January/February 2024 **140**
ISSN 1470-5745

industrial ethernet book

Industrial Ethernet Automation Networking & IIoT

Special Report

OPC UA Technology Update

Page 21

Industrial networking role in digital transformation 6

Visualization next big thing in smart factories? 18

Constrained EtherNet/IP on-machine sensors 30

Role of NAT routers for remote access 38

Digital transformation of smart grids 40

Visit us on the web ■ www.iebmedia.com

groov MANAGE
Home
I/O
Controller
groov View
Node-RED
Ignition
Data Service
System
Network
Security
Maintenance
Accounts
Info and Help
OPTO 22
groov
OPTO 22

GET CONNECTED...

Visit our new website at: www.iebmedia.com

Focus on digital transformation

According to the Lumen research report, *How Next-Generation Technologies Are Powering Digital Transformation*," digital transformation remains a driving force for organizations worldwide. Enterprises are racing to take advantage of new opportunities to differentiate themselves and grow revenue made possible by artificial intelligence (AI), machine learning (ML), virtual and augmented reality (VR/AR) and the Internet of Things (IoT)."

Three core trends emerged from the research, underscoring the tremendous impact of emerging technologies on enterprises around the world.

One finding is that, "in just over two years, the edge has gone from an exciting concept to a must-have reality. Organizations that want to develop, deploy and take advantage of next-generation technologies such as AI, AR/VR and the IoT need access to low-latency computing. And demand is driving them to adopt edge-first architectures to support their latency-sensitive, high-bandwidth apps."

A second key trend is that securing and scaling key applications remains a challenge.

According to the report, "this calls for a completely new approach to enterprise network architecture: the combination of networking and security into a single service controlled and managed in the cloud."

The third trend is that network modernization is vital to efficiently support hybrid enterprises.

Check out our cover story, "Industrial networks playing key role in digital transformation," starting on page 6 to learn what industry experts told the Industrial Ethernet Book about these trends.

According to Dr.-Ing. Frank Possel-Dölken, Chief Digital Officer and Member of the Group Executive Board for Phoenix Contact, "in the overall discussions on Digital Transformation, there is mostly a focus on developing new digital solutions/business models for gaining revenue – and partly the necessity of implementing new and more capable software systems for raising the potential out of digital transformation."

Possel-Dölken added that "our main statement and remark to other companies, of course with regards to our own activities and experiences, is to emphasize the protection of both enablers for Digital Transformation as well as the basic infrastructure of industrial enterprises."

For our industry, network platforms play the key role in modern IT-OT environments and are vital for businesses that want to leverage all the advancements made possible by emerging technologies.

Al Presher

OPC UA technology bridges gap: 21

New Products: 52

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2024.**
Deadline for editorial: March 12, 2024 **Advertising deadline:** March 12, 2024

Editor: Al Presher, editor@iebmedia.com

Advertising: info@iebmedia.com

Tel.: +1 585-598-6627

Free Subscription: iebmedia.com/subscribe

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

CIP Security firewall offers enhanced intrusion deterrence

Device-based firewall profile has been added to CIP Security to further protect EtherNet/IP networks and help discourage bad actors from infiltrating industrial networks.

ODVA HAS ANNOUNCED THAT CIP SECURITY^{TM}, the cybersecurity network extension for EtherNet/IP^{TM}, has added a new device-based firewall for enhanced intrusion deterrence. The CIP Security device-based firewall provides users with a simple traffic filter similar to how the IP Tables program enables a firewall to be setup in Linux.

The device-based firewall is enabled via a CIP Security Device-Based Firewall Profile, which allows flexibility to enable or disable this feature as desired. CIP Security now offers robust device level protections with a device-based firewall to discourage bad actors from infiltrating EtherNet/IP industrial networks.

The CIP Security device-based firewall is a mechanism to filter traffic based on IP address, port, and protocol. The device-based firewall is implemented via a new CIP object called the Ingress Egress Object, which enables an allow list of known IP addresses, configuration of available cipher suites, and routing rule definitions based on IP addresses and port numbers. This means that EtherNet/IP devices with CIP Security can determine what nodes can be safely communicated with and whether TLS or DTLS encryption is required. Additionally, the user can decide whether other devices can route CIP communications through the configured CIP Security device. The new device-based firewall adds another layer of deterrence as a part of a defense in depth approach to help protect physical and digital assets from harm.

SOURCE: LoRa ALLIANCE

CIP Security update provides users simple traffic filter similar to how the IP Tables program enables a firewall to be setup in Linux.

"CIP Security continues to add additional security capabilities such as the new device-based firewall to help protect EtherNet/IP devices from misuse that could lead to critical system damage or information loss," stated Jack Visoky, EtherNet/IP System Architecture Special Interest Group (SIG) vice-chair.

Dr. Al Beydoun, President and Executive Director of ODVA said "the prevention of unauthorized IP address and port numbers from accessing CIP Security enabled EtherNet/IP devices allows for another layer of protection for critical industrial automation applications as a part of a defense in depth approach. The addition of the device-based firewall profile for CIP Security is another important update to continue the fight against malicious cyber intrusions that can lead to financial and reputational loss."

The new profile allows for only known IP addresses to communicate using standard EtherNet/IP. Additionally, permitted CIP routing can be configured based on a set of trusted IP addresses, ports, and encryption. As a result, data packets without matching IP address and/or ports will be dropped and therefore won't be able to complete intended malicious tasks.

News report by ***ODVA***.

PROFINET security specification updated

OT SECURITY IS PROVING ITSELF TO BE a decisive requirement for secure data collection, which is of crucial importance when it comes to implementing digitalization projects. Digitalization means, for example, the optimization of production processes and alignment between the physical and digital worlds. At the same time, normative requirements on the cyber security of machines, systems and companies are becoming stricter.

PI (PROFIBUS & PROFINET International) already realized some time ago that the underlying requirements in the area of OT security are of utmost importance. Step-by-step specifications, proofs of concept and guidelines were developed by technical working groups. This process makes it possible to adapt the scope in a manageable and flexible way.

PROFINET Security Class 1 has transitioned to concrete implementation. For this purpose, PI established infrastructure for the signing of GSDs. The basic elements for Security Classes 2 and 3 have been defined in the most recent specifications and include a definition of crypto-algorithms and certificate handling, among other things. This means that hardware and firmware producers have already been able to get started with development. At present, the final functions—some of which have also been derived from IEC62443—are being specified in detail, including security reporting.

As expected by both members and users alike, PI is establishing certification alongside this. The result will be applicable and recognized security technology which meets the respective requirements and has been developed in close cooperation with manufacturers, users and relevant institutions and authorities.

With this concrete progress, PI is making a valuable contribution to the strengthening of cyber security in the OT field and is also helping to make the digital transformation in industry more secure.

News report by ***PI***.

| V11-01E |

Vision: Complete and system-integrated

reddot winner 2023

iF GOLD AWARD 2023

- 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**

Industrial networks playing key role in digital transformation

Digital Transformation (DX) is a goal for manufacturers with advances in artificial intelligence and machine learning, along with augmented and virtual reality, adding new possibilities. But the overall focus for industrial networks is still on speed of deployment, enhanced visibility and flexible, resilient software-defined operation.

SOURCE: PHOENIX CONTACT

"Our main statement and remark to other companies, of course with regards to our own activities and experiences, is to emphasize the protection of both enablers for Digital Transformation as well as the basic infrastructure of industrial enterprises." -- Frank Possel-Dölken, Chief Digital Officer and Member of the Group Executive Board, Phoenix Contact.

DIGITAL TRANSFORMATION IS AN ONGOING quest for manufacturers poised to harness advanced manufacturing networking and software solutions to create new avenues for continuous innovation, strategic success and long-term profitability.

In this special report, the Industrial Ethernet Book reached out to industry experts to gain their insights into the megatrends driving Digital Transformation (DX), and new fuel for the fire with recent advances in artificial intelligence, machine learning and more.

Effective management of networked assets

Fast, scalable and automated updates for network-enabled, operational technology (OT) and devices.

A team of industry experts from Phoenix Contact responded to our questions on what technologies and/or megatrends are shaping and enabling Digital Transformation in 2024 and beyond.

"One major topic for shaping and enabling future Digital Transformation is the development of solutions for fast, scalable and automated device and update management (DaUM) of network-enabled operational technology (OT) devices." Dr.-Ing. Frank Possel-Dölken, Chief Digital Officer and Member of the Group Executive Board, told IEB. "This is largely motivated by increased activity of cyber criminals attacking not only classic IT infrastructure (for example, credential phishing for Microsoft, Apple or Google services) but also directly targeting operational technology (OT) systems."

Possel-Dölken said that it is of high importance to understand the need for action at industrial enterprises. For cyber criminals, it is easy to gain access to OT systems because factories contain a variety of network-enabled devices from different manufacturers relying on different communication technologies and protocols. 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. Further exacerbation results from upcoming regulatory requirements.

"In the overall discussions on Digital Transformation, there is mostly a focus on developing new digital solutions/business models for gaining revenue – and partly the necessity of implementing new and more capable software systems for raising the potential out of digital transformation," Possel-Dölken said. "Our main statement and remark to other companies, of course with regards to our own activities and experiences, is to emphasize the protection of both enablers for Digital Transformation as well as the basic infrastructure of industrial enterprises."

Asset Administration Shell

Possel-Dölken added that the implementation of device and update management for

SOURCE: PHOENIX CONTACT

Machines usually consist of several hardware-software-devices from multiple vendors. During both development and maintenance phase, the availability of latest information is required – e.g. master data or information about software updates. The process of gathering all the information initially – most probably from the webpages of the numerous manufacturers – and keep them updated is costly.

networked OT devices requires seamless and barrier-free data logistics across manufacturer specific systems. The Asset Administration Shell (AAS) as a standardized technology for developing digital twins plays an essential role in establishing this solution. Why? The AAS operates as a data container and enables the standardized data transmission via common sub models, structure and security requirements. The big advantage: it is standardized! Both the transmitting and receiving enterprise understand and use the identical semantic (=semantic of AAS) for the information/data. The further processing of the received data, e.g. the integration into the internal PLM system of the receiving company, is executed fast.

"A good example that highly benefits from this solution is an internal machine building department, developing and building highly automated production equipment for production facilities," said Dr.-Ing. Guido Hüttemann, Assistant to Chief Digital Officer. "Such machines usually consist of several hardware-software-devices from multiple vendors. During both development and maintenance phase, the availability of latest information is required – e.g. master data or information about software updates. The process of gathering all the information initially – most probably from the webpages of the numerous manufacturers – and keep them updated is costly, requiring both a lot of time and binding scarce human resources."

He added that 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.

Another major driver for the operational implementation of data-driven use case such as device and update management is the cross-industry initiative called Manufacturing X. The overall goal of this initiative is to develop a sovereign data space for the entire industry. This is an enabler for exchanging data securely and confidentially along value chains without relinquishing control.

Currently, several consortia are awaiting the approval of their project proposals. The initiative is funded by the German Federal Ministry for Economic Affairs and Climate Action and lasts until mid of 2026.

Interoperability challenges

Dr.-Ing. Christoph Kelzenberg, Director Digital Innovations said that, overall, the missing interoperability of software systems within one enterprise as well as between different enterprises is addressed by the technologies mentioned before. The consistency of data is not only required from customers (e.g. traceability as a customer requirement), it is also required by law (e.g. supply chain act in Germany).

"An exemplary customer benefit of the AAS technology is the ability to develop the real digital twin of an asset. To understand that, it is very important to distinct between an "As-Built" bill of material and an "As-Is" bill of material! Nowadays, the end customer receives a bill of material that includes all information of the factory state of an asset – meaning a status as built in the factory," Kelzenberg said. "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 control cabinet – different entities add, configure and adjust components. They do parameter adjustments, apply software updates and perform other customizations. The consistent usage AAS technology allows to capture changes, such as a configuration of a power supply within a cabinet, and thus to develop the "real" digital twin of an asset."

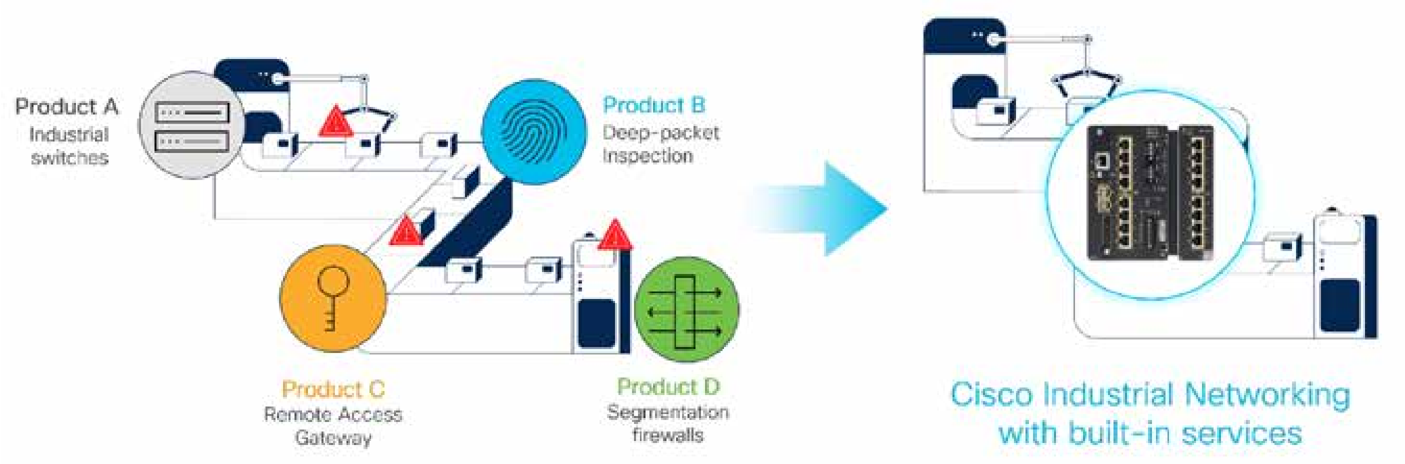
With regards to the automation and control engineers itself, Kelzenberg said the solutions allow them to focus on the essential, value-adding tasks during a typical workday. Time-consuming and barely value adding tasks – such as gathering information and data and putting them into a software system – will be obsolete as the described IoT technologies/ solutions would be in place.

Building more capable networks

Focus on speed of deployment, enhanced visibility and flexible, resilient software-defined operation.

Carlos Rojas, Global Manufacturing Solutions Lead, Industries Group, at Cisco said that there are a number of noteworthy trends continuing to push Digital Transformation forward.

"First, workforce shortages are fueling the demand for more automation and software-based decision making. Secondly, the desire for more flexibility in operations is driving greater investments in robotics, mobile systems, and wireless technologies. And finally, increasing number of cyberattacks is triggering a renewed focus on cybersecurity and the necessity of secure remote access into operations. And of course, ubiquitous connectivity is paramount to shaping and enabling a sustainable digital environment,"



SOURCE: CISCO

"An effective digitization solution not only relies on switches, routers, and wireless equipment to enable connectivity between assets, but this equipment must be supported by intelligent management and security systems. Together such a solution provides several technical benefits that enable new IIoT applications," Carlos Rojas, Global Manufacturing Solutions Lead, Industries Group, Cisco.

Rojas told IEB recently.

With these new requirements there is also a renewed need for simplifying deployments. The addition of single-function point solutions for each technology is only adding complexity and difficulty in scaling.

“A better answer lies in building a more capable network. Building such a network starts with equipment that is designed to withstand the most challenging of environments and can scale with your operations. Managed networking equipment such as switches and routers that are fit for use in industrial environments, that is, are ruggedized and designed in an environmentally friendly manner can enable digital transformation at scale,” Rojas said.

Look to equipment that’s faster to deploy and enhances visibility into the operations for managing planned and unplanned downtimes. They help build a scalable, flexible, resilient, software-defined network critical for success for any digitization initiative. Such a network can ease deployment of advanced future-ready AI/ML applications that avoid obsolescence and protect operations from becoming “brownfields of the future.”

Technical benefits

Rojas said that an effective digitization solution not only relies on switches, routers, and wireless equipment to enable connectivity between assets, but this equipment must be supported by intelligent management and security systems. Together such a solution provides several technical benefits that enable new IIoT applications.

These technical benefits start with the networking devices themselves. Today’s highly capable equipment is ruggedized to withstand extreme conditions, rivals enterprise equipment in performance, supports lossless resiliency protocols, all the while maintaining a high MTBF. Paired with an intelligent management system, networking tasks can be automated, reducing errors which saves time and costs. With proactive detection of network faults and guided remediation, the network can be relied on to be at its optimum performance. Such a system also lets you segment your operations for further protection.

Previously, a lot of advanced applications used to require additional hardware. With edge-computing capabilities, the network equipment can autonomously run these applications reducing complexity and costs.

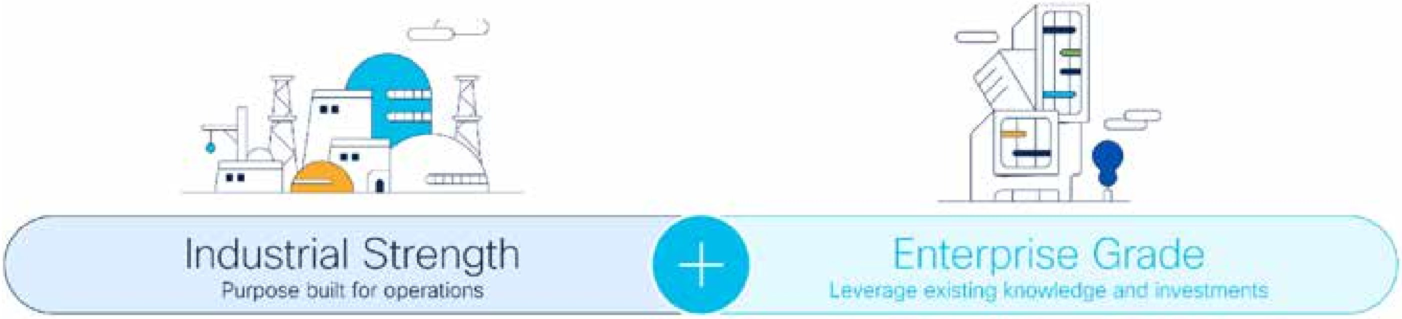
One such applications performs DPI on network traffic to identify connected devices, their interactions, and vulnerabilities, providing you with deep visibility into your operations. Another application enables remote zero-trust network access to industrial assets avoiding more complex methodology. Yet another application collects real-time process data and transmits it to AI/ML aided analytical applications in the cloud that can help monitor product quality, maintenance needs, etc. These innovations would not be possible without advancements in industrial networking equipment.

Industry applications

“Manufacturers are rapidly modernizing their operations by introducing new data driven and software-controlled decision making. They are using these techniques to minimize unplanned downtimes, add production flexibility, improve security, and reduce costs,” Rojas said.

For example, a software driven, deterministic, resilient, and secure network is helping virtualize discrete hardware systems on a factory floor, replacing them with software functions that run in collocated hyper converged infrastructure. This is bringing huge benefits to manufacturers by reducing their maintenance costs, lowering the threat surface, and improving sustainability.

These solutions are also helping industries comply with increasing cybersecurity regulations. For example, European legislators are being asked to implement EU’s NIS2 directive. NIS2 aims to improve cybersecurity, enhance resilience, create a uniform standard,


Industrial Strength
Purpose built for operations
Enterprise Grade
Leverage existing knowledge and investments

SOURCE: CISCO

An industrial network that combines the best of two worlds eases control engineers' jobs.

SOURCE: ISTOCK

"The Digital Transformation landscape is significantly influenced by the capability of edge computing to facilitate real-time AI/ML applications through local processing. The distinct advantage lies in the ability to execute computations at the edge, ensuring real-time decision-making without solely relying on distant cloud resources. ," Marian Hönsch, Product Manager - Industrial IoT at TTTech Industrial.

and foster better cooperation between member states. A unified industrial networking and security architecture with visibility, segmentation, and secure remote access is well positioned to easily meet these new requirements.

Responding to challenges

"A proven standardized network architecture removes risks for automation and control engineers and lets them focus on their jobs and bringing about innovation. Such a network can remove one of their biggest challenges of not having a connectivity solution that interoperates across multiple protocols, connects both legacy and modern equipment, and one that is easy to scale and troubleshoot," Rojas added.

"A dependable network makes it easy for them to add new devices, expand their digitization initiatives, validate their POC efforts, and bring new technologies and solutions into their operations quickly and easily, knowing that the network has their back."

Real-time data collection capability of the network helps them gain insights into their processes, allowing them to determine the changes necessary for optimization, improve yield and quality, or data needed for Digital Twin, AI and M/L.

Secure remote access to industrial assets allows engineers to configure, monitor, troubleshoot, or collect logs from these assets, helping them ensure that these assets are always running efficiently.

Leveraging edge IoT platforms

Technology facilitates real-time AI/ML applications through local processing.

Marian Hönsch, Product Manager - Industrial IoT at TTTech Industrial, said that "in 2024, key technologies shaping Digital Transformation include AI/ML integration, edge computing, and secure IoT connectivity. The importance of n flexible and secure edge IoT platform emphasizes the vitality of a secure collaboration between IO and OT. Edge computing enables data preprocessing locally, ensuring efficient use of bandwidth. In EU. the industry stakeholders will be confronted with the impact of the NIS2 Directive and the EU Cyber Resilience Act. The distinction of AI/ML into cloud and edge parts ensures flexibility and efficiency in processing and decision-making in real-time."

Hönsch said that secure edge IoT platforms provide local preprocessing, reducing data exposure and enhancing resilience against cyberthreats. Failure to incorporate robust security measures in the foundation of applications renders them incapable of being part of and connected to the IIoT, underlining the indispensable role of secure edge computing in shaping the digital future.

"The Digital Transformation landscape is significantly influenced by the capability of edge computing to facilitate real-time AI/ML applications through local processing. The distinct advantage lies in the ability to execute computations at the edge, ensuring real-time decision-making without solely relying on distant cloud resources. This not only enhances the efficiency of IIoT applications but also addresses the critical aspect of cybersecurity and the fact that even the best Internet connection can be unavailable sometimes," Hönsch said.

Anticipated impact

The application of cutting-edge solutions in 2024 involves not only the integration of secure edge IoT platforms but also a keen emphasis on swift responses to potential threats. The imperative lies in the need for a robust patch management system spanning all vertical levels of an IIoT application throughout the complete supply chain. This approach ensures a proactive stance against exploits and vulnerabilities as required by upcoming regulations. Specifically, in the realm of AI/ML applications integrated into real-time machine operation cycles, the agility to address emerging threats becomes even more critical.

According to Hönsch, the technologies under consideration address challenges for automation and control engineers by fortifying cybersecurity and optimizing data processing. They alleviate concerns related to bandwidth constraints and latency, providing local preprocessing capabilities.

Moreover, the need for secure edge IoT platforms, influenced by the NIS2 directive and the EU Cyber Resilience Act, plays a pivotal role in ensuring the integrity of automation systems.

"A notable challenge for engineers is the diversion of focus from their core value-added applications. As they are increasingly compelled to engage in infrastructure tasks and self-developed edge hosting maintenance, there's a pressing need for regaining development capacity. To overcome this challenge, engineers can benefit from adopting cloud-managed edge solutions as products, enabling them to refocus on their company's core competencies and innovative applications," she concluded.

Impact of AI and ML technologies

Overall push is to access data, contextualize it and put it in front of employees to drive better decision making.

According to Andrew Stump, director of business development at Rockwell Automation, "we'll likely continue to see industrial producers adopting digital technology at a faster pace in 2024. This is partially a continuation of the pandemic having forced companies to accelerate their digital transformation efforts to keep workers connected and mitigate risks like supply chain challenges."

"But there's another force driving the accelerated adoption – the technology itself. In 2023, ChatGPT burst onto the scene and thrust artificial intelligence (AI) and machine learning (ML) into the spotlight. This changed how work could be done almost overnight. And as ChatGPT and many new industrial tools have shown, these technologies can be used by nearly anyone. They don't require specialized expertise in data science or coding. Now, leadership teams are feeling an urgency to act and unleash the potential of these technologies, or risk falling behind," Stump said.

Adoption of digital technologies

He added that the accelerated adoption of digital technologies is also driving another trend – the need for help. While pilot projects can demonstrate how technologies like AI and ML can deliver value, producers want to realize that value as soon as possible. Companies need partners who understand these technologies and can help craft a strategy to apply them efficiently, cost effectively and with intent.

Stump said that, for years, industrial producers have been working to access data from their operations, contextualize it and put it in front of employees to drive better decision making. Now, AI and ML technologies can help producers use data in new ways and unleash new possibilities in production.

AI and ML technologies allow broader and easier analysis of information. They can use more inputs and make decisions more quickly, without the bottleneck of requiring humans to interpret, understand, and act on information.

For example, add-on modules with built-in AI engines can be paired with industrial controllers to help optimize production in several ways. They can learn the baseline for a production process and detect anomalies against that baseline to help maintain quality levels. They can also create virtual sensors, which analyze variables from line assets and predict measurements that may otherwise be too difficult or costly to obtain using physical sensors.

"It's important to note, however, that these technologies shouldn't all simply be deployed in the cloud. Improving quality and optimizing processes requires being able to access and analyze data in real time. And that happens at the edge. This is why producers should have an edge-to-cloud strategy that allows them to use data and technologies like AI and ML tools where it best serves their applications' needs," Stump said.

Impact of new technology

"A top priority in the industrial world right now – and a key opportunity for AI and ML technologies – is to improve sustainability performance. The Eastern Municipal Water District (EMWD) in California provides a good example of what's possible," he added.

EMWD serves nearly 1 million people in Southern California and is the state's sixth-largest retail water agency. Recently, it deployed an AI solution at its aeration operations, which is an energy-intensive process in water treatment. Installed on the

SOURCE: ISTOCK

"AI and ML technologies allow broader and easier analysis of information. They can use more inputs and make decisions more quickly, without the bottleneck of requiring humans to interpret, understand, and act on information," Andrew Stump, director of business development," Rockwell Automation.

existing plant automation network, the AI solution learns the current state of aeration operations and optimally adjusts PID response as conditions change – all with minimal staff intervention.

The solution has improved process control in the operation and delivered an estimated savings of 2,330 kWh of electricity per day – and more than $100,000 of cost savings per year.

Companies are also exploring how they can combine AI and machine vision to optimize quality through closed-loop control. Maintenance is another area of opportunity. An ML-based supervisory application, for instance, can alert technicians if a machine deviates from normal behavior that may signal maintenance is needed. And AI-based tools for CMMS software can help maintenance teams predict and prevent asset failures before they happen.

Addressing challenges for automation and control engineers

Stump said that, for industrial engineers, production optimization is a never-ending quest. As we've discussed, AI and ML have great potential to help engineers improve KPIs like quality, throughput and uptime in their operations.

These technologies can also improve worker effectiveness in a tight labor market. They can capture the knowledge of long-time workers and pass it on to newer, less-experienced workers. They can also provide important context – like which alarms require the most urgent attention.

"The current focus on creating simpler tools can also help workers take advantage of technologies like AI and ML without having specialized knowledge in them. In some cases, workers can simply point AI-enabled tools toward the data points that are most relevant to what they're trying to solve, and the tool will create a model for them," he said.

"And it's not just in technologies like AI and ML where greater simplicity is making a difference. There's a growing demand for industrial robotics to help lighten the loads for operators. Through eased integration between robot and machine control systems, vendors are making it easier to configure, operate and maintain these technologies without having specialized knowledge in robot programming."

Pervasive connectivity

From unconnected components into a unified group of devices focused on specific results.

According to Dr. Al Beydoun, President and Executive Director at ODVA, "pervasive connectivity is positioned to transform industrial automation in 2024 and beyond. The combination of new technologies including Single Pair Ethernet (SPE), wireless 5G, and Artificial Intelligence (AI) will enable more devices than ever before to be connected to the network while also allowing for continuous feedback loop optimization based on real world input being fed into data models and back onto the production floor. SPE will enable low cost, remotely located devices - such as those positioned far away on a warehouse conveying system, constrained devices in cabinets, and process devices in hazardous areas - to all become a part of the Ethernet plant network."

Beydoun said that 5G has already started to enable the emerging use of Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs) to move freely throughout the factory floor to allow processes to become more flexible and to allow workers to focus on higher value-added tasks instead of being tied up making sure that parts are loaded into a machine, for example. AI is a powerful tool that is able to analyze current production data relative to data models based on operating information over a much longer timeframe to be able to deliver both automated production optimization as well as actionable recommendations for operators in much less time than previously possible.

Focus on technology solutions

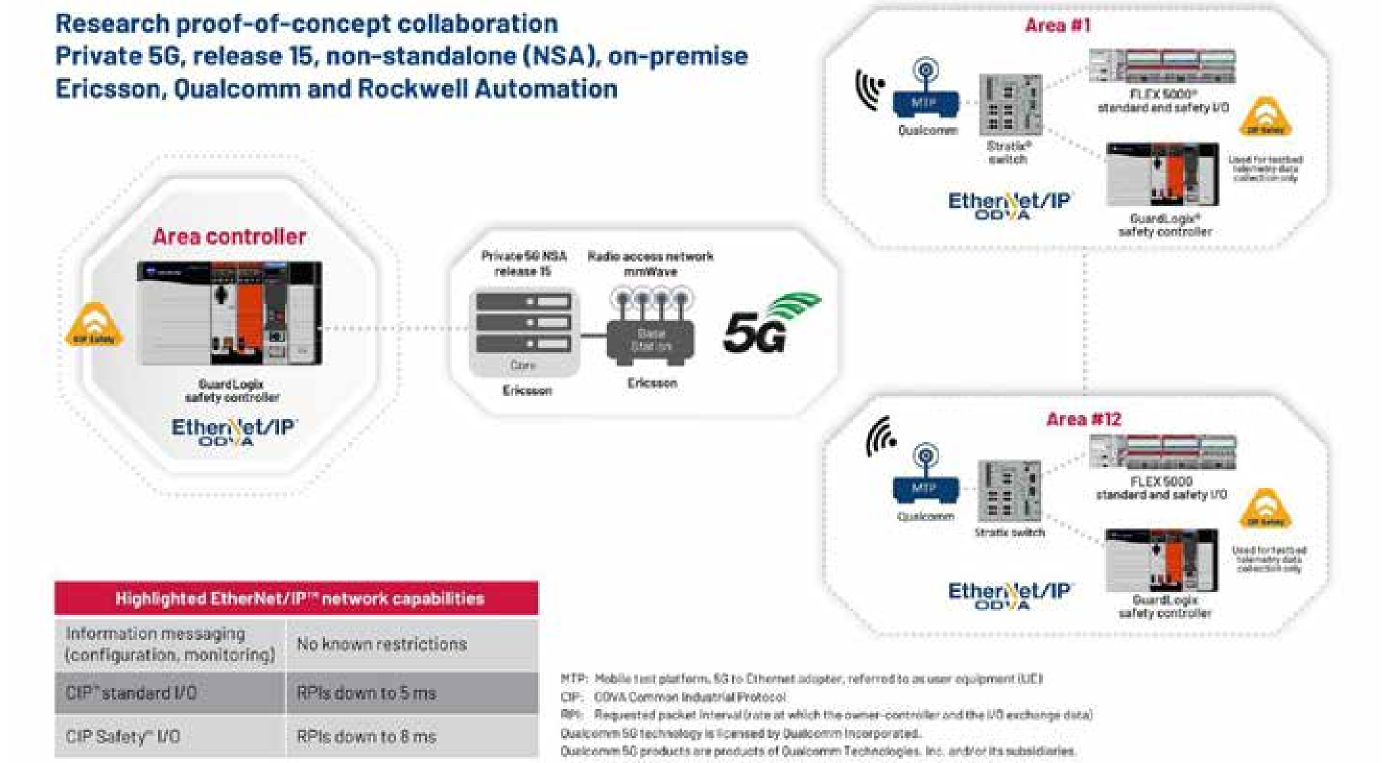
"Pervasive connectivity will help transform plant operations from being an assortment of unconnected components that operate in an opaque manner into a unified group of devices across the network with readily available insights that point to actions that lead to results. In the current paradigm, it takes a significant amount of time to collect data from different sources, to clean the data to remove blank or erroneous entries, to collate all of the information, to conduct a manual data analysis, and to finally create an action plan," Beydoun added.

He said that solutions like SPE and 5G will allow for data to be more easily collected both saving time and providing a more complete picture of operations. Additionally, AI will allow for a reusable optimization model to be built, allowing for multiple analyses going forward based on the existing operations data that indicates what ideal performance is, as well as what conditions such as imminent failure or maintenance needed look like.

The use of Ethernet at the device level and beyond also enables powerful tools like SQL to be taken advantage of. The unmodified, standard Ethernet foundation of EtherNet/IP along with its ease of use is one of the reasons that it's possible today to push factory floor data from CIP objects into powerful tools like SQL for analysis and action. ODVA Members such as Softing help enable the seamless transfer of CIP object data from EtherNet/IP into SQL databases.

Application implementations

Many experienced workers are also transitioning into retirement, leaving a large knowledge gap behind in the companies and industries that they are departing, including within industrial automation. Additionally, since productivity gains are often tied to increases in wages, there is further incentive across companies to find novel ways to accomplish more with fewer resources.



Research proof-of-concept collaboration
Private 5G, release 15, non-standalone (NSA), on-premise
Ericsson, Qualcomm and Rockwell Automation

Area controller
CIP Safety
GuardLogix safety controller
EtherNet/IP ODVA
Private 5G NSA release 15
Radio access network mmWave
Core
Ericsson
Base Station
Ericsson
5G
Area #1
MTP
Qualcomm
Stratix® switch
FLEX 5000® standard and safety I/O
CIP Safety
Used for testbed telemetry data collection only
GuardLogix® safety controller
EtherNet/IP ODVA
Area #12
MTP
Qualcomm
Stratix switch
FLEX 5000 standard and safety I/O
CIP Safety
Used for testbed telemetry data collection only
GuardLogix safety controller
EtherNet/IP ODVA

Highlighted EtherNet/IP™ network capabilities	
Information messaging (configuration, monitoring)	No known restrictions
CIP™ standard I/O	RPIs down to 5 ms
CIP Safety™ I/O	RPIs down to 8 ms

MTP: Mobile test platform, 5G to Ethernet adapter, referred to as user equipment (UE)
CIP: ODVA Common Industrial Protocol
RPI: Requested packet interval (rate at which the owner-controller and the I/O exchange data)
Qualcomm 5G technology is licensed by Qualcomm Incorporated.
Qualcomm 5G products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

SOURCE: ODVA

"Pervasive connectivity will help transform plant operations from being an assortment of unconnected components that operate in an opaque manner into a unified group of devices across the network with readily available insights that point to actions that lead to results," Dr. Al Beydoun, President and Executive Director at ODVA.

Utilizing SPE to connect additional devices to the Ethernet network enables benefits such as remote commissioning, standardized diagnostic alarms, and even prognostic forecasting made possible by edge and cloud appliances running optimization models enabled by AI. Additionally, the latest 5G technology releases are enabling low latency and sufficiently high bandwidth for many automation applications including AGVs and AMRs. Additional benefits of 5G include not having to manage physical access points that will require upgrading over time. 5G has recently been demonstrated by multiple ODVA Members, including Rockwell Automation and HMS Networks to be capable of powering EtherNet/IP devices, including those utilizing the CIP Safety network extension.

"It's also important to note that while technology can develop in an exponential way, many times organizations progress linearly due to the time it takes to diffuse new information across culture and processes. That means that although SPE, 5G, and AI may be technically ready for use, it will still take time to see widespread adoption across industrial automation," Beydoun said.

Leveraging remote connectivity powered by SPE

He added that automation and controls engineers can leverage remote connectivity powered by SPE to help reduce time needed for plant and machine startup and troubleshooting. Instead of spending a day chasing down a line break, an offline device can indicate the problem in short order. Wireless 5G as an all-encompassing plant wide network can also make it much easier to add additional devices over time for additional diagnostics information. 5G can also easily accommodate modifications to the production line flow.

Additionally, AI will help what were stressful and time-consuming projects to identify production bottlenecks and quality problems to become much more manageable daily tasks after the work of developing a comprehensive model is completed. While today AI model creation typically requires a highly trained data scientist, there are efforts in the works to develop more user-friendly tools to allow existing IT/OT networking and operations workers to be able to handle the tasks with the aid of standardized software tools. Removing the requirements for specialized skills to fully utilize AI will be a key driver in the next phase of significant productivity improvements in automation.

Impact of artificial intelligence

AI looks to provide valuable insights, predictive capabilities, and automation to ensure business resiliency.

According to Dale Tutt, VP Industry Strategy at Siemens Digital Industries Software, "while there are several technologies and/or megatrends that I think will shape and enable digital transformation in 2024 and beyond, the one that has everyone talking these days is artificial intelligence (AI). It is already changing how businesses work and can be transformative in ways that we are not even predicting yet. As companies continue to face growing pressures to innovate faster, manage costs, navigate supply chain disruptions more effectively, fill open positions and produce more sustainable products, AI's impact will continue to grow."

Tutt said that companies are looking for technologies like AI to provide valuable insights, predictive capabilities, and automation to ensure business resiliency. For example, this could help navigate supply chain disruptions caused by pandemics, natural disasters or political conflict.

And, on the shop floor, AI can help automate mundane tasks to allow engineers more time to focus on solving design challenges. It is important to note that in this scenario, AI will not take away jobs but instead enable workers to focus on innovation. These are just a few examples. I expect AI's capabilities will prove to be even more impactful and help provide the foundation for the highest level of digital transformation.

"We are also going to continue to see an increase in the use of augmented reality (AR) and virtual reality (VR) to create a truly immersive engineering environment. With digital solutions, we are always looking for

SOURCE: ISTOCK

"The changing workforce is also a place where the impact of the industrial metaverse will be seen. The next gen workforce has advanced expectations of working and collaborating in the digital world with AR/VR and AI," Dale Tutt, VP Industry Strategy at Siemens Digital Industries Software.

enhanced ways to present data to the user in a way that enables them to increase their efficiency. The same immersive environments being used for design and design reviews can also be used to augment how people work, how they build, and how they maintain products. The more companies can present in virtual and augmented reality, the more effective they are going to make their technicians and engineers," Tutt said.

He added that advances in AI and AR/VR will set the stage for the industrial metaverse to play a significant role in enabling digital transformation this year. The industrial metaverse can be thought of as a virtual world that is almost indistinguishable from reality, a similar concept to a digital twin. But to reach its full potential, the industrial metaverse must become more than a visualized version of the digital twin. On the manufacturing floor, every movement and action must be accounted for precisely, demanding real-world physics.

"Some may think it is overhyped, but the foundational technology of the industrial metaverse is still going to be in demand for customers: the greater computing power, the ability to do faster, real-time, high-definition visualizations, and access to cloud-based computing, which will support the industrial metaverse with the necessary computational power," he added.

When combined with AI, the industrial metaverse will enable companies to instantaneously work together to address real-world challenges. Companies will be empowered to adopt new technologies faster to accelerate innovation and enhance sustainability. The industrial metaverse has the power to transform entire industries.

The changing workforce is also a place where the impact of the industrial metaverse will be seen. The next gen workforce has advanced expectations of working and collaborating in the digital world with AR/VR and AI.

"Finally, I expect the digital thread itself to be even more impactful in 2024. Companies are interested in the connectivity they can get when they are moving from one application to another. The digital thread and digital transformation are the foundation and key to leveraging these new digital trends, including AI and the industrial metaverse," Tutt said.

Technology payoff

The technical benefits these solutions provide are how they can optimize production processes and connect factories. A factory with increased connectivity can bring data from the production floor anywhere, at any time, analyze it, and find and optimize interactions that might not have been previously available or would have taken significantly longer to find with typical applications. The data has always been there but now you can see it in real-time and visualize it differently. Today, companies have significantly more options to integrate their solutions and manage and optimize their production processes.

"Connectivity and additional computing power are something that we are doing a lot with the executable digital twin. IIoT is bringing all of the data together in a big data lake and doing data analytics, but at the same time it is also moving some of that computation to the machine and feeding it into the digital twin to enable even further optimization," Tutt said.

He added that "one of our customers is a battery supplier and they have been using Insights Hub, our solution that drives smart manufacturing through IIoT. This customer uses Insights Hub to gain actionable insights from their asset and operational data. They are using this to optimize their production processes and help improve the yield of their battery production. This is a great example of how to bring data and data analytics together in a way that could not have been done five or 10 years ago, maybe even two or three years ago. Companies are seeing a significant improvement in the yield and the impact of that is how it affects the bottom line."

Another customer is doing the same thing in their new production facility for engine blade production. They are getting a much more holistic view of their factory operations because they have more data available to them, enabling them to improve their yield. This goes back to the convergence of IT and OT, which provides manufacturers with greater flexibility and visibility and encourages collaboration across planning, scheduling, and factory performance, leading to superior efficiency. "We are seeing these successes and I know of customers who are experiencing production increases of 15 to 20 percent," Tutt said.

Process optimization

These technologies help automation and control engineers optimize their production lines faster and in a more controlled way, especially when they are managing their data and their applications with good configuration control. They can now track changes much more effectively over time.

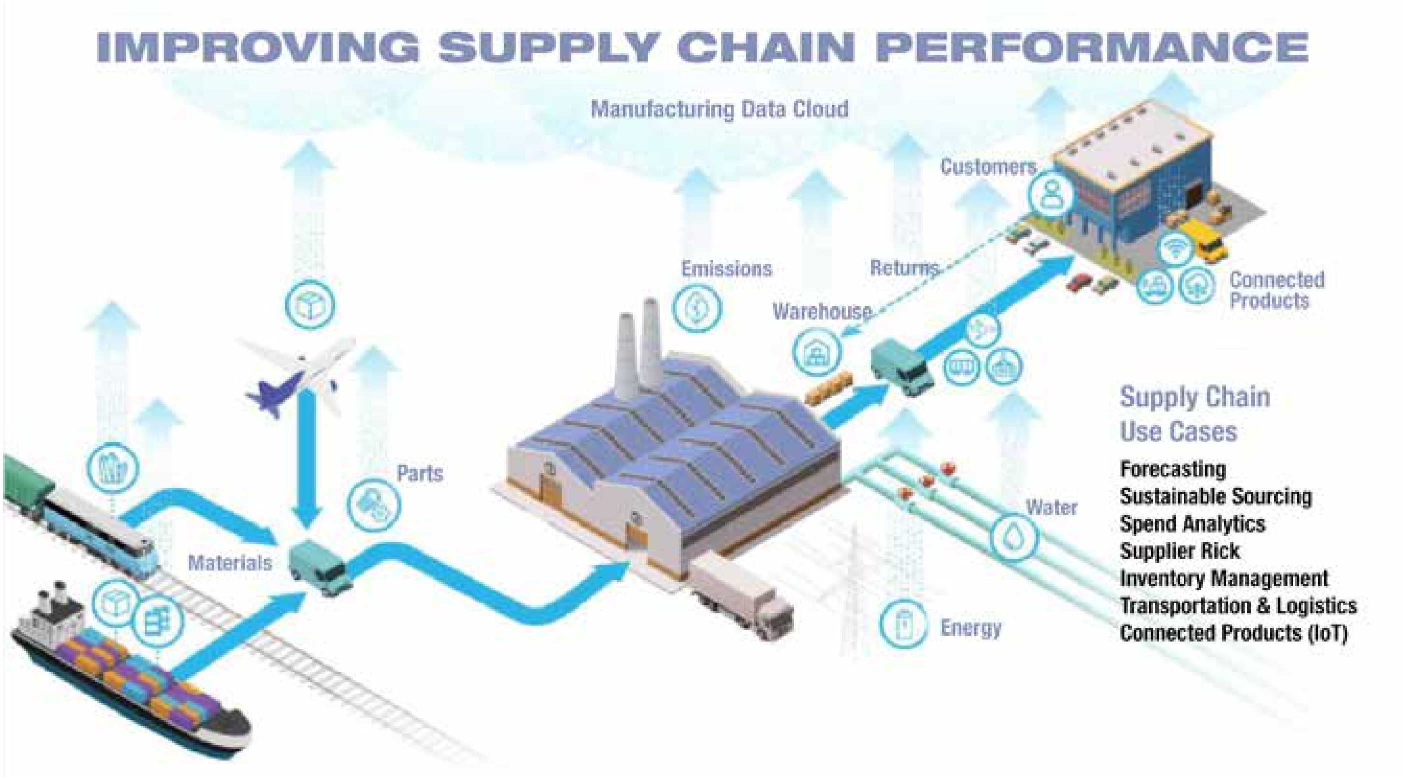
"Digital transformation enables companies to combine the real and digital worlds and unlocks a critical resource, data, the flow of which can now be shared between all stakeholders involved in a project. Using digitalization in this manner can also guide and support companies on their sustainability journeys, facilitating energy and resource efficiency and decarbonization by using fewer resources to achieve results," Tutt said.

"While digital transformation can help companies address the more immediate pressures coming in 2024, it can offer much more to companies that build a plan to evolve beyond connecting data into higher level functions such as automation of data management and eventually the closed-loop optimization of products and processes. It is not a short-term fix but instead a long-term strategy for smart companies," he added.

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

Snowflake solution from industrial edge to the cloud

By leveraging machine and production data, companies can leverage smart manufacturing solutions to optimize business operations, forecast parts usage, assess supplier quality, and adopt preventive maintenance, thereby improving efficiency and maintaining market competitiveness.



SOURCE: OPTO 22

Snowflake's data warehousing solution is designed to offer a cloud-native platform that simplifies the way users can handle large volumes of data.

AS A FORWARD-THINKING MANUFACTURER, you're constantly seeking ways to optimize your operations and streamline your supply chain. The challenges of maintaining efficiency, reducing downtime, and adapting to rapidly changing market demands are always at the forefront of your strategy.

By leveraging machine and production data, companies can optimize business operations, forecast parts usage, assess supplier quality, and adopt preventive maintenance, thereby improving efficiency and maintaining market competitiveness.

This is where the combined power of Snowflake's data warehousing and Opto 22's automation solutions comes into play. Data travels securely from groov products (edge hardware on the plant floor) up to Snowflake (data storage in the cloud). This combination gives you the tools needed to both collect and harness the power of big data, leveraging advanced analytics and machine learning to optimize plant floor operations and drive innovation.

In this article, we'll not only explore how these technologies address immediate challenges but also delve into the technical mechanics, explaining how it all works and ties together–paving the way for a more efficient, responsive and data-driven manufacturing environment.

Snowflake creates paradigm shift for data warehousing

In the complex world of manufacturing, effective data management is key to optimizing operations. Snowflake's data warehousing solution is designed with this in mind, offering a cloud-native platform that simplifies the way users can handle large volumes of data.

Snowflake is built on a unique architecture that supports the separate scaling of computing and storage resources. Inclusion of familiar technologies ensures a streamlined transition and easy adoption for users.

SQL-based query language

Snowflake uses a variant of SQL for its query language. So if a user is familiar with SQL, they will find Snowflake's query language quite intuitive. It supports most of the standard SQL commands and functions, allowing users to perform complex data manipulations and analyses–helping to make informed decisions quickly.

Relational data

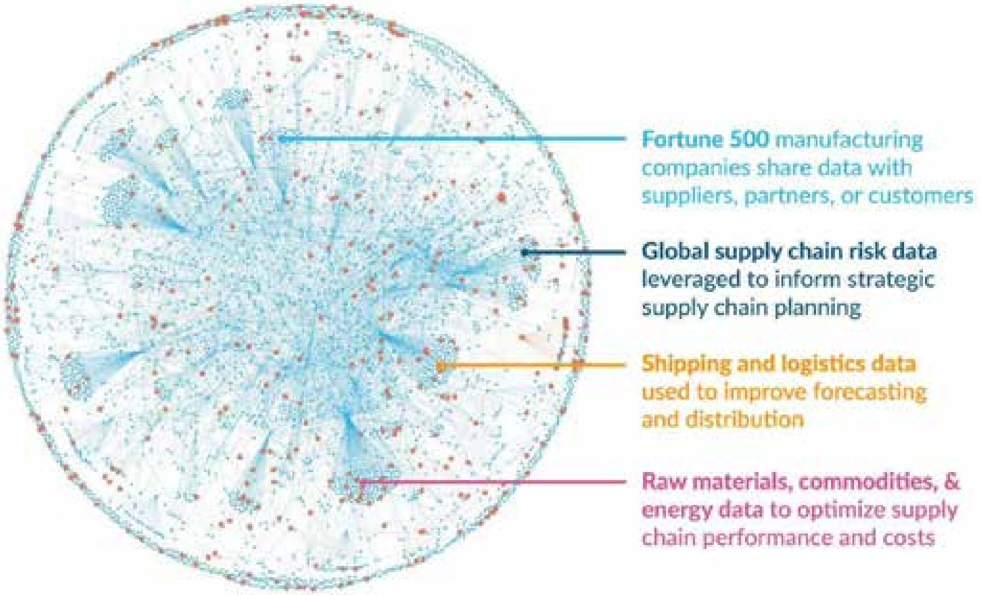
Snowflake's architecture lets you store, process, and analyze relational data, so you can run complex queries and transactions. Inclusion of relational data modeling means you can create tables, set primary and foreign keys, and establish relationships between different tables on various data types.

AI integration

With AI, ML, and anomaly detection (AD)–plus the integration of large language models (LLMs)–Snowflake helps you unearth patterns and insights from your data. Given the scale of data storage available in the cloud, a single human would be hard pressed to make sense of it all. But think of using simple language prompts like, "When was my peak energy consumption last quarter?" or "How many widgets did I produce between 11AM and 3PM on November 8, 2023?" This. Is. Powerful.

Security and compliance

Knowing that data is secure and compliant is vital. Snowflake's encryption and access control measures ensure that sensitive information is protected, both when stored and transferred. Users can trust in robust authentication, network policies, and comprehensive audit logs for secure and transparent data management. Sensitive information is protected at all times.


Fortune 500 manufacturing companies share data with suppliers, partners, or customers
Global supply chain risk data leveraged to inform strategic supply chain planning
Shipping and logistics data used to improve forecasting and distribution
Raw materials, commodities, & energy data to optimize supply chain performance and costs

SOURCE: OPTO 22

Modern supply chains require a strategy to quickly and securely share large amounts of data between manufacturing operations and suppliers, partners and customers.

Opto 22's groov products

Data comes in many forms, from the tiniest building block, a single bit, all the way up to UDTs and complex data models. But even before that, it starts as a real-world signal—an output from a sensor in your facility that could be measuring voltage, current, temperature, pressure, vibration, fluid level, proximity switches—and the list goes on.

That's where Opto 22's groov family comes into play, comprising groov EPIC, groov RIO, and the new groov RIO Energy Monitoring Unit (EMU). The robust hardware platform and comprehensive suite of software solutions has current users describing groov as a "Swiss Army Knife" for IIoT applications. More than a PLC platform, groov products combine the standard functionality of a PLC with a myriad of cybersecure, IIoT enabling technologies.

Communications

Planning to connect a variety of disparate devices and systems across greenfield and/or brownfield applications? Perhaps each device uses a different protocol?

The groov family offers extensive communication protocols, including MQTT (SparkplugB or string payloads) for lightweight and efficient messaging, OPC UA for interoperability between different industrial equipment, and support for legacy protocols like Ethernet/IP, ProfiNet, OptoMMP, and Modbus/TCP.

Cybersecurity

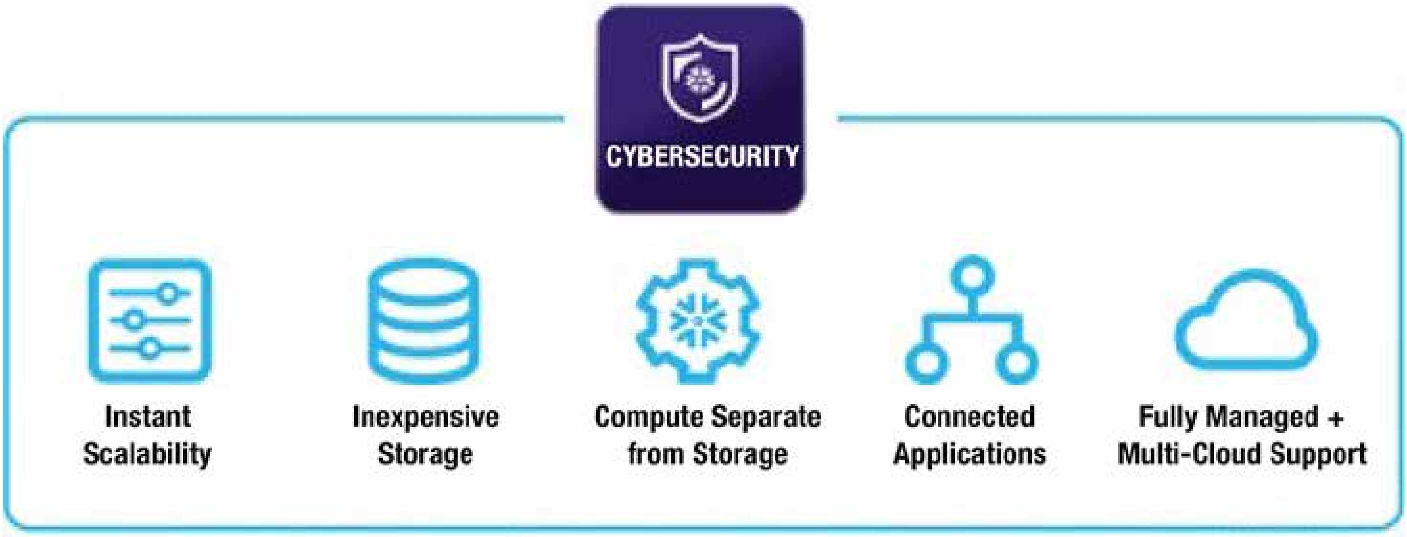
Opto 22 ensures robust protection for your industrial network with groov products, incorporating an onboard firewall, port conduits for secure traffic management, and an OpenVPN client for protected remote access. SSL/TLS certificate management enhances communication security, while LDAP integration streamlines user management, ensuring that only authorized individuals have access to your critical systems and data.

Physical I/O

Need flexibility to connect to various sensors, actuators, and other industrial devices across your plant? The groov family supports a versatile range of physical I/O options, including AC/DC inputs and outputs, digital and analog signal support, serial communication (RS232/422/485), and CAN bus connectivity.

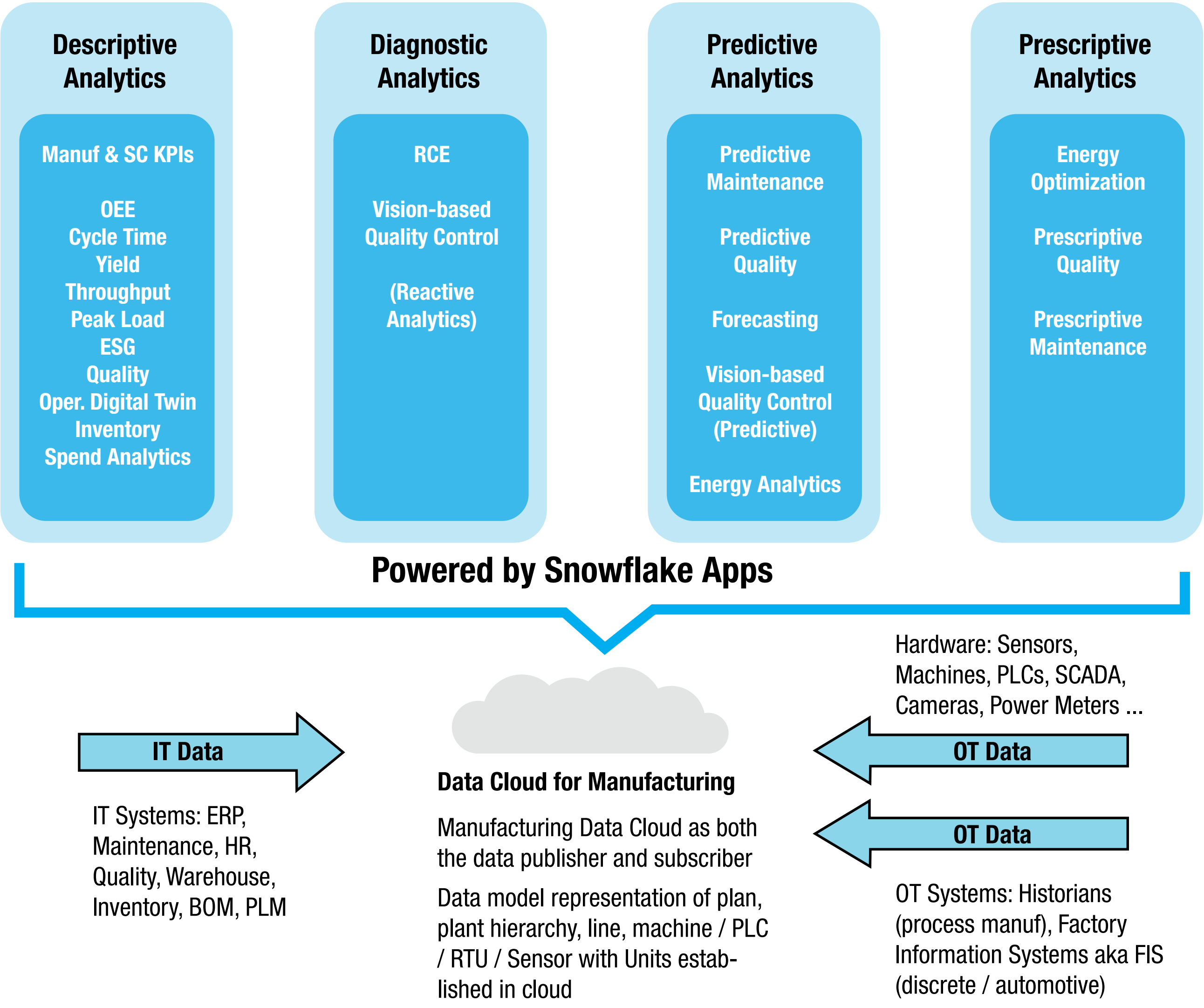
User-friendly programming and configuration

The groov family offers an accessible programming experience with intuitive interfaces, catering to both novice and experienced automation users. Integration with popular third-party software like Ignition Edge, CODESYS, and Node-Red enhance versatility and application development. These features collectively ensure a hassle-free setup and efficient management of industrial automation and IIoT solutions.



SOURCE: OPTO 22

Effective cybersecurity strategies must address a wide range of technical issues.



Descriptive Analytics

Manuf & SC KPIs

OEE
Cycle Time
Yield
Throughput
Peak Load
ESG
Quality
Oper. Digital Twin
Inventory
Spend Analytics

Diagnostic Analytics

RCE

Vision-based Quality Control

(Reactive Analytics)

Predictive Analytics

Predictive Maintenance

Predictive Quality

Forecasting

Vision-based Quality Control (Predictive)

Energy Analytics

Prescriptive Analytics

Energy Optimization

Prescriptive Quality

Prescriptive Maintenance

Powered by Snowflake Apps

IT Data

IT Systems: ERP, Maintenance, HR, Quality, Warehouse, Inventory, BOM, PLM

Data Cloud for Manufacturing

Manufacturing Data Cloud as both the data publisher and subscriber

Data model representation of plan, plant hierarchy, line, machine / PLC / RTU / Sensor with Units established in cloud

Hardware: Sensors, Machines, PLCs, SCADA, Cameras, Power Meters ...

OT Data

OT Data

OT Systems: Historians (process manuf), Factory Information Systems aka FIS (discrete / automotive)

SOURCE: OPTO 22

The coordinated flow of IT and OT is vital to achieving digital transformation in modern manufacturing systems.

Technical mechanics: how it works

Understanding how Snowflake and Opto 22 work together to improve manufacturing processes is key. The big question: How does it work?

Step 1: Data begins its journey on the plant floor with devices such as Opto 22's groov EPIC, RIO, or EMU, collecting real-time data from various industrial processes. Tag data can originate from real world signals—voltages, currents, resistances, etc.–or from other 3rd party devices–PLCs, VFDs, meters, or from any device with a serial or Ethernet connection, including web sites, services, and databases. The data is transmitted as individual tags or packaged up as data models or user defined types (UDTs).

Step 2: Data is then published using MQTT SparkplugB, a lightweight pub/sub messaging protocol designed to be efficient and reliable in challenging network conditions. The data flows upstream to an MQTT broker, serving as a central hub for data communication. This can be any broker of your choosing and can reside either on premises or in the cloud.

Step 3: From the MQTT broker, data is subscribed to by the IoT Bridge for Snowflake, a software package developed by Cirrus Link Solutions. The bridge plays a crucial role in the integration—translating MQTT SparkplugB data into a format easily digestible by Snowflake using their native API. IoT Bridge for Snowflake can be deployed on various cloud platforms, including AWS, Azure, and Google Cloud.

Step 4: Once IIoT data is in Snowflake, leverage its advanced analytics and machine learning capabilities for predictive maintenance and anomaly detection. Utilize AI-driven insights and large language models to streamline operations and enhance decision-making, ensuring optimal performance and efficiency in manufacturing processes.

Streamlining operations with targeted solutions

The integration of Snowflake's data warehousing and Opto 22's automation technology can provide tangible benefits to your production process.

With Snowflake, cloud based management of industrial data enables improved decision-making and operational insight. SQL derived tool sets you already know combined with a new wave of artificial intelligence tools will help you optimize processes and take swift action when required.

And with Opto 22, you've got an automation solution that paves the way to the cloud. Integration of various software suites on top of plentiful native protocol support ensures your valuable data doesn't get trapped on the plant floor, but rather, makes its way into a secure, data centric ecosystem.

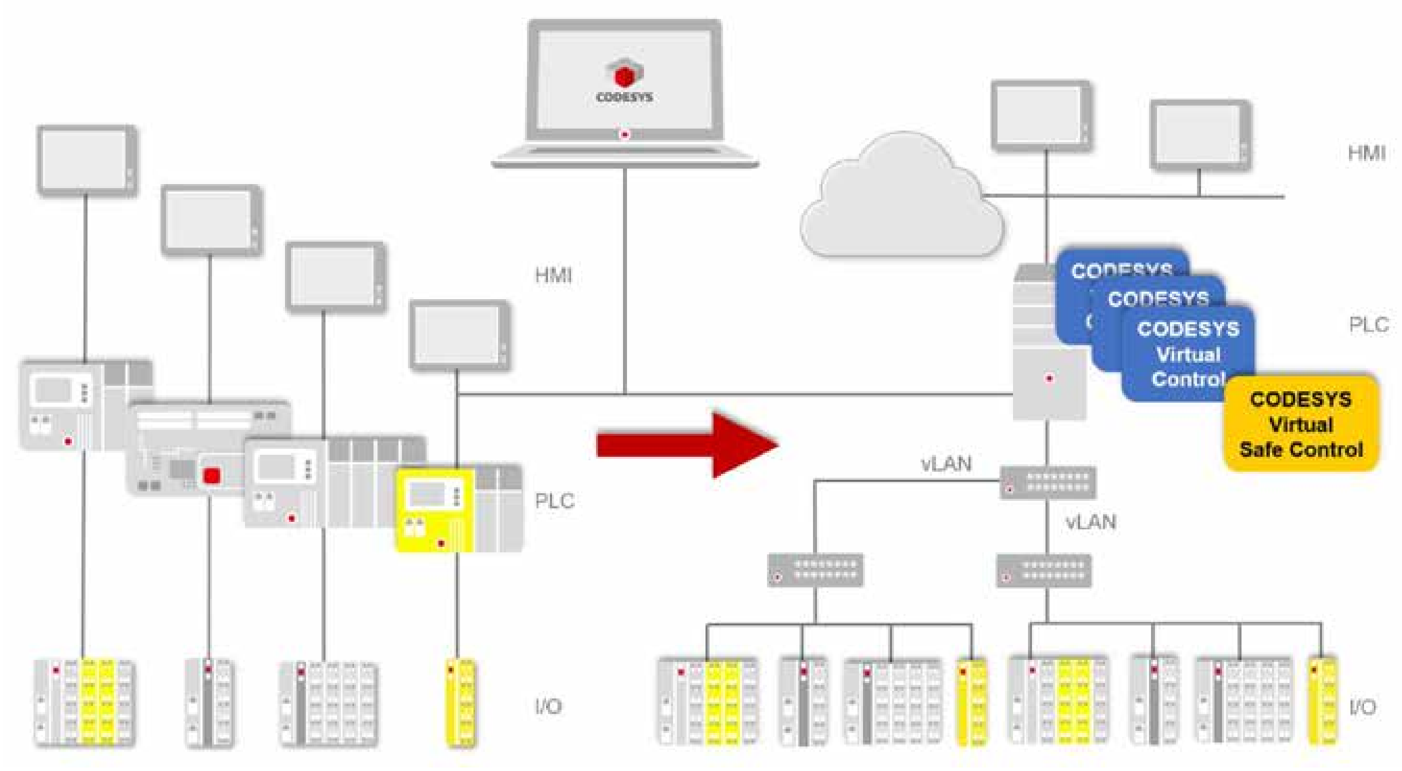
The bottom line is that this is not just about keeping pace with industry trends; it's about directly enhancing your operational capabilities, reducing downtime, and improving overall efficiency.

Daniel White - Director of Technical Marketing, ***Opto 22.***

Learn More

Next big thing in smart factories? Control systems virtualization.

Virtualization technology has dramatically changed the way IT resources are used, but the benefits of virtualization have yet to benefit industrial operations in any significant way. In this article, the authors describe the benefits manufacturers can expect to see by virtualizing IACS systems and solutions to get there.



SOURCE: CISCO

Figure 1: From discrete to virtualized industrial control systems.

VIRTUALIZATION TECHNOLOGY HAS BEEN extensively applied in IT systems. Several aspects ranging from server, storage, applications, desktops, to operating systems and more have been virtualized.

Server virtualization is the most common use of virtualization. It involves partitioning a physical server into several smaller virtual servers. Each of these virtual servers can run their own operating system and applications, making it seem as though they are individual machines. This helps to optimize resources and reduce costs. Storage virtualization involves pooling physical storage from multiple network storage devices into a single storage device that is managed from a central console. This helps in backup and archiving, improving efficiency and speed. Similarly, application virtualization allows running of applications in a self-contained virtual environment without the need for dedicated host computers. Desktop virtualization involves hosting a desktop operating system within a virtual machine that runs on a server. This means that the server does all the processing, and the users just need a small device (called thin or zero-clients) to connect to the server. This reduces the hardware requirements for the users and increases data security.

Virtualization technology has dramatically changed the way IT resources are used, and services are delivered, enhancing efficiency, flexibility, and scalability. However, the benefits of virtualization have yet to benefit industrial operations in any significant way. Industrial Automation and Control Systems (IACS) hardware resources in these environments continue to exist as discrete resources. With digitization, the number of such hardware resources has risen rapidly and so has the time and expense of monitoring, updating, and troubleshooting, which could require extended downtimes and result in productivity losses.

In this article, we will describe the benefits manufacturers can expect to see by virtualizing their IACS systems, what is holding them back, and the solutions that can help them get there.

What can virtualization do for your operations?

Manufacturing facilities stand to gain a lot by virtualization. They can consolidate Programmable Logic Controllers (PLC), Industrial PCs (IPC), Human Machine Interfaces (HMI), Gateways, and other physical compute resources currently on their factory floors onto local virtual machines which run on a hyperconverged compute and storage infrastructure.

Figure 1 shows how several individual PLCs can be replaced by a centralized pool of virtual PLCs. This arrangement has many advantages:

Scalable and agile operations: Virtualization enables manufacturers to easily scale their operations by adding or removing virtual machines as required instead of purchasing and deploying new hardware. It also facilitates adding new applications, making updates, and adapting to changing conditions, product redesigns, etc., easier.

Increased security: Removing discrete

SOURCE: ISTOCK

Virtualization has the potential to change the way we view manufacturing systems using local virtual machines which run on a hyperconverged compute and storage infrastructure.

hardware from the factory floor minimizes potential avenues that an attacker can exploit to gain unauthorized access to manufacturing assets and processes. Virtualization can improve the security of IACS by isolating critical control systems. By separating networks and implementing security measures at the virtualization layer, manufacturers can minimize the risk of malware propagation. And in case of a successful breach, the compromised virtual control system can easily be shut down and replaced by a newly deployed virtual machine.

Improved disaster recovery: Virtualization allows for efficient backup, replication, and restoration of virtual machines, making disaster recovery planning and execution more streamlined. It enables manufacturers to recover from system failures or disasters, reducing downtime and minimizing any impact more quickly on production.

Testing and development: Virtualization provides an ideal environment for testing and development activities. Manufacturers can create virtual replicas of their production systems for testing new software, configurations, or system updates, ensuring they do not impact the actual production environment.

Reduced costs: Virtualization can help reduce both operating and capital expenses. Hardware upfront purchase costs can be reduced by running multiple virtual machines on a single server. Fewer physical servers also mean fewer machines to maintain and repair. Virtualization often comes with management tools that simplify and automate the maintenance of virtual machines. This can reduce the need for manual administration and raise productivity.

Better sustainability: Consolidation of computing and storage resources into a set of central services helps reduce the total energy requirements. In addition, easier access to more processing data can help increase efficiencies, reduce waste, and lower energy consumption.

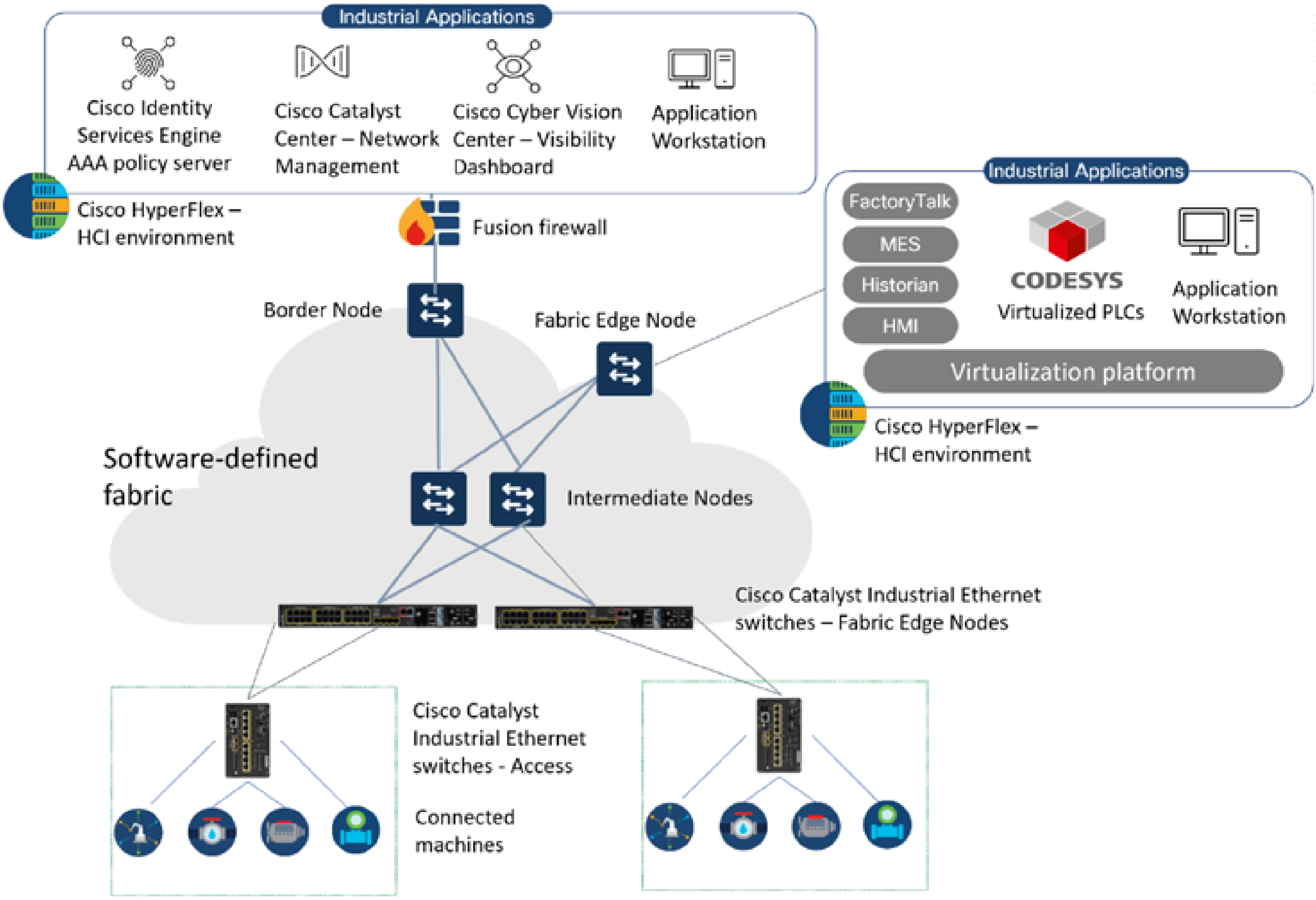
Why is virtualizing industrial control systems so hard?

Even with these benefits, virtualization of control systems is not yet mainstream in the manufacturing sector. Manufacturers are hesitant to change their tried-and-true processes and systems without assurance of a solution that addresses challenges in the transformation. An effective virtualization strategy would require:

Precision timing: Industrial control systems mostly require real-time performance with deterministic responses. These systems control physical equipment where delays can lead to serious problems, including safety issues. Virtualization could add latency that may be unacceptable in these environments. The network must be deterministic and ensure adequate performance.

Industrial protocols: Traditionally, industrial control systems and machinery have been designed to communicate via Layer 2 network given the emphasis on precision timing requirements. Layer 2 connectivity has the advantage of having fewer network hops and avoiding routing resulting in lower latency. Replacing individual controllers with a central computing environment would require a Layer 3 network as packets will need to be routed between the machines and controlling applications. Not only would a Layer 3 network need to tunnel Layer 2 traffic, but it would also need to satisfy strict timing and packet loss requirements.

Resiliency and reliability: Substituting a Layer 2 network with a routed Layer 3 adds new links and network functions between the machines and controlling applications, that exposes manufacturing processes to risk of interruptions. A resilient network able to withstand link and device failures can ensure continuity of operations.


Industrial Applications
Cisco Identity Services Engine AAA policy server
Cisco Catalyst Center – Network Management
Cisco Cyber Vision Center – Visibility Dashboard
Application Workstation
Cisco HyperFlex – HCI environment
Fusion firewall
Border Node
Fabric Edge Node
Industrial Applications
FactoryTalk
MES
Historian
HMI
CODESYS Virtualized PLCs
Application Workstation
Virtualization platform
Cisco HyperFlex – HCI environment
Software-defined fabric
Intermediate Nodes
Cisco Catalyst Industrial Ethernet switches – Fabric Edge Nodes
Cisco Catalyst Industrial Ethernet switches - Access
Connected machines

SOURCE: CISCO

Figure 2: A software-defined networking architecture defined jointly by Cisco and CODESYS for IACS virtualization.

Security: With more connected industrial assets and a greater dependence on the network, securing operations in a virtualized environment becomes even more important. The solution must provide detailed visibility, be able to spot vulnerabilities, segment the network granularly, and monitor connected devices continually for any breaches.

Scalability and flexibility: The network infrastructure should be scalable to accommodate the growing demands on virtualized systems. This includes considering factors such as network capacity, scalability of switches and routers, and the ability to add, remove, and reconfigure virtual machines as needed.

The network is the key to IACS virtualization

The network is the key to migrating individual PLCs, HMI, IPCs, and other discrete hardware resources to central hyperconverged environments. A simplified architecture that illustrates the major components and their connectivity is shown in Figure 2.

The following are the main elements of this architecture:

1. **Industrial Ethernet switches** provide high-capacity packet switching and lossless resiliency required for uninterrupted connectivity of IACS applications with the controlled machines.

2. **An intelligent network management system** directs all functions of the network starting from onboarding devices, initial and ongoing configurations, performance monitoring, proactive troubleshooting, networking and security policies, and everything else needed for maintaining network performance and security. It enables the software-defined fabric and ensures that the network is always ready.

3. **AAA policy repository and server** ensures secure network access and enforces security policies. It allows organizations to control access to their network and the resources they can access.

4. **Visibility application** running within industrial switches helps identify connected assets, identify network traffic, and uncover security vulnerabilities. Using this level of visibility, you can define zones and conduits as per ISA/IEC 62443 and enforce segmentation using the policy server and industrial switches

5. The centralized **hyperconverged infrastructure** brings together computing, networking and storage in a single system to power applications, including virtualization.

6. **Virtual PLC** is an integrated development system (IDE) in accordance with IEC 61131-3 for programming the control logic and contains various textual and graphical editors.

Time to get started is now

Admittedly, virtualization of IACS is not mainstream, and it may not be on your radar quite yet. But with all the benefits it can offer, it is easy to see how it will be a gamechanger soon. In fact, Audi, the German manufacturer of technologically advanced luxury cars, has embraced virtualization and is transforming its production lines.

Watch Dr. Henning Löser, head of Production Labs, Audi, explain how they intend to transform their next-generation smart factories. Click here.

It is not too early to start laying the networking foundation for the future of manufacturing.

*Vivek Bhargava, Product Marketing Manager at **Cisco**, and Roland Wagner, Head of Product Marketing at **CODESYS.***

Learn More

OPC UA technology bridges gap between IT and OT systems

The OPC UA information modeling framework turns data into information. With complete object-oriented capabilities, even the most complex multi-level structures can be modeled and extended. Industry experts weigh in on OPC UA as the interoperability standard for secure, reliable exchange of data in industrial automation.

SOURCE: ISTOCK

"In a nutshell, OPC UA allows for better data management and analysis, leading to process optimization, predictive maintenance, and other Industry 4.0 use cases," Konstantin Selnack, Product Manager Industrial Connectivity Products at Siemens AG.

OPC UA PROVIDES STANDARDIZED SOLUTIONS for important requirements such as information modelling, information exchange, cloud connectivity and asset identification. But now the scope of its published standards has expanded with a new *metaverse concept* and real world examples for Digital Twins in industrial automation.

For this OPC UA solutions update, the Industrial Ethernet Book reached out to industry experts to gain their perspectives on how OPC UA is continuing to move forward with a range of effective solutions for factory automation.

Integrating OT with IT

Increasing need for data acquisition and exchange in an open, interoperable manner.

According to Konstantin Selnack, Product Manager Industrial Connectivity Products at Siemens AG, the adoption of OPC UA in automation is driven on the one hand side by the increasing need for data acquisition and exchange in an open, interoperable manner across Operational Technology (OT) and Information Technology (IT), which is critical for Industry 4.0 implementations.

But also, the standard itself, with its compelling capabilities for highly sophisticated communication is driving the adoption. Continuously providing new features and involving more industrial Domains, is a convincing factor to apply OPC UA.

"In the end, these developments come together in products and solutions of the technology providers," Selnack said. "Today, OPC UA is not only found in controllers, but also in RFID readers, network management software and even power supplies. At the same times, these products are being expanded with additional OPC UA capabilities."

Selnack added that, first and foremost, OPC UA is the interoperability standard for industrial communication. It allows for seamless integration of different systems and devices, making it a universal language in industrial automation.

In addition, the information modeling of OPC UA provides the "grammar" which allows industrial domains to build their own semantics within Companion Specifications. The AutoID companion specification for instances, provides a standardized information model for RFID readers, allowing to seamlessly integrate a RFID reader independent from the vendor specifics.

"In a nutshell, OPC UA allows for better data management and analysis, leading to process optimization, predictive maintenance, and other Industry 4.0 use cases," Selnack added.

"All this is based on a highly sophisticated communication standard. It is utilizing Ethernet and therefore can be adapted to any network configuration, making it a versatile solution for connecting various systems of different scale within the industrial domain. But it also provides a robust security architecture, which is essential for industrial communication. It includes features like authentication, authorization, encryption,

"OPC UA offers robust security features like encryption and authentication to ensure secure data communication between various systems. HMIs and protocol converters play a critical role in the adoption of OPC UA making it a user-friendly way to control and monitor industrial processes," Megha Agrawal, Software Product Manager, Red Lion.

and data integrity checks."

The core concept of integrating OT with IT remains the primary focus, and OPC UA continues to expand its functionalities to support this integration. A significant development is OPC UA PubSub, which incorporates MQTT to facilitate the connection with cloud-based applications. By utilizing OPC UA PubSub with MQTT, these solutions offer a direct data flow to cloud and IoT platforms, facilitating advanced data analysis and better decision-making, helping enterprises to achieve greater operational efficiency or reduce downtimes and maintenance cost.

But also managing OT devices with OPC UA capabilities is getting more attention. The addition of e.g., standardized REST-interfaces, certificate management via the Global Discovery Service or device updates via OPC UA shows, that the adoption of IT technology is of big interest.

"Another area of interest is interoperability on the field level. Here, OPC UA FX has been introduced, providing an open communication standard for connection establishment and data exchange of PLCs," Selnack said. "UAFX is therefore bringing OPC UA benefits like interoperability or built-in security to the controller level.

Engineering challenges

Selnack added that OPC UA FX is a response to the need for seamless integration between diverse controller platforms, which traditionally has been a complex and painful process for line integrators and end-users.

"UAFX helps to reduce the integration and maintenance cost in these setups by providing a standardized information model and methods to interconnect controllers with each other. It also supports the offline engineering of systems - an UAFX machine description will provide the required machine data which have to be exchanged, allowing to do the engineering upfront," he said.

Another challenge is the realization of the increasing security requirements in operational environments. Certificate management for instance is a huge challenge and requires today a high effort. OPC UA Part 12, discovery and Global Services introduces the Global Discovery Server, which provides a framework to roll out and maintain certificates for OPC UA devices, providing a solution to this issue.

"Overall, the main challenge of data integration is being continuously addressed with a growing offering of OPC UA functionality and implementations. Thus, the evolution of OPC UA reflects the ongoing needs of the industry and provides answers to todays and tomorrow's challenges," Selnack concluded.

Leveraging open standards

Security features such as encryption and authentication ensure secure data communication.

Megha Agrawal, Software Product Manager at Red Lion said that the widespread use of OPC UA (Unified Architecture) is driven by its open and vendor-neutral characteristics. This ensures smooth interoperability among a variety of industrial devices.

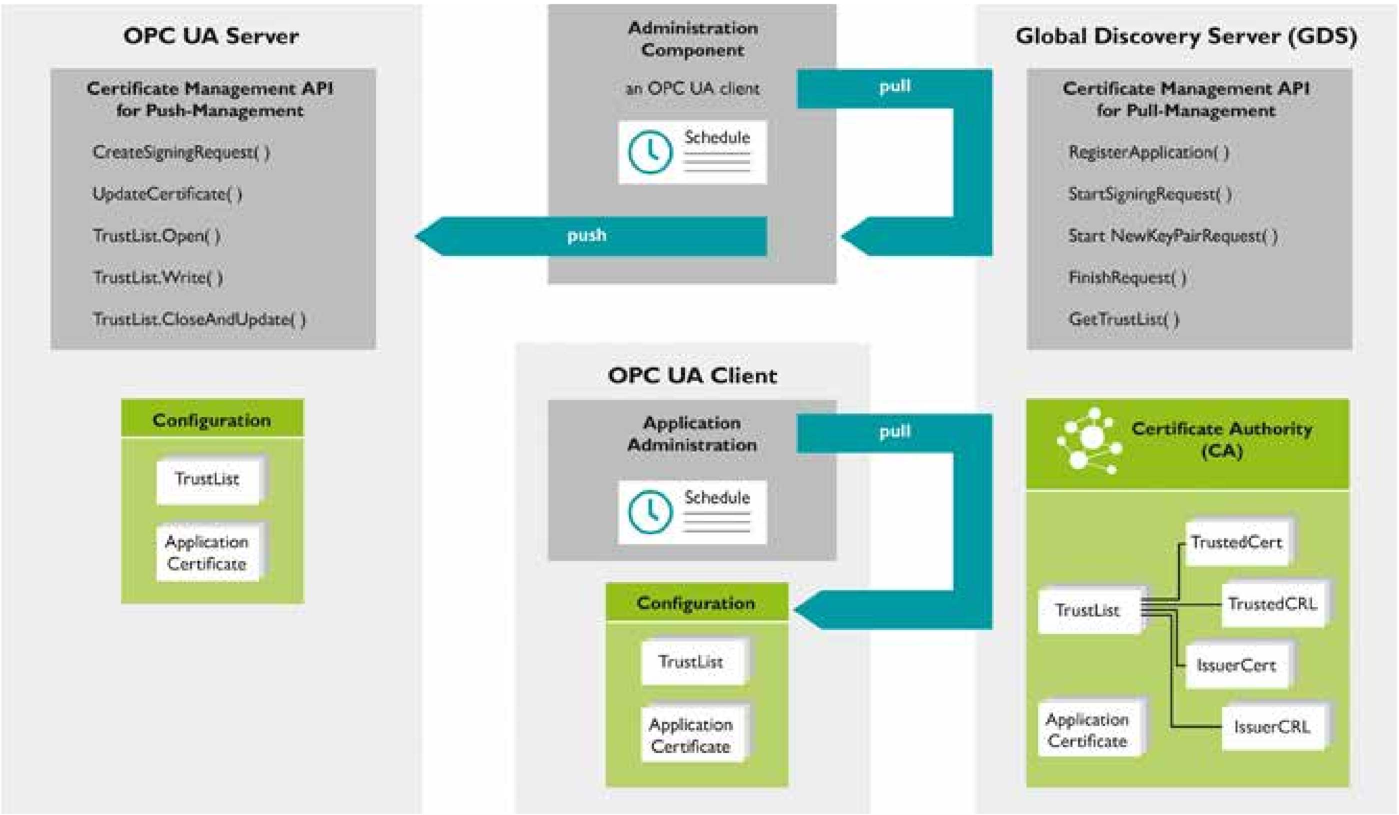
"OPC UA offers robust security features like encryption and authentication to ensure secure data communication between various systems. HMIs and protocol converters play a critical role in the adoption of OPC UA making it a user-friendly way to control and monitor industrial processes," Agrawal said. "They utilize OPC UA to effectively collect and showcase data from various devices, promoting a unified working environment. These devices also support multiple protocols which can provide compatibility between OPC UA and older devices that might use legacy protocols."

Platform independence

Agrawal said that one of the key advantages of OPC UA relates to platform independence because it can run on various operating systems such as Windows, Linux, Apple, Android. It is also designed with robust security features along with high reliability and fault tolerance.

It supports redundant servers and communications paths along with historical data access to ensure seamless communication and access to past data. Additionally, OPC UA supports a wide range of data types, including complex data structures and arrays giving it the flexibility to represent diverse information in industrial processes. These features contribute to making OPC UA a widely used standard.

"OPC UA is widely used in smart manufacturing where the plant floor has various machines from different manufacturers.



SOURCE: PHOENIX CONTACT

"One major advance is the ability to carry out software updates via OPC UA. Here, users benefit from the standardized solution to provide automation devices with new firmware or software across manufacturers, which enable new functions or close known security vulnerabilities," Arno Martin Fast, Senior Specialist, PLCnext Technology and Business Area Industry Management and Automation, Phoenix Contact.

These machines communicate in different languages and data needs to be gathered from all these platforms and sent to a centralized location," Agrawal added.

"Edge devices can be utilized to gather data from various machines and send it to a centralized location via OPC UA in a secure and standardized manner. The data can then be utilized to provide meaningful insights about operations to increase productivity and reduce downtime. These solutions contribute to IoT and enterprise connectivity by providing a standardized, secure, and scalable communication framework."

Increased adoption of OPC UA

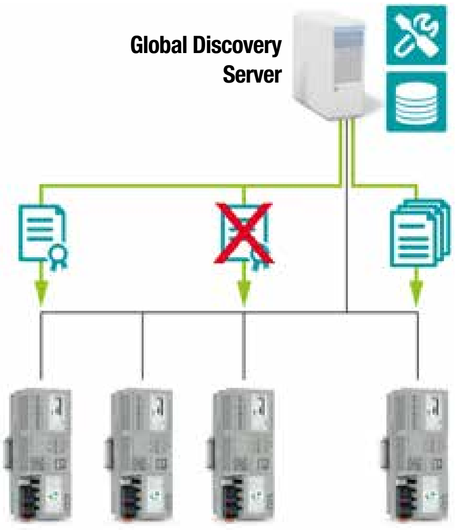
Standardized solution to provide automation devices new firmware or software across manufacturers.

Arno Martin Fast, B.Eng., Senior Specialist, PLCnext Technology and Business Area Industry Management and Automation for Phoenix Contact said that technology solutions are driving the adoption of OPC UA automation, control and networking.

"One major advance is the ability to carry out software updates via OPC UA. Here, users benefit from the standardized solution to provide automation devices with new firmware or software across manufacturers, which enable new functions or close known security vulnerabilities," Fast told IEB recently.

"Another aspect is the distribution and updating of OPC UA certificates with the OPC UA Global Discovery Server (GDS). This makes it much easier to handle and manage own certificates for OPC UA communication, which increases acceptance during implementation."

Fast added that networking for automation technology without taking cyber security into account would be very negligent in today's world.



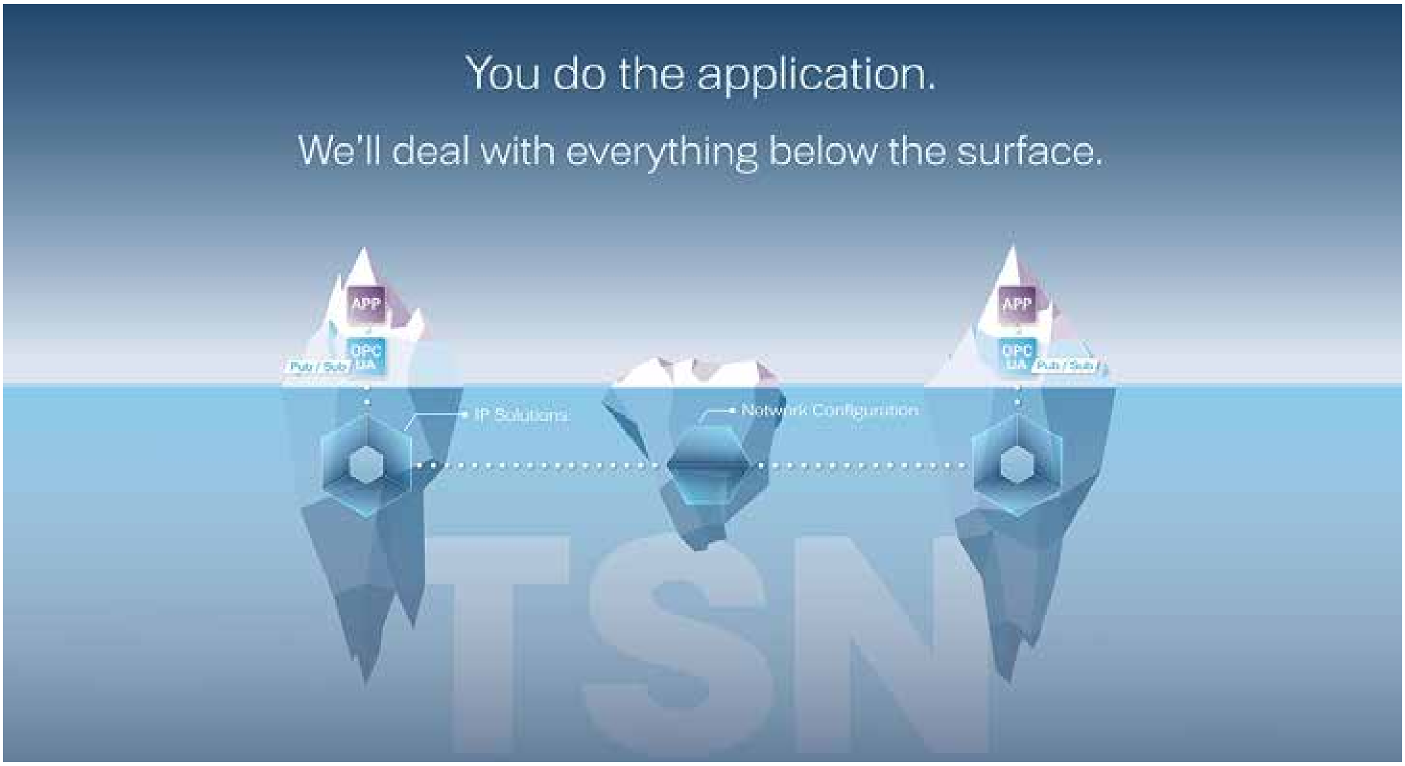
SOURCE: PHOENIX CONTACT

The OPC UA Global Discovery Server offers a standardized solution for managing certificates.

"Secure networking in automation is essential, especially in areas of critical infrastructure, but also in all other areas in which automation technology is used. With OPC UA, the networking of devices can be secure and certificate-based, so that unwanted communication with a potentially dangerous attacker is not possible," he said. "A defined expiring date for the certificates required for communication and the ability to revoke certain certificates in the event of danger are basic requirements for managing communication in automation technology. The OPC UA GDS as a standardized solution for managing certificates offers a great advantage here."

IoT and enterprise connectivity

He added that the solutions mentioned above are aimed at applications that often consist of widely distributed applications, i.e. where communication to or between automation devices takes place over long distances. In these applications, the requirements for secure communication and secure automation components are very high. The secure and automated updating of automation components minimizes the risks of cyberattacks. With the certificate-based communication of OPC UA, IoT applications can be implemented with a high level of security.



SOURCE: TTTECH INDUSTRIAL

"By incorporating features for Time-Sensitive Networking (TSN) for real-time communication, OPC UA is expanding its scope to address OT communication in edge computing. This evolution ensures OPC UA remains a key enabler for Industry 4.0 initiatives," Georg Stöger, Director Training & Consulting at TTTech Industrial.

In the case of locally distributed applications or if the automation devices are installed in a location that is difficult to access, it takes a lot of time and effort for users to update these devices with new software or firmware. Each device must be managed individually at the installation site or temporarily secure communication channels (such as VPN) must be configured.

"Thanks to OPC UA with the GDS and the software update model, these tasks can be solved centrally. A central OPC UA client can be used to securely update the software of the automation devices. I am curious to see what possibilities future developments of OPC UA, such as OPC UA over REST, will offer for a standardized device management and software updates on other levels," Fast said.

Seamless data exchange

Expanding to address OT communication for effective edge computing.

"We consider the combination of an open, flexible information model, a security framework based on widely accepted robust mechanisms, the platform independence and the integration of real-time capabilities using Publish/Subscribe and TSN (time-sensitive networking) as the key technology solution for automation and control, including the network layer," Georg Stöger, Director Training & Consulting at TTTech Industrial said recently.

"This combination fosters connectivity and data exchange in a secure and scalable manner while supporting the requirements of OT/edge applications such as control and real-time data acquisition, supporting the integration of disparate devices and systems in industrial environments."

Stöger said that OPC UA based solutions are using the standardized information model, which provides open, vendor independent interoperability. OPC UA enables the integration of legacy systems into a wider ecosystem which provides flexibility and scalability beyond these systems' original scope.

OPC UA solutions

"OPC UA is highly relevant for solutions in quite diverse, well established industries including manufacturing, energy, and in novel applications such as smart cities," Stöger said. "IoT is a key aspect in all of these because cloud connectivity and computation are essential; enterprise connectivity is ensured by standardized communication framework. OPC UA facilitates seamless data exchange between devices and systems, enabling the creation of interconnected ecosystems. This contributes to the development of smart, data-driven enterprises with improved visibility and control over industrial processes."

Stöger added that the major engineering challenges for IoT architectures revolve around data integration, interoperability, IT/OT integration, and cybersecurity. These challenges are well addressed by the flexible and scalable information model, standardized communication protocols, and the set of security measures defined by OPC UA.

"By incorporating features for Time-Sensitive Networking (TSN) for real-time communication, OPC UA is expanding its scope to address OT communication in edge computing. This evolution ensures OPC UA remains a key enabler for Industry 4.0 initiatives," he said.

Impact of OPC UAFX

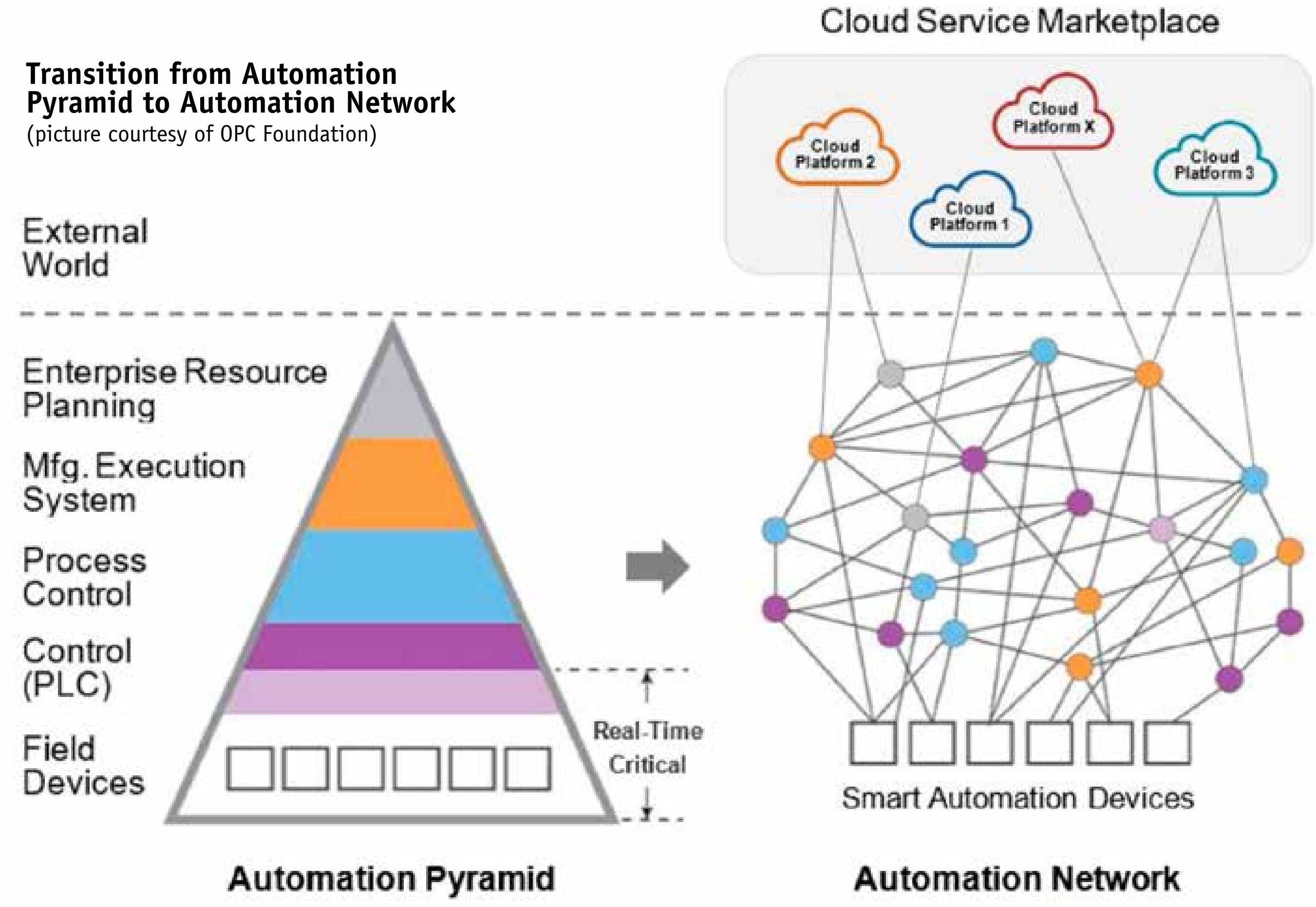
Provides data model, protocol stack and key networking technologies including security.

According to Maik Seewald, Member of IEC and ISA99 industrial security workgroups and Senior Technical Lead, Industrial IoT at Cisco, until recently, OPC UA has been a technology to support solutions and use cases in industrial automation, infrastructure monitoring, energy management, and other domains. The client/server mechanism allows it to fetch data from devices used for SCADA and other monitoring applications in an interoperable and multi-vendor way using a built-in information model as well as integrated security mechanisms.

"With OPC UAFX (initially Field Level Communication), the Publish/Subscribe mechanism and the underlying Time-Sensitive Networking (TSN) capabilities, OPC UA provides the technologies for a broad variety of use cases, often described as 'from the sensor to the cloud'. This includes applications for Industrial IoT and for Machine-to-Machine communication meeting the essential

SOURCE: OPC FOUNDATION

Transition from Automation Pyramid to Automation Network
(picture courtesy of OPC Foundation)



"With OPC UAFX (initially Field Level Communication), the Publish/Subscribe mechanism and the underlying Time-Sensitive Networking (TSN) capabilities, OPC UA provides the technologies for a broad variety of use cases, often described as 'from the sensor to the cloud'," Maik Seewald, Member of IEC and ISA99 industrial security workgroups and Senior Technical Lead, Industrial IoT at Cisco.

requirements for predictive maintenance, agile manufacturing, use of AI/ML, digital twins, or the use of virtualized control hosted in a cloud-based infrastructure. These applications are key features of the Industry 4.0 initiative which refers in many places to OPC UA," Seewald said.

He added that the continuous drive to standardize how data from industrial automation and control systems, devices and machines is generated, exchanged, and understood is critical to enabling Industry 4.0 capabilities. This is possible because standard networking technologies, such as Ethernet for wired networks, Wi-Fi & 5G for wireless, and security technologies, make the OPC UA data reliable and accessible in a secure manner. This "virtuous cycle" of making more data available reliably and securely will continue to grow and expand as more improvements in sustainability, performance, and quality in industrial systems is delivered via Industry 4.0 capabilities.

Key technical advantages

"With initiatives and trends such as Industry 4.0 or Digital Factory, system and networking paradigms are changing from a static automation pyramid model to an automation network being part of a cyber physical system," Seewald said. "OPC UAFX provides the data model, the protocol stack and the networking technologies including security for this important evolution, in enabling flexible and secure access to devices and data over a fully converged network. This enables innovation and new use cases that allow much higher flexibility and productivity. The interoperability OPC UA delivers, along with deterministic features based on Time-Sensitive Networking (TSN), allows agility regarding workflows and components (plug and produce) in an advanced automation network."

He went on to say that Industrial IoT (IIoT) is a key application area where solutions based on OPC UAFX can help to enable secure access to data and devices over a variety of physical layers such as Ethernet, Wi-Fi, 5G, or Single-Pair Ethernet. Such applications are needed in industrial and process automation, energy automation or in the oil & gas domain. Furthermore, OPC UAFX provides the technical capabilities to support essential use cases such as Controller-to-Controller, Controller-to-Device (e.g. synchronization of axes) or Device-to-compute (Cloud-based Controller) along with precise time synchronization. Such characteristics make OPC UAFX an alternative to existing field-bus technologies but with inherent interoperability and security that are needed to meet requirements for ubiquitous access to devices over a converged network.

Engineering challenges

"Challenges in engineering have been the limitation of existing technologies and protocols regarding applicability to new use cases as well as of missing interoperability," Seewald added. "Such technologies were often designed to meet the requirements for a fixed set of application scenarios (e.g. controller to device) often within a single layer or between two layers of the automation pyramid. Gateways are needed to cross domains and layers which prevents real end-to-end connectivity."

"Furthermore, they were typically designed for a particular protocol stack and physical layer. Scope and architecture of OPC UAFX addresses interoperability over a variety of technologies (wired, wireless) using standardized networking and security technologies as a key design goal. A strict layering and separation of concerns allows deterministic data exchange over a converged industrial network."

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

OPC UA: interoperability for cloud solutions

The goal of the OPC UA Cloud initiative is to recommend, harmonize, and steer the activities of individual technical working groups and create best practices, an overall reference architecture, as well as open-source reference implementations, combining the output of the individual working groups.

SOURCE: ISTOCK

Greater interoperability between different cloud solutions will enable the use of OPC UA Information Models for semantically-rich data analytics in the cloud, but also lead to cost reductions of these solutions.

DIGITALIZATION IN MANUFACTURING IS resulting in a world divided between those who possess and effectively utilize data and those who lack access to those resources.

This is a barrier to both corporate success and macro-economic growth. Legislators (such as the EU with the upcoming Data Act) are responding to this by requiring vendors to share data among much broader eco-systems. In parallel to require broader eco-systems, central use-cases for traceability like the Digital Product Passport (DPP) and security aspects like in the Cyber Resilience Act (CRA) are defined.

At the OPC Foundation, we believe that this will create a greater need for interoperability of end-to-end information models and data communication to support these legislative demands.

We will replicate the best-practice collected in the OPC Foundation Field Level Communications Initiative bringing in experts in applications to complement the technology experts from the OPC Foundation. By initiating an OPC Foundation Cloud Initiative, to bring greater focus of existing working groups on actionable user challenges and opportunities for enhancement and initiating new working groups to develop OPC UA technology into new cloud-centric applications.

Today, OPC UA has established itself as the industrial interoperability standard in on-premises, OT environments, field-level communication (OPC UA FX), as well as industrial Edge applications. Therefore, it is not surprising that OPC UA users also want to leverage their existing investment in OPC UA Information Models and communication patterns in IT and cloud applications by creating secure, interoperable, cloud architectures. These architectures must focus on open solutions for data analytics, digital twins, industrial metaverse, and artificial intelligence; but also avoid vendor lock-in. They must further define edge-to-cloud and cloud-to-cloud communication patterns and a means to securely store OPC UA Information Models in the cloud.

Thankfully, the OPC Foundation established several working groups in this area in prior years and can now combine them under a single OPC UA Cloud initiative. This will also help bring clarity to seemingly overlapping national and international standards and other initiatives in this area.

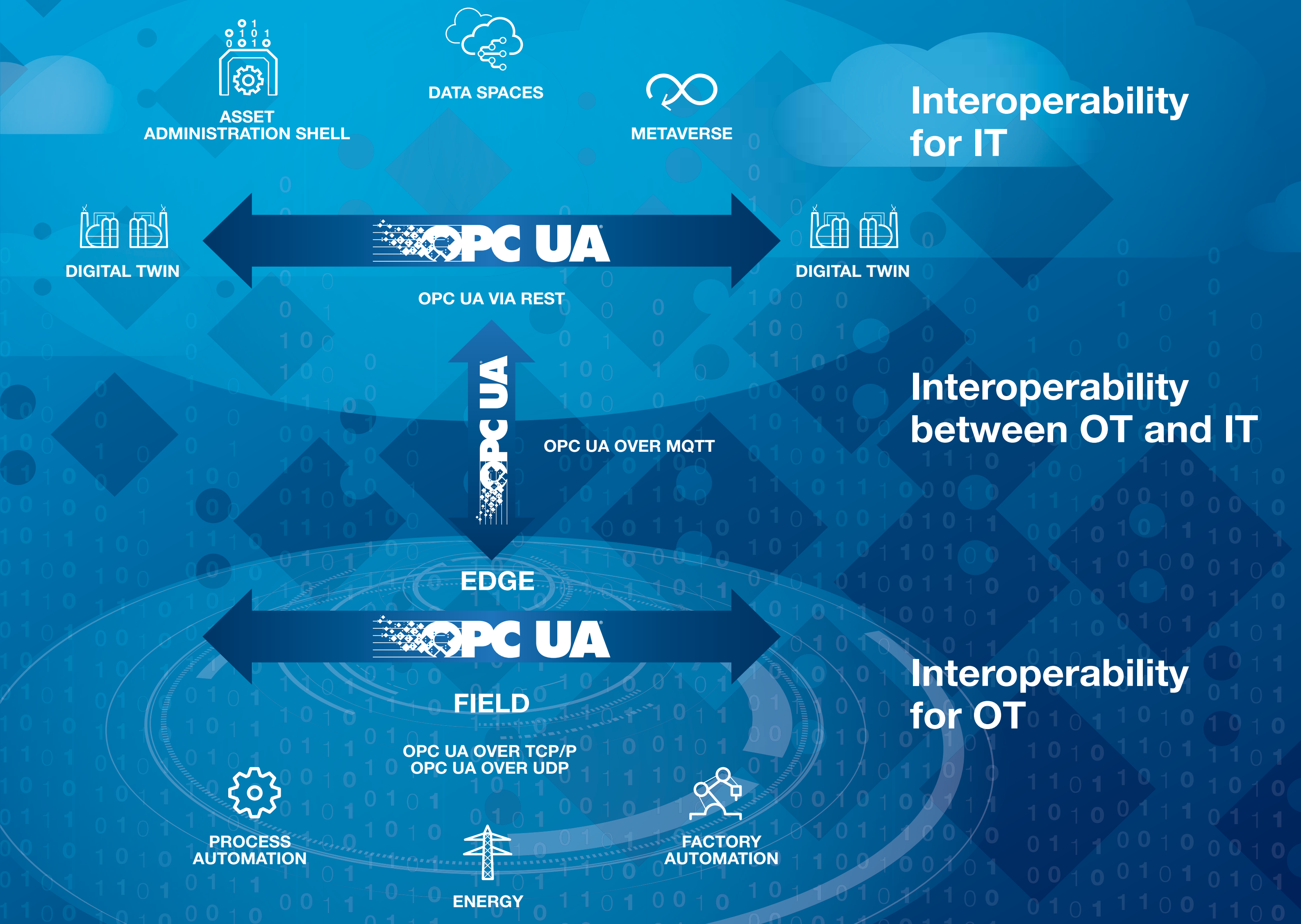
OPC UA cloud interoperability

List of OPC Foundation working groups with focus on OPC UA Cloud Interoperability:

1. UA Cloud Library – A query-able online store of OPC UA Information Models.
2. OPC UA over MQTT Working Group –

OPC Unified Architecture: Industrial Semantic Interoperability

One modeling language for OT and IT including flexible transport and security



www.opcfoundation.org

© Panuwat/ stock.adobe.com

secure transport from edge to cloud and cloud to cloud.

3. OPC UA over MQTT Prototyping Group.
4. OPC UA over MQTT Testbed.
5. OPC UA REST Interface – cloud-based OPC UA server access.
6. OPC UA WoT Connectivity – standardized industrial connectivity software configuration.
7. OPC UA Industrial Metaverse Working Group.
8. OPC UA AI leveraging Large Language Models Working Group (currently getting established).
9. OPC UA Data Spaces Working Group (currently getting established).

Open source solutions

Here is a list of open-source reference solutions with an overall focus on OPC UA Cloud Interoperability:

1. UA Cloud Library: Cloud-neutral reference implementation.
2. UA Cloud Publisher: An OPC UA PubSub telemetry publisher.
3. UA Cloud Commander: An online command & control app for OPC UA servers.
4. UA Cloud Action: A cloud-based app to trigger an action for UA Cloud Commander.
5. UA Cloud Dashboard: An online dashboard for OPC UA PubSub data.
6. UA Cloud Twin: Digital Twin adapter for OPC UA PubSub data from the Digital Twin Consortium.
7. UA Cloud Viewer: An online viewer for OPC UA Information Models.
8. AAS Repository: An Asset Admin Shell Repository with OPC UA modelling support.
9. UA Edge Translator: a reference implementation for industrial connectivity software.
10. IIoT Starter Kit: A set of quick-start samples for OPC UA over MQTT.

The goal of the Steering Committee of the OPC UA Cloud initiative is responsible to recommend, harmonize, and steer the activities of the individual technical working groups and create best practices, an overall reference architecture, as well as open-source reference implementations, combining the output of the individual working groups.

This will not only lead to greater interoperability between different cloud solutions and enable the use of OPC UA Information Models for semantically-rich data analytics in the cloud, but also lead to cost reductions of these solutions.

Find more information on the OPC Foundation website: ***www.opcfoundation.org/cloud***.

Stefan Hoppe, President & Executive Director, ***OPC Foundation.***

Learn More

Building the Digital Product Passport

DIGITAL PRODUCT PASSPORT

SOURCE: OPC FOUNDATION

The Digital Product Passport is coming. And sooner than you think!

Soon, the European Commission will be voting on the specification of the Digital Product Passport (DPP). While the specification is written in a technology-neutral fashion, it is clear that very soon, the first implementations based on concrete technology need to appear. Realistically, to meet the Commission's goal of introducing the DPP by 2027, these implementations need to be started now.

One Candidate: The Asset Administration Shell

The Asset Administration Shell (AAS) has been developed by the German Plattform Industrie 4.0 over the last 10 years. It now has a file exchange format, a technology-neutral meta model and a REST interface specified and all three are currently being standardized through the IEC. The AAS is evaluated as a standardized data exchange framework for the manufacturing supply by consortia in Germany and beyond. There are also several data model templates released by the Industrial Digital Twin Association (IDTA), the new owner of the AAS specification. However, what the AAS still lacks today are commercial tools to develop and build Asset Admin Shells and broad industry adoption.

OPC UA: the Industrial Interoperability Standard

At this point it is important to bring OPC UA into the equation: OPC UA has vast industry adoption and is an IEC standard since 2010. Most manufacturers have adopted OPC UA and some even made it a requirement in purchasing agreements. There is a very large ecosystem of commercial OPC UA modelling tools available and there are over 153 standardized data models available free of charge via the OPC Foundation. Incidentally, the OPC Foundation is close to reaching the 1000-member mark and it is still seeing exponential growth in its member ecosystem. Millions of products use OPC UA today.

Combining Ecosystem to Accelerate DPP Adoption

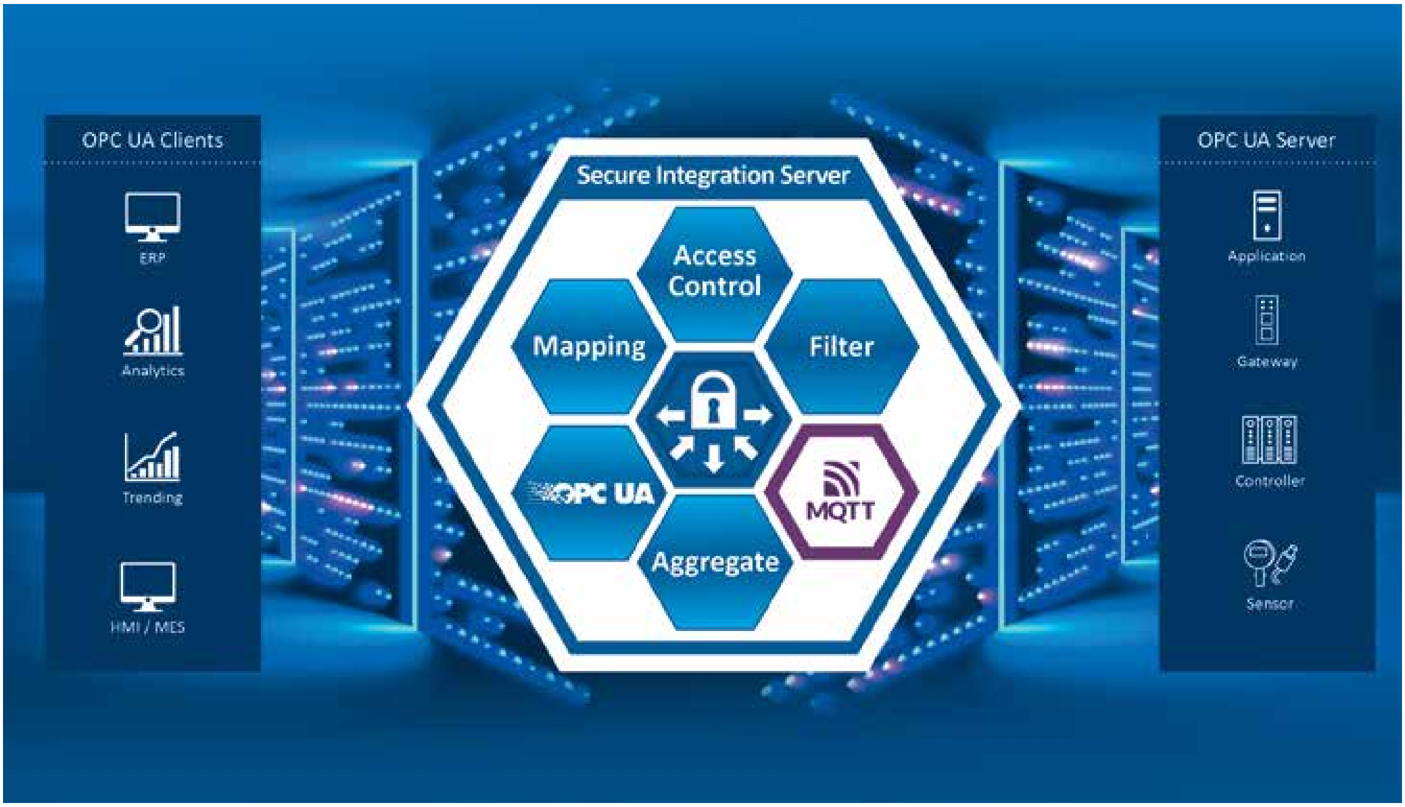
It doesn't take a rocket scientist (although OPC UA is also used in rockets!) to figure out how both the AAS and the OPC UA technologies can fulfill and accelerate the adoption of the DPP. What the AAS is still lacking today, OPC UA can cover, and many believe that a combination of the two ecosystems of AAS and OPC UA is the winning formula. In such a scenario, both technologies can play to their strengths: The AAS covers the data exchange for the DPP along a manufacturing supply chain while OPC UA covers the DPP modelling requirements.

Seeing is Believing

Most folks only believe something can work when they see it in action. Therefore, together with their partners Clean Energy and Smart Manufacturing Innovation Institute (CESMII) and the Digital Twin Consortium (DTC), the OPC Foundation built a demonstrator showcasing the combination of AAS and OPC UA technology at last year's Smart Production Solutions (SPS) trade show in Germany. Incidentally, this demonstrator was built in just 3 days! It uses OPC UA to model the DPP while using the AAS file exchange format as well as the AAS REST interface to distribute the DPP. With this combination, the successful rollout of the DPP can be easily achieved.

OPC UA aggregation server leverages MQTT protocol

An OPC UA aggregation server from Softing, enhanced by the use of the MQTT communications protocol, now offers a full range of OPC UA security features for secure and flexible inclusion of aggregated product and machine data in a wide variety of IT applications.



SOURCE: SOFTING

Use of the MQTT protocol sets new standard for connectivity and security in Secure Integration Server from Softing Industrial.

THE SECURE INTEGRATION SERVER (SIS) FROM Softing Industrial now supports the MQTT protocol which improves connectivity and security for data integration in IT/OT cloud applications.

The Secure Integration Server (SIS) from Softing Industrial offers a structured solution for complex server architectures. It combines various OPC UA servers at the automation level with their associated address spaces. This enables a standardized mapping of these address spaces in accordance with the OPC UA Companion Specification. The data provided in this way is then available for IoT cloud applications via a standardized OPC UA interface.

The interface abstraction of Secure Integration Server enables continuous adaptation and scaling of OPC UA-based IoT solutions throughout their entire lifecycle. Users gain a high degree of flexibility and at the same time significantly reduce integration and configuration costs.

The latest version of the SIS, V1.30, integrates the MQTT protocol (versions 3 and 5), making data integration more secure and flexible. The most significant benefits include:

MQTT Publisher & Subscriber: enables bi-directional data traffic for efficient communication.

MQTT Authentication Settings: Ensure security and identification between clients and brokers through various authentication methods such as anonymous, username or certificates.

MQTT Store&Forward Function: Protects against data loss.

Various Publishing Modes and "Dynamic Payload": Guarantee high flexibility for different data requirements.

Up to 25 MQTT Connections: Ensure seamless communication and provide a scalable solution.

Product Manager Andreas Röck commented on this development: "The integration of the MQTT protocol into our Secure Integration Server underlines our commitment to advanced solutions in industrial data integration. The enhanced security and connectivity features open up new possibilities for efficient and reliable data transmission for our customers."

Summary

The Secure Integration Server (SIS) provides a powerful OPC UA data integration layer. Based on the OPC UA aggregation server, users implement flexible solutions combining the various OPC UA Servers at automation level with their associated address spaces and making the data available to IT applications via a consistent OPC UA interface. Secure Integration Server covers the full range of OPC UA security features and enables the implementation of state-of-the-art security solutions.

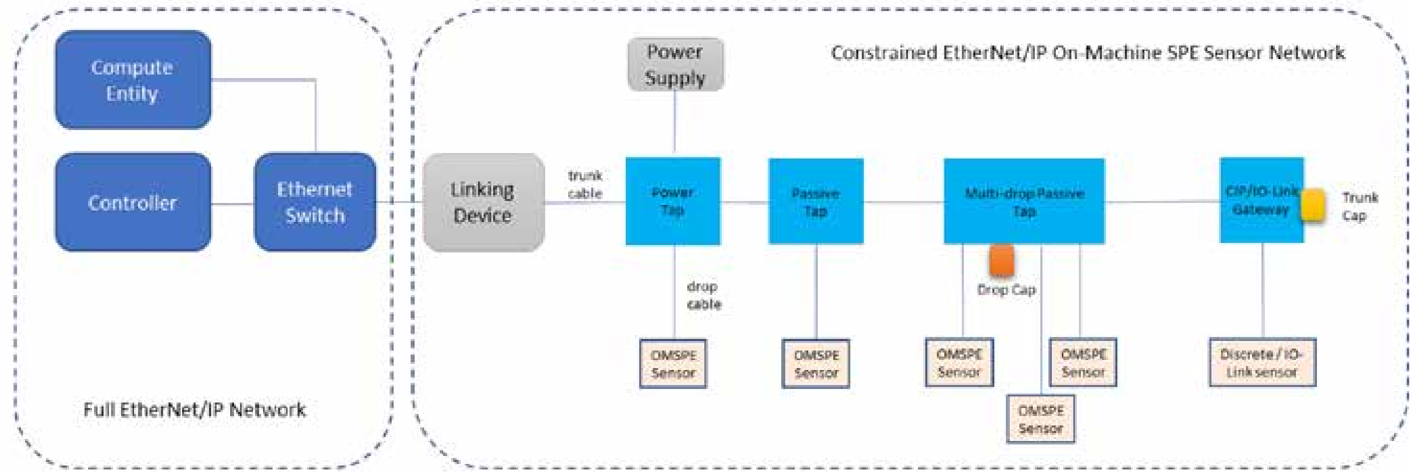
Further information and details on the new features of the Secure Integration Server can be found on the website.

Product news from ***Softing.***

Learn More

Constrained EtherNet/IP for on-machine sensor networks

An OMSPE sensor network concept enables EtherNet/IP connectivity from sensor to controller and compute. It also enhances the current DLR protocol with new linear network discovery and commissioning functions to simplify the OMSPE sensor network discovery, commissioning, and diagnosis.



SOURCE: ODVA

Figure 1 - An On-Machine SPE Sensor Network in an Automation System.

SINCE IEEE802.3CG TASK FORCE COMPLETED the 10BASE-T1S and 10BASE-T1L Ethernet standard development in September 2019, ODVA started its own adoption of these Ethernet technologies. In- cabinet EtherNet/IP usage profile based on 10BASE-T1S Ethernet and Ethernet-APL Instrument profile based on 10BASE-T1L Ethernet have been introduced into the EtherNet/IP Specification.

This article discusses another potential EtherNet/IP usage profile: the On-Machine sensor EtherNet/IP usage profile. A couple of thoughts on the constrained EtherNet/IP On-Machine Single Pair Ethernet (OMSPE) sensor network are explored, including the OMSPE system architecture (the physical topology, the media, the infrastructure taps, the SPE sensor), the communication architecture, the power delivery architecture, and the DLR Plus (DLR+) protocol with the network discovery, commissioning, and diagnosis function etc.

With the sensor supporting the constrained EtherNet/IP connectivity, it not only simplifies the communication technology from the sensor to controller for the traditional industrial control use cases, but also opens new opportunities for the information analytics use cases with the direct communication channel from the sensor to the compute/cloud. As a result, this will add value to the ODVA technology adopters. Most of the concepts discussed have been proved to work within the scope of research prototyping.

Constrained EtherNet/IP on-machine SPE sensor network

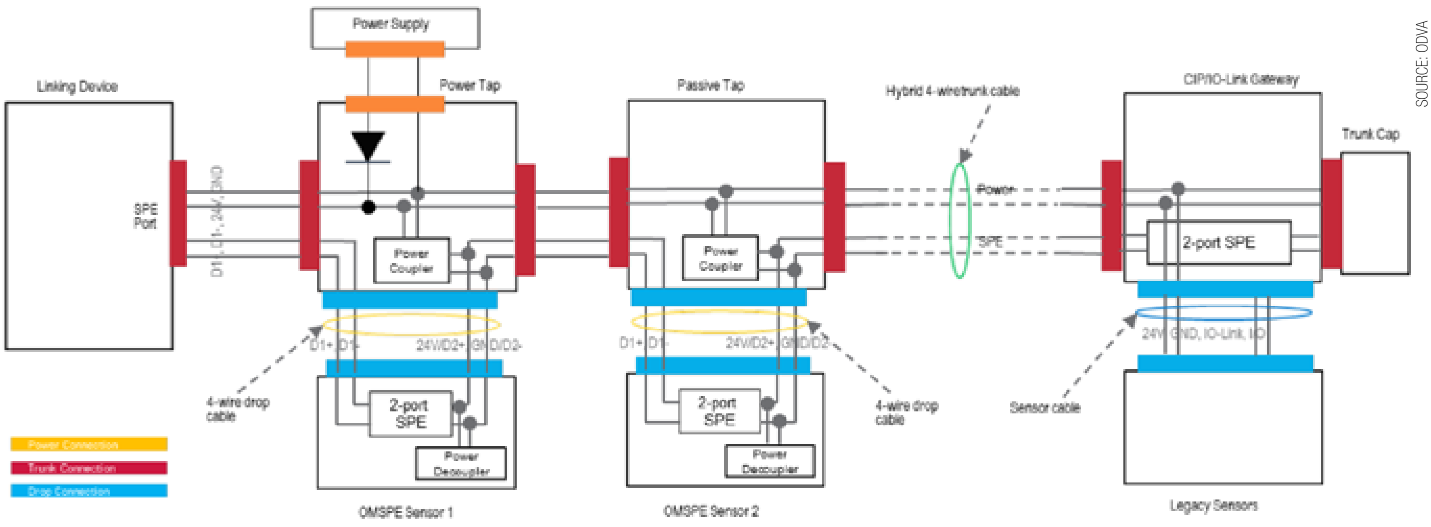
One of the main objectives for the OMSPE sensor network architecture work is to optimize the system cost of the OMSPE sensor network to enable a cost-effective and competitive solution on the market. Several concepts are adopted to support this objective: using passive taps instead of 3-port SPE switch taps to reduce the cost of taps and the system cost, adopting low cost EtherNet/IP concepts used in the In-Cabinet EtherNet/IP usage profile into the OMPSE sensor, using standard 2-pair Ethernet media on the drop, using unshielded cable, using powered SPE technology on the drop, …

Figure 1 illustrates a constrained EtherNet/IP OMSPE sensor network in an industrial automation system. The OMSPE sensor network adopts the trunk-drop physical topology. There are different types of taps connected with the trunk media from the trunk. OMSPE sensors are connected to the drop port of taps with the drop media. Caps are used to terminate the trunk and the unused drop ports on taps. Power is provided to the network via the Power Tap. The OMSPE sensor network is connected to the full EtherNet/IP network via a Linking Device.

Figure 2 further details the system architecture for the OMSPE sensor network. A linear SPE network and a bus power network are deployed in principle. The powered SPE technology is adopted on the drop. All OMSPE sensors are connected in a linear network topology via the OMSPE sensor network infrastructure (i.e., the SPE pair of taps and trunk/drop media). The power is provided from the power supply to OMSPE sensors in a bus topology via the OMSPE sensor network infrastructure (i.e., the power pair of the trunk and the powered SPE pair on the drop). The OMSPE sensor network combines the merits of In-cabinet T1S network (low cost EtherNet/IP) and APL/T1L instrument network (powered SPE, long distance SPE) to address the constrained OMSPE sensor use cases.

Active tap (i.e., 3-port switch) approach was considered initially. Reviewing the target system costs (device + network + installation) we concluded that while an active tap removes cost from the sensor (2 PHYs to one PHY and simplified connector), total cost of deployment (2 PHYs to 4 PHYs for connecting single sensor, more complex network commissioning and diagnosis) would increase.

We therefore elected to focus on the passive tap approach rather than the active tap approach. The primary disadvantage is that when a sensor fails, all downstream sensors are unable to communicate. The same is true for the active three-port switch tap component. Further, target applications are likely to be dependent on the failed sensor and unlikely to be able to operate in the case of a failed sensor. Other applications can still be served by classical star topologies.



SOURCE: ODVA

Figure 2 - On-Machine SPE Sensor Network System Architecture.

Network components

The following OMSPE sensor network components are described in detail: Linking Device, Power Tap, Passive Tap, OMSPE Sensor, Trunk Media, Drop Media, End Cap and Drop Cap.

Linking device

The primary functions of Linking Device are:

- As a media converter, to convert between SPE and standard 4-pair Ethernet,
- As a LNDC manager, to perform network discovery, commissioning, diagnostic, ...,
- As a protocol converter, to convert between TCP/TLS and UDP/DTLS,
- As a security proxy to authorize the user permissions/access rights on behalf of sensors,
- As a CIP router, to integrate two EtherNet/IP transport profiles seamlessly,
- As an I/O connection aggregator, to reduce number of I/O connections for controller.

Power Tap

The primary function of Power Tap is to inject the power from the power supply to the OMSPE sensor network.

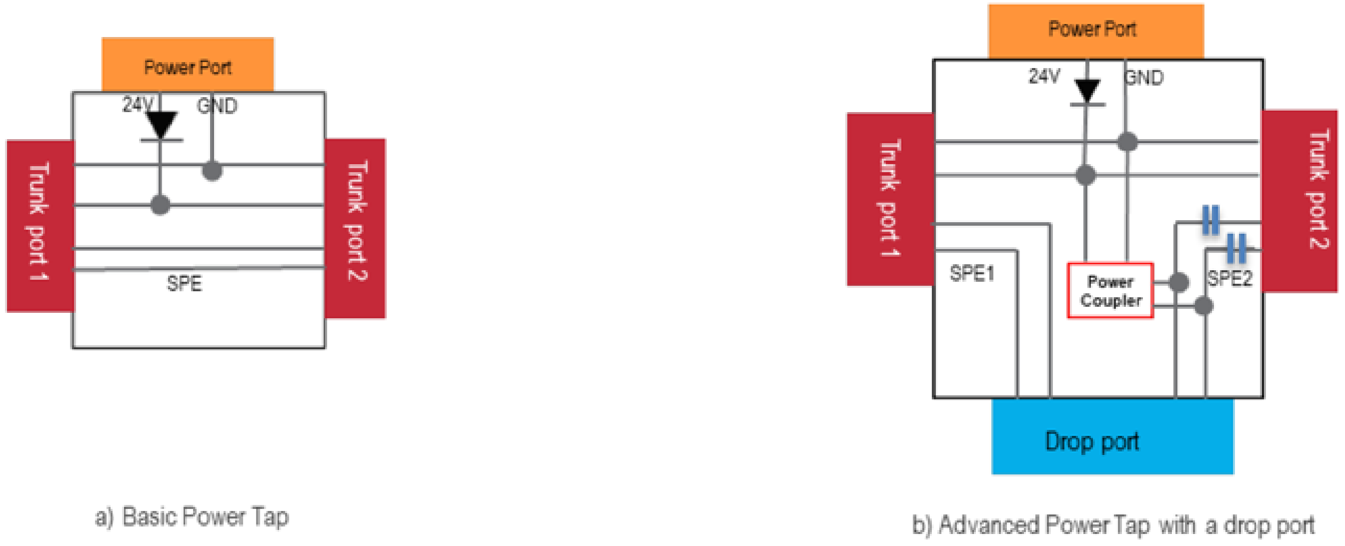
The basic power tap (as shown in Figure 3 a) has one power port and two trunk ports. The power port is connected to the power source (e.g., a 24V DC power supply). The 24V DC power is injected to the trunk power pair of the OMSPE sensor network. A diode on the 24V line prevents the current loop in the case that multiple power taps are used on an OMSPE sensor network. The first trunk port of the power tap is connected to the upstream trunk cable, and the second trunk port of the power tap is connected to the downstream trunk cable. The power tap delivers the power to the upstream and downstream network through two trunk ports. The power tap passes through the SPE signal from the first trunk port to the second trunk port.

The advanced power tap as shown in Figure 3 b) has an additional drop port. Besides the power injection function, it also can connect one OMSPE sensor onto the network via this drop port. Different from the basic power tap, the advanced power tap connects the upstream SPE pair (SPE1) and the downstream SPE pair (SPE2) to the drop port for connecting the OMSPE sensor. In addition to delivering power to the upstream and downstream network, the advanced power tap couples the power from the trunk power pair to the drop SPE2 pair via a power coupler. Two capacitors on the SPE2 pair between the power coupler and the second (downstream) trunk port prevent the power from flowing to the downstream network.

Passive tap

The primary function of a passive tap is to connect the OMSPE sensor to the OMSPE sensor network.

The single drop passive tap as shown in Figure 4 a) has two trunk ports and one drop port. The first trunk port of the passive tap is connected to the upstream trunk cable, and the second trunk port of the passive tap is connected to the downstream trunk cable. The single drop passive tap connects the upstream

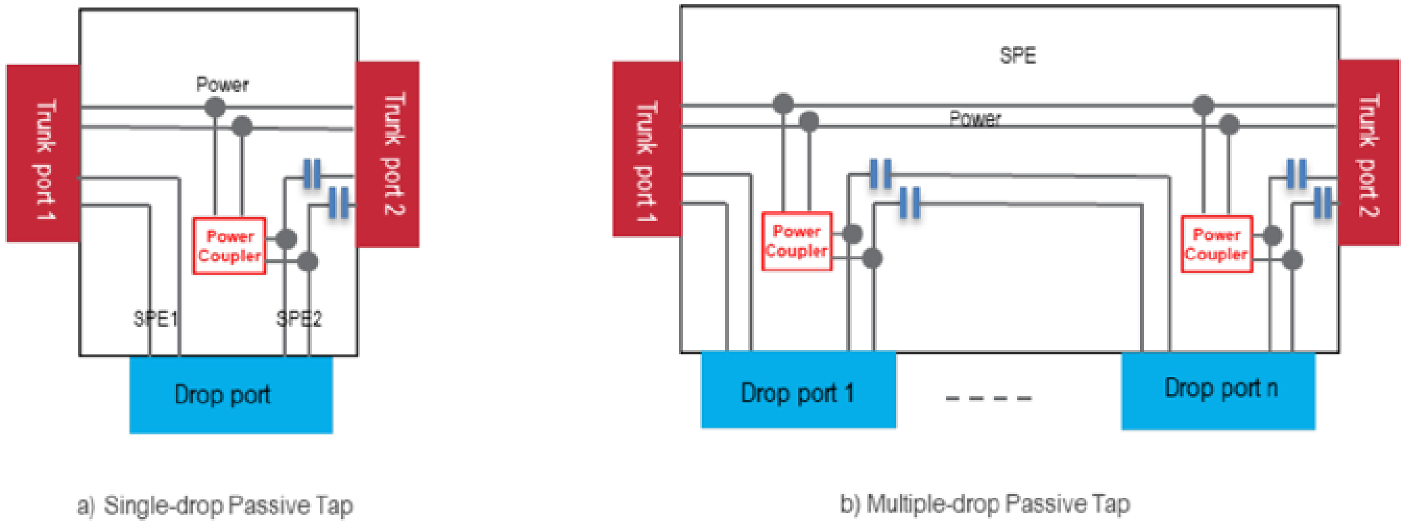


a) Basic Power Tap

b) Advanced Power Tap with a drop port

SOURCE: ODVA

Figure 3 - Power Tap Architecture.



a) Single-drop Passive Tap

b) Multiple-drop Passive Tap

SOURCE: ODVA

Figure 4 - Passive Tap Architecture.

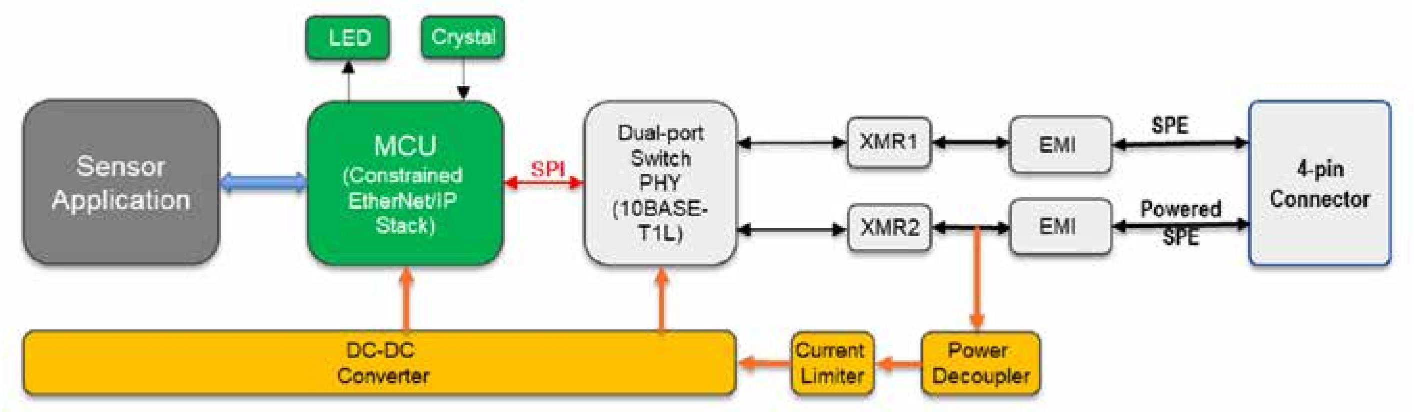


Figure 5 - OMSPE Sensor Function Block Diagram.

SPE pair (SPE1) and the downstream SPE pair (SPE2) to the drop port for connecting the dual-port OMSPE sensor. The single drop passive tap passes through the power from the first trunk port to the second trunk port and couples the power from the trunk power pair to the drop SPE2 pair via a power coupler.

Two capacitors on the SPE2 pair between the power coupler and the second (downstream) trunk port prevent the power from flowing to the downstream network.

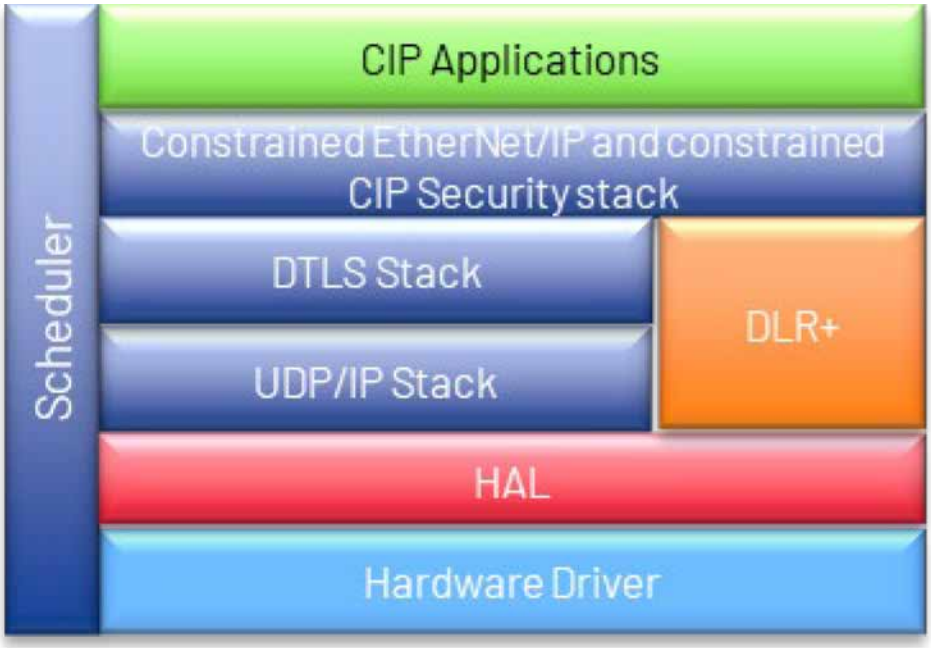
For a multiple drop passive tap as shown in Figure 4 b), each individual drop port has a power coupler and associated capacitors for the powered SPE operation on the drop.

OMSPE sensor

Figure 5 illustrates a block diagram for an OMSPE sensor as an implementation example. Conceptually, the OMSPE sensor circuitry consists of four parts: MCU, SPE, power, and sensor application. MCU, SPE and Power circuitries are common while the sensor application circuitry is product specific.

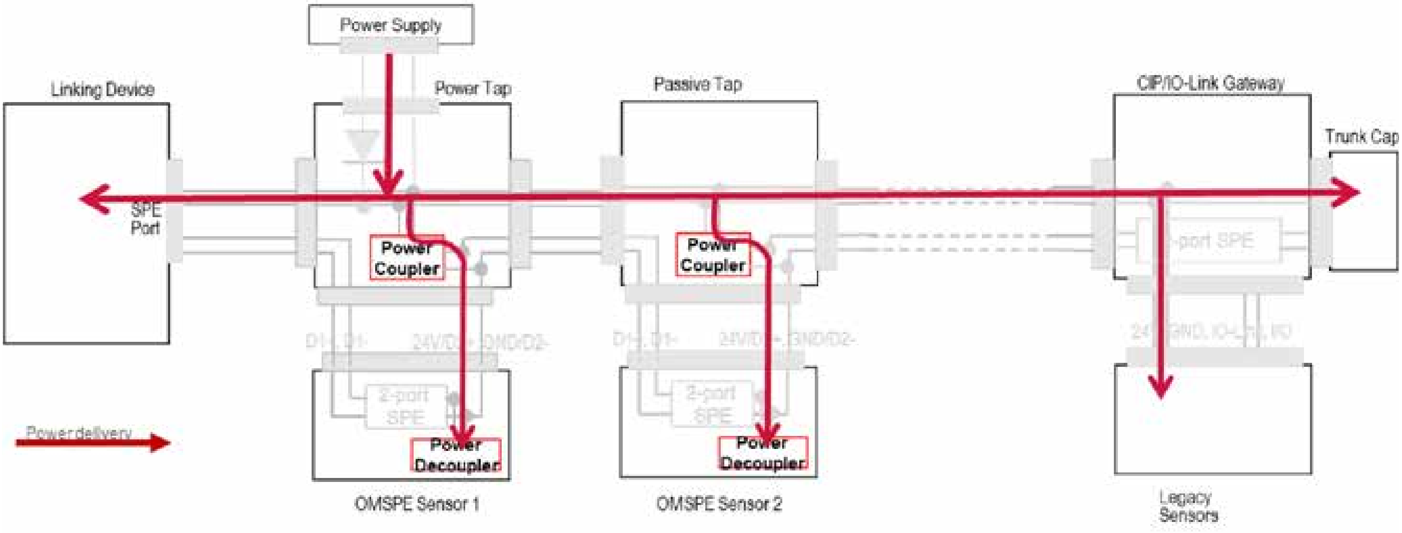
The SPE circuitry has upstream and downstream SPE communication channels. Each SPE communication channel is designed with an industrial level front end interface circuitry by having an EMI protector/filter and a SPE signal transformer. A single chip with a 3-port embedded switch, dual 10BASE-T1L PHYs and a SPI host interface is used for low cost and small footprint design. A single 4-pin standard M12-D Ethernet connector is used for both upstream and downstream SPE signal connections, which is different from the normal dual port EtherNet/IP device.

The downstream SPE pair also carries 24V DC power. A power decoupler module separates the power from the SPE communication signal. A current limiter limits the maximum current consumed from the OMSPE sensor network



SOURCE: ODVA

Figure 6 - Constrained EtherNet/IP Stack for OMSPE Sensors.



SOURCE: ODVA

Figure 7 - OMSPE Sensor Network Power Architecture.

in the case of a short circuit fault, which minimizes the impact on the OMSPE sensor network.

A low-cost non-Ethernet MCU (no MII/RMII) is used to reduce the cost. Standard OPEN Alliance SPI protocol is used between the MCU chip and the switch-PHY chip. Constrained EtherNet/IP stack as shown in Figure 6 is deployed.

The constrained EtherNet/IP stack conforms to the ODVA UDP-only transport profile and constrained CIP Security profile. The constrained EtherNet/IP stack may operate with a Scheduler instead of RTOS to reduce the memory consumption. The DLR+ protocol is also contained in the stack to support the network discovery, commissioning, and diagnosis functions.

Trunk media

The trunk media of the OMSPE sensor network are hybrid SPE cable and connector. The hybrid SPE cable has one power pair and one SPE pair. The power pair must endure at least 4A DC current so its gauge should be AWG18 or thicker. The SPE pair should be twisted and separated from the power pair in the cable. The electrical parameters of the SPE pair shall meet the IEEE PHY link segment specification. If possible, the trunk cable is preferred to be unshielded, and the trunk connector is preferred to be M12 4-pin connector.

Drop media

The drop media of the OMSPE sensor network are standard unshielded 2-pair Ethernet cable and 4-pin M12-D Ethernet connector. One pair is used for the SPE communication, and the other pair is used for the SPE communication and power delivery.

Trunk cap

The trunk cap is installed on the last tap's downstream trunk port. There is no electronic termination in the trunk cap.

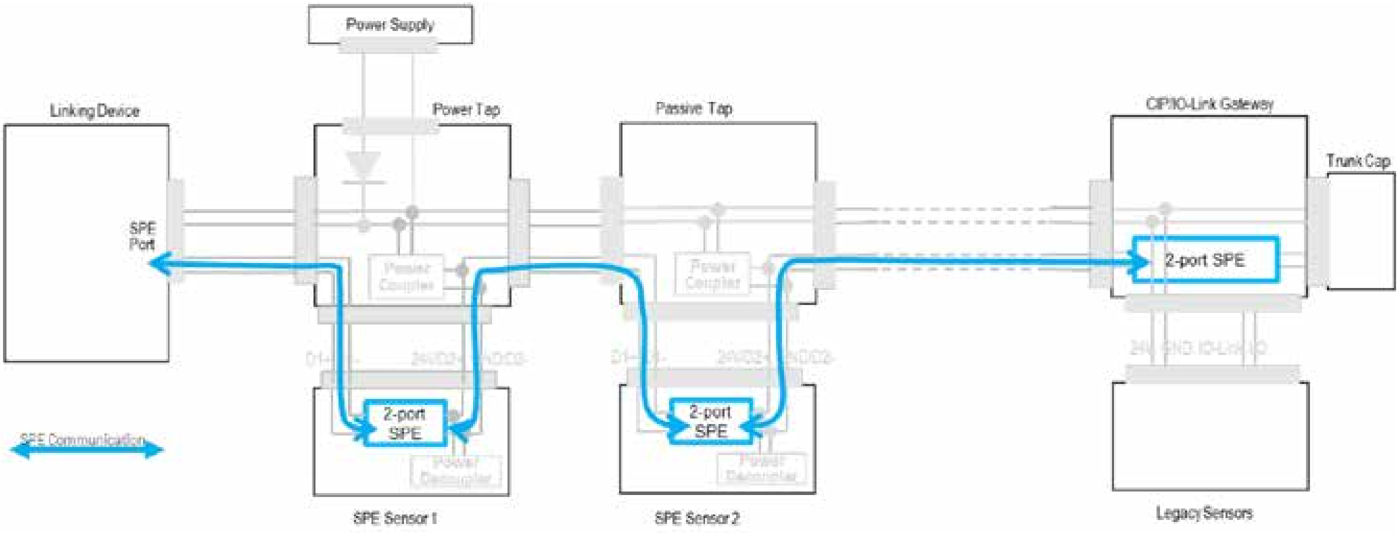
Drop cap

The drop cap is installed on a drop port reserved for future use. The drop cap connects the first SPE pair to the second SPE pair on the drop port via internal capacitors, which prevents the power on the second SPE pair from flowing back to the first SPE pair.

Power Architecture

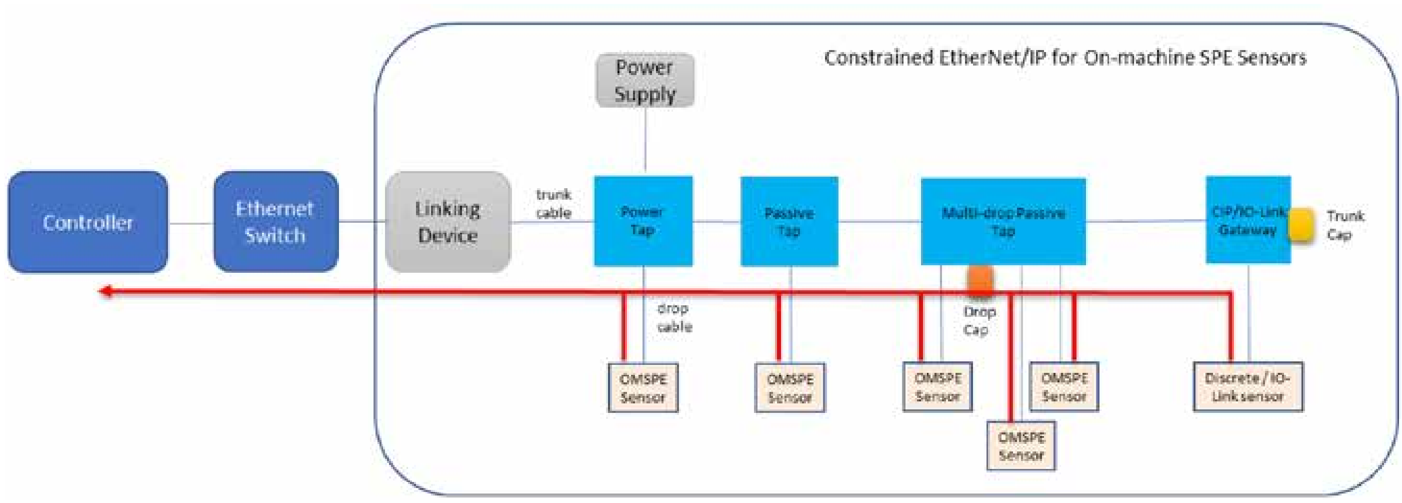
As shown in Figure 7, the OMSPE sensor network distributes the power on the power pair of the trunk media and delivers the power to each drop via the powered SPE concept. The powered SPE concept requires a power coupler in the passive tap and a power decoupler in the OMSPE sensor. The power coupler in the passive tap couples the power from the trunk power pair to the drop SPE pair. The power is delivered to the OMSPE sensor via the powered SPE pair. The power decoupler in the OMSPE sensor decouples the power from the SPE pair and provides the power to the OMSPE sensor' circuitry. Two adjacent OMSPE sensors communicate over the same SPE pair on this drop. Two capacitors in the passive tap are used to prevent the power from flowing to the adjacent OMSPE sensor.

This powered SPE architecture enables the



SOURCE: ODVA

Figure 8 - OMSPE Sensor Network and Communication Architecture.



SOURCE: ODVA

Figure 9 - Sensor to Controller Communication.

use of standard 2-pair Ethernet drop cable and connector. The power coupler/decoupler circuitry (power inductor) is small and low cost since the power coupler/decoupler only needs to pass the current for a single OMSPE sensor (0.5W).

Communication architecture

As shown in Figure 8, the SPE sensors are connected in a linear topology from the SPE communication point of view. Each OMSPE sensor has dual SPE ports. The first SPE port communicates with the upstream device and the second SPE port communicates with the downstream device.

The SPE link segment between two OMSPE sensors may consist of a trunk media, two trunk taps, and two drop media. The SPE link segment between the first OMSPE sensor and the linking device consists of one trunk media, one drop media and one trunk tap.

Sensor to controller communication

IO-Link is the current most popular communication technology for sensors. To integrate IO-Link Sensor with EtherNet/IP Controller, a specialized EtherNet/IP to IO-Link gateway function is required to translate between IO-Link and EtherNet/IP protocol and map between CIP and IO-Link data.

With the OMSPE sensor network, the sensor to controller communication is simplified because the OMSPE sensor natively communicates with EtherNet/IP. There is no complexity of the application protocol translation and data mapping.

Sensor to “compute” communication

With the OMSPE sensor network, the sensor to “compute” communication is simplified too compared to IO-Link technology. Because the OMSPE sensor uses IP and Ethernet communication, it is easy to add IIOT protocols into the sensor (e.g., MQTT). It could also use EtherNet/IP to communicate with a “compute entity” such as HMI, Workstation, or Edge device for Cloud. Direct access to rich sensor information such as sensor identity, configuration, and diagnostics enables new data analytic use cases.

DLR+ with LNDC functions

The protocol to simplify the OMSPE sensor network discovery, commissioning, and diagnosis is studied to support the objective of delivering the “ease of use” user experience. LLDP is a link layer discovery protocol, which is used for the network topology and device capabilities discovery. DHCP is a dynamic host configuration protocol, which is used for the device IP and network configuration. Using LLDP and DHCP for the OMSPE sensor network discovery, commission and diagnosis were considered at the beginning, however a couple of challenges are identified:

- LLDP is a link layer protocol. It would be quite complex to discover the location of the sensor on the network by the LLDP messages because the OMSPE sensor network is a switch-based linear network where LLDP messages are not allowed to cross the switch for the sensor position discovery.
- Knowing the whole topology by the linking device needs to read all Data Table objects in Sensors. This assumes the IP address is assigned in Sensors, however at this stage, the IP address is not determined.
- When the network changes (sensor insertion, removal, replacement), it will be quite difficult to detect these changes by the linking device because the LLDP messages from

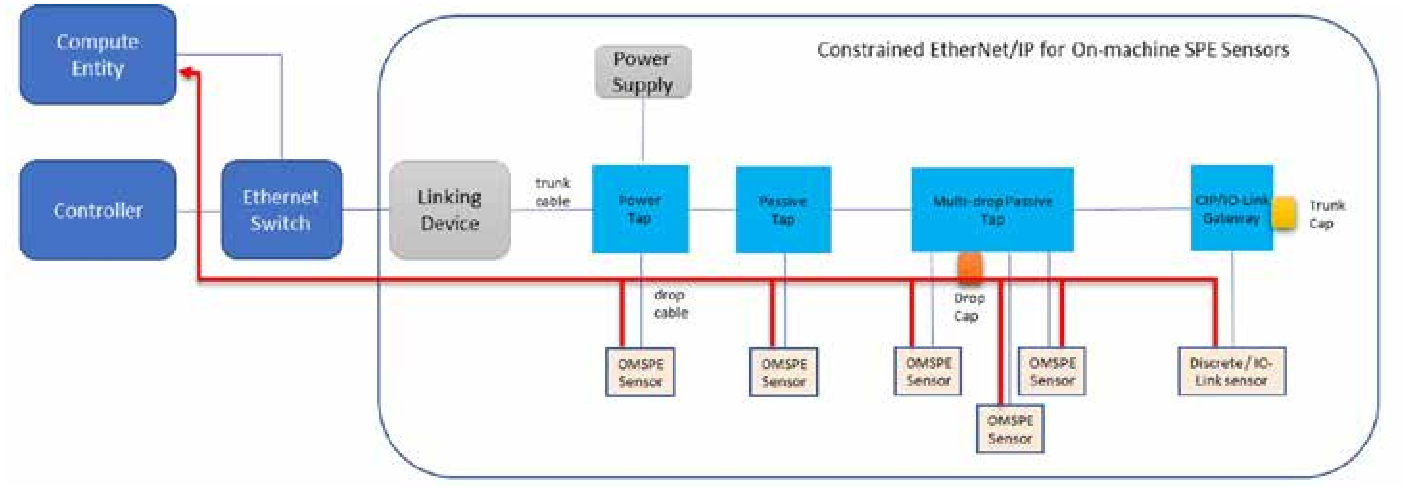
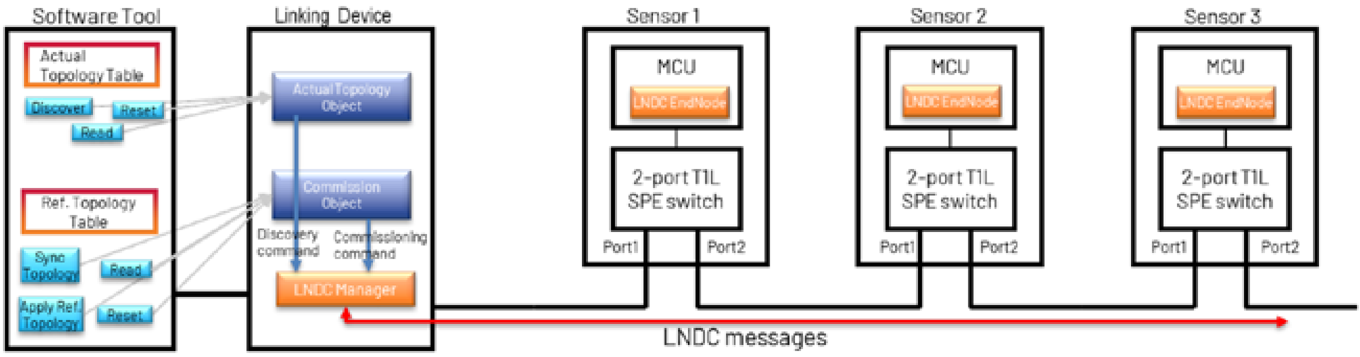


Figure 10 - Sensor to Compute Communication.



SOURCE: ODVA

Figure 11 - LNDC Protocol Architecture.

that device cannot reach the linking device. This will complicate the user experiences on the network diagnosis and the network upgrade.

DLR is a link layer protocol for the linear and ring network operation. Enhancing DLR with Linear Network Discovery and Commissioning (LNDC) functions to address the OMSPE sensor network use cases is proposed.

In specific, LNDC provides the following functions:

- Discover the network topology and apply it as reference topology,
- Commission the network easily including the initial network configuration and network device replacement,
- Diagnose the network quickly by detecting the device insertion, removal and change at a specific location.

The enhanced DLR protocol (DLR+) is also applicable to a general linear EtherNet/IP network.

EtherNet/IP In-Cabinet Usage Profile has already specified a network topology discovery and commissioning protocol for 10BASE-T1S multi-drop EtherNet/IP network. Main concepts of In-cabinet Actual topology object (discover current network topology, detect the changes to the last discovered topology) and In-cabinet Commissioning object (sync the reference topology, allocate IP address for devices, detect the topology change) are reused for the OMSPE sensor network.

As shown in Figure 11, there are four primary LNDC entities in an OMSPE sensor network: Software Tool, CIP Objects, LNDC Manager and LNDC End Node. The LNDC Software Tool provides user interfaces to display the actual topology information and the reference topology information and to issue the discovery and commissioning commands to the OMSPE sensor network. The Actual Topology object and Commissioning object in the Linking Device provides discovery and commissioning services to the LNDC Software Tool. The LNDC Manager initiates the discovery and commissioning process on the OMSPE sensor network under the commands from the Actual Topology object and Commissioning object. The LNDC End Node reports its network information in response to the Discovery Topology request and applies the network configuration retrieved from the Commissioning request message and responds with the state code indicating the configuration is successful or not.

As shown in the table below, the new DLR messages Discovery Topology and Commissioning are defined for LNDC functions. All messages use the Ring EtherType (0x80E1) and Ring protocol Subtype (0x02). The Discovery Topology Request is a multicast message. All LNDC End Nodes shall receive and process this message. All other three messages are unicast messages.

Discover network

Figure 12 illustrates the message sequences among LNDC entities for the network discovery process.

1. The LNDC Software Tool sends a CIP Discover Topology request to the Actual Topology object in the Linking Device.

2. The Actual Topology object replies to the LNDC Software Tool with a CIP Discover Topology response.

3. The Actual Topology object notifies the LNDC Manager to start the network discovery.

4. The LNDC Manager generates a Discover Topology Request message with a multi-cast MAC address (01-21-6C-00-00-02) and initial position ID (1) and sends the Discover Topology Request to the first OMSPE sensor on the OMSPE sensor network. The position ID indicates the location of the OMSPE sensor in the logical linear SPE network. The linking device always has the position ID 0, the first sensor following the link device has the position ID 1, the second sensor following the first sensor has the position ID 2, etc. The LNDC Manager also starts the discovery timer with 500ms timeout value. The discovery timer is used to determine the completion of the discovery process.

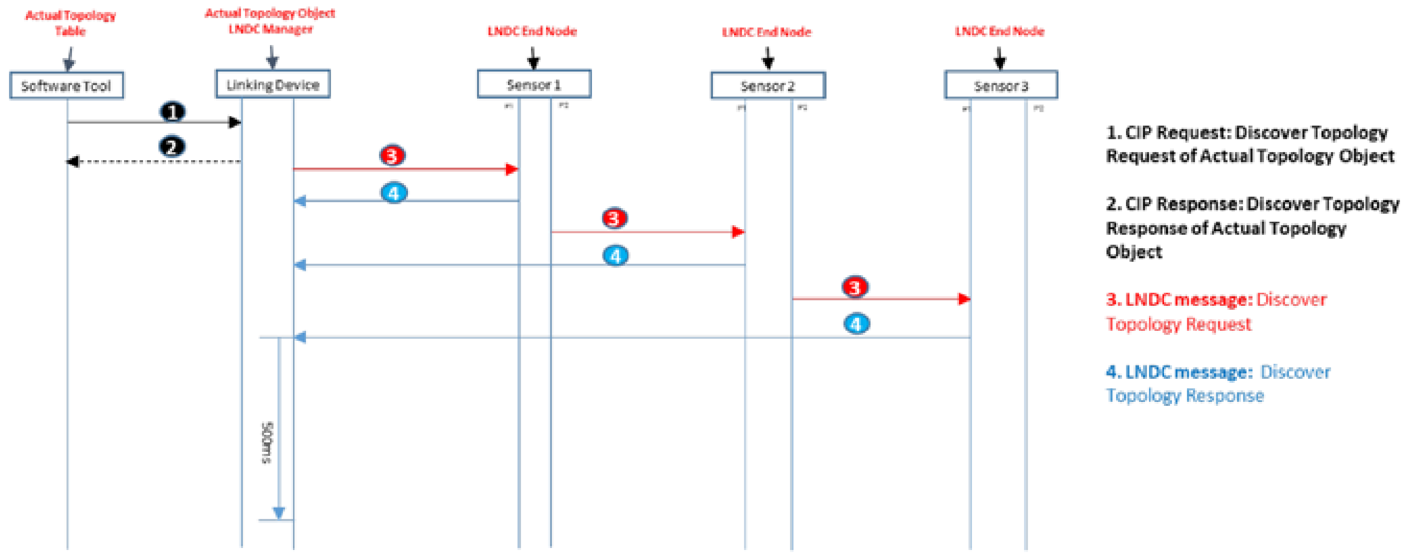
5. The LNDC End Node in the first OMSPE sensor generates a Discover Topology Response message with the OMSPE Sensor's position ID, MAC address, IP address, and CIP product key in response to the received Discover Topology Request message and sends the Discover Topology Response message to the LNDC Manager, then increases the position ID and forwards the Discover Topology Request message to the second OMSPE sensor.

6. The LNDC End Node in the second OMSPE sensor generates a Discover Topology Response message with the OMSPE Sensor's position ID, MAC address, IP address, and CIP product key in response to the received Discover Topology Request message and sends the Discover Topology Response message to the LNDC Manager, then increases the position ID and forwards the Discover Topology Request message to the third OMSPE sensor.

7. Step 6 repeats one by one until the last OMSPE Sensor is discovered.

8. The LNDC Manager completes the network discovery once the 500ms discovery timer expires. The discovery timer is reset whenever a Discovery Topology Response

Frame type	Frame Type ID	Dest. MAC Address	Direction
Discover Topology Request	0x10	01-21-6C-00-00-02	Manager -> End Node
Discover Topology Response	0x11	Manager MAC address	End Node -> Manager
Commissioning Request	0x12	End Node MAC address	Manager -> End Node
Commissioning Response	0x13	Manager MAC address	End Node -> Manager


Actual Topology Table
Actual Topology Object LNDC Manager
LNDC End Node
LNDC End Node
LNDC End Node
Software Tool
Linking Device
Sensor 1
Sensor 2
Sensor 3
1
2
3
4
3
4
3
4
500ms
1. CIP Request: Discover Topology Request of Actual Topology Object
2. CIP Response: Discover Topology Response of Actual Topology Object
3. LNDC message: Discover Topology Request
4. LNDC message: Discover Topology Response

SOURCE: ODVA

Figure 12 - LNDC Network Discovery.

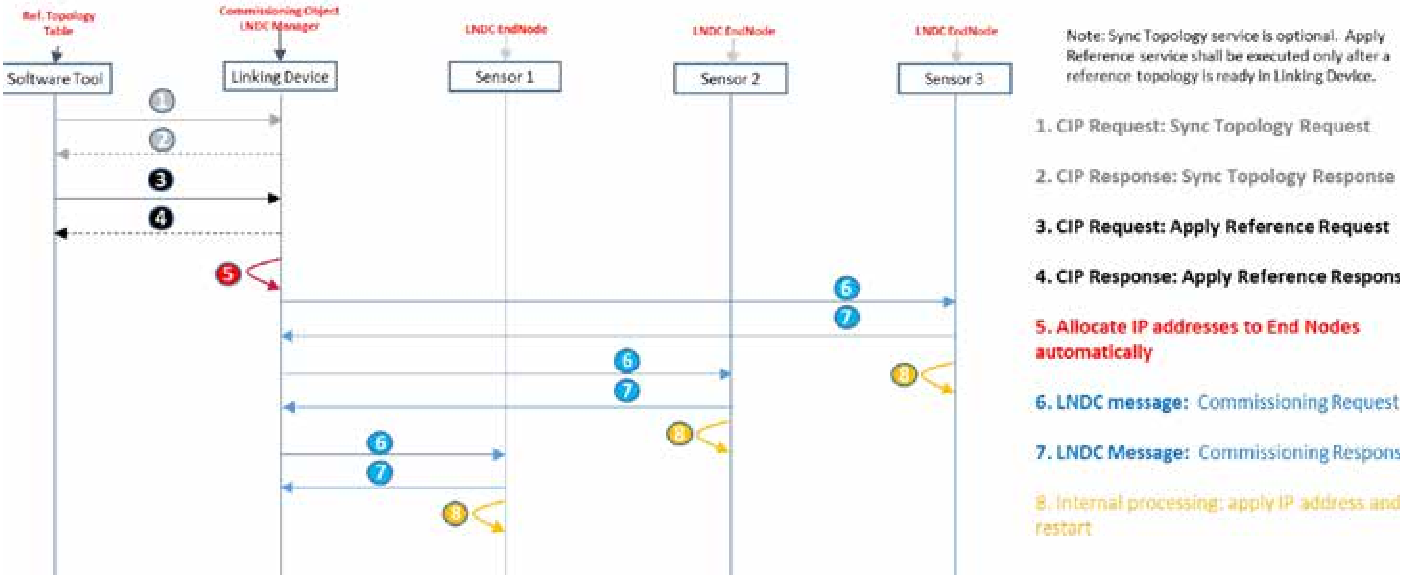

Ref. Topology Table
Commissioning Object LNDC Manager
LNDC EndNode
LNDC EndNode
LNDC EndNode
Software Tool
Linking Device
Sensor 1
Sensor 2
Sensor 3
1
2
3
4
5
6
7
6
7
8
8
6
7
8
Note: Sync Topology service is optional. Apply Reference service shall be executed only after a reference topology is ready in Linking Device.
1. CIP Request: Sync Topology Request
2. CIP Response: Sync Topology Response
3. CIP Request: Apply Reference Request
4. CIP Response: Apply Reference Respons
5. Allocate IP addresses to End Nodes automatically
6. LNDC message: Commissioning Request
7. LNDC Message: Commissioning Respons
8. Internal processing: apply IP address and restart

Figure 13 - LNDC Network Commissioning.

message is received. So, the discovery timer will not expire until the last OMSPE sensor is discovered.

9. The LNDC Manager checks the integrity of the discovered topology information. An error is reported if there is a gap in the actual topology table or the number of nodes is not equal to the actual topology table size.

Commissioning network

Figure 13 illustrates the message sequences among LNDC entities for the network commissioning process.

1. The LNDC Software Tool sends a CIP Sync Topology request to the Commissioning object in the Linking Device.

2. The Commissioning object replies to the LNDC Software Tool with a CIP Sync Topology response and retrieves the actual topology information from the Actual Topology object and sets it as the reference topology. Note that the reference topology in the Commissioning object might be generated by the user configuration instead of the discovered actual topology.

3. The LNDC Software Tool sends a CIP Apply Reference Topology request to the Commissioning object in the Linking Device.

4. The Commissioning object replies to the LNDC Software Tool with a CIP Apply Reference Topology response.

5. The Commissioning object automatically allocates IP addresses for the end nodes whose IP addresses are not configured and notifies the LNDC Manager to start the network commissioning.

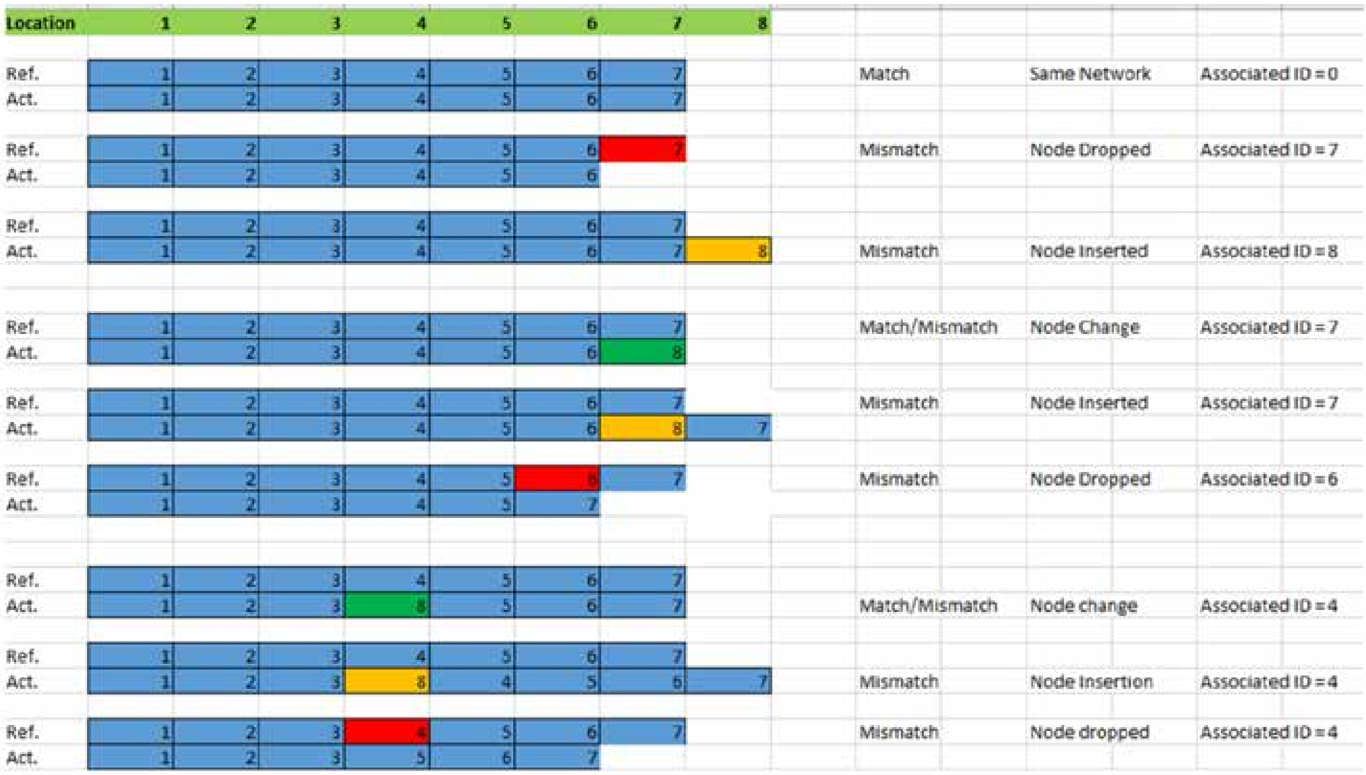
6. The LNDC Manager generates a Commissioning Request message with the allocated IP address in the Commissioning object for the last OMSPE Sensor and sends the Commissioning Request message to the last OMSPE Sensor on the OMSPE sensor network.

7. The LNDC End Node in the last OMSPE sensor generates a Commissioning Response message with the status code in response to the Commissioning Request message and then applies the IP address and other configurations internally.

8. After the LNDC Manager receives the Commissioning Response, it generates another Commissioning Request message with the allocated IP address in the Commissioning object for the penultimate OMSPE Sensor node and sends the Commissioning request to the penultimate OMSPE Sensor on the OMSPE sensor network.

9. The LNDC End Node in the penultimate OMSPE Sensor generates a Commissioning Response message with the status code in response to the Commissioning Request message and then applies the IP address and other configurations internally.

10. Step 6-7 repeats one by one in reverse order until the first OMSPE Sensor is commissioned.



Location	1	2	3	4	5	6	7	8			
Ref.	1	2	3	4	5	6	7		Match	Same Network	Associated ID = 0
Act.	1	2	3	4	5	6	7				
Ref.	1	2	3	4	5	6	7		Mismatch	Node Dropped	Associated ID = 7
Act.	1	2	3	4	5	6					
Ref.	1	2	3	4	5	6	7				
Act.	1	2	3	4	5	6	7	8	Mismatch	Node Inserted	Associated ID = 8
Ref.	1	2	3	4	5	6	7		Match/Mismatch	Node Change	Associated ID = 7
Act.	1	2	3	4	5	6	8				
Ref.	1	2	3	4	5	6	7		Mismatch	Node Inserted	Associated ID = 7
Act.	1	2	3	4	5	6	8	7			
Ref.	1	2	3	4	5	6	7		Mismatch	Node Dropped	Associated ID = 6
Act.	1	2	3	4	5	7					
Ref.	1	2	3	4	5	6	7				
Act.	1	2	3	8	5	6	7		Match/Mismatch	Node change	Associated ID = 4
Ref.	1	2	3	4	5	6	7				
Act.	1	2	3	8	4	5	6	7	Mismatch	Node Insertion	Associated ID = 4
Ref.	1	2	3	4	5	6	7		Mismatch	Node dropped	Associated ID = 4
Act.	1	2	3	5	6	7					

SOURCE: ODVA

Figure 14 - LNDC Network Diagnosis Scenarios.

Diagnose network

The LNDC manager can detect the network changes (node removal, insertion, and change) by comparing the reference topology to the current actual topology. Figure 14 LNDC - Network Diagnosis Scenarios, where the reference topology and actual topology are compared and the corresponding network diagnosis result are derived.

For a device replacement case (node change), the network match/mismatch is reported by comparing the product key of the old device to the product key of the new device based upon the key matching criteria. If a compliant device is replaced, the same IP address (and device configuration) is applied.

For a system upgrade case (node inserted), a network mismatch is always reported. The new devices' IP address will be automatically allocated by the commissioning object and assigned to the new devices inserted onto the network.

For a device fault case (node dropped), a network mismatch is always reported.

For all above cases, the associated position ID is reported. The user can easily identify the location of the node removal, insertion, and change.

LNDC software prototype

Figure 15 illustrates a LNDC software prototype.

In the network discovery area, the user can start the network discovery process by clicking the "discover topology" button. The discovery results are shown in the table. Each node has the position, MAC ID, IP address and CIP product key displayed at a row. The IP address 0 or a default IP address value is shown if the device is not commissioned. The number of devices on the network and the current network topology status are shown above the actual topology table. The user can also reset or retrieve the network topology by clicking the "reset" or "read" button.

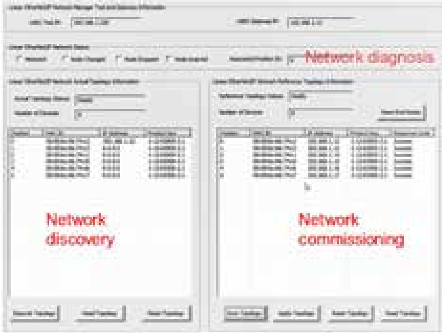


Figure 15 - LNDC Software Tool Prototype

In the network commissioning area, the user first syncs the reference topology to the actual topology by clicking the "Sync" button after the current network topology has been discovered. The IP addresses will be automatically allocated for devices whose IP addresses are not assigned. The user then applies the reference topology to the network by clicking the "Apply Topology" button. During this process, the IP addresses will be commissioned to the devices. The user can also reset or retrieve the reference network topology by clicking the "reset" or "read" button.

During the operation, the LNDC manager might periodically monitor or detect the network change. The network diagnostics information (network mismatch, node changed, node inserted, node removal, and associated position ID) is displayed in the network diagnostic area.

Summary and outlook

An OMSPE sensor network concept enables EtherNet/IP connectivity from sensor to controller and compute. It also enhances the current DLR protocol with new linear network discovery and commissioning functions to simplify the OMSPE sensor network discovery, commissioning, and diagnosis.

Most of the concepts have been proved to work within the scope of research prototyping. Further collaborations on this topic within the ODVA community are expected, in the areas of concept optimization for product design, specification enhancements on On-machine sensor EtherNet/IP usage profile and the whole ecosystem development. The optimization and enhancement should focus on the system cost optimization and ease of use, such as achieving reliable communication with the unshielded cable, developing highly integrated low-cost dual-port T1L SPE chip and minimizing the user configuration of the network, etc.

Dayin Xu, Principal Research Scientist, David Brandt, Engineering Fellow, and Paul Brooks Sr., Manager, ***Rockwell Automation.***

Learn More

The vital role of NAT routers in secure remote access

When building machines for automation, the same block of IP addresses is often used for each machine. If there are multiple machines with duplicate IP addresses, it can create an issue and NAT routers are used. 1:1 NAT tables can be set up, so multiple systems can be accessed from outside the concealed address block.

NETWORK ADDRESS TRANSLATION (NAT) IS A widely-used Layer 3 technology in which one or more local or "private" IP addresses are translated into one or more Global or "public" IP addresses in order to provide Internet access to the local hosts.

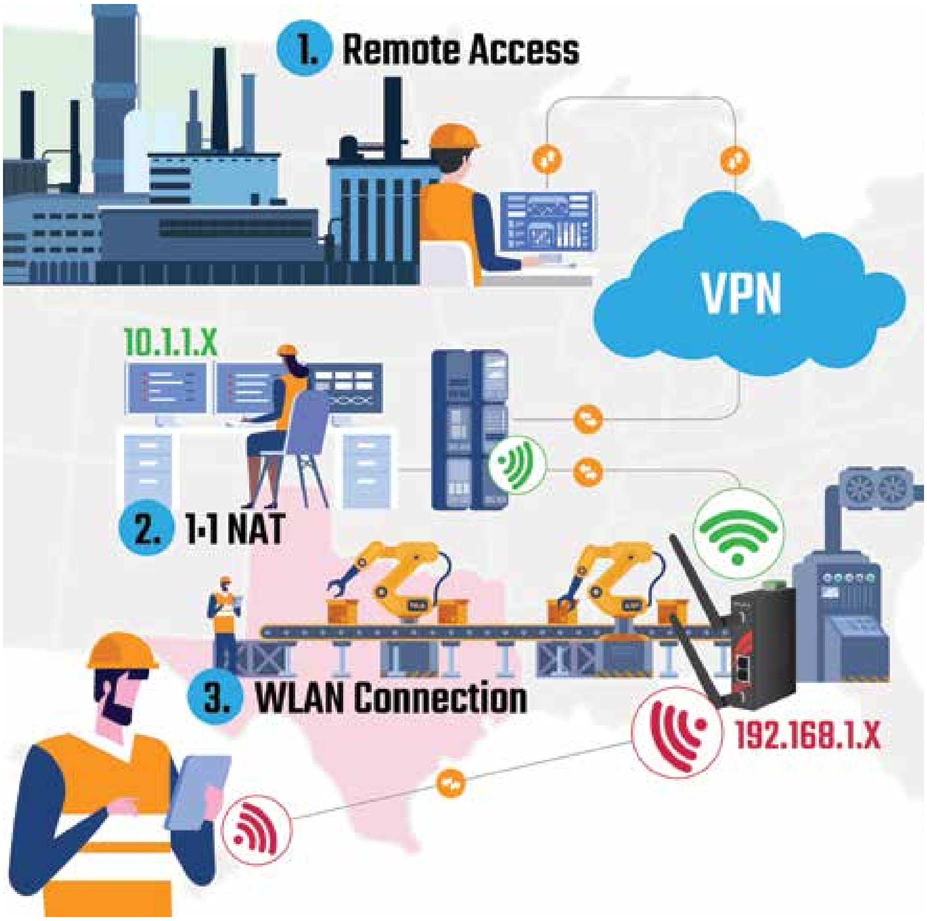
Compared to NAT applications in residential or commercial networks, NAT in Industrial Automation and Control Systems (IACS) is more varied and complex, although the overall concept remains the same.

In IACS, NAT is primarily about gaining access to information buried within a system outside your own. Consider a situation where a higher-level network outside the plant, for instance, the IT department, needs to access data located on a separate lower-level network or subnet in the OT department, consisting of a 12-port industrial Ethernet switch connecting PLCs, motor drives, IP cameras, and I/O devices. For the purpose of illustration, also assume there is a preventive maintenance application on a PC in the IT department.

This industrial application is seeking data such as heat, energy, and cycle times from a motor drive to predict its future maintenance needs. Since the two networks are on different addresses, however, the IT department PC is prevented from “talking” to the motor drive.

In this situation, an industrial NAT router can be deployed to assign a new IPv4 public address solely for the PC’s messages. Keep in mind this new address is not the private IP address of the PC itself.

When a data packet is sent from the PC, the NAT knows to convert it to the motor drive’s address, therefore bridging the gap. When the motor drive responds with the requested data, the NAT subsequently converts the drive’s address back to the PC message address which in turn is sent to the PC.



SOURCE: ANTAIRA

NAT (Network Address Translation) routers can be used to conceal the identity of an IP address block being used on a network, and can become part of a company's remote access strategy.

Port address translation

The above describes a straightforward example of the one-to-one static NAT protocol. In IACS, the Port Address Translation (PAT) version of the dynamic NAT protocol is often required when multiple devices are involved yet only one IPv4 address is available.

So, let’s assume the same situation as above. Now, however, we need data from the motor drive as well as from three PLCs. Since we only have one IPv4 address we’ll need to assign a port number to each device’s IP address by adding a colon, i.e., 192.155.100.18 to 192.155.100.18:3 where the “3” indicates the port.

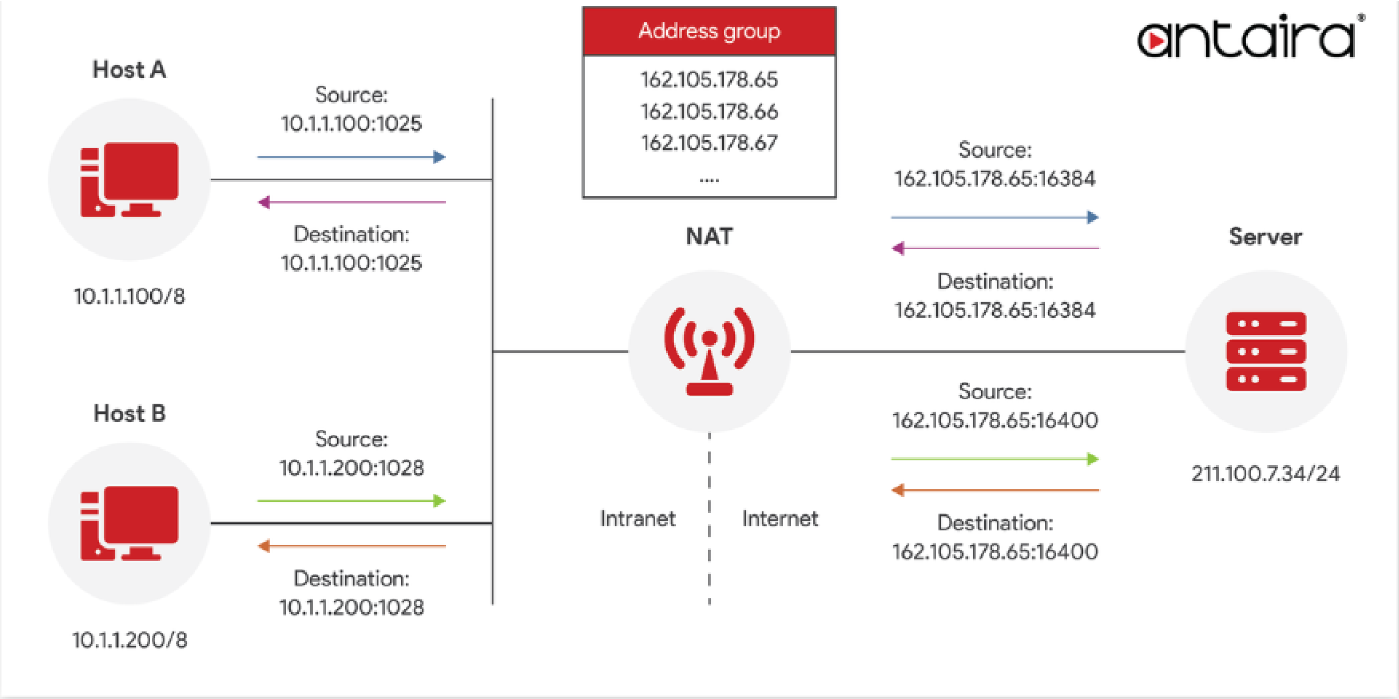
When the PC sends a message requesting information from one of the three PLCs or the drive, the NAT router reads the address and knows to send it to whatever device is assigned to port 3, although all the devices share the same IPv4 address.

For an OEM machine maker, NAT is equally valuable. NAT allows an OEM to reuse IPv4 addresses without introducing a duplicate IP address error into the network architecture.

For example, an OEM may use NAT for the replication of multiple control systems on skids and machines, including IP addressing, to help reduce development and commissioning costs. This way the end-user can have multiple machines on the same line configured with identical network settings and be able to perform remote support through a VPN connection.

Industrial strength

Like other industrial network devices, industrial NAT routers must be hardened to operate in environments where they will be subjected to extreme temperatures, heavy vibration, and electromagnetic interference. Carefully review a router's environmental specifications before deploying it, especially in an industrial area rated as Hazardous due to the presence of explosive levels of gases, dust, or liquids.



SOURCE: ANTAIRA

→	Packet from Host A to Server
→	Packet from Server to Host A
→	Packet from Host B to Server
→	Packet from Server to Host B

NAPT table		
Way	Before NAT	After NAT
Outbound	10.1.1.100:1025	162.105.178.65:16384
Inbound	162.105.178.65:16384	10.1.1.100.1025
Outbound	10.1.1.200:1028	162.105.178.65:16400
Inbound	162.105.178.65:16400	10.1.1.200.1028

Along with translating addresses, NAT provides an additional layer of security by hiding internal IP addresses from malicious actors. In this way, a NAT router works somewhat like a firewall guarding the LAN network against hacking and denial-of-service (DoS) attacks.

NAT router applications

Control Rooms or Network Cabinets: Many industrial facilities have control rooms or network cabinets where networking equipment is housed. This is a common location for NAT routers, along with other networking components such as switches, firewalls, and communication gateways. The NAT router in this context would provide a gateway between the local industrial network and the external network (e.g., the Internet).

Remote Monitoring Stations: Industrial facilities might have remote monitoring stations where engineers and technicians can access and monitor industrial processes from a distance. These stations might be equipped with NAT routers to facilitate secure remote access to the industrial network.

Communication Gateways: In complex industrial systems, there are often communication gateways that connect different protocols and networks. These gateways might incorporate NAT routing functionality to manage communication between different parts of the system and the outside world.

IoT and Edge Devices: As industrial IoT devices become more prevalent, NAT routers can be integrated into edge devices to manage communication between these devices and central servers or cloud platforms. This helps ensure that IoT devices can securely send data to and receive commands from remote locations.

Robotics and Manufacturing Cells: In manufacturing environments that utilize robotic systems or individual manufacturing cells, NAT routers can be used to provide remote access for maintenance and troubleshooting, as well as to facilitate data collection and analysis.

Energy Monitoring and Control Systems: Industries like energy production and distribution might employ NAT routers to enable remote monitoring and control of power generation, distribution, and consumption.

Process Control Systems: In industries such as chemical manufacturing, food and beverage production, and pharmaceuticals, NAT routers can be used to securely access and control critical processes remotely.

Water and Wastewater Treatment Plants: Facilities responsible for water treatment and wastewater management may use NAT routers to enable remote monitoring and control of pumps, valves, sensors, and other equipment.

Mining and Extraction Operations: Industries involved in mining, oil extraction, and natural resource management can use NAT routers to establish secure connections for remote management and optimization of operations.

Transportation and Logistics: In sectors like transportation and logistics, NAT routers can be employed to enable remote tracking and management of fleets, as well as for maintaining communication with vehicles and sensors.

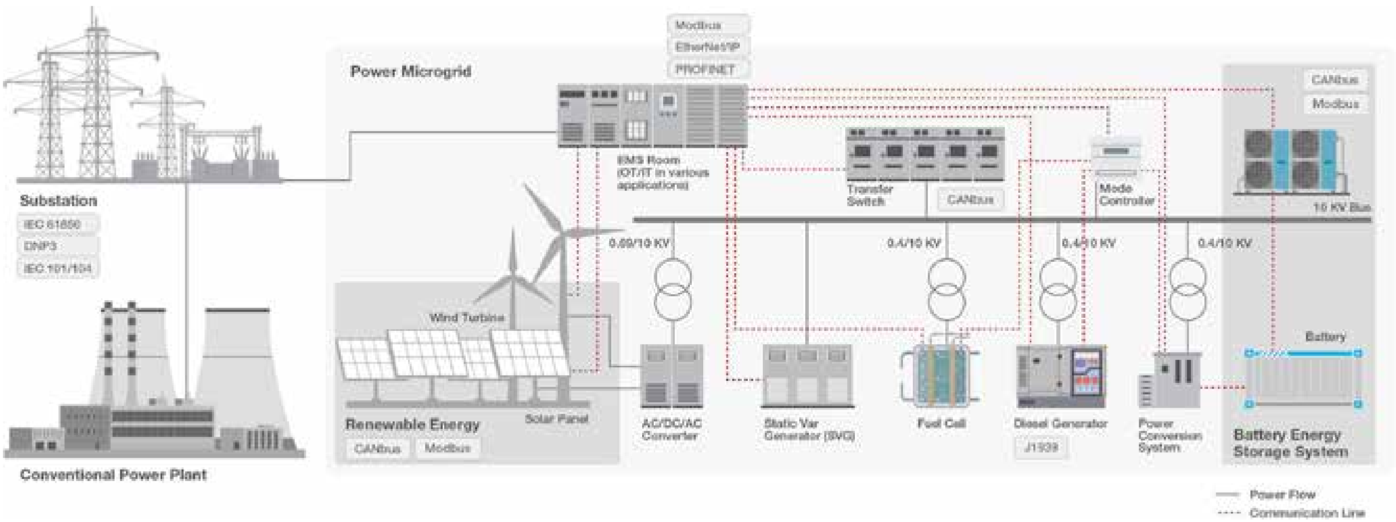
Remember that the specific location and implementation of NAT routers in industrial automation setups can vary greatly depending on the complexity and requirements of the system. The primary goal is to ensure secure, efficient, and reliable communication between industrial devices and external networks.

Technology report by ***Antaira.***

Learn More

Protocol gateways enable digital transformation of smart grids

In the era of smart grids, protocol gateways play a key role in smooth data flow between different systems. Because of the various communication protocols used among the different subsystems that make up the electrical grid, effective protocol conversion and seamless data communication are essential.



SOURCE: MOXA

Smart grids are highly complex systems made up of multiple subsystems with unique requirementson the same network.

DIGITAL TRANSFORMATION IS CONVERTING outdated utility infrastructure into smart grids as the race to achieve net zero carbon emissions picks up speed. This model aims to improve energy management by collecting and analyzing data in real-time.

However, maintaining a smart grid's smooth operation is no easy feat, which has engineers scrambling for ways to enable timely notifications, data analysis, and acquisition among complex subsystems.

Smart grids are highly complex systems made up of multiple subsystems with unique requirements.

Challenges and solutions

A smart grid is a vast system comprising multiple subsystems, ranging from traditional power generation, renewable energy sources, and transmission and distribution networks to digital substations, microgrids, and energy storage systems. Each subsystem has its own characteristics and requirements, including power distribution control, power monitoring, energy storage management, and more.

The challenge arises from the diverse communication protocols used among these subsystems. For instance, feeder lines commonly use IEC 61850, DNP3, or IEC 101/104, while meters rely on Modbus, renewable energy systems utilize CANbus, and backup power employs J1939. Unifying all this data poses a complex problem.

In this scenario, effective protocol conversion and data integration become crucial. This is typically done with programmable logic controllers (PLCs), but it is more costly and complex because PLCs require extensive programming.

Industrial computers are another option, but such a solution demands expertise in numerous communication protocols. Even after the system has been operating for a while, potential problems can still occur, so installing diagnostics and troubleshooting tools on location is required. Furthermore, the solution must comply with cybersecurity requirements and the hardware robust enough across various environmental conditions.

Protocol gateways have proven to be an effective solution. They facilitate protocol conversion through simple configuration, eliminating the need for complex programming. Therefore, it is possible to accomplish data integration and system communication even without extensive programming knowledge.

Here are a few features to look for:

Remote troubleshooting

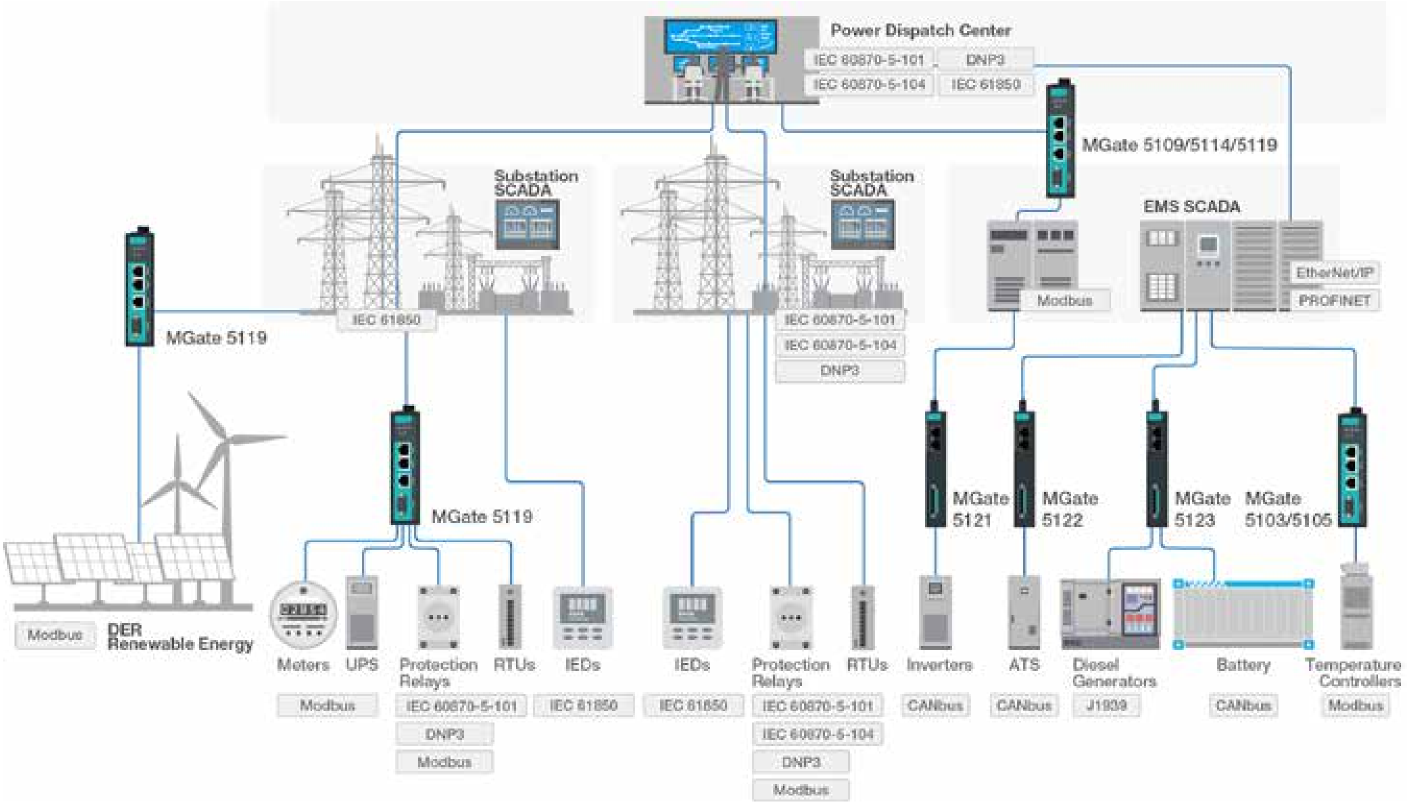
In a smart grid, many devices are in remote locations. Remote access and troubleshooting are crucial to minimize the time spent sending out staff to resolve issues on-site. Protocol gateways provide built-in tools for troubleshooting, significantly reducing the time needed for fault diagnosis while also cutting the cost of external debugging tools.

The Importance of Security

Because remote connections to protocol gateways are possible, security becomes paramount. Protocol gateways need to provide secure connection features, including HTTPS and SSH connections, strict account and password management, and event log recordings. These features can mitigate potential risks of hacker attacks and ensure system security.

Smart grids optimized with protocol gateway

Connecting legacy power systems to IEC 61850 communication networks can be complex, as a variety of industrial protocols are used in field sites. Furthermore, bringing them into networks raises serious security concerns. Moxa’s MGate 5119 Series IEC 61850 gateways support power industry-related protocols such as Modbus, DNP3, IEC 60870-5-101/104, and IEC 61850, to easily enable communication between power SCADA systems and a variety of field devices.



SOURCE: MOXA

Smart grids optimized with protocol gateways.

Reliability in harsh environments

Equipment in smart grids typically operates in harsh environments. Therefore, protocol gateways need to be designed for ruggedness. This includes resistance to wide temperature ranges and electromagnetic interference to ensure the overall reliability of the system. You can consider adding something about fiber options as well as dual redundant power inputs and relay outputs provide added flexibility in challenging applications.

Easy configuration via web console

Quick setup guides make configuration faster and more cost efficient. With Quick Setup, like that featured on the Moxa MGate Series of Ethernet Gateways, you can easily access protocol conversion modes and finish the configuration in a few steps. These gateways also support Auto Detection for DNP3 serial outstations, allowing the protocol gateway to automatically acquire all outstation objects when configured as a DNP3 master.

Modbus and DNP3 traffic monitor

Troubleshooting, especially during the installation stage, is crucial to minimizing downtime. Communication issues are frequently caused by incorrect software parameters such as slave ID and register address or incorrect command configuration. If your gateway supports Modbus/DNP3 Protocol Traffic Monitor, you can check the captured data and easily identify the root cause.

The Moxa MGate 5119 industrial Ethernet gateway features 2 Ethernet ports and 1 RS-232/422/485 serial port. It supports Modbus RTU/ASCII/TCP, IEC 60870-5-101, IEC 60870-5-104, and IEC 61850 MMS Protocol Traffic Monitor for easy troubleshooting, especially during the installation stage.

Remote maintenance functions

Protocol gateways should provide a web and Telnet console for remote maintenance. Support for encryption communication functions, including HTTPS and SSH, ensure better network security.

In addition, look for industrial gateways with firmware log functions that can record connection events and Modbus maintenance events.

Conclusion

In the era of smart grids, protocol gateways play a pivotal role in facilitating smooth data flow between different systems. Because of the various communication protocols used among the different subsystems that make up the electrical grid, effective protocol conversion and seamless data communication are essential to fully realizing smart grid potential.

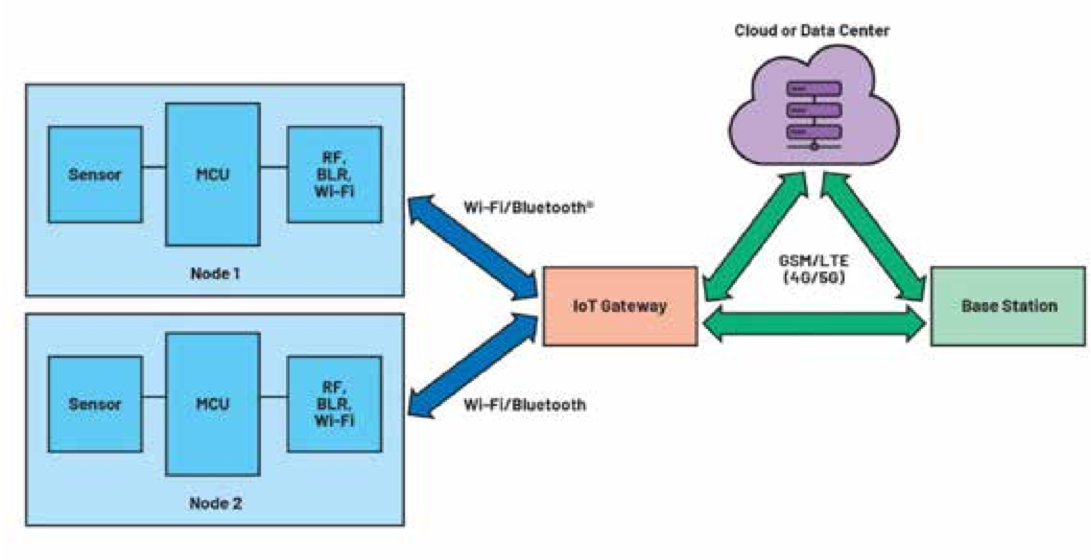
Protocol gateways allow for easy protocol conversion through simple configuration, remote troubleshooting, and system security. The application of this networking technology will contribute to achieving smarter, more efficient energy management, transforming the way electricity is delivered around the world.

Kuru Kuruvilla, Industry Marketing Manager, ***Moxa.***

Learn More

How to greatly improve battery power efficiency for IoT devices

Addressing the critical role of managing battery power in the exploding world of IoT devices, optimizing ship and sleep mode is one of the best ways to improve battery efficiency. The MAX16163 solution from ADI enables a design with a more precise control over those functions.



SOURCE: ANALOG DEVICES

Figure 1. The typical building blocks of an IoT system.

EXPLORING HOW TO MAKE INTERNET OF THINGS (IoT) devices more power efficient requires a quick refresher of battery management we focus on the critical role of nanopower ship mode and sleep mode. Finally, in this article, we overview a new solution that better optimizes these two aspects of battery management which reduces the power consumption levels and board space over traditional methods.

Introduction

In the connected world of the internet, the IoT plays a crucial role by connecting different sensing nodes and transmitting the data to a secure server. Power management is one of the focus areas to increase the efficiency of the IoT application. In most applications, the sensor node (data acquisition element) is placed in a remote area and powered by a battery. The life of the battery depends on how efficiently we design the power strategies for the sensor node. Most of the time, the sensor node stays in sleep mode and switches to active mode only when it requires data acquisition. The duty cycle of these devices is low. To maximize the battery life, we need to improve the sleep current of IoT applications.

Basics of power management in an IoT device

In a typical IoT system, as shown in Figure 1, the wireless sensor node is mostly battery operated and, thus, inherently constrained by battery life. To maximize the life of the sensor node, power management is crucial. The duty cycle concept is a common practice for saving power in a sensor node.

Since overhearing and idle listening are major sources of energy wastage in the sensor node, we can evaluate a wireless sensor node's power consumption using three different areas:

- Sensor
- Microcontroller
- Radio operation

The sensor collects the raw data like temperature and humidity and sends this data to the microcontroller. The microcontroller processes the raw data and transmits this data to the cloud or data center using a radio link.

However, given that typical sensor applications operate at very low duty cycles (ranging from 0.01% to 1%) and are idle most of the time, adopting a power management scheme where sensor node sleep current is ultralow will conserve battery life. A smart irrigation system where the sensor node measures the soil moisture and collects data only once per hour is an example of such an application.

Critical roles of ship mode and sleep mode

The ship mode and sleep mode are the common jargon used in battery-operated IoT devices and are crucial aspects of power management in IoT applications. The ship mode is a nanopower state that prolongs battery life during the shipment stage of a product. In ship mode, the battery is electrically disconnected from the rest of the system to minimize power drain while the product is idle or not used. Push-buttons are used to release the ship mode and start the normal operation of the device.

Once the device is in an active condition, sleep mode is used to extend the battery life. In sleep mode, all the peripherals of the system are either shutdown or operating at their minimum power requirement. IoT devices wake up periodically, perform a specific task, and then return to sleep mode.

Different sleep modes can be achieved by

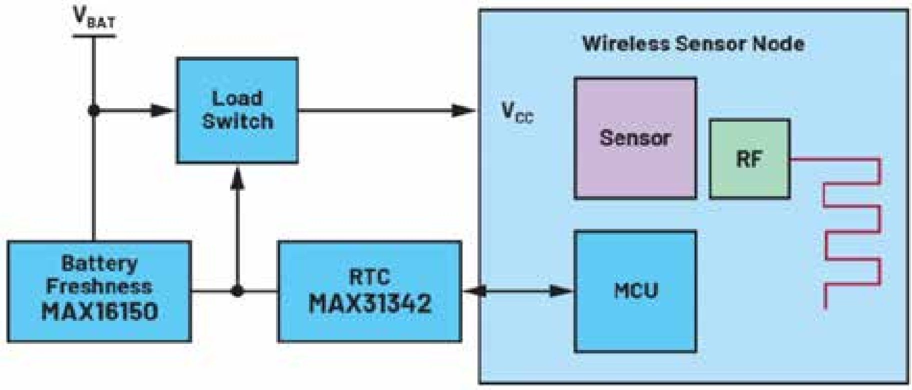
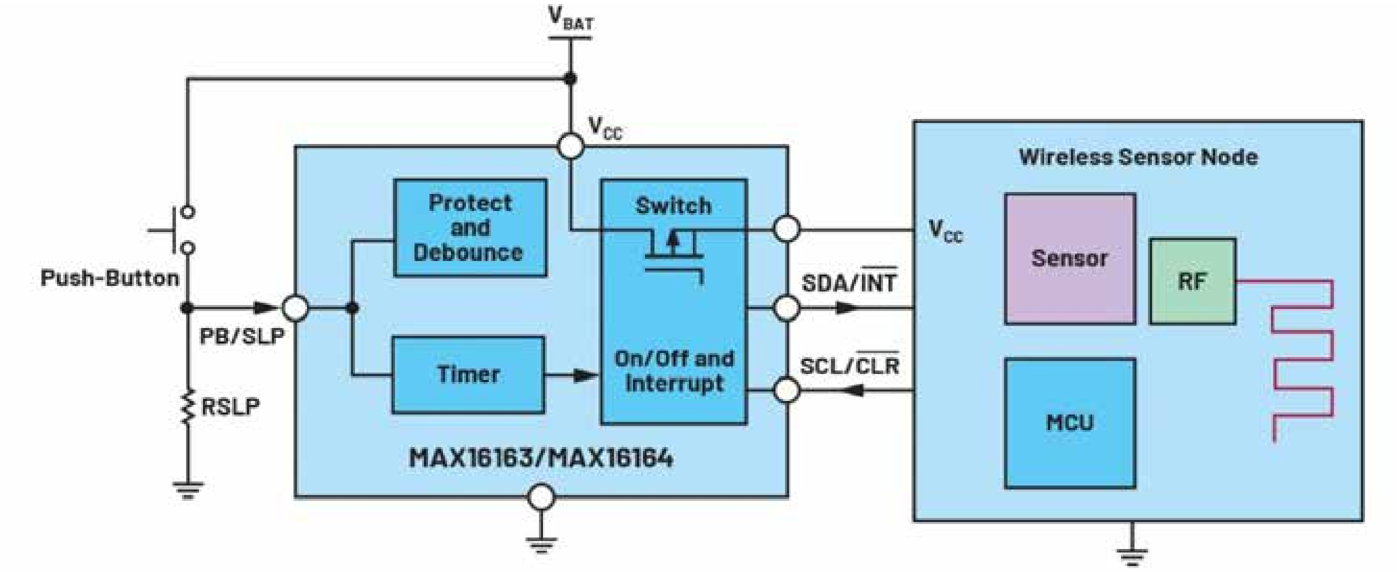


Figure 2. A discrete solution block diagram.



SOURCE: ANALOG DEVICES

Figure 3. An integrated solution using the MAX16163.

disabling various peripherals of the wireless sensor node. For example, in modem sleep, only communication blocks are disabled. In light sleep mode, most of the blocks including the communication block, sensor block, and digital blocks are disabled, and, in deep sleep mode, the wireless sensor node is completely powered off.

Enabling the deep sleep mode in the sensor node can maximize the battery life; therefore, optimizing the deep sleep current is the only way to improve the overall battery life.

Duty cycling method enables deep sleep mode in IoT applications

Duty cycling in the IoT module is one of the popular techniques for enabling the deep sleep mode. While a wireless sensor node is in deep sleep, most of the peripherals are off or in shutdown mode, consuming only new nanoampere current. A time-keeping device like the real-time clock (RTC) will wake up the IoT module after a programmed timeout.

In this technique, the microcontroller is completely off while the system is in deep sleep mode. However, after recovery, there is always a start-up boot time involved that will add an undesirable delay. Given this trade-off, the impact of the proposed principle depends on the characteristics of each node and the duty cycle of the application.

Conventional solution using RTC, load switch, and push-button controller

In the conventional solution, a load switch and an RTC are used to power on/off the

Functional Block	Part Number	Sleep Mode Current (nA) (Typ)	Shutdown Current (nA) (Typ)
RTC	MAX31342	150	6
Load Switch	TPS22916	10	10
Battery Freshness	MAX16150	10	10
Total System Current (Typ)		170	26

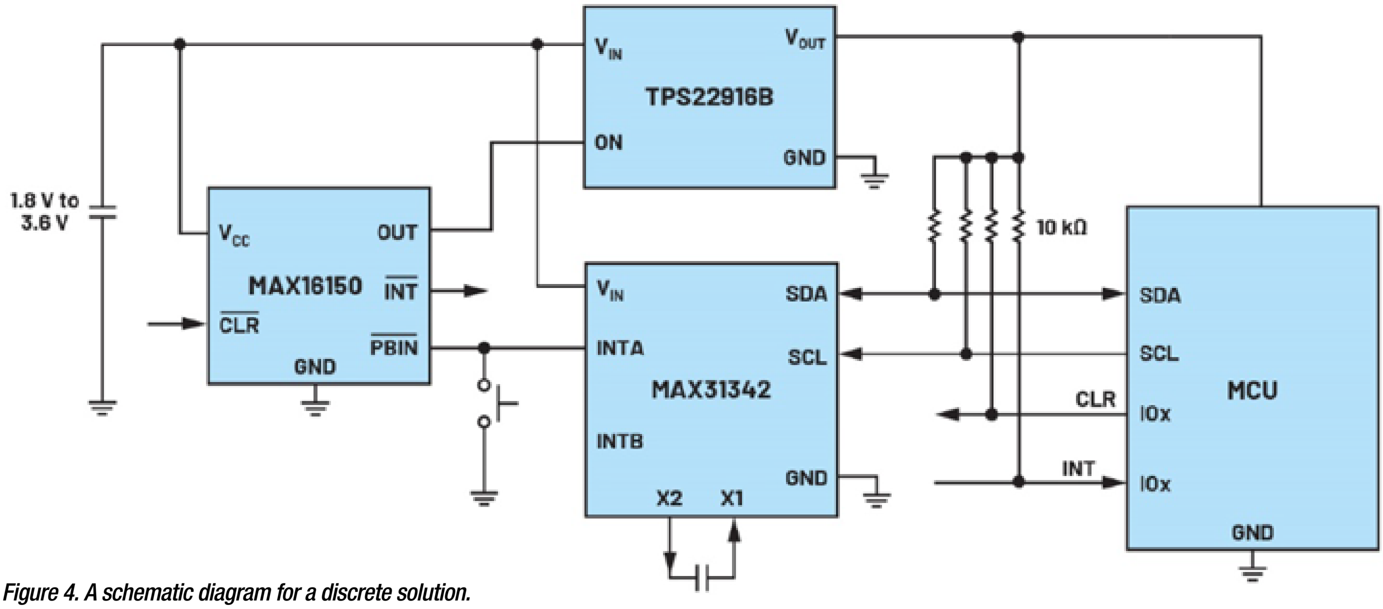


Figure 4. A schematic diagram for a discrete solution.

Specification	Discrete Solution Using MAX31342, MAX16150 and TPS22916	Integrated Solution MAX 16163
Coin Cell Capacity	250 mAh	250 mAh
Shutdown Current	146 nA	30 nA
Sleep Current	170 nA	10 nA
Number of ICs	3 (RTC + load switch + battery freshness)	1 (MAX 16163)
Crystal Oscillator	Required	Not required
Solution Size	130 mm^2 (typical)	50 mm^2 (typical)

SOURCE: ANALOG DEVICES

Table 2. Comparison of two different solutions.

wireless sensor node. In this approach, only the load switch and RTC are active, decreasing the total quiescent current to nanoamperes. The sleep time can be programmed with the microcontroller inside the wireless sensor node.

An external push-button controller can be connected to a load switch to enable the ship mode feature. The external push-button will exit the ship mode and enter the wireless sensor node into normal operation.

Improved solution for deep sleep and ship mode

MAX16163/MAX16164 are nanopower controllers with on/off controllers and programmable sleep time. The devices integrate a power switch to gate an output, which provides up to 200 mA load current. The MAX16162/MAX16163 can replace the conventional load switch, RTC, and battery freshness ICs to save the BOM count and to reduce costs.

The wireless sensor node unit is connected to the battery via MAX16162/MAX16163. The sleep time can be programmed by the microcontroller or can be set using an external resistor from PB/SLP to the ground or using the I2C command from the microcontroller. The external push-button is used to exit the device's ship mode.

Solution performance comparison

The performance comparison of both schemes is dependent on the duty cycle of the IoT application. In an application with a small duty cycle, the sleep current is a measure of how efficient the system is when the IoT device is running, and the shutdown current is a measure of ship mode power consumption.

To demonstrate the mode of the solution, we have chosen the industry's smallest quiescent current RTC MAX31342, battery freshness seal MAX16150, and tiny load switch TPS22916. The RTC is programmed using I2C communication that sets the sleep time of the IoT application, and when the timer expires, the interrupt signal pulls down the PBIN pin of the MAX16150, which sets the OUT high and turns on the load switch. During the sleep time, only TPS22916, MAX31342, and MAX16150 consume power system power.

In the experiment, we evaluate the lifetime of two state-of-the-art under fixed duty cycles, comparing their performance of the conventional solution and improved solution using the MAX16163.

The lifetime of the battery can be calculated using the average load current and battery capacity.

$$\text{Battery Life (Hours)} = \frac{\text{Battery Capacity (mAh)}}{\text{Average Load Current (mA)}}$$

The average load current can be calculated using the duty cycle of the system.

$$\text{Duty Cycle (D)} = \frac{\text{Active Time}}{\text{Active Time} + \text{Sleep Time}}$$

$$\text{Average Load Current} = \text{Active Current} \times D + \text{Sleep Current} \times (1 - D)$$

An active current is the system current when the wireless sensor node is active. To compare the two solutions, let's assume the system wakes up once every two hours, performs the specific task, and enters sleep mode after. The system active current is 5 mA. The battery life depends on the duty cycle of the operation. Figure 5 shows the plot of the battery life of two schemes with different duty cycles, varying from 0.005% to 0.015%.

In summary, this article addressed the critical role of managing battery power in the exploding world of IoT devices. It demonstrated that optimizing ship and sleep mode is one of the best ways to improve battery efficiency. The MAX16163 solution from ADI enables a design with a more precise control over those functions. It extends the battery life by about 20% (for a typical 0.007% duty cycle operation, as seen in Figure 5) and reduces the solution size to 60% as compared to a conventional approach.

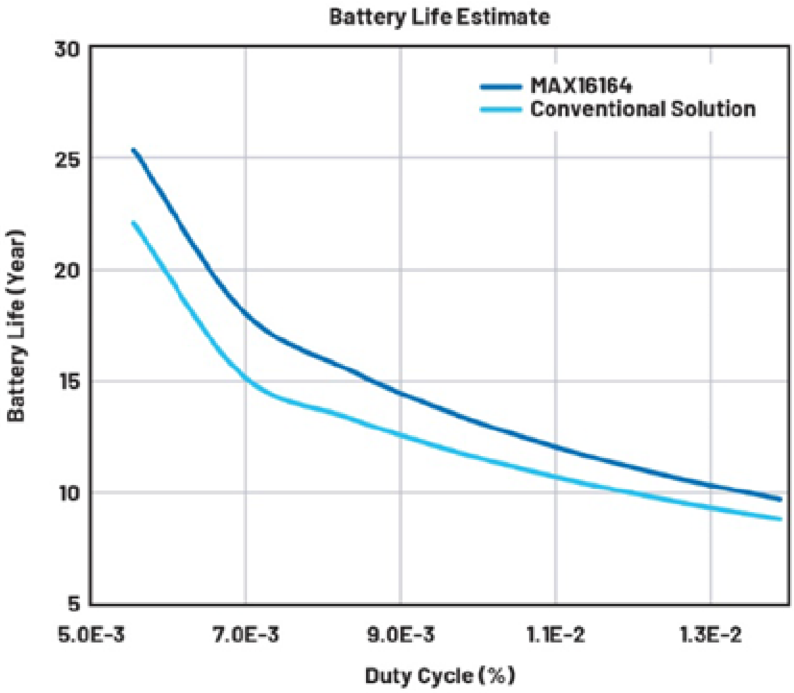


Figure 5. A graph showing battery life vs. duty cycle of a wireless sensor node.

Suryash Rai, Product Applications Engineer, ***Analog Devices.***

Learn More

Robust Ethernet communication in commercial vehicles

The increasing digitization and connectivity present new opportunities for integrating cameras, sensors, and other networked systems in commercial vehicles. Camera and sensor systems play a crucial role in commercial vehicles, particularly in the field of driver assistance systems and safety.

RELIABLE ETHERNET COMMUNICATION IS OF utmost importance for stable operation and the use of IP65/67-rated Ethernet switches, as well as the future integration of Single Pair Ethernet (SPE) in new commercial vehicles, offers immense advantages. This article explores the technical application of camera and sensor systems in commercial vehicles and emphasizes the significance of reliable Ethernet communication in this context.

The integration of cameras and sensors in commercial vehicles allows for improved safety, efficiency, and monitoring. Camera systems provide enhanced visibility for drivers and operators, especially in areas that are typically challenging to observe. Sensors enable real-time collection and analysis of crucial vehicle data. The networking of these systems requires reliable Ethernet communication, ensuring stable data and image transmission, seamless integration, and enhanced vehicle safety and efficiency.

IP65/67-rated Ethernet switches

In demanding industrial environments where reliability, robustness, and protection against environmental influences are paramount, IP65/67-rated Ethernet switches play an increasingly important role. These specially designed switches offer a range of advantages that make them an ideal choice for various industrial applications.

IP65/67 certification indicates that Ethernet switches are dust-tight and provide high protection against the ingress of dirt particles. This is particularly critical in harsh industrial environments where dust and dirt present constant challenges. Waterproofing is another essential advantage. The switches are protected against water jets or temporary submersion, making them suitable for high-humidity environments, outdoor applications, or situations requiring regular water cleaning.

Future: SPE in commercial vehicles

With technological advancements, Single Pair Ethernet (SPE) offers promising possibilities for networking in commercial vehicles.

Through weight and space savings, easy installation, and robustness, SPE can further enhance the performance and flexibility of vehicle networking. The implementation of SPE in new commercial vehicles allows for optimized integration of cameras, sensors, and other systems. SPE is based on the Ethernet standard, which is continuously evolving, ensuring high future-proofing and compatibility with new technologies and applications. Commercial vehicles equipped with SPE are well-prepared to benefit from future innovations in vehicle communication.

SOURCE: TERZ

Single Pair Ethernet is not just a technological advancement; it's a game-changer that unlocks new possibilities for various industries. Its cost-effectiveness, ease of installation, space-saving properties, weight reduction, and digital networking capabilities are all poised to make a significant impact.

One of the primary benefits of SPE is its ability to drastically cut down on investment costs. Traditionally, complex cabling systems were required to support communication in automation systems. However, SPE streamlines this by using just a single pair of wires.

Additionally, SPE simplifies installation efforts. With fewer cables to manage, the setup process becomes more straightforward, saving valuable time and labour. Space constraints are a common challenge in many industrial settings. SPE addresses this issue by minimizing space requirements. Its compact design and simplified cabling systems free up valuable floor space that can be better utilized for other purposes.

Weight is another critical consideration, especially in applications involving mobile autonomous systems. SPE's lightweight infrastructure reduces the overall weight of vehicles, which can contribute to improved energy efficiency and performance. Perhaps the most transformative aspect of SPE is its support for completely digital, IP-based networking.

Conclusion

The networking of cameras in commercial vehicles, such as construction and agricultural machinery, requires reliable Ethernet communication to ensure clear visibility of the working environment and improved safety. IP65/67-rated Ethernet switches provide the necessary environmental protection and enable stable real-time image and data transmission. The implementation of Single Pair Ethernet in new commercial vehicles promises a multitude of benefits that once again elevate efficiency, safety, and flexibility in vehicle communication.

Technology report by ***TERZ.***

Learn More

Evolving the CIP Energy Objects for greater efficiencies

There is a growing movement of energy awareness in all industries and a strong marketing push for better optimization of energy usage in industrial automation. All of the ODVA Energy Objects will need to be updated to reflect the information in a new power consumption management OPC UA specification.

SOURCE: ISTOCK

Energy is an indispensable component of industrial production but has been ineffectively managed as a production resource. Acquiring energy information detailed enough for action has been difficult and costly.

THE INTENTION OF THE CIP ENERGY™ INITIATIVE is to allow for the optimization of energy usage and scalability of implementation from basic energy awareness to advanced functions of energy control including dynamic demand-response. The ODVA Energy Applications SIG originally defined three specific objects, the Base Energy Object, the Electrical Energy Object, and the Non-Electrical Energy Object. Later, the Power Management Object and the Power Curtailment Object were added. These five CIP Objects became the basis for CIP Energy™.

When developed between 2010 and 2015, these objects were state of the art and sufficient for the times. It was discovered during the design of the Power Curtailment Object that revisions were needed for the Power Management Object. A specification enhancement was started but not completed before the ODVA Energy Applications SIG became dormant.

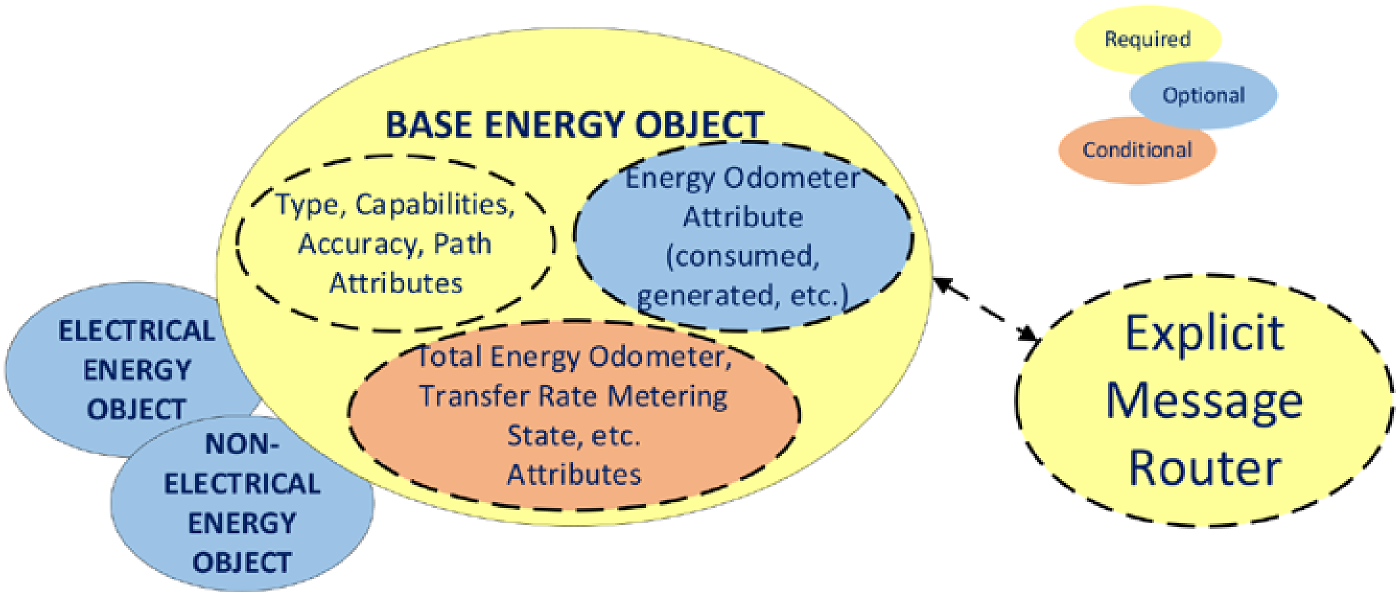
With stronger industry concerns over cost savings in production, energy usage is one of the largest costs and a big concern. It is time to rediscover and modernize the CIP Energy Objects.

This article will discuss the strengths and weaknesses of the current CIP Energy Objects and suggest ways to modernize them, which could include working closely with the OPC Foundation, for today's industrial operations.

Overview of CIP Energy objects

Energy is an indispensable component of industrial production but has been ineffectively managed as a production resource. Acquiring energy information detailed enough for action has been difficult and costly.

Automation to control energy usage and related costs has likewise been costly, characterized by one-of- a-kind designs, hours of custom engineering effort and difficulty in cost justification. ODVA's Optimization of Energy Usage (OEU™) comprises a three-tiered


Required
Optional
Conditional
BASE ENERGY OBJECT
Type, Capabilities, Accuracy, Path Attributes
Energy Odometer Attribute (consumed, generated, etc.)
Total Energy Odometer, Transfer Rate Metering State, etc. Attributes
ELECTRICAL ENERGY OBJECT
NON-ELECTRICAL ENERGY OBJECT
Explicit Message Router

SOURCE: ODVA

Figure 1: Relationship between the Base Energy Object and the Electrical and Non-Electrical Objects.

approach to increasing the availability of less costly, more granular energy information, and standardizes approaches to the automation of power and energy management.

The three phases of OEU are:

- Awareness of energy usage,
- Consuming energy more efficiently, and
- Procuring energy at the lowest cost.

Between 2010 and 2015, the ODVA Energy Applications Special Interest Group (SIG) published specifications for a family of independent but related CIP Energy Objects to support the OEU strategy and support the addition of energy capabilities to a variety of CIP devices.

Awareness of energy usage

Three related object specifications comprise the energy awareness suite of ODVA energy capabilities.

The Base Energy Object lets devices from simple to complex report their energy usage in a standardized way, in units of kilowatt-hours (kWh). This native electrical energy unit was selected because many ODVA members are electrical device vendors. The Global Reporting Institute (GRI) specifies units of gigajoules (GJ) for energy reporting; however, values in kWh may be easily converted to values in GJ by multiplying by 0.0036. This object also reports accuracy and information on how the data is generated. The Base Energy Object can also be used to report the aggregated usage of a collection of devices, and can act as a proxy, reporting energy usage for devices that cannot do so themselves, or can but are not CIP devices.

The Electrical Energy Object reports a variety of electrical measurements, including voltages, currents, complex power and energy, power factor, frequency, etc., similar to the types of parameters you would find in a high-end meter or power monitor.

The Non-Electrical Energy Object reports usage of energy resources such as natural gas, steam, fuel oil, hot water and chilled water, each in their native energy units (for example, therms, pounds, gallons, Btus, joules, etc.).

Some devices may report very accurate energy data, but high accuracy is not really needed at the device level. There will usually be revenue-accurate meters upstream in the energy distribution network. The energy awareness objects are intended to cost-effectively fill in missing pieces of the energy usage picture where today little or no information exists. This more complete energy picture provides valuable information on the energy behavior of a machine, zone, line, or area, allowing users to make decisions that result in reduced energy usage and cost.

One or more Electrical Energy or Non-Electrical Energy Object instances are associated with an instance of the Base Energy Object. A Base Energy Object instance can report the aggregated usage of a collection of similar Non-Electrical Energy Object instances (“similar” means the instances report usage of the same energy resource in the same units) and/or Electrical Energy instances. It then reports the aggregated usage in kWh in its own instance attributes, and in the native non-electrical energy units in an associated instance of the Non-Electrical Energy Object.

That way, the user can get a single view of all of the energy being used in multiple devices and subsystems in the base units (kWh) while also being able to monitor the non-electrical loads in the units that make sense for those types of devices and subsystems.

Together, this collection of energy objects provides a standardized way to obtain detailed energy usage information in an industrial setting at very low cost. This can help users apply a more direct relationship between products and the energy utilized to manufacture them.

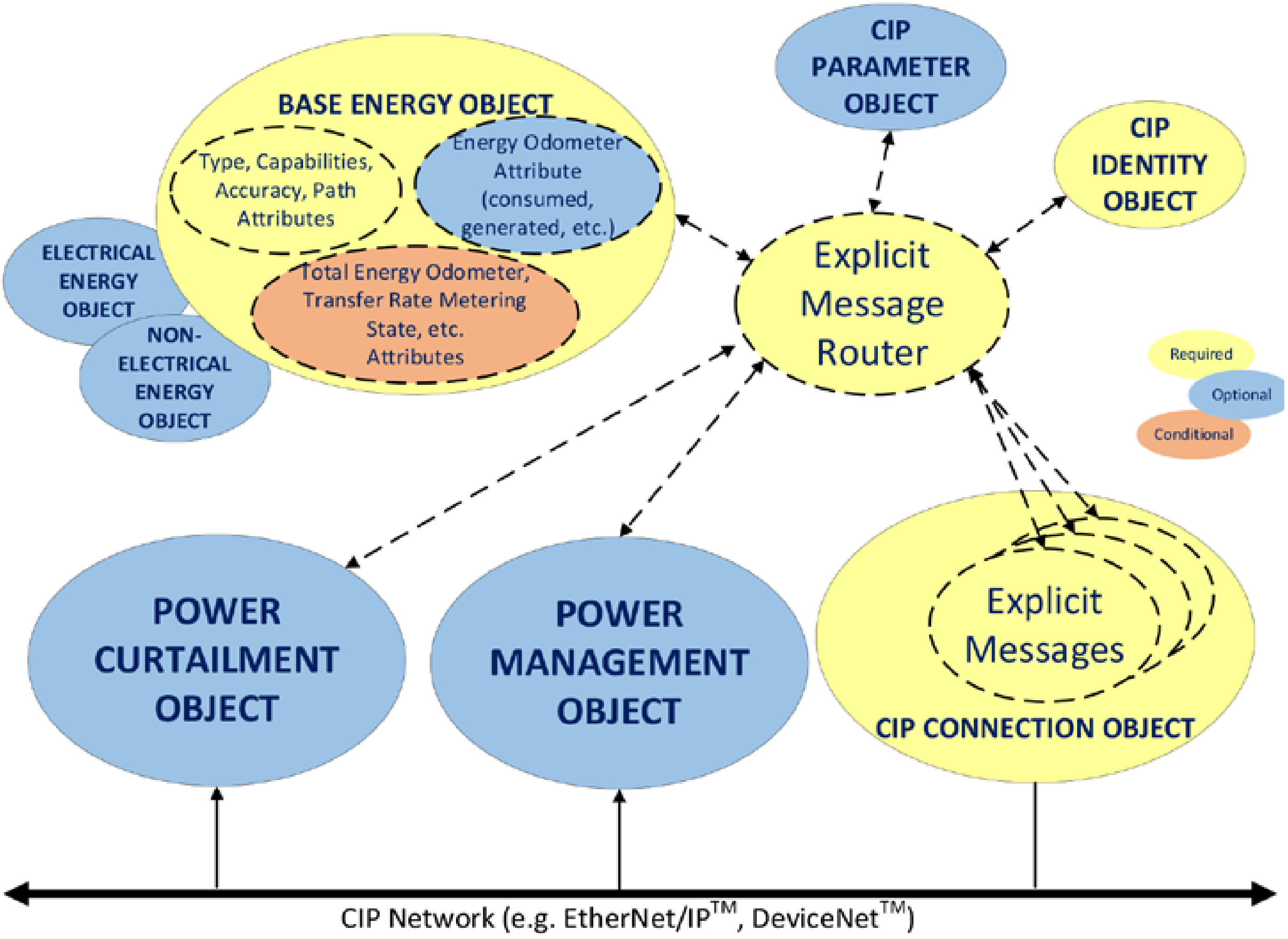
Consuming energy more efficiently

The Power Management Object provides a simple, standardized interface for commanding devices, machines, work cells, and production lines into low-power modes at lunch time, shift changes, weekends, when a bottleneck or breakdown occurs, or during other significant idle periods.

A controller or software application requests a pause expected to last for a specified time. In response, the device reduces the power it uses by going to a predefined pause mode, and letting the application know how much notice to give so the device will be ready when needed. Based on the requested pause time, a device selects a pause mode that saves the most energy possible for the duration and condition of the device. The lowest power level is the “sleeping” mode, where it effectively shuts down except for just enough communications hardware capability to listen for a wake-up call.

Where the Power Management Object saves energy during idle periods, the Power Curtailment Object helps to save energy and avoid demand peaks while production continues at a lower rate of energy consumption. The Power Curtailment Object uses predefined curtailment levels to reduce power.

Curtailment levels are similar in function to pause modes, except the energy managing application requests a desired power level instead of the duration of a pause.


BASE ENERGY OBJECT
Type, Capabilities, Accuracy, Path Attributes
Energy Odometer Attribute (consumed, generated, etc.)
Total Energy Odometer, Transfer Rate Metering State, etc. Attributes
ELECTRICAL ENERGY OBJECT
NON-ELECTRICAL ENERGY OBJECT
CIP PARAMETER OBJECT
CIP IDENTITY OBJECT
Explicit Message Router
Required
Optional
Conditional
POWER CURTAILMENT OBJECT
POWER MANAGEMENT OBJECT
Explicit Messages
CIP CONNECTION OBJECT
CIP Network (e.g. EtherNet/IP™, DeviceNet™)

SOURCE: ODVA

Figure 2: Relationship between the Power Objects and the Energy Objects.

Both the Power Management and Power Curtailment objects act as servers to an energy management client application. The client, which may in turn be a server itself to another higher-level energy management client application, needs to maintain awareness of the big-picture operational environment to manage the energy behavior of its owned devices using services defined in the object specifications.

CIP Network (e.g. EtherNet/IPTM, DeviceNetTM)

Both the Power Management and Power Curtailment objects provide a cascade capability, allowing child objects to be controlled by the parent, simplifying the interface to a controlling energy client.

Improvements for better energy management

Changes are needed in the CIP Energy™ Objects for better utilization and execution in products and systems. Some of the proposed changes are simple and quick to implement. The majority of the changes will require more work and possibly some form of prototyping before release.

The easiest and simplest changes to consider are to align the naming convention of the various objects. The Base, Electrical, and Non-Electrical Energy Objects all use “Energy” in the title and descriptions, while the Power Management Object and the Power Curtailment Object use “Power” in their titles and descriptions. To maintain consistent naming and to prevent confusion for the users and developers, the Power Management Object could be renamed the Energy Management Object and the Power Curtailment Object could be renamed the Energy Curtailment Object. A question may be raised if the power objects manage power or energy. Power is amount of work done over a time period (P=W/t).

Where, energy is power multiplied by time (E=Pt). It can be argued that the objects manage both power and energy, so energy in the titles would be fitting.

The CIP Energy objects defined an Odometer data type for tracking energy data. This data type consists of multiple elements, each with a range from 0 to 999. While this data type makes sense for visual display purposes, it is an inefficient data type for internally managing energy data. A 64-bit signed or unsigned integer would be a better choice. Additionally, the rollover behavior of the signed odometer data type does not follow typical rollover behavior of native signed integer types, returning to zero instead of the max positive or negative number.

During the development of the Power Curtailment object, several similar services or properties defined in the Power Management object were enhanced or revised. As a result, the ODVA Energy Applications SIG drafted a Specification Enhancement (CIPSE) CIPSE 0243 008 that was started in May 2014. This CIPSE went through an initial review from several SIG members but was never completed. This CIPSE update was a major rewrite of the Power Management Object.

One of the most powerful features of the Power Management and Power Curtailment objects is the ability to establish parent-child relationships (cascade). This provides the capability for a single parent object, located in, for example, a line controller, to manage or curtail energy in the remaining devices in a system or machine, effectively giving an energy management system a single point of access to the system or machine. This cascading feature was significantly revised during the development of the Power Curtailment object and this enhancement is reflected in in CIPSE 0243 008.

The released energy objects have a reduced set of features. When compared to vendors that have very feature rich metering products, there is functionality in meters that cannot be managed or measured in the current energy objects.

Additional use cases for energy

The working hypothesis for Optimization of Energy Usage Use Cases is as follows:

1. Energy is essential to produce products but has been an invisible line item on production bills of materials and consequently an unmanaged resource;
2. Energy should be a managed resource in the production domain, and;
3. The availability of energy information and visibility of energy consumption will promote awareness by industrial consumers of the need to manage energy as a production resource which, in turn, will lead to best practices in OEU for the industrial consumer.

The additional elements of Optimization of Energy Usage that will be addressed in ongoing work within ODVA are transacting energy for the best results. By leveraging asset management and internal facility and process energy delivery systems, the industrial consumer can interface with the Power Grid domain to procure and exchange energy for the best result. By dynamically and transparently managing demand-response mechanisms, industrial consumers will be able to transact energy to achieve individualized best results based on cost, source, supply, or environmental impact.

Working with OPC Foundation

The Power Consumption Management Group was announced at the Hannover Fair on the 30th of May 2022. This group is a partnership between ODVA, OPC Foundation, Profibus & Profinet International (PI), and Verband Deutscher Maschinen und Anlagenbau (VDMA).

The intention of the group is “to harmonize and standardize energy consumption information on the shop floor” as quoted from the ODVA webpage. Al Beydoun, President, and Executive Director of ODVA, states “This Power Consumption Management collaboration will help ensure end users have a highly standardized and interoperable means to reach their environmental, social, and corporate governance (ESG) goals.”. Further, this group is backed by the European Union’s goal to make Europe climate-neutral by 2050 under the “European Green Deal”.

As a result of the partnership, a new specification in the OPC United Architecture (OPC UA) will be written and published.

It will be important that CIP Energy™ and the associated power and energy objects are updated to align with power consumption management OPC UA specification. Since the intended goal of OPC Foundation and ODVA, under the Power Consumption Management Group is ensure standardization of energy information, then updates to the power/energy objects mentioned in this paper must be a priority for ODVA and its member companies.

Market and customer readiness

It is time to restart the Optimization of Energy Usage and the ODVA Energy Applications SIG. There is a strong concern over energy usage throughout sectors of automation, including industrial automation businesses. The best way to address this concern is through better energy management systems.

The market is ready. Market.us estimates the current value of the Global Energy Management System market at 55.2 billion dollars. Further, they estimate that this market will grow to 208.4 billion dollars by 2032. The Compound Average Growth Rate (CAGR) over this period would be 14.6%. There is a strong market pull for OEU™.

The customer wants better energy management systems, as evidenced by the predicted market growth. However, the customer must have certain needs satisfied in order to adopt the systems. The energy management systems must be easy to install and have ease of use. The customer wants the cost of implementation to be as low as possible. A multiple vendor solution is needed so the customer is not locked to a single vendor and can install best-in-class devices throughout the system. When the customer looks at the cost of energy today, the customer sees a higher return on investment (ROI) with the application of energy management systems. Since the CIP Energy™ Initiative through the ODVA Energy Applications SIG can provide the required solution and answers the customer needs, it is time to restart both.

There is governmental and societal pressure on our customers to reduce energy usage. Many country and local governments have policies and programs to reduce GreenHouse Gases (GHG) and companies’ carbon footprints. The World Economic Forum states “With industry responsible for 30% of global CO2 emissions, industrial clusters will be a critical player in accelerating the path towards net zero”. The ideal goal is net-zero carbon emissions. All levels of society and governments are calling for a solution. We can provide that solution, together.

Evolving energy management work

There are many reasons to update or evolve the CIP Energy Initiative. But to do so, the ODVA Energy Applications SIG would need to be restarted. The SIG will need to be actively supported in ODVA by the member companies. It cannot be a one or two company effort. There is plenty of work for the CIP Energy SIG to enhance the current object specifications. The changes made to cascading for the Power Curtailment Object will need to be reflected in Power Management Object.

The ODVA Energy Applications SIG identified additional material that needed to be included in the CIP Energy Objects. However, the SIG went into hibernation before completing this work. To incorporate the enhancements, the uncompleted work, and to collaborate with the OPC Foundation energy partnership, the member companies of ODVA need to drive this activity. The timing could not be better to focus on the Optimization of Energy Usage for all ODVA members. If the CIP Energy Initiative is going to be promoted by ODVA, the initial plan needs to be completed.

Conclusion

There is a growing movement of energy awareness in all industries. There is a strong marketing push for better optimization of energy usage in industrial automation. ODVA was ahead of its time when it introduced the CIP Energy Initiative. However, the CIP Energy Initiative has fallen behind other energy management activities.

The implementation of the CIP Energy^TM Objects in ODVA vendor products has been limited. However, the market needs to see valid and complete energy management solutions for implementation. The current CIP Energy Initiative is not complete. The ODVA Energy Objects need to be enhanced to reestablish their state-of-the-art behavior.

The mix of naming conventions for the energy and power objects can be confusing to the users of the objects. Consistent use of “Energy” in these objects would unify the message and usage of the objects. We would have five energy objects: Base Energy Object, Electrical Energy Object, Non-Electrical Energy Object, Energy Curtailment Object, and the Energy Management Object. These would be the basis for the ODVA CIP Energy Initiative.

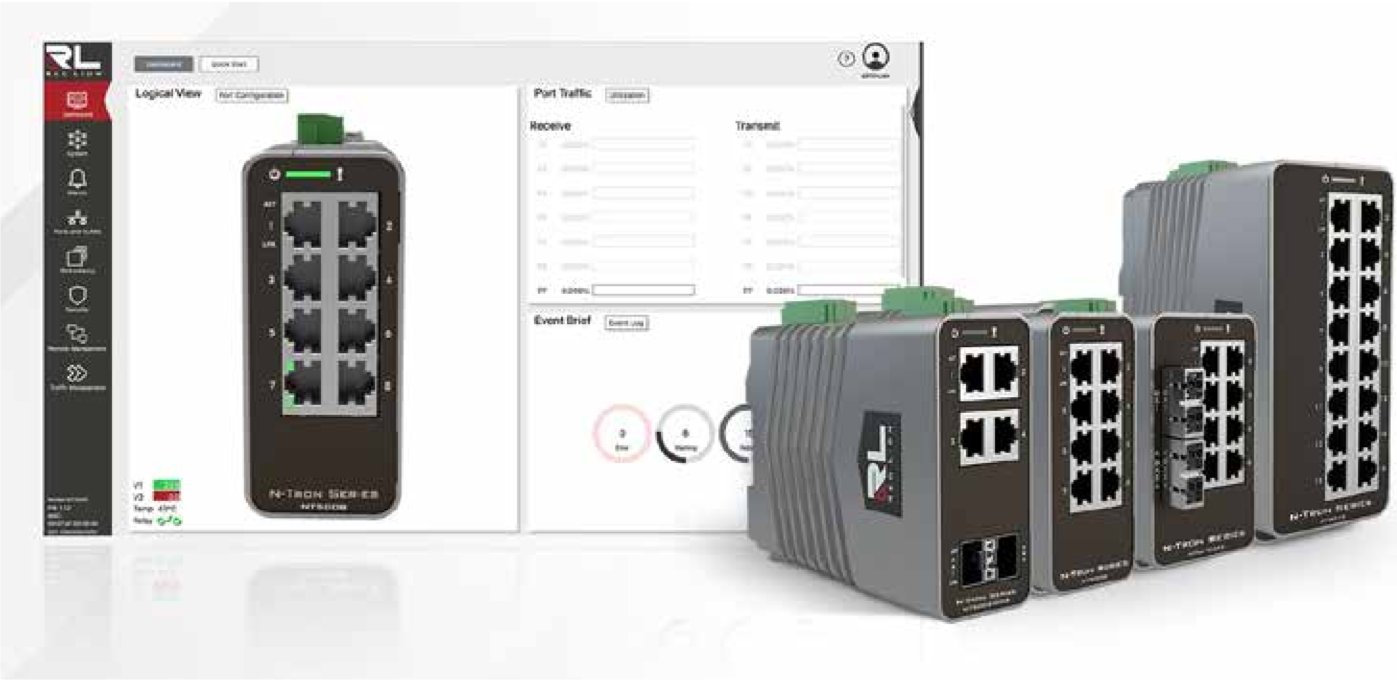
All of the ODVA Energy Objects will need to be updated to reflect the information in the power consumption management OPC UA specification as drafted by the Power Consumption Management Group. There is plenty of work needed to update and complete the ODVA CIP Energy Initiative plan. The time is right to re-energize this effort. It will take a multi-membership effort to make the ODVA CIP Energy Initiative relevant in the market and useful to our customers.

Rick Blair, Senior Principal Network Architect; and Todd Andrew Snide, Consulting Engineer, ***Schneider Electric.***

Learn More

Gigabit Ethernet switch series

N-Ring™ Manager adds reliability to switches by offering fast ring healing times of ~30ms to prevent disruptions.



SOURCE: RED LION

Red Lion has announced feature enhancements to its N-Tron Series NT5000 Gigabit Managed Layer 2 Ethernet switches.

The N-Tron Series NT5000 Gigabit Ethernet Switch Series from Red Lion, with N-Ring™ technology and DHCP Server, provides high-speed redundancy and increased usability to the company's Industrial Ethernet switch series.

As industries modernize their facilities and digitally transform operations to leverage the power of industrial data, switch performance and speed are essential, along with the simplicity of configuration and management. Red Lion’s proprietary N-Tron® Series N-Ring™ Manager adds reliability to these standout switches, with fast ring healing times of ~30ms to prevent disruptions.

Robust ring management and diagnostic tools provide notification of a break as well as a detailed fault map. The new firmware also includes a DHCP Server for automatic IP address assignments. Support for DHCP Server option 61 and Relay agent with option 82 further simplifies the process of assigning IP addresses when field devices are moved or added to the network.

Red Lion gigabit managed switches are designed for ease of use, security and reliability. Innovative features make installation and setup easy via a configuration wizard, while an industry-ready, rugged design ensures smooth operation in harsh environments.

And with authenticated access and VLANS, you can be sure that it’s only your team accessing your devices. Our industrial networking portfolio is one of the most robust in the market, so infrastructure is available when customers need it.

Connectivity, reliability and security

Clear, comprehensive and fast network management is essential for organizations to achieve maximum uptime. The NT5000’s simple graphical user interface includes a logical view showing active ports, power supply, temperature and contact relay status of the switch and color-coded gauges for port traffic and events to allow administrators to quickly identify and address possible network disruptions in real-time, helping lower total cost of ownership. The NT5000 gigabit switches are available in 6, 8, 10, 16 and 18 port configurations in all copper or a mix of copper and fiber options that can meet specific installation requirements.

Key Features

- Password encryption
- MAC security
- Configurable password length and multi-level user access
- Automatically disable user or port credentials after failed attempts
- IEEE 802.1X with RADIUS remote server authentication
- VLANs
- N-Ring™ technology with ~30ms healing
- Port mirroring

Red Lion

Visit Website

HMS Networks acquires Red Lion Controls

HMS Networks, a global provider of industrial information and communication technology, has entered into a binding agreement with Spectris Group Holdings Limited to acquire the Red Lion Controls business, a well-established US-based provider of industrial automation solutions, through the acquisition of 100 percent of the shares in Red Lion Controls Inc. and Red Lion Europe GmbH as well as certain assets in other jurisdictions, significantly expanding HMS´ presence in the North American market and complementing HMS´ offering.

Red Lion is a well-established US-based provider of industrial automation solutions with an innovative product portfolio with premium brands. The acquisition will significantly strengthen HMS´ presence in North America and enable cross-selling of both HMS´ and Red Lion´s products through their respective market channels.

OPC UA Pub/Sub via MQTT

An OPC UA SDK from Softing offers OPC UA Pub/Sub via MQTT for targeted, resource-saving data transmission.

SOURCE: SOFTING

The OPC UA C++ SDK is available for Windows, Linux, and VxWorks.

The OPC UA C++ SDK from Softing Industrial has received a major update and now supports OPC UA Pub/Sub via MQTT.

Softing Industrial has expanded the functionalities of its OPC UA C++ SDK (Software Development Kit) with the new version 6.30. Data transmission using OPC UA Pub/Sub (Publisher/Subscriber) via MQTT (Message Queuing Telemetry Transport) is now possible in addition to the previously available UDAP protocol (Universal Data Augmenting Processor). The new implementation supports both the widely used MQTT version 3.x and the new version 5.0. Data security is guaranteed by encrypting the communication using SSL (Secure Sockets Layer). Easy data evaluation at the application level is possible because OPC UA JSON coding (Java Script Object Notation) serves as the transmission format.

Data transmission with Pub/Sub via MQTT offers many benefits to users. These include:

Scalability: Pub/Sub via MQTT can be easily scaled to a large number of devices or subscribers without compromising performance.

Efficiency: The protocol overhead with MQTT is low, which makes data transmission efficient and resource-saving.

Reliability: MQTT provides mechanisms for Quality of Service (QoS), which make it possible to control message delivery and ensure that messages are delivered reliably depending on the requirements of the use case.

Flexibility: Thanks to the clear separation of publishers and subscribers, MQTT enables flexible and dynamic communication between different devices and applications, which is particularly suitable for distributed systems or the IoT.

The OPC UA C++ SDK is available for Windows, Linux, and VxWorks. It offers developers, system integrators, and device and control manufacturers an easy and fast way to integrate OPC UA into their automation and Industry 4.0 applications. A comprehensive collection of libraries with a concise, clearly documented programming interface as well as corresponding sample applications, and test and simulation tools are included in the software package and enable a fast time to market. All SDKs have the OPC UA Testlab certification. Users can therefore be sure that they are choosing the safest and fastest way to compliant, robust, and high-performing OPC UA products.

OPC UA SDKs offer fast and easy integration of client/server and publisher/subscriber communication. A comprehensive collection of libraries with a comfortable programming interface, sample applications and test and simulation tools enable a fast time-to-market for programs with OPC functionality.

A demo version with full functionality and a limited runtime as well as detailed release notes and technical data sheets are available for download on the Softing Industrial website using the link below.

Softing

Visit Website

Distributed edge AI platform

Platform-as-a-Service option streamlines delivery and management of Edge AI applications.

Rajant Corporation has introduced a new edge AI platform, known as the Cowbell, to provide a distributed computing hub and platform-as-a-service that streamlines and simplifies the delivery and management of AI applications at the edge.

According to Muthu Chandrasekaran, Ph.D. RHI VP of Artificial Intelligence, "There has been explosive growth in the number of connected devices in recent years, and without edge computing, the amount of data generated from these devices would severely overwhelm and adversely impact most of today's enterprise networks. Furthermore, the inflated costs and latencies introduced by the cloud render cloud-hosted AI-based low-latency decision support systems almost impossible, not to mention that the productization of AI and its maintenance is very difficult and complex. The Cowbell platform simplifies this complex problem by providing software, hardware, and networking infrastructure necessary to bring distributed cloud native computing to the edge with what we're calling MLOps-in-a-Box. By leveraging Rajant's patented InstaMesh® networking technology, the Cowbell platform facilitates a secure, fault-tolerant, highly available distributed computing cluster over mesh, the first of its kind. Scaling the cluster is automatic when additional Cowbells are added to the deployment."

Those visiting Rajant at CES will also be introduced to Q-Stat, a cutting-edge wearable device created to transform your work experience. The Q-stat's flexible design strategy allows for all types of different packaging, intended to serve various markets, from people to animals. Packed with advanced sensors, including skin temperature, 02, pulse rate and EKG, along with integrated Wi-Fi and BLE in a sleek, compact design, the Q-stat offers a seamless and enriching experience that caters to your safety and wellness needs.

Rajant Health EVP Giana Schena, Ph.D. shares, "RHI will offer demonstrations of Trovomics, a user-friendly platform designed to provide a fast, no-code solution for omics analysis, empowering researchers to easily and quickly turn their sequencing data into stunning, interactive visualizations. Trovomics has received outstanding feedback and results from academic researchers in biomedical science since its debut, and we are thrilled to bring the platform to CES to show individual users the power to investigate their own data."

Robert Schena, CEO of Rajant and RHI, states, "What we have accomplished here is an ecosystem that includes the enterprise Edge (Cowbell), personal Edge (Q-Stat), and analytics (Trovomics). This ecosystem is called Angelverse™ because we at Rajant believe that people should own and control their own data locally, choosing where, when, and who they wish to share it with. This ecosystem fully integrates Rajant's industry-leading Kinetic Mesh and the Reios IoT suite of solutions offered by Rajant Italia SRL."

SOURCE: RAJANT

By leveraging Rajant's patented InstaMesh® networking technology, the Cowbell platform facilitates a secure, fault-tolerant, highly available distributed computing cluster over mesh.

Rajant EVP of Sales and Marketing Geoff Smith adds, "The Cowbell and Q-Stat unveiled at CES will be featured as fully integrated solutions with the Rajant Kinetic Mesh family of wireless networking BreadCrumb® solutions and Kinetic Mesh-enabled Reios IoT platform, which provides comprehensive automated operational intelligence anywhere, which is fast and easy to deploy. Reios brings intelligent insights to all facets of an operation through various devices that support the platform's different applications – Smart Lighting, sTrack, IoT BMS, sDesk, and Smart Picking.

More on Cowbell

Housed in a rugged industrial-grade IP-rated enclosure, the Cowbell is a versatile platform perfect for indoor and outdoor use. It constitutes a powerful multi-core CPU and GPU with a plethora of wired (Serial, Ethernet) and wireless (Bluetooth, Wi-Fi, LoRa, Rajant Kinetic Mesh) connectivity interfaces and high-speed storage enabling ingestion, hardware-accelerated processing, and network-resilient transfer of multi-modal data from disparate sensors and peripherals. Applications deployed on the Cowbell can leverage the platform's microservices-based software architecture and foundational services to serve custom machine learning models and facilitate dynamically configurable data pipelines.

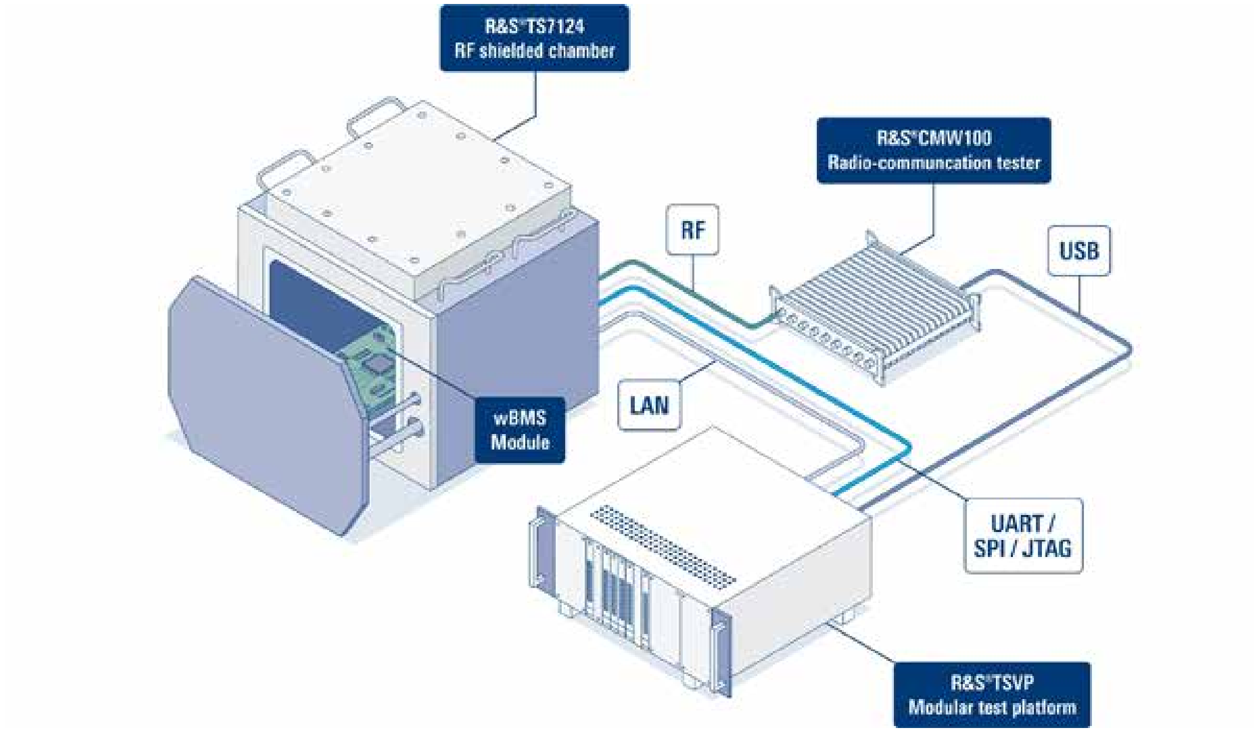
This state-of-the-art solution provides all the necessary data APIs to bring customers' own (containerized or non-containerized) applications into the platform. It automates their deployment and orchestration to ensure availability. Rajant's Kinetic Mesh ensures secure network transport and complete network isolation when needed. The Cowbell offers an integrated centralized cluster and applications management plane with a simple user interface, providing a seamless cluster provisioning, management, and application deployment experience. Secure remote access is enabled by a lightweight zero-trust VPN solution. Take advantage of the application-level logs, cluster- and node-level resource consumption metrics, and other dashboards for full observability of the health of the cluster and applications.

Rajant Corporation

Visit Website

Wireless battery management system

Rohde & Schwarz leverages technology from Analog Devices to develop a wireless battery management system production test solution tailored for verification and mass production tests of wireless device tests.



SOURCE: ROHDE & SCHWARZ

With this test setup, the necessary wBMS module calibration, receiver, transmitter and DC tests can be conducted fast and executed.

Analog Devices (ADI) and Rohde & Schwarz are helping the automotive industry to adopt wireless battery management system (wBMS) technology which brings technical, environmental, and cost advantages compared with wired battery management systems (BMS). A new automated test solution is tailored for verification and mass production tests of wireless device tests. This development builds on existing efforts for wBMS RF robustness testing.

Wireless battery management

The battery management system (BMS) is one of the most vital components of an electric vehicle (EV), ensuring safe and efficient management of the battery pack and thereby influencing the safety, range and performance of EVs.

Traditional BMSs are wired systems which limit the design flexibility and EV production scalability, as well as increase the weight of the vehicle. A more advanced approach is to perform the communication between the Cell Monitoring Controller (CMC) for each battery module and Battery Management Controller (BMC) wirelessly. This simplifies the assembly, maintenance, and exchange of cells resulting in cost and effort advantages. In addition, it saves space and provides weight reduction in the vehicle.

ADI, has developed a complete wBMS. ADI's wBMS, currently in production across multiple EV platforms, is the first ISO21434 CAL4 compliant wBMS which adheres to the strictest cybersecurity standards. It also meets high requirements in RF performance and robustness to maximize battery capacity and lifetime value.

Ultra-compact automated test system for production lines

Rohde & Schwarz, together with ADI, has developed an ultra-compact automated test equipment (ATE) system for wBMS. With this test setup, the necessary wBMS module calibration, receiver, transmitter and DC tests can be conducted fast and executed reliably for verification in the lab as well as for production tests for high yield. It consists of the R&S CMW100 radio communication tester, the R&S WMT wireless automated testing software framework, and the new R&S ExpressTSVP universal test and measurement platform. Due to radiated test, the device under test (DUT) is placed in an interference-free environment such as the R&S TS7124 RF shielded box.

Record/playback solution for RF robustness testing of wireless BMS

For RF robustness testing, they worked to get an off-the-air recording solution to capture real-world RF spectrum. They then played it back in the lab to confirm the correct operation of wBMS in demanding RF environments. This solution from Rohde & Schwarz allows a realistic, repeatable, and efficient verification of wireless devices. During several test drives in various complex RF environments, an R&S FSW signal and spectrum analyzer monitored the RF spectrum and sent it to an R&S IQW wideband I/Q data recorder. For playing back the recorded spectrum profiles in a lab, the R&S IQW is connected with an R&S SMW200A vector signal generator.

From the development lab to the production line, Rohde & Schwarz offers a comprehensive portfolio of test solutions for wBMS.

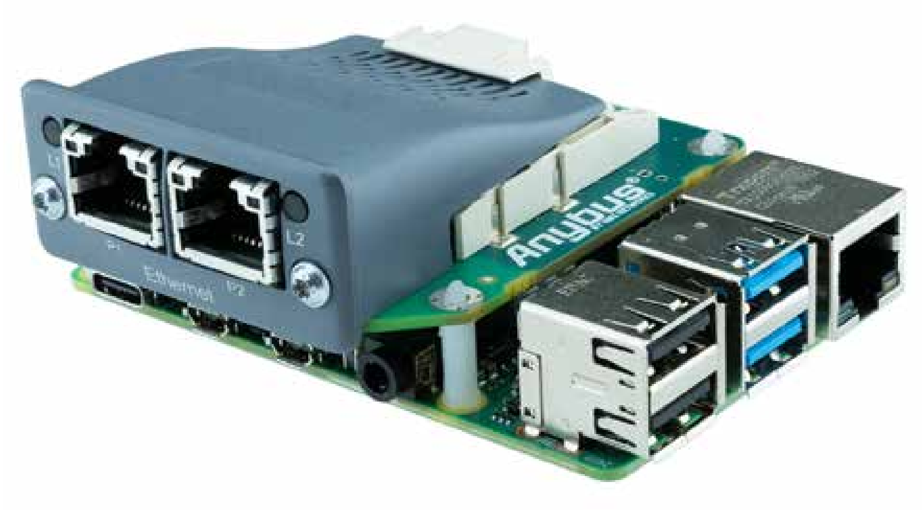
Juergen Meyer, Vice President Market Segment Automotive at Rohde & Schwarz said: "We apply our market-leading technical expertise to develop innovative solutions through the entire lifecycle from pre-development to production. We are glad that we are working with ADI to mitigate wBMS test challenges from R&D to mass production, maximize the robustness and performance of wBMS and help enable the automotive industry to fulfil the potential offered by wBMS."

Rohde & Schwarz

Visit Website

Raspberry Pi adapter

Raspberry Pi Adapter Board simplifyies the integration of the Anybus CompactCom.



SOURCE: HMS NETWORKS

HMS Networks announced that it has launched the Raspberry Pi adapter board, providing industrial device manufacturers with a simplified method to test and evaluate the Anybus CompactCom, a ready-made communication interface that connects devices to any industrial network.

While previous adapter boards were designed for testing Anybus CompactCom modules with STM32 or NXP (formerly Freescale) microcontroller platforms, this new adapter board is specifically tailored for use with the Raspberry Pi.

The adapter board provides compatibility with the widely popular Raspberry Pi. Easy installation and usage. Full compatibility with the free-to-download Anybus Host Application Example Code (HAEC).

Andreas Stillborg, Anybus Embedded Product Manager at HMS Networks, explains, "The Raspberry Pi is incredibly popular, with over 45 million units in use around the world. Many of our customers already own a Raspberry Pi and are familiar with it. Therefore, we were keen to develop an adapter board that enables our customers to easily use the Raspberry Pi to test and evaluate Anybus CompactCom."

The Raspberry Pi adapter board is fully compatible with the free-to-download Anybus Host Application Example Code (HAEC). This code includes a reference port designed for the Raspberry Pi, which customers can use with the adapter board and an Anybus CompactCom module to quickly start their embedded development project.

"We´re excited about this new adapter board, as it will allow our customers to quickly get set up and familiarize themselves with our Anybus CompactCom offering," concludes Andreas Stillborg.

HMS Networks

Visit Website

Generative AI capabilities

SambaNova Suite facilitates breakthrough Generative AI capabilities at enterprise scale.

SOURCE: ANALOG DEVICES

Analog Devices and SambaNova Systems, makers of a purpose-built, full-stack AI platform, announced ADI is deploying SambaNova Suite to spearhead its global AI transformation, making AI pervasive enterprise-wide.

As part of the initial deployment, ADI will leverage the SambaNova Suite to accelerate field sales and customer enablement across its business. ADI plans to leverage the technology to streamline access to its extensive data sheets, helping inform recommendations in the field, and deepen its customer connections.

According to the companies, SambaNova Suite is the first full stack, generative AI platform, from chip to models, for the enterprise. Delivered on-premises or in the cloud, it is a fully integrated platform offering state-of-the-art open-source models, which can be fine-tuned using customer data for greater accuracy. Customers retain model ownership in perpetuity, so they can turn generative AI into one of their most valuable assets.

"Generative AI adoption in the enterprise will be accelerated by more complete offerings that avoid costly and lengthy integration while also providing data privacy and model ownership to enable investment protection and high ROI," said R "Ray" Wang, Founder and Principal Analyst at Constellation Research. "Seeing generative AI moving beyond experimentation to enterprise use cases signals the next wave of market maturity has begun."

“The global deal being announced today is a significant technological advancement for the industry,” said Marshall Choy, Senior Vice President of Product at SambaNova Systems.

For more information on SambaNova Suite, please click on the website link below.

Analog Devices / SambaNova Systems

Learn More

High performance robot teaching box

Mitsubishi Electric´s new teaching box speeds up MELFA robot deployment.

SOURCE: MITSUBISHI ELECTRIC

Mitsubishi Electric has launched the R86TB, a new, high-performance teaching box. This is designed to help users, machine builders and system integrators setup, program, repurpose, maintain as well as troubleshoot industrial and collaborative MELFA robots. As a result, the latest solution simplifies human-machine interactions and supports the creation of highly effective automated operations.

The R86TB multifunctional operating and programming panel offers a cost-effective, even more intuitive and easy to use platform with enhanced functionalities to monitor and program both the latest MELFA robots as well as prior generations. The device facilitates the comprehensive control of the connected robot via a variety of easy-to-use screens. These can be accessed from a large, high definition 10.1" display. This means that the newly released solution can support users with limited robotics skills in the effective implementation of entry-level applications as well as help more experienced professionals streamline the creation of advanced applications.

The R86TB features 3D visualisation capabilities to help machine builders, system integrators and end users plan, set up and program robotic tasks in an environment that mimics the physical settings. This function is complemented by programming support capabilities, parameter inputting and programming interfaces, as well as a dedicated section for diagnostics. All these are based on the robot engineering software RT Toolbox3, simplifying user adoption and use of these platforms while ensuring consistency.

The R86TB high-performance teaching box also supports quick and early troubleshooting without the need for a computer. As a result, it can optimize the uptime and performance of automated applications.

Mitsubishi Electric

Visit Website

Gigabit security routers

New high-performance security routers for OT networks from Phoenix Contact.

SOURCE: PHOENIX CONTACT

The security routers of the mGuard product family from Phoenix Contact protect industrial OT networks against unauthorized access, either by people or malware. The new FL MGUARD 2105 and FL MGUARD 4305 versions with integrated switch were presented for the first time at SPS 2023.

The new Gigabit security routers make it possible to control and secure communication within a production network. Machines, systems, and plants will be protected against cyberattacks and manipulation.

The mGuard product family features a high processing speed. The devices achieve a data throughput of almost 1,000 Mbps. This means that the mGuard security routers ensure a high level of security without compromising network performance.

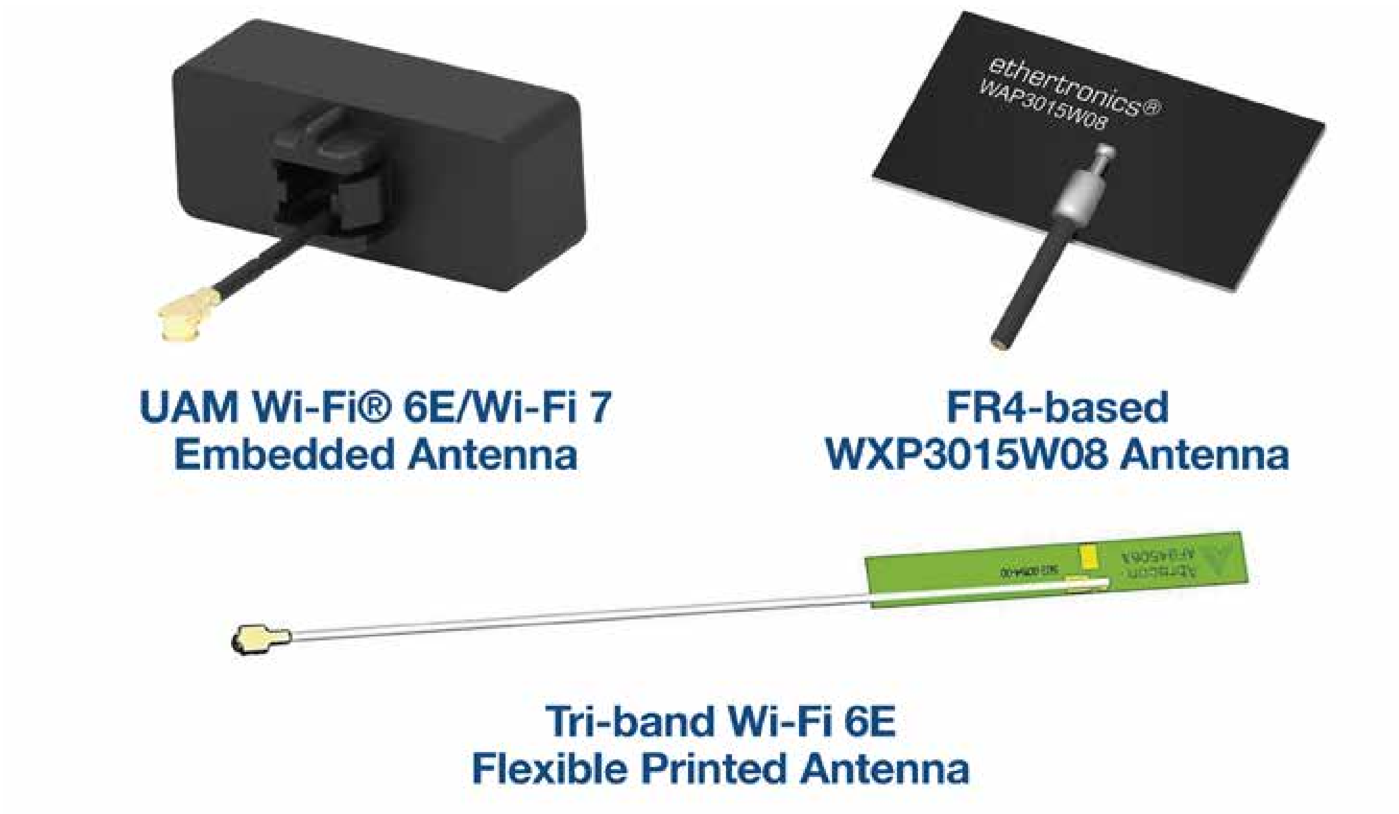
In addition to the high processing speed, the routers feature extensive security functions, including an integrated firewall that filters the data traffic in the network. Undesired communication and access attempts to the network devices are blocked. By segmenting the networks, it is also possible to check and control the exchange of data between the individual segments. This means that the individual network segments are protected against excessive data volumes, network overload, and unauthorized access. Secure remote maintenance is also possible with the mGuard security routers. Encrypted VPN communication enables machines and systems to be maintained remotely via any network. A firewall function in the VPN tunnel further increases security. The new versions are ideal for machine builders and system manufacturers, as well as system operators.

Phoenix Contact

Learn More

Wi-Fi 6E antenna solutions

Mouser Electronics expands antenna range with new embedded, flexible and external Wi-Fi 6E solutions.



SOURCE: MOUSER

The IEEE's 802.11ax wireless standard brought forth several technical initiatives aimed at advancing connectivity for the next generation of devices.

Mouser Electronics has broadened its range of antennas designed for high-speed Wi-Fi 6E communication.

The introduction of IEEE's 802.11ax wireless standard brought forth several technical initiatives aimed at advancing connectivity for the next generation of devices. One key addition was the inclusion of Wi-Fi 6E, enabling Wi-Fi communication on the 6GHz spectrum for the first time. By operating at frequencies above the existing 2.4 and 5 GHz networks, Wi-Fi 6E enables better optimisation, less interference, and lower latency. Security is also enhanced, as Wi-Fi Protected Access 3 (WPA3) certification is mandatory for all Wi-Fi 6E devices. Since its introduction in 2020, the deployment of Wi-Fi-6E has expanded to a diverse range of industrial and consumer locations, including offices, manufacturing facilities, clinical environments, and residential areas. Consequently, supporting Wi-Fi-6E has become essential for the latest high-performance wireless devices.

Mouser stocks a wide range of antenna designs needed to fulfil the diverse technical requirements of Wi-Fi 6E devices. Some of the newly added solutions include:

UAM Wi-Fi® 6E/Wi-Fi 7 Embedded Antennas from Linx Technologies / TE Connectivity offer a range of omnidirectional tri-band antennas designed for the latest Wi-Fi 6E devices. As an externally mounted solution, they can be easily attached to a metal chassis using the unique snap-in feature, removing the need for fixings, allowing for unambiguous mounting direction, and increasing assembly speed. Alongside Wi-Fi 6E functionality, they allow for wireless Bluetooth® and ZigBee communication, as well as supporting future Wi-Fi 7 networks. The RoHS-compliant range includes multiple cable lengths, with MHF4l and MHF termination available, and is suitable for a wide range of indoor applications.

Tri-band Wi-Fi 6E Flexible Printed Antennas from Abracon provides high-performance communications in low-profile and easy to integrate packaging. The omnidirectional tri-band operation provides high performance across 2400MHz to 7125MHz frequencies, covering vital 2.4 GHz, 5 GHz, and 6 GHz bands. The antenna helps to enhance the range of Wi-Fi signals, providing dependable and high-speed connectivity in congested public spaces and complex industrial settings. In conjunction with Wi-Fi 4/5,6/6E and 7 connectivity, it is also ideal for devices using Bluetooth, ZigBee, Thread, and Matter protocols. System assembly is incredibly simple, with the flexible design allowing for quick adhesive mounting even along contours. The antenna is suitable for a variety of routers and network devices, as well as home automation and IoT sensors.

Kyocera AVX's range of antennas includes solutions designed to suit a variety of Wi-Fi-connected applications. The FR4-based WXP3015W08 antenna features an embedded Wi-Fi dipole design and delivers high-performance connectivity and signal sensitivity in miniaturised packaging. It consumes minimal space and can easily be mounted through simple adhesion. For Wi-Fi 6E connections, it features a peak gain of 5.90dBi and an average efficiency of 60%, ensuring a strong connection. It is also suitable for previous iterations of Wi-Fi, as well as Bluetooth, BLE, and ZIGBEE protocols. Kyocera's RoHS-compliant AVX range also includes stamped metal and flexible printed circuit Wi-Fi 6E antennas, which use its patented isolated magnetic dipole (IMD) technology, as well as several cable lengths and termination options.

Mouser

Visit Website

Industrial Ethernet Book

The only publication worldwide dedicated to
Industrial Ethernet 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