*, details 12 specific guidelines an EtherNet/IP network designer should use to create practical, optimized and reliable EtherNet/IP control systems. It is a unique resource of proven, time-tested technologies, architectures and recommendations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

Using the recommendations from the book and the Layer 3 switches described in this article, control engineers can learn about practical, effective and reliable ways for deploying factory and facility wide EtherNet/IP control systems.



Ongoing developments in xDS device descriptions

The development of Digital Device Description technology will lead to a more robust and secure device description than is currently available. Moving ahead, efforts at ODVA are continuing toward development of xDS, the publication of both an xDS specification and tools needed to prove these concepts.



SOURCE: ODVA

Figure 1 - Typical interaction of xDS, Tools, and ICS.

THE ODVA SPECIAL INTEREST GROUP FOR xDS Digital Device Descriptions is working to develop a specification for next generation of device description as a robust, extensible, and secure artifact.

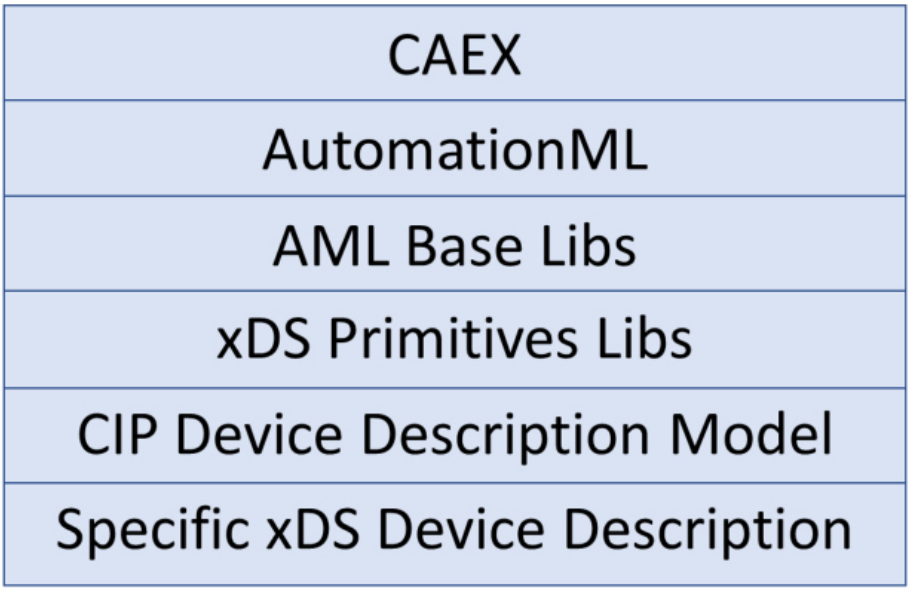
This article describes the state of the art in the development of xDS and details about the use of AutomationML constructs to describe components, the use of Open Packaging Conventions to package the various components, security approaches, and proposed tools to ease the adoption of xDS.

Introduction

With ever-increasing interconnectivity of machines and processes, and escalating demands for device data, the need exists to provide a more robust and secure device description for CIP™ devices than can be achieved using the current EDS file. Initiated February 2019, the xDS Digital Device Descriptions SIG has been working on developing such a replacement.

The goal is to provide a scalable digital device description which is as simple and reusable as possible while still providing a means of representing the rich, robust information provided in CIP. The xDS artifact provides the necessary information to tools to be able to configure, monitor, control, diagnose, and conformance test CIP devices in an Industrial Control System (ICS) over the network. The primary workflows for which xDS provides information to the tool are:

- Network and Security Configuration
- Device Configuration
- Network Diagnostics
- Device Diagnostics
- Device Conformance



SOURCE: ODVA

Figure 2 - xDS Layers

Similar to EDS files, the xDS artifact may be embedded within the device itself or provided through some other external means such as a website or device description database. While xDS is being designed to be applicable to any CIP network, the primary focus at this time is for EtherNet/IP networks.

This article represents the understanding and proposal for the xDS representation, as developed by the xDS SIG for the latest ODVA technical conference. Four main topics will be discussed. First, the use of AutomationML constructs is presented as a basis for modeling device information such as features and configuration parameters.

Second, a packaging scheme and format is presented for aggregating various components of differing formats into a single, compact, logically arranged artifact. Third, a discussion of security considerations and the proposed

approach, and finally, a proposal for some tools to aid in the adoption of xDS.

Choice of AutomationML as Device Description Modeling Language

The xDS SIG investigated several approaches for representing device description information and has settled on the use of AutomationML (AML). AutomationML is an XML based, object-oriented data modeling language developed for representing plant engineering information, based on the representation format of CAEX as defined in IEC 62424. AML is an open standard, and its specifications may be implemented on a royalty-free basis.

AML is a logical choice as the base description language for xDS, as it was developed specifically for the purpose of automation data exchange. It uses existing industry data formats specifically designed for storage and exchange of different aspects of engineering information. AML interconnects engineering tools.

The AutomationML Organization supports and maintains AutomationML. This organization has celebrated its 15th anniversary. Membership has continued to grow within the AutomationML Organization highlighting the stability and improvement of the organization as a standards consortia. Several technologies related to the automation industry have already adopted use of AML, such as the Asset Administration Shell for Industrie 4.0.

AML has a defined structure which is flexible and extensible, allowing predefined ODVA structures to be built on top. Additionally, some tooling has already been implemented to simplify the development of xDS. The AutomationML Editor provides a logically oriented, graphical tool to aid in the initial design and testing of xDS concepts. The AML Engine library provides a freely available library based on the .NET framework for processing and editing AML files. Because AML is based on the XML format, support for platforms other then .NET can easily be adapted, and many have already been demonstrated.

Modeling CIP Devices Using AutomationML

Details about AutomationML are beyond the scope of this paper. However, the following basic AML concepts are required to understand the xDS approach. There are three types of AML classes used by xDS:

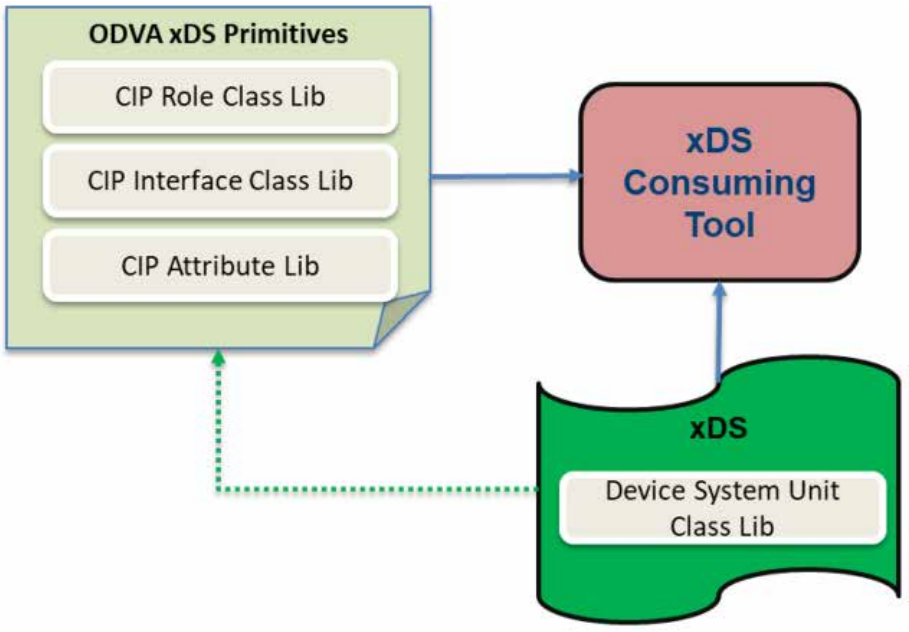
- *Role Class:* Provides abstract semantic information about an object.
- *System Unit Class:* Represents a specific type of object. A System Unit Class can reference one or more Role Classes to represent the roles the object performs.
- *Interface Class:* Models an interface between components.

Each of these types of classes can be collected into libraries of similar classes and can inherit from other classes in the same library or from another referenced library. Along with these class libraries, AML allows the definition of custom attributes, collected into an Attribute Class library. A set of common AML base libraries are defined, from which more specific classes can be inherited.

For xDS, a set of standard libraries is created from the AML base libs to define the Role Classes, Interface Classes, and custom CIP attributes required to describe a CIP device. These libraries comprise the ODVA xDS Primitives, which will be an ODVA-provided reference library to be used by any tools creating or interpreting an xDS. Specific device descriptions are created as a System Unit Class referencing the CIP role classes and interface classes. The format of this device description will be defined in the xDS specification (noted in Figure 2 as the CIP Device Description Model). This creates a layered approach, as shown in Figure 2.

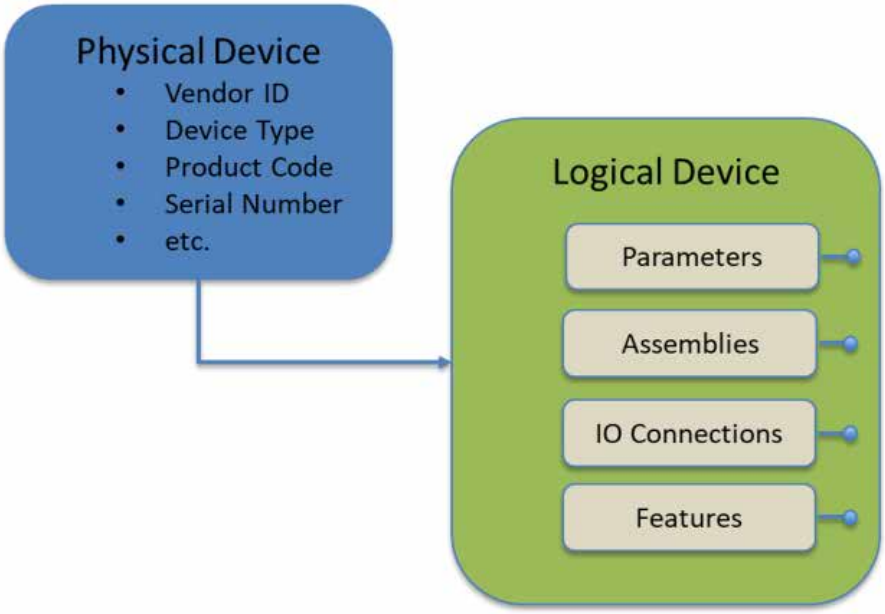
Figure 3 shows the interactions between these components, where a specific xDS device description references the ODVA xDS Primitives definition file, and any tool interpreting the xDS will require the primitives to fully understand the xDS definitions.

This structure is accomplished through a set of custom Role classes in the ODVA xDS Primitives library which inherit from the AML CommunicationRoleClassLib. The physical device is modeled inheriting from the AML PhysicalDevice Role class, and attributes are defined for required CIP device identification.



SOURCE: ODVA

Figure 3 - Interaction of xDS and ODVA xDS Primitives



SOURCE: ODVA

Figure 4 - CIP device Description Model.

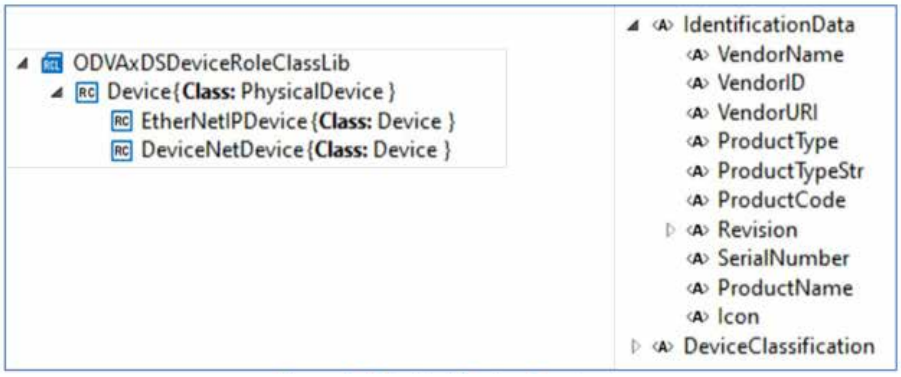
The inherited role classes EtherNetIPDevice and DeviceNetDevice provide a means of distinguishing between the two. (It should be noted that xDS development is focusing on EtherNet/IP, but efforts are being made to ensure that the design is able to be adopted to DeviceNet in the future). Figure 5 shows the physical device role classes and associated attributes, as visualized using the AutomationML Editor.

The logical device is modeled as CIPDeviceDescription, inheriting from the AML LogicalDevice Role class. The logical device is further broken down into several collections of components. The ConnectionList collects a list of supported IO connection definitions. The ParameterGroup component is used to collect a list of Parameter definitions. Multiple ParameterGroup instances may be included as a means of grouping common parameters together. Likewise, the AssemblyList component is used to collect a list of Assembly interface definitions. Multiple AssemblyList instances may be included. The FeatureList component is used to collect predefined feature declarations, such as DLR support. Finally, the CIPObjectModel role class provides constructs to declare the entire CIP Object model supported by the device. This is used to declare all supported public CIP objects with declaration of supported attributes and services. Details about how the FeatureList and CIPObjectModel components will be modeled have not yet been determined. See Figure 6,

Three custom interface classes are defined in the xDS Primitives file for modeling the key CIP interfaces to device configuration information. The Parameter interface class is used to declare configuration parameters in the same way as the EDS ParamN. By leveraging AML constructs and flexibility, the ability exists to define parameter dependencies, complex range requirements, multi-language help strings, International Registration Data Identifier (IRDI) references, and other custom information to the parameter. The Connection interface class provides constructs to declare supported I/O connections. Finally, the Assembly interface class is used to declare supported assemblies and their data layout. Figure 7 shows interface class library entries.

CIP Device Model Example

A simple reference device based on a software simulation of a General Purpose Discrete IO is used to demonstrate creating an xDS device description. The device consists of four discrete input points and four discrete output points, and follows the device profile as described in Volume 1 of The CIP Networks Library. There is a configuration assembly (instance 100), input assembly 3, and output assembly 33. For demonstration purposes, several configuration and diagnostic parameters have been defined. Details are presented in Table 1 and Table 2.



SOURCE: ODVA

Figure 5 - Physical Device Constructs.

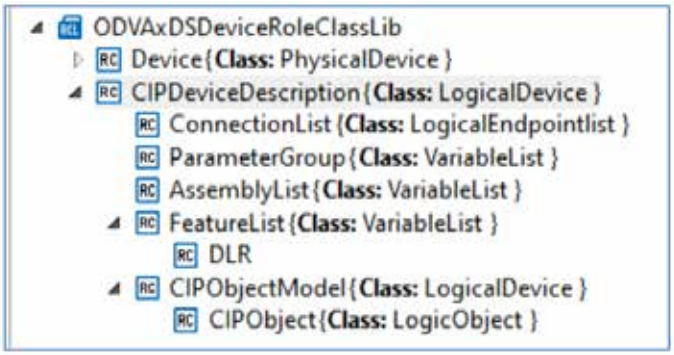


Figure 6 - Logical Device Constructs.

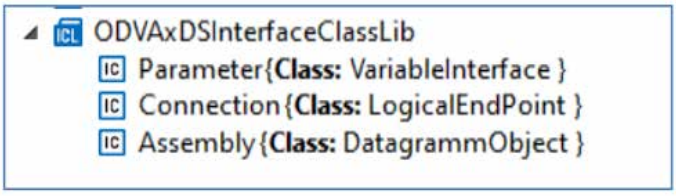


Figure 7 - Interface Classes.

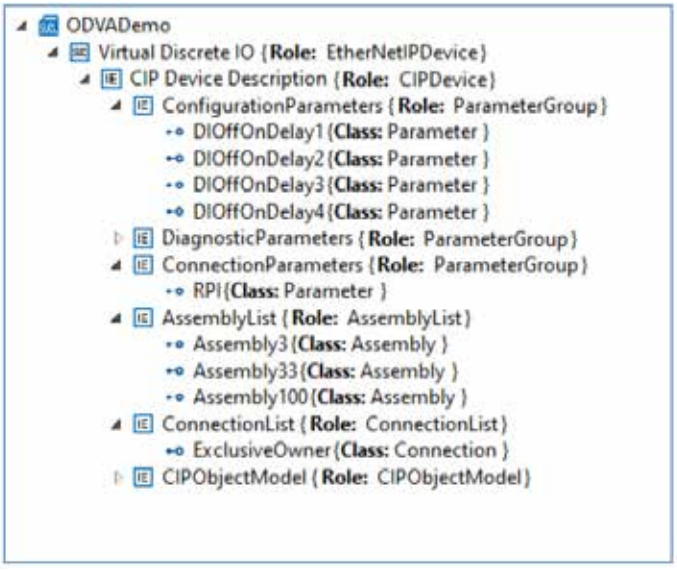


Figure 8 - Reference Device Modeled in AML Using xDS Constructs.

Using the proposed CIP Device Description Model and the ODVA xDS Primitives libraries, the reference device is modeled as shown in Figure 8. A System Unit Class library named ODVADemo is the top-level container for the device description. Multiple device descriptions could be created within this container to describe a number of related devices such as a product family. A physical device description with the name "Virtual Discrete IO" is created with the role EtherNetIPDevice. The device Identity information is stored in attributes

Vendor ID	24 – ODVA
Device Type	7 – General Purpose Discrete IO Device
Product Code	20
Revision	1.001
Product Name	Virtual Discrete IO Device

Table 1 - Reference Device Identity.

Object	Instances
Identity	1
Message Router	1
Ethernet Link	1
TCP/IP Interface	1
Connection Manager	1
Assembly	3, 33, 100
Discrete Input Point	1, 2, 3, 4
Discrete Output Point	1, 2, 3, 4

Table 2 - Reference Device Object Model.

associated with the EtherNetIPDevice role class.

The logical device description is modeled within the element named "CIP Device Description". This element includes three ParameterGroup containers, one for configuration parameters, one for diagnostic parameters, and one for connection parameters. These groupings can be made in any way the xDS creator sees as helpful.

The AssemblyList contains all published assemblies. Figure 9 shows the layout of the input assembly instance 3. The member list in this example consists of four entries of type AssemblyMember labeled DI1Value, DI2Value, etc. Each of these entries includes a reference to one of the four digital input value parameters defined in the parameter group section. The member list is flexible, allowing various constructs to be referenced and individual bitfields to be defined.

In the same way, the ConnectionList contains all the connection definitions. A connection definition contains the standard set of attributes required to define an IO connection as shown in Figure 10.

The design for describing the CIP Object Model section and the Feature List section has not been completed at this time, so our model of the General Purpose Discrete IO device does not include completed entries for those sections. However, this modeling exercise has demonstrated a proof of concept for using this approach.

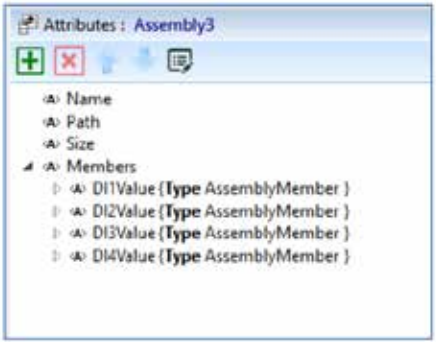


Figure 9 - Assembly Attributes.

Use of Open Packaging Conventions to package xDS Components

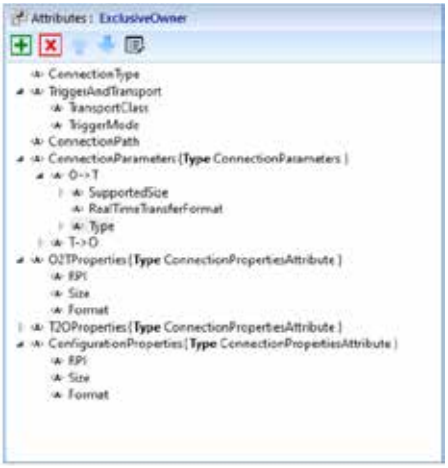


Figure 10 - Connection Attributes.

Along with the device information model which may be represented using AutomationML, there are various additional components which may be needed within the device description. These may include icons and graphics, user manual, Declaration of Conformity, and other vendor-specific files. There is also the desire to support multiple similar devices of a product family within a single xDS artifact, as well as multiple revisions of the same device. To aggregate these various components into a single, organized, compact artifact, Open Packaging Conventions is used.

The Open Packaging Conventions (OPC) originated out of the Office Open XML file formats for representation of Microsoft Office documents. The OPC specification has been standardized in ISO/IEC 29500-2 [5] and ECMA-376 [6]. The specification provides a framework for structured storage of information within a file which itself is just a "zip" file. The specification allows for the expression of relationships between parts of the file through a directed graph of relationship associations. Additionally, the specification provides a standardized approach for digitally signing the contents or portions of the contents which meets the requirements proposed in the Security Considerations section below.

Implementation details for xDS have not been clarified at this time, but a basic structure using OPC has been proposed which will:

- Allow support for both required and optional sections
- Support future expansion for additional sections
- Support independent digital signing of sections

The support of multiple, independent digital signatures which can be applied to selected sections in the package is a very powerful feature. The SIG envisions two different signatures applied to various portions of the xDS package. Upon completion of developing the xDS, the vendor will apply a signature to the critical, required sections and any other sections desired. Then, upon successfully receiving an ODVA Declaration of Conformity, ODVA will insert the DoC into the package and generate an ODVA signature based on certain critical sections which may not be modified without updating the DoC. Conversely, sections which are not under the ODVA signature could be modified after the fact by the vendor.

The following sections have been proposed:

1. File Version: This section will contain specific file version information including creation timestamp, revision number, modification history, and xDS specification version this file conforms to. This content is

required to be included in the vendor digital signature.

2. Devices: Multiple device descriptions may be included in a single package to represent different devices in a product family, as well as to represent different product revisions of each device. The Devices section will include a listing of all the variations included in this package. Each entry provides a link to the associated AML description of the device, also included in this section. This content is required to be included in both the vendor digital signature and the ODVA signature.

3. Graphics: Any graphics images related to the device. A variety of allowable common image formats will be specified. Optional for vendor digital signature; not included in ODVA signature.

4. Icons: Icon files used by the devices. Optional for vendor digital signature; not included in ODVA signature.

5. Localization: Text in the various languages supported by the vendor, such as help strings is maintained here. This section is required to be signed by the vendor, but not part of the ODVA signature, allowing for corrections or additions to be made by the vendor without requiring recertification by ODVA.

6. EDS Files: Vendors may optionally include legacy EDS files in the xDS package for use by systems not supporting xDS device description format. If present, required to be included in vendor digital signature; not included in ODVA signature.

7. Vendor Documentation: Optional vendor supplied documentation may be packaged in this section, including manuals or drawings. If present, required to be included in vendor digital signature; not included in ODVA signature.

8. Vendor Specific: A location for any optional vendor-specific content. Vendors may choose to encrypt this content. Optional for signature by vendor; not included in ODVA signature.

9. ODVA Conformance: As part of the ODVA conformance certification process, ODVA will insert the Declaration of Conformity here. Not allowed for vendor signature; required for ODVA signature.

10. Signatures: This section contains all of the digital signature information. This information follows the OPC specification for signatures and complies with the security recommendations in the following section.

Security Considerations

A key aspect for xDS is the concept of a secure device description artifact. A simplified threat model identifies two primary areas of concern for xDS information:

1. Invalid xDS device descriptions: This could be accidental or malicious modifications which could cause a tool and/or the device to become a bad actor in the ICS.

2. Nonconformant Device: An xDS which misrepresents a device as conformant, allowing it to be incorporated into the ICS, possibly as a bad actor.

There are three primary use cases in which the threat model concerns must be addressed:

Vendor deelopment of the device: During device development, the xDS package will be digitally signed by the vendor to authenticate the source and to prevent modification.

- To be a conformant product, the vendor shall digitally sign the xDS.
- The signature shall be based on a recommended algorithm in NIST FIPS 186-4 or its successors.
- The xDS specification shall define mandatory portions which must be protected by a signature.
- Some portions of the xDS, as well as vendor-specific regions may be included in the signature but are not mandatory.
- Keys used to sign xDS files shall be kept private through a Hardware Security Module (HSM).
- Access to the HSM shall be documented. Any access to keys shall generate an audit trail.

ODVA Conformance: Upon successful conformance test, ODVA will insert the Declaration of Conformity document into the xDS and add a digital signature. The signature is tied to both the declaration and the xDS content, providing a secure indication of device conformity.

- Insert the Declaration of Conformity into the xDS of a conformant device.
- Digitally sign the DOC along with other critical components of the xDS.
- Keys used to sign xDS files shall be kept private through a Hardware Security Module (HSM).
- Access to the HSM shall be documented. Any access to keys shall generate an audit trail.
- Maintain and make available a list of trust anchors (root certificate authority) used by vendors for signing their xDS.

End User Tools: End user tools will validate an xDS upon loading. Tools will verify existence of a Declaration of Conformity against the ODVA signature and verify overall xDS content against the vendor signature. Tools must notify the user of any discrepancies. Because there will always be examples in which an unsigned or modified xDS must be used, an override mechanism is recommended. The user must be informed of the security concerns and required to acknowledge this before being allowed to use an unsigned or modified xDS.

- All tools consuming xDS shall verify contents based on the digital signature of the vendor.
- All tools consuming xDS shall verify presence of the ODVA DOC and verify the ODVA signature.
- Tools may provide the ability to bypass verification.
- If verification is bypassed, tools shall provide warning messages to the user before allowing the bypass.
- Signatures shall be validated on first retrieval of a signature. Any subsequent validation should ignore any certificate expiration concerns.
- Tools shall periodically retrieve trust anchor list from ODVA.

Tools to Aid in Adoption of xDS

The SIG recognizes that a large hurdle for vendors will be the lack of established tools. The AutomationML Editor provides a flexible tool for the initial prototyping and validation of xDS concepts but is not an adequate tool for vendors to easily create a complete xDS device description. Therefore, some tools have been proposed and some initial prototyping of these tools has begun.

The first tool is an xDS creation tool. This would be analogous to the current EZ-EDS tool. The intent is to make it as simple as possible for a device vendor to create a device description for their devices. Some of the basic capabilities of this tool include:

- Device Description: Provide a simple hierarchical view to easily create the description. Handle all required AML boilerplate constructs according to the defined CIP device model.
- Packaging: Allow specification of component files from various sources to be added.
- Digital Signatures: Create and validate signatures.
- Conformance: Analyze an xDS for proper required content and format.

The second proposed tool is an xDS library reference implementation. This library would be an opensource reference to demonstrate how tools can read and interpret the information contained in an xDS file.

Summary and Future Work

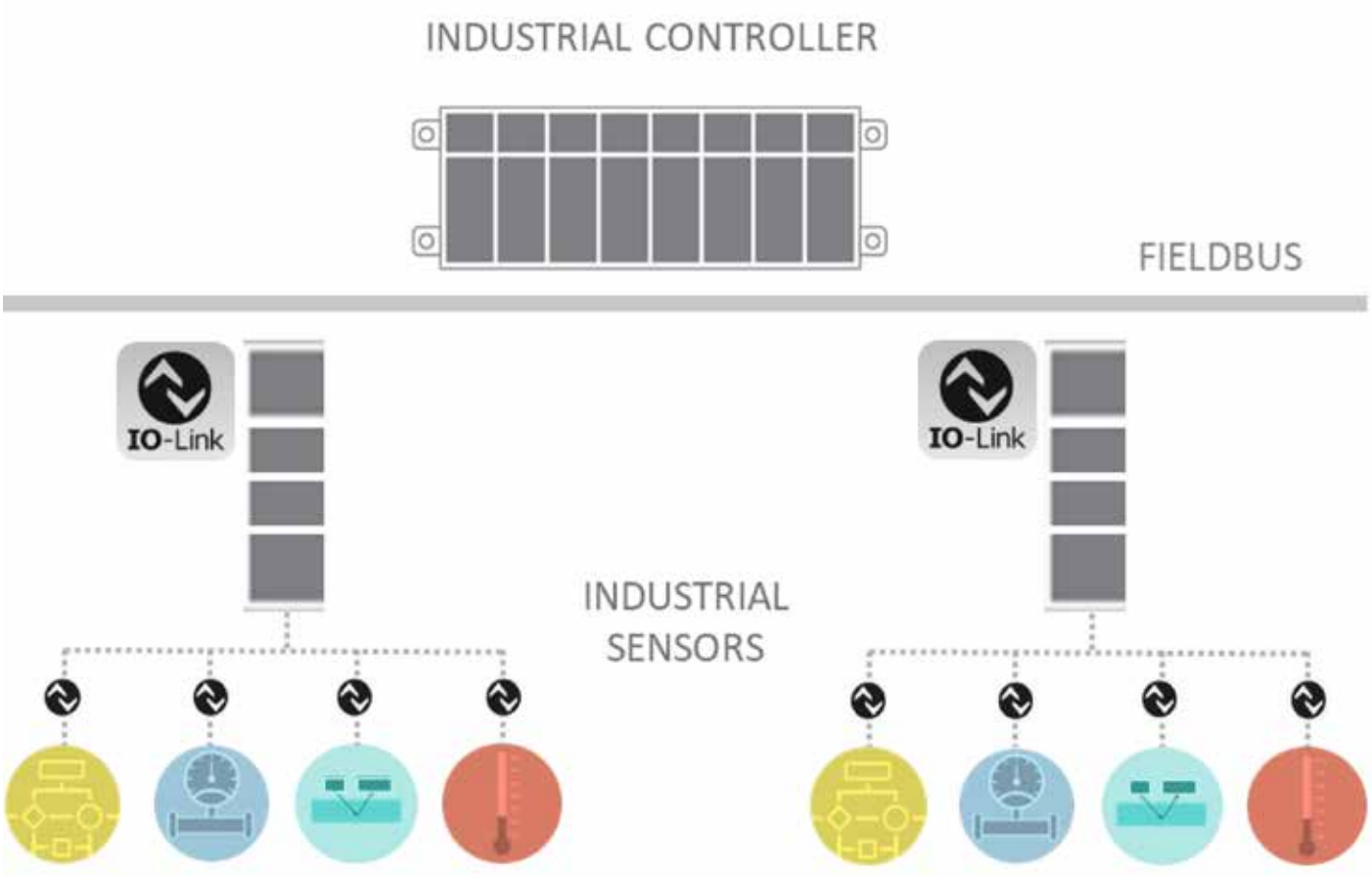
This article has highlighted the current state of development for xDS by the xDS SIG. This effort will lead to a more robust and secure device description than is currently available. The article has described the use of AutomationML to model CIP devices, the use of Open Packaging Conventions to package the information, security considerations, and proposed tools for adoption of xDS. Going forward, the SIG will be continuing development of xDS toward the publication of the xDS specification and coordinating the development of tools to prove these concepts.

Matthew Frazer, ***ODVA, Inc.*** *and Todd Snide,* ***Schneider Electric.***

Visit Website

Implementing efficient industrial field sensors with IO-Link

The newest generation of IO-Link transceivers integrate both protection and a high-efficiency DC-DC buck regulator to reduce the size and the heat dissipation of the sensor subsystem. As IO-Link technology gets deployed in more industrial sensors, these specifications are key small, ruggedized, power-efficient sensors.



SOURCE: ANALOG DEVICES

Figure 1: IO-Link protocol is used to connect intelligent edge devices to the factory network.

INDUSTRIAL SENSORS HISTORICALLY WERE, and still are in many cases, analog. They include a sensing element and some way to get the sensing data to a controller. Data was unidirectional analog.

Then came binary sensors, which provided a digital on/off signal, and included a sensing element: inductive, capacitive, ultrasonic, photoelectric, etc. with a semiconductor switching element. The output could be: high-side (HS) switching (PNP) or low-side (LS) switching (NPN) or push-pull (PP). But data was still limited to unidirectional communication from the sensor to the master, had no error control, and still required a technician on the factory floor for tasks such as manual calibration.

A better solution was needed to meet the demands of "Industry 4.0", smart sensors, and reconfigurable factory floors. The solution is the IO-Link protocol, a standard for industrial sensors that is showing a phenomenal growth trajectory. The IO-Link organization estimates that over 16 million IO-Link enabled nodes are being used in the field and is still growing.

About IO-Link

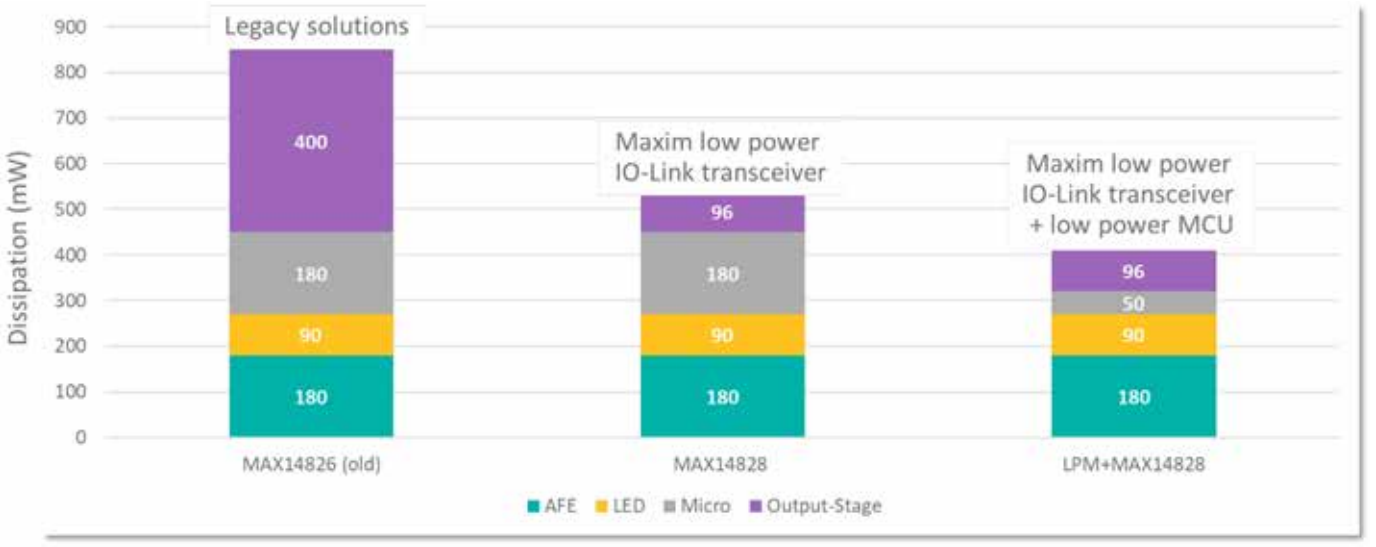
IO-Link is a standardized technology (IEC 61131-9) that regulates how sensors and actuators in industrial systems interact with a controller. IO-Link is a point-to-point communication link with standardized connectors, cables, and protocols. The IO-Link system is designed to work within the industry standard 3-wire sensor and actuator infrastructure and comprises an IO-Link Master and IO-Link Device products.

IO-Link communication is between one master and one device (sensor or actuator). Communication is binary (half-duplex) and is limited to a distance of 20m, using unshielded cables. Communication requires a 3-wire interface (L+. C/Q, and L-). The supply range in an IO-Link system is 20V to 30V for the master and 18 to 30V for the device (sensor or actuator).

Analog Devices' IO-Link handbook elaborates IO-Link advantages as follows:

"IO-Link is a technology that enables a traditional binary or analog sensor to become an intelligent sensor that no longer just gathers data but allows a user to remotely change its settings based on real-time feedback obtained on the health and status of other sensors on the line, as well as the manufacturing operation it needs to perform.

IO-Link technology enables sensors to become interchangeable through a common physical interface that uses a protocol stack



SOURCE: ANALOG DEVICES

Figure 2: A hypothetical IO-Link industrial sensor power budget.

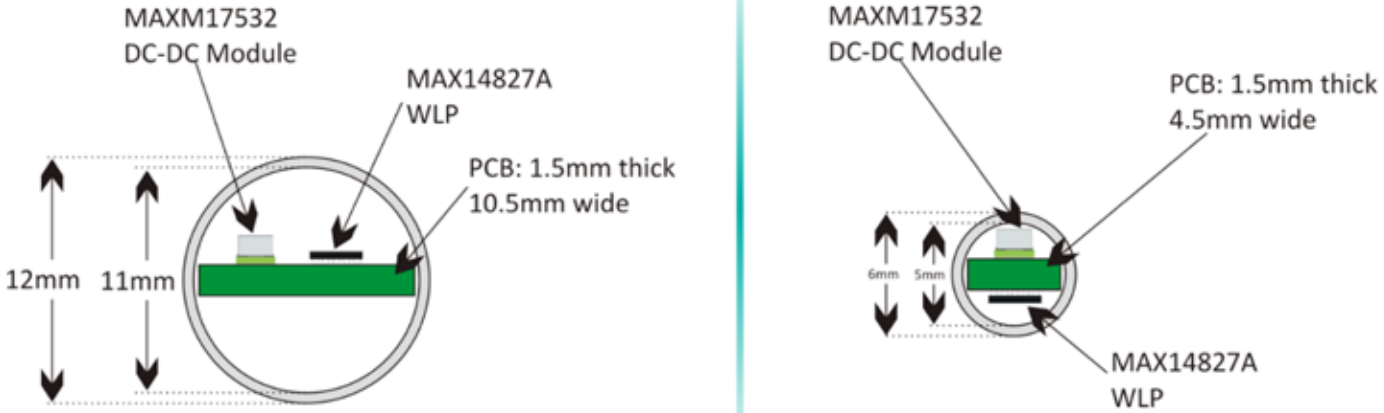


Figure 3: Size is another big issue in the newest IO-Link sensor designs.

and an IO Device Description (IODD) file to enable a configurable sensor port. It is truly plug-and-play ready while providing the ability to reconfigure parameters on-the-fly."

Within the factory network hierarchy, the IO-Link protocol sits at the edge, which are typically sensors and actuators as shown in Figure 1. Many times, the edge devices communicate to a gateway that translates the IO-Link protocol to the fieldbus of choice.

Designing IO-Link Sensors

Industrial field sensors must be rugged, small, and very energy efficient so that the heat dissipation is kept to a minimum. Most IO-Link sensors have the following components:

- Sensing element with the associated analog front end (AFE)
- A microcontroller that processes data, and in the case of an IO-Link sensor, also runs the lightweight protocol stack.
- An IO-Link transceiver that is the physical layer.
- Power supply and in many cases protection (TVS for surge, EFT/burst, ESD, etc.).

Heat Dissipation (Power Efficiency)

Once we understand the typical components, we can look at how a hypothetical sensor power is budgeted. See Figure 2. All of these numbers are estimates. They show that the transceiver (output stage) power consumption matters when budgeting the total system power consumption of a sensor.

Let's start at the left-most side, which specificifies an older generation of IO-Link sensor. That way it becomes clearer how advances in technology in the microcontroller (MCU) and the output stage (i.e., the transceiver) has contributed to the lowering of the total system power over the years.

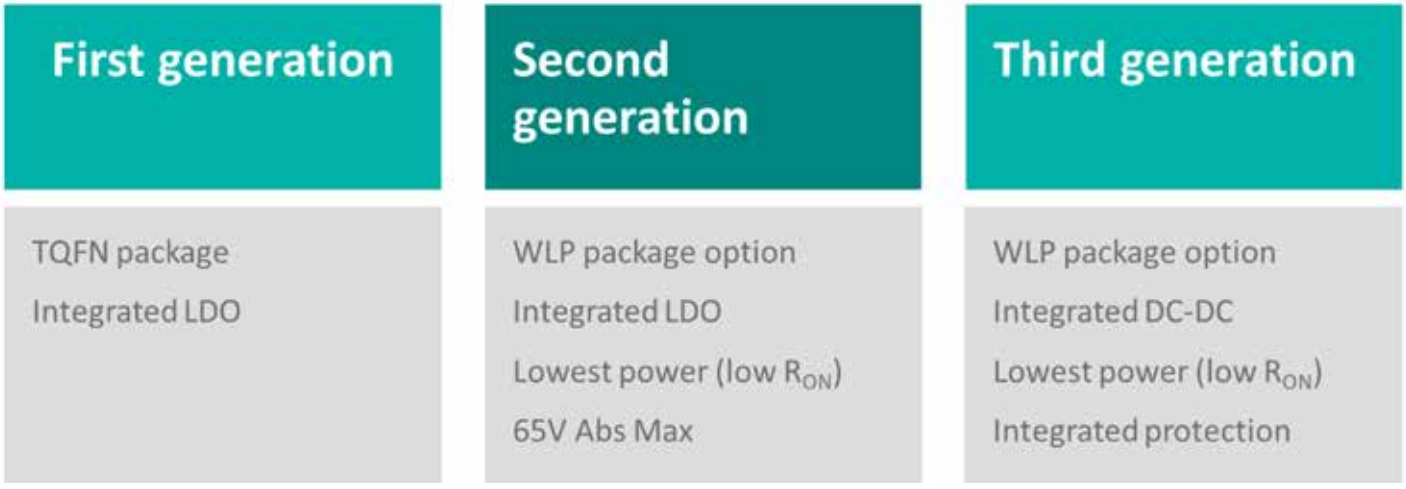
Original or first generation IO-Link transceivers consumed 400mW or higher. The newest low-power Analog Devices IO-Link tranceivers consume less than 100mW. Also, the MCUs have helped. A legacy MCU consumes as much as 180mW, but the newer low-power MCU can go down to 50mW.

A state-of-art IO-Link transceiver coupled with a low-power MCU can keep the total sensor power budget can be in the range of 400mW to 500mW.

Power dissipation is directly related to heat dissipation. The smaller the sensor the more stringent the power dissipation specification. By some estimates, an 8mm diameter (M8) enclosed cylindical IO-Link sensor will specify a maximum power dissipation of 400mW and a 12mm diameter (M12) enclosed cylindical IO-Link sensor will specify a maximum power dissipation of 600mW.

And the technology keeps getting better. One of the new IO-Link transceivers from Analog Devices, the MAX14827A, dissipates a remarkably low 70mW when driving a 100mA load. This is achieved by optimizing the technology to deliver a very low 2.3Ω (typ.) RON (on-resistance).

For sensors that use very low operating current, say 3 to 5mA, and require a 3.3V and/or a 5V supply; the regulated power can be sourced via an LDO. And indeed, Analog Devices' IO-Link transceivers have included an integrated LDO. But as the current demand increases to say 30mA, the LDO will soon become the dominant source of power/heat



SOURCE: ANALOG DEVICES

Figure 4: Progression of IO-Link transceiver technology.

dissipation in the system. To compare at 30mA, the power consumption of an LDO can be as high as 600mW.

LDO Power @30mA = (24-3.3) x 30mA = 621mW

In comparison, a DC-DC buck converter supplying a 30mA sensor with a 3V output voltage will dissipate just 90mW. Assuming the converter is 90% efficient (just 9mW power loss), the overall power consumption is just 90 + 9 = 99mW 3.

Size of IO-Link sensor

After heat dissipation, size is the next biggest concern for all industrial sensors, and it applies as well to the new IO-Link sensors. Board space becomes increasingly at premium as we migrate to a smaller form-factor.

Figure 3 shows that for a 12mm diameter housing, the transceiver (in a wafer level package – WLP – package) and the DC-DC can sit side by side on a regular PCB which has 10.5mm width. There is still room for vias and wires on the same side. If the sensor housing is 6mm, then the PCB width is down to 4.5mm.

To enable these sizes, the transceiver must be available in a wafer-level package (WLP) that allows for the smallest size. This size limitation is also one of the reasons we have integrated a DC-DC inside our newest IO-Link transceiver as shown before. But most industrial sensors also must be designed to work in a rugged environment, which means they must incorporate protection circuitry such as TVS diodes. This is where it is important to pay attention to the Absolute Maximum Ratings specification for the IO-Link transceivers.

Let's elaborate: Why does 65V Absolute Maximum Ratings on the IOs reduce the size of the sensor subsystem? Typically, the sensor needs to survive surge pulses between the 4-pins: GND, C/Q, DI, DO. IO-Link transceivers have a spec of 65V Absolute Maximum Ratings. If we take an example of a 1KV at 24V surge between C/Q and GND.

	IO-Link TRANSCEIVER WITH ABSOLUTE MAXIMUM RATING 65V	IO-Link TRANSCEIVER WITH ABSOLUTE MAXIMUM RATING 45V
Smallest TVS Diode	SMAJ33	SMCJ33
Max Voltage	61V	45V
Total PCB Area	40.5mm2	144mm2

Table 1: Advantages of 65V Absolute Maximum Rating on Sensor Size

Voltage between C/Q and GND = TVS clamp voltage + TVS forward voltage

With the higher Absolute Maximum Ratings specification, a small TVS diode such as SMAJ33 whose clamp voltage is 60V at 24A, and TVS forward voltage is 1V at 24A.

Voltage between C/Q and GND = 61V

This value above is within the Absolute Maximum Ratings specification of the Analog Devices transceiver.

However, if the Absolute Maximum Ratings specification is lower, typically in the industry it is around 45V, then a much larger TVS diode such as the SMCJ33 is required to clamp the voltage down to an acceptable level. This diode is more than 3x the size than the one required for the Analog Devices transceiver.

The size impact of a larger TVS diode in the overall sensor design is significant if the transceiver Absolute Maximum ratings specification is lower. Table 1 shows an estimated difference in the PCB area. The assumption is that the sensor must be able to withstand a high-level surge of ±1KV/24A.

The next generation of IO-Link transceivers have even improved upon this. The newer IO-Link transceivers from Analog Devices now feature an integrated protection on IO-Link line interface pins (V24, C/Q, DI, and GND). All pins feature integrated ±1.2kV/500Ω surge protection. In addition, all pins are also reverse-voltage protected, short-circuit protected and hot-plug protected.

Even with all the integrated protection features as well as the integrated DC-DC buck regulator, these devices are available in a tiny WLP package (4.1mm x 2.1mm); enabling a really small IO-Link sensor design.

Conclusion

The first-generation IO-Link transceiver technology came in easy-to-use TQFN packages with integrated LDOs that would meet the needs of a small sensor design. As power and size considerations mounted, the second-generation transceiver technology optimized power consumption by moving to a technology that gave us lower RON to further reduce power consumption and were made available in even smaller WLP packages.

The newest generation of transceivers recognize the need to integrate both the protection and a high-efficiency DC-DC buck regulator to further reduce the size and the heat dissipation of the sensor subsystem.

As IO-Link technology gets deployed in even more industrial sensors, these device specifications are key to implement small, ruggedized, power-efficient sensors.

Suhel Dhanani, Director of Business Development, Industrial & Healthcare Unit, ***Analog Devices.***

Visit Website

Industrial Ethernet Book

The only publication worldwide dedicated to Industrial Networking and the IIoT.

Visit iebmedia.com for latest updates.

New website offers deepest, richest archive of Industrial Ethernet and IIoT content on the web.

View and/or download latest issue of Industrial Ethernet Book and past issues.

Search our database for in-depth technical articles on industrial networking.

Learn what's trending from 5G and TSN, to Single Pair Ethernet and more.

Keep up-to-date with new product introductions and industry news.

industrial ethernet book

Industrial Networking & IIoT

Low-power IIoT track and trace

Semtech and AWS enable low-power IIoT track and trace services using LoRa Cloud™ geolocation.

SOURCE: SEMTECH

AWS IoT Core launches location service powered by LoRa Cloud. Collaboration simplifies the creation of asset tracking solutions and easily connects LoRa Edge devices to AWS.

Semtech announced a strategic agreement with Amazon Web Services (AWS) to license its LoRa Cloud™ global navigation satellite system (GNSS) geolocation services to help the AWS global developer community build asset tracking and monitoring solutions and connect Internet of Things (IoT) enabled devices, using LoRa Edge, to the Cloud.

AWS IoT Core Device Location is globally available across seven regions and is available for immediate use with AWS IoT Core. The LoRa Edge device-to-Cloud solution from Semtech is highly versatile with a low power software-defined platform providing indoor and outdoor geolocation capability together with a multi-band LoRa® and LR-FHSS transceiver supporting global terrestrial and satellite LoRaWAN® networks. The scalable, low power technology is suited for IoT applications such as industrial, building, agriculture, transportation, and logistics markets.

Key benefits of AWS IoT Core Device Location, powered by LoRa Cloud, include:

- Simplified development experience to create asset tracking solutions using LoRa Edge devices and AWS, reducing time to market for these solutions
- LoRa Edge platform enables ultra-low-power devices, which can last several years on a single battery
- Single console experience with AWS IoT Core, including LoRa Cloud
- Regional availability across seven regions

Customers are excited about the opportunities and beginning adoption.

"We are pleased to build on top of LoRa Cloud, as provided through AWS IoT Core Device Location," Shunichi Higashi, Senior Executive Officer at Ryoden Corporation. "The ability to have an ultra-low power LoRa Edge geolocation solution for logistics tracking, combined with the ability to build the entire application on AWS in the Asia-Pacific (Tokyo) Region with all services on a single bill is a gamechanger."

Klika Tech, US-headquartered global systems integrator and product developer leveraged Semtech's LoRa Edge asset tracking platform using Amazon IoT Core Device Location to build a smart pill blister pack for its customer Counted. "Semtech's scalable, low power and cost-effective LoRa Edge geolocation solution makes this a perfect offering for the Counted consumer medical application," said Gennadiy M. Borisov, president and co-CEO of Klika Tech.

The feature will be compatible with several hardware devices incorporating Semtech LoRa Edge silicon that are either already commercially available such as from Semtech and Miromico or will become available in the next few months including Tektelic and Mikrotik.

"We are excited about the opportunities created with the integration of LoRa Cloud geolocation services into the AWS IoT Core platform. This greatly expands the availability of LoRa Cloud geolocation services across the globe, making it easier for developers to build world class asset tracking and monitoring solutions to connect and enable new IoT solutions," said Mohan Maheswaran, president and CEO, Semtech. "Delivering seamless and reliable LoRaWAN connectivity at scale is critical in developing a smarter, more sustainable and connected planet."

"The complexity of working with multiple vendors to create and deploy asset management geolocation services has traditionally been a challenging and time-consuming process for IoT solution developers," says Yasser Alsaied, vice president of IoT at AWS. "Today, our customers can combine the capabilities of LoRa Edge with an array of AWS services through a single console and billing experience. This gives our AWS global ecosystem the ability to build and connect track-and-trace solutions very quickly and very easily."

Semtech

Learn More

Single Pair Ethernet enables IIoT

Future-proof, compact, ruggedized and sustainable offers reliable network connectivity for Industry 4.0.

Belden has introduced a Single Pair Ethernet (SPE) portfolio of connectivity products, designed to optimize Ethernet connection possibilities in harsh environments, including industrial and transportation operations. The SPE portfolio includes IP20-rated PCB jack, patch cords and cordsets for clean-area connections and IP65/IP67-rated circular M8/M12 patch cords, cordsets and receptacles for reliable field device industrial ethernet connections.

For industrial applications, the products create the foundation for real-time communications between all devices on the network, the enterprise backbone and the cloud to improve process efficiency and reduce operational costs. As Industry 4.0 evolves and the number of sensors and actuators in automated production cells that connect to the factory backbone grows, the new SPE product portfolio is the simple, affordable solution to further enable predictive maintenance, digital twins and more.

For transportation applications, the Belden SPE products offer a 30% improvement on bending ratio and 30% smaller outer diameter, alleviating issues caused by tight spaces between vehicle bodies. In addition, the products simplify cabling to improve customer experience with a greater range of connectivity and reduce the weight added by existing connectivity products by nearly half.

The Belden SPE portfolio of connectivity products provides:

- *Future-proof innovation:* Ethernet-based, the simplified network topology enables seamless connectivity from sensors to the cloud; gateways become optional.
- *High-performance bandwidth support:* up to 10Gbits/s.
- *Rugged protection from harsh conditions:* IP65/67 design protects against mechanical shock, vibration, dust, chemicals and temperature extremes; suitable for M3I3C3E3 environments.
- *A compact, lightweight design:* increased flexibility and bending ratios make the cordsets easy to commission and overcome tight space constraints.
- *Built for sustainability:* manufactured with 55% less metal and plastic than popular Ethernet cordsets, resulting in improved carbon footprint and ESG Rating without sacrificing performance; IEC 63171-6, Lead-free RoHS compliant.

"The communication network plays an increasingly important role in both Industry 4.0 and modern transportation applications. In both areas, it's critical for real-time data from connected field devices to be monitored, seamlessly shared and analyzed simultaneously to ensure the optimal performance of the operation," said Chen Zhang, product manager at Belden. "Our SPE product portfolio ensures reliable connectivity and gives customers a future-forward solution for mission-critical industrial applications and radical new transportation applications."

SOURCE: BELDEN

New SPE product portfolio offers potential solution to further enable predictive maintenance, digital twins and more.

Belden's new SPE portfolio is a one-stop shop of connectivity products that are compact and durable, provide much greater coverage, and are the ideal network connectivity choice for machine building, automotive manufacturing, food and beverage manufacturing, intralogistics, mass transit systems, traffic control/systems, railway, train stations, and rail-rolling stock.

For more information on Belden's SPE portfolio of connectivity products please visit https://www.belden.com/products/connectors/industrial-connectors/Single-Pair-Ethernet-SPE-Connectors.

Belden

Learn More

Single-Pair Power over Ethernet

Long-reach, Single-Pair Power over Ethernet (SPoE) solutions for building and factory automation.

SOURCE: ANALOG DEVICES

New offerings facilitate powered, last-mile connectivity for factory and building automation through real-time power management, telemetry and extremely low standby power.

Analog Devices has announced what they claim is the world's first Single-pair Power over Ethernet (SPoE) Power Sourcing Equipment (PSE) and Power Device (PD) solutions to help customers drive greater levels of intelligence into smart buildings, factory automation, and other applications at the edge of traditional networks.

The new offerings facilitate powered, last-mile connectivity for factory and building automation through real-time power management, telemetry, extremely low standby power consumption, and ease of installation.

"The Intelligent Edge is one of the most exciting developments of the digital era as computing power is pushed to previously inaccessible applications and locations," said Leo McHugh, Vice President of Industrial Automation at Analog Devices. "Analog Devices is committed to delivering the unrivaled technology and solutions our customers need to leverage the full potential of the Intelligent Edge in smart buildings and factories as well as many more applications in the future."

Enabling digital buildings

Analog Devices' new SPoE solutions, LTC4296-1 and LTC9111, address the challenges of providing power and data to devices, even in remote, difficult to access endpoint locations. The solutions aim to help new families of endpoint applications to be seamlessly powered and accessed across the network and used to assess local factors such as asset health, environmental conditions, security metrics, and more. The localized awareness and control they offer are the building blocks of the digital buildings of tomorrow.

Analog Devices' SPoE solutions reduce reliance on localized power and batteries by using a single twisted pair of Ethernet cables to provide efficient, reliable, easily installed power at reduced size and weight. Combined with ADI Chronous™ ADIN1100 and ADIN1110 10BASE-T1L, Industrial Ethernet solutions, customers can reliably transfer both power and data over one kilometer – a significant increase from previous Ethernet standards.

Interoperable Efficiency

New LTC4296-1 5-port SPoE PSE with Classification and LTC9111 SPoE PD with Polarity Correction products support both SPoE and Power over Data Line (PoDL) variants of single-pair powering. SPoE augments Single Pair Ethernet to provide more reliable, fault-tolerant, and interoperable point-to-point power solutions, delivering up to 52W. Both products are 802.3cg compliant and support Serial Communication Classification Protocol.

Analog Devices

Learn More

Industrial cellular routers

Westermo industrial cellular routers enable secure access to remote assets.

SOURCE: WESTERMO

Ultra-compact and rugged wireless routers enhance connectivity to remotely located equipment and systems in demanding utility, infrastructure and transportation applications.

Westermo has expanded its range of industrial cellular routers designed to provide resilient data communications for remote sites. The new Merlin 4400 series of ultra-compact and rugged LTE Cat 4 wireless routers has been developed specifically to support extremely secure remote access to equipment and systems within demanding utility, industrial and trackside applications. High connection security gives users the confidence to expand their IP networks to include remote assets.

Resilient and reliable high-speed data communications are essential to the digitisation of the rail network, the implementation of smart grids and improving the operational performance of utilities. Network security is a fundamental requirement in these applications and to defend against increasing cyber threats, the Merlin 4400 series is equipped with a complete set of cybersecurity tools as standard. These include a TPM (trusted platform module) chip that keeps cryptographic keys secure, Secure Boot functionality ensuring the routers boot using only trusted software, and virtual private network (VPN) and stateful firewall support for data security and user authentication.

The Merlin 4400 series offers high-speed connectivity, with support for Ethernet and RS-232/485 communications to ensure suitability for a range of applications. It is suited to replace traditional modems when migrating to an IP infrastructure. Serial ports enable connection to legacy devices and equipment, and a built-in protocol gateway enables seamless connection to multiple devices using different communication protocols.

Westermo

Learn More

Studio 5000 software enhancements

Hardware support and productivity tools offered by new version of Studio 5000 Logix Designer® V35.

SOURCE: ROCKWELL AUTOMATION

One of the most desired improvements to the Studio 5000 Logix Designer experience in the process industry is the expansion for the SequenceManager™ to include 5x80P controller support. Customers will now be able to extend the same functionality that has been available and proven to a process application with the latest in process controller technology.

V35 supports the latest hardware, including the introduction of support for FLEXHA™ 5000 I/O, GuardLink® and 1756-EN4TR enhancements.

A top enhancement request from users within Studio 5000® to support the Motion applications is the ability to virtualize motion for Kinetix®, PowerFlex® and iTRAK® 5730 CIP Motion devices. Axis-Test Mode supports physical controllers and emulated controllers using FactoryTalk® Logix Echo. This allows for greater flexibility and design time experimentation via virtualization.

A new benefit with V35 is the expansion of three new process instructions that will be added and embedded in the software, including P_SD, P_nPOS, and P_valveMP. These instructions, along with the various process improvements made in the software, can be paired with PlanxPAx® seamlessly, making programming a process application more streamlined.

The latest version will align with FactoryTalk Logix Echo V2 and the upcoming Studio 5000 Logix Designer SDK, offering the first publicly available user scripting utility for Studio 5000. This improvement allows users to write C++ script commands to automate repetitive tasks in the Logix Designer application environment.

Rockwell Automation

Learn More

Gateways optimize data transfer

New gateways optimize communication from ModBus edge devices to Azure and AWS cloud platforms.

SOURCE: MOXA

Bringing the cloud closer to the edge, new AIG-100 Series of industrial-grade gateways support data conversion and reliable transfer from Modbus TCP/RTU/ASCII devices to Azure, Amazon Web Services (AWS), and MQTT cloud platforms. Adding to its value, AIG-100 Series gateways support Modbus TCP slave mode, enabling simultaneous transmission of data to a cloud platform and local SCADA system to help accelerate the deployment of the Industrial IoT (IIoT).

With AIG-100 gateways, the benefits of the cloud — lower costs, increased agility, ability to scale up and down, faster innovation — can be extended from the plant floor to remote field sites where sensors, meters, and inverters collect data critical to the IIoT's convergence of operational technology (OT) with information technology (IT). To bridge the IT/OT gap, the gateways have built-in traffic monitoring and diagnosis tools for troubleshooting communication issues for both IT (Azure, AWS, MQTT) and OT (Modbus) protocols. These tools let engineers remotely access the gateway, identify the root cause, and quickly bring operations back online.

As the number of sites grow, the gateway's provisioning tool reduces downtime associated with initial deployments and provides remote administration of devices. An intuitive software wizard configures ioLogik remote I/Os and UPorts hubs with a few clicks, eliminating complex driver installation and device setup so network administrators can realize plug-and-play ease for I/O and serial interfaces.

Most edge systems require additional programming to process data. Moxa AIG-100 Series gateways will pre-process edge data and directly transfer meaningful data back to the application, such as on-site conditions, operational trends, and energy usage. It will also support store-and-forward and datalogger functions to prevent data loss.

Moxa

Visit Website

Ethernet-APL HART converter

Easily convert existing HART transmitters to the new Ethernet Advanced Physical Layer (APL) interface.

SOURCE: PROCOMSOL

Using new Ethernet-APL HART Converter (HM-APL-PCB), transmitter manufacturers can easily convert existing HART transmitters to the new Ethernet Advanced Physical Layer (APL) interface. The PCB can be customized to incorporate custom features or size requirements (see HART-APL-DEV). You can also quickly design "direct to APL" transmitters without using HART. According to Jeffrey Dobos, President of ProComSol, "Ethernet-APL is an exciting new technology. Manufacturers who want to add it to their product portfolio can now do it quickly and without high cost."

The HM-APL-PCB consists of a ready to use PCB with a HART connector and an APL connector. Simply connect the HART transmitter to the HART connector and now the HART transmitter is an APL transmitter. The APL connection supplies all power needed for the PCB and the connected HART transmitter. Full documentation and support is included. ProComSol offers customization capabilities, to fit an existing HART transmitter enclosure.

The HART-IP protocol is used by the host system to configure and monitor the transmitter using Ethernet. Any HART-IP compliant host (such as ProComSol's DevCom family of Apps) can access the APL transmitter via Ethernet through an APL Switch. No software development required. The PCB can also be used as a baseline "direct to APL" design for new transmitters. The PCB supports various hardware peripherals such as Analog I/O, I2C, and SPI Flash memory so you can quickly prototype and demonstrate APL functions on a new transmitter without using HART. Again, full documentation and support is available along with customization services.

ProComSol

Visit Website

Industrial Ethernet Book

The only publication worldwide dedicated to Industrial Networking and the IIoT.

Visit iebmedia.com for latest updates.

New website offers deepest, richest archive of Industrial Ethernet and IIoT content on the web.

View and/or download latest issue of Industrial Ethernet Book and past issues.

Search our database for in-depth technical articles on industrial networking.

Learn what's trending from 5G and TSN, to Single Pair Ethernet and more.

Keep up-to-date with new product introductions and industry news.

industrial ethernet book

Industrial Networking & IIoT