2.2020 Issue 116
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Networking and IoT

Enabling IIoT connectivity for virtual power plants 10

SIEMENS
Ingenuity for life

Nobody knows you better

RUGGEDCOM cybersecurity solutions

We build your systems. Whether you're in the electric power, transportation, or other industry in a harsh environment, our unique expertise in industrial networks means that we get it. We know what you need when it comes to cybersecurity – inside and out.

siemens.com/ruggedcom/cybersecurity

DIPA-A10073-00-7600

Cybersecurity Focus

No topic has attracted more continuous attention in the last ten years than network security. The goal for all companies has been to deploy defensive strategies that in their totality combine people, processes, and technology all working together to support OT network security.

Attacks against safety and critical systems are still a growing concern and solutions to secure these systems are becoming even more critical. Ensuring the safety and availability of these networks are paramount in protecting our modern way of life.

In this issue of IEB, we look in detail at the importance of cybersecurity measures and how companies can work to effectively protect their networks. Here are some of the highlights.

In "Securing OT networks with Unidirectional Gateways and Data Diodes" (beginning on page 34), Daniel Paillet from Schneider Electric discussed how data diodes provide a hardware-enforced solution to defend OT networks and safety systems.

His argument is that data diodes can present a level of network complexity despite being a simple concept to understand. Data diodes provide defense against malevolent agents, negligent users, malware, and viruses. Before installing a data diode, a concise strategy must be incorporated. The objective can be to protect either an entire OT network or a specific safety system, for example, requiring information to be sent out to the IT network for reporting or analysis.

In "Cybersecurity Challenges in Discrete Manufacturing" (page 22), Gary DiFazio, Director of Marketing, Industrial Cybersecurity, Belden Corporation concludes that "the time to implement visibility, protective controls and continuous monitoring is now—every minute that you don't is a minute that leaves your network vulnerable to a host of costly threats."

DiFazio notes that production is the lifeblood of every discrete manufacturing business. Advances in operational technologies and factory floor networking are giving OT professionals powerful tools to boost yields and reduce waste, but such tools cannot in good stewardship be implemented without an understanding of the resulting cybersecurity risk they open up.

He concludes that fortunately, with heightened awareness and subsequent action, cybersecurity and automation control professionals in discrete manufacturing can work to optimize profitability with the most sophisticated automation solutions driven by the advent of the IIoT, while also maintaining optimum, best-in-class cybersecurity levels on the plant floor.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2020**
Deadline for editorial: February 14, 2020 **Deadline for artwork:** March 6, 2020

Product & Sources Listing

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

Update your own products

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

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

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

First standalone 5G network in industrial environment

Installation in Automotive Showroom and Test Center enables testing in standalone 5G network under actual operating conditions, and coming up with solutions for industrial applications in the future.

SIEMENS AND QUALCOMM HAVE IMPLEMENTED the first private 5G standalone (SA) network in a real industrial environment using the 3.7-3.8GHz band. Siemens is providing the actual industrial test conditions and end devices such as Simatic control systems and IO devices and Qualcomm Technologies is supplying the 5G test network and the relevant test equipment.

The 5G network was installed in Siemens' Automotive Showroom and Test Center in Nuremberg. Automated guided vehicles displayed are primarily used in the automotive industry. New manufacturing options and methods are also developed, tested and presented before they are put into action on customer sites. This allows customers, such as automated guided vehicle manufacturers, to see the products interact live.

The Automotive Showroom and Test Center enables Siemens and Qualcomm Technologies to test all the different technologies in a standalone 5G network under actual operating conditions and to come up with solutions for the industrial applications of the future. Siemens provided the actual industrial setup including Simatic control systems and IO devices.

"Industrial 5G is the gateway to an all-encompassing, wireless network for production, maintenance, and logistics. High data rates, ultra-reliable transmission, and extremely low latencies will allow significant increases in efficiency and flexibility in industrial added value," says Eckard Eberle, CEO Process Automation at Siemens. "We are therefore extremely pleased to have this collaboration with Qualcomm Technologies so that we can drive forward the development and technical implementation of private 5G networks in the industrial sector. Our decades of experience in industrial communication and our industry expertise combined with Qualcomm Technologies' know-how are paving the way for wireless networks in the factory of the future."

SOURCE: SIEMENS

Siemens is providing actual industrial test conditions and end devices such as Simatic control systems and IO.

"This project will provide invaluable real-world learnings that both companies can apply to future deployments and marks an important key milestone as 5G moves into industrial automation," said Enrico Salvatori, Senior Vice President & President, Qualcomm Europe Inc. "Combining our 5G connectivity capabilities with Siemens' deep industry know-how will help us deploy technologies, refine solutions, and work to make the smart industrial future a reality."

The German Federal Network Agency has reserved a total bandwidth of 100 MHz from 3.7 GHz to 3.8 GHz for use on local industrial sites. German companies are thus able to rent part of this bandwidth on an annual basis and to make exclusive use of it on their own operating sites in a private 5G network whilst also providing optimum data protection. Siemens is using this principle to evaluate and test industrial protocols such as OPC UA and Profinet in its Automotive Showroom and Test Center together with wireless communication via 5G. This allows solutions to be tested and developed which industry will be able to use with the up-and-coming Release 16 of the 5G standard.

*News from **Siemens and Qualcomm.***

5G on factory floor needs more than telco approach

5G WILL DRAMATICALLY GAIN IMPORTANCE in providing wireless connectivity to industrial environments, especially in the context of Industry 4.0 and the automation of production processes and monitoring of machine conditions. According to ABI Research,by 2026, there will be 5.3 million 5G connections on the factory floor which will generate a revenue of more than US$184 million (with a CAGR of 623% between 2021 and 2026).

"As a technology, 5G will be a fit to provide wireless connectivity on the factory floor, since it enables, for example, establishing a massive wireless sensor network or implementing Virtual Reality (VR) and Augmented Reality (AR) applications for predictive maintenance and product monitoring. Therefore, 5G offers immense operational benefits and productivity enhancements to the implementing manufacturer," says Leo Gergs, Research Analyst at ABI Research. "Furthermore, the technology opens up new production opportunities by enabling artificial intelligence applications to be integrated into manufacturing processes."

Early 5G trial deployment at companies such as Schneider Electric in France and Germany's Osram, and Mercedes hint that bringing 5G connectivity to the factory floor will decrease maintenance costs by 30% and increase overall equipment efficiency by 7%.

While there are many use cases and areas of application for 5G in industrial manufacturing, targeting the enterprise vertical will fundamentally change the value chain associated with 5G. A much closer collaboration between network operators, infrastructure vendors, and manufacturers will be required.

Targeting enterprise verticals, however, is vitally important for Communication Service Providers (CSPs) and the successful deployment of 5G.

*News from **ABI Research.***

[EK1-15E]

Highend measurement technology

Extremely accurate, fast and robust

24 bit
10 kSps per channel
simultaneous
25 approx. 100 ppm @ 23 °C

www.beckhoff.com/measurement-technology

With ELM series EtherCAT measurement I/O modules, high-precision, fast and robust measurement technology becomes a system-integrated function of PC-based control from Beckhoff. The ELM modules can be integrated directly into the modular EtherCAT I/O system, enabling combination with the comprehensive portfolio of more than 500 EtherCAT Terminals.

- fast: sampling rates of 50,000 samples/s
- precise timing: exact synchronisation < 1 µs
- precise values: measurement accuracy of 100 ppm
- proactive: integrated functional diagnostics for individual modules
- flexible connector front-end: LEMO, BNC, Push-in
- input circuitry: voltage 20 mV…60 V, current 20 mA, IEPE, SG, RTD/TC

A seamless measurement chain from data acquisition to analysis in the cloud.

New Automation Technology **BECKHOFF**

Joint update on an Advanced Physical Layer

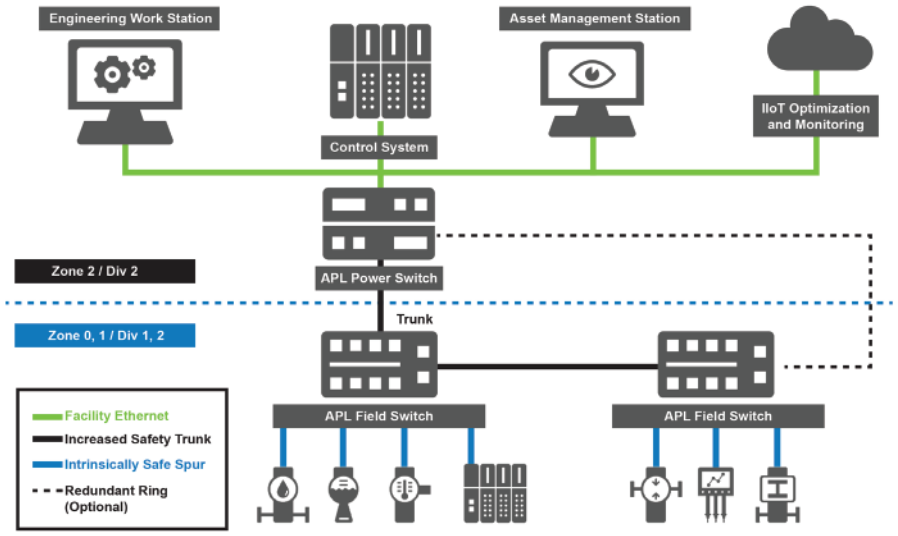
Base standards approved as Emerson Joins APL Project group promoting developments for Industrial Ethernet to expand use of EtherNet/IP, HART-IP and PROFINET into hazardous locations in process industry.

FIELDCOMM GROUP, ODVA AND PI (Profibus & Profinet International) have announced that Emerson has joined the APL Project as an industry partner. Emerson joins 11 other industry partners to support the Project's goal of developing an advanced physical layer for Industrial Ethernet, suitable for use in demanding applications in process instrumentation, named "Ethernet-APL". In addition to the industry partners, APL Project members include three standards development organizations Profibus & Profinet International (PI), FieldComm Group and ODVA.

Significant updates in the development of "Ethernet-APL" have been achieved recently. First, the IEEE Std 802.3-2019 (10BASE-T1L) standard, which is the basis for Ethernet-APL and defines 10Mbit/s over one single twisted pair Ethernet with optional power delivery, was approved as an IEEE standard in November 2019 with publication of the standard expected in the coming months. This enhancement to the IEEE 802.3 standard for long-reach, single pair Ethernet will be the basis for the integration into the Ethernet protocol specifications, which is anticipated to be completed within organizations PI, FCG and ODVA in 2020.

Also, to ensure that Ethernet-APL supports intrinsic safety in hazardous areas, the IEC PT60079-47 technical committee is working on a technical specification for the 2-Wire Intrinsically Safe Ethernet (2-WISE). The technical committee agreed during the TC31 meetings in Nanyang (CN) that the principles defined in the Fieldbus Intrinsically Safe Concept are also suitable for the 2-WISE technical specification, including adaptations for the new physical layer. The perception is supported by successful tests executed at DEKRA Testing and Certification GmbH. The final technical specification (IEC TS 60079-47) is expected by the end of 2020.

Finally, Ethernet-APL technology has been tested successfully at BASF, incorporating first prototype devices from different industry partners. The following topics were in the focus: integration and configuration of the field devices, installation and commissioning of an Ethernet-APL network, mixed/multi-protocol operation, redundancy, device exchange and export of device diagnostic and configuration data in parallel to cyclic data exchange. All tests concluded successfully and demonstrated the advantages of Ethernet-APL as a physical layer in the field of process automation and an enabling technology for higher-level applications.



SOURCE: ODVA

APL is a ruggedized, two-wire, loop-powered Ethernet physical layer that uses 10BASE-T1L plus extensions.

*News by **FieldComm Group, ODVA and PI**.*

EtherNet/IP adaptation for process adds diagnostics

Enhancements to the EtherNet/IP specification which outline integration of NAMUR NE 107 diagnostics for process automation into CIPTM architectures have been published. The addition of this capability provides industry standard diagnostic information for process users while leveraging the benefits of industrial Ethernet. "The integration of NE 107 diagnostics is another step in fulfilling ODVA's vision for the Optimization of Process Integration," said Dr. Al Beydoun, President and Executive Director at ODVA.

The process diagnostics update creates a CIP Process Device Diagnostics Object, which provides a known, public interface to a device's current diagnostics and NE 107 status according to the NAMUR recommendation NE 107 for Self-Monitoring and Diagnosis of Field Devices. The NAMUR NE 107 status signal now available with EtherNet/IP provides status information: Failure, Function Check, Out of Specification, Maintenance Required, or None. The CIP Process Device Diagnostics Object expands the amount of useful data available with EtherNet/IP by providing access to the current NE 107 diagnostics information of a field device from different vendors.

In addition to the status signal, the CIP Process Diagnostics Object maps up to 64 diagnoses from a device, such as flow, pressure or temperature status, that the user can group as desired. Vendor-specific additional diagnoses can be added as well. Applications can now efficiently poll supported EtherNet/IP field devices for changes of diagnostic status and can obtain additional diagnostics information using explicit messaging or object specific services. For example, all devices diagnosed with a certain NE 107 signal (such as Maintenance Required) can be polled by a single common service request. With EtherNet/IP, this vital diagnostic information can be easily transported where it needs to go, such as to a DCS for an operator's review and potential maintenance action or to an edge device for predictive maintenance analysis. Future efforts include profiles for field devices to simplify device integration and comprehensive device configuration methods.

*Press release by **ODVA**.*

Exceptional Performance and Reliability

NT328G LAYER 3 GIGABIT SWITCH

Designed for use in harsh industrial environments, the NT328G Layer 3 Gigabit Ethernet switch, offers 28 high-speed ports **(24-Gigabit, 4-10 Gigabit)** to meet the performance requirements of bandwidth intensive applications. Robust feature set includes wire-speed switching performance, network redundancy, advanced security, policy-based traffic control and easy-to-use configuration and management.

WWW.REDLION.NET

Designed to comply with IEC 61850-3

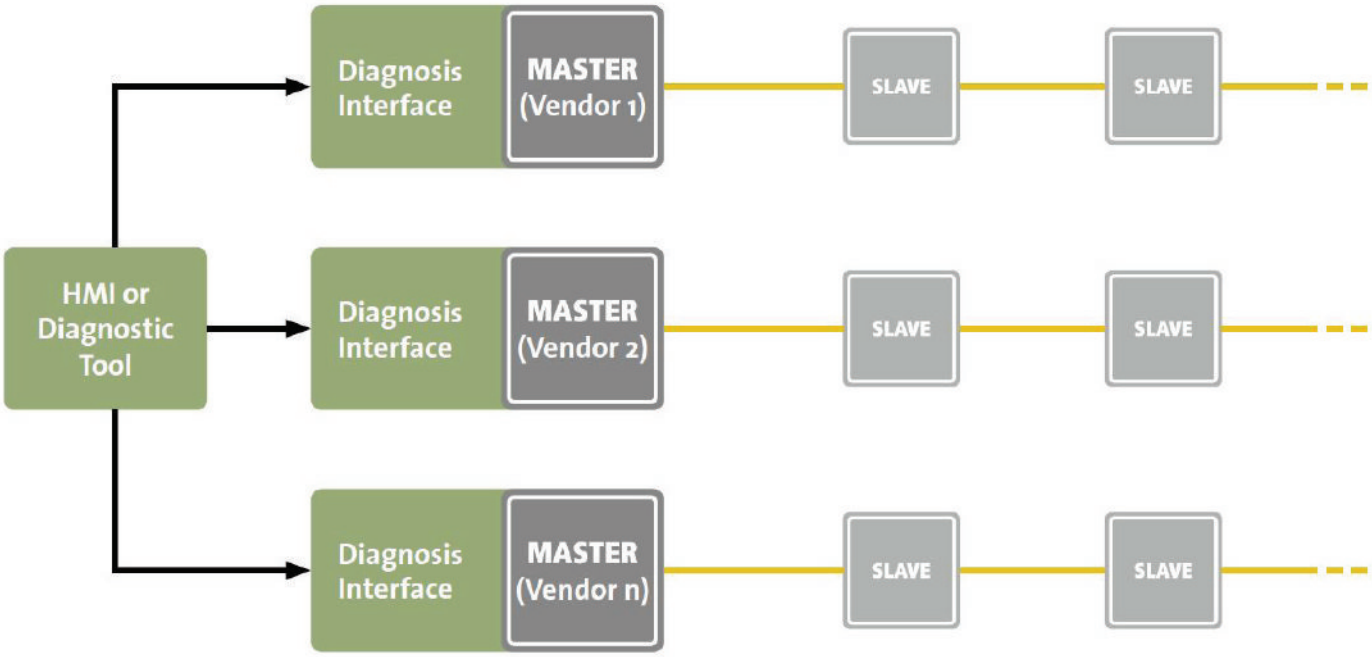
EUROPE
+31 (0) 33 4723-225 | europe@redlion.net

AMERICAS
+1 (717) 767-6511 | info@redlion.net

EXCELLENCE. REDEFINED.

Master-independent diagnostic interface for EtherCAT networks

The EtherCAT diagnosis interface provides machine and network diagnostic tools a general purpose, universal interface for EtherCAT networks. Tools can be used without the need to change specific master manufacturer or a vendor-proprietary access protocol for each different master implementation.



SOURCE: ETG

EtherCAT master independent diagnostic interface.

DIAGNOSTIC CAPABILITIES ARE KEY features in determining the success of a fieldbus technology. To further improve the diagnosis in EtherCAT networks, the EtherCAT Technology Group (ETG) has defined a vendor independent diagnostic interface with the specification ETG.1510 "Profile for Master Diagnosis Interface". This enables EtherCAT masters to provide detailed network diagnostic information and health status to third party tools in a user friendly and standard way.

Importance of availability

In modern industry machine and plants, availability represents one of the most important factors in order to guarantee efficiency and competitiveness. EtherCAT enables this by means of a well-proven technology relying on a robust communication infrastructure. Yet, industrial environments can be challenging even for reliable communication technologies like EtherCAT. Constantly moving parts or continuous vibrations could cause temporary link losses or even cable breaks in the long term, while EMC disturbances could falsify signals travelling on the communication path. In all these cases, the diagnostic capabilities of the fieldbus represent the key element in order to detect errors, determine its location and possible causes, and reduce thereby the machine downtime as much as possible.

In terms of diagnostic capabilities, EtherCAT supports outstanding features that go far beyond the corresponding capabilities of traditional Ethernet. The necessary information is either provided by the EtherCAT communication chips (ESCs) directly in hardware or by software functionalities. Therefore, no specific extensions are required on slave side.

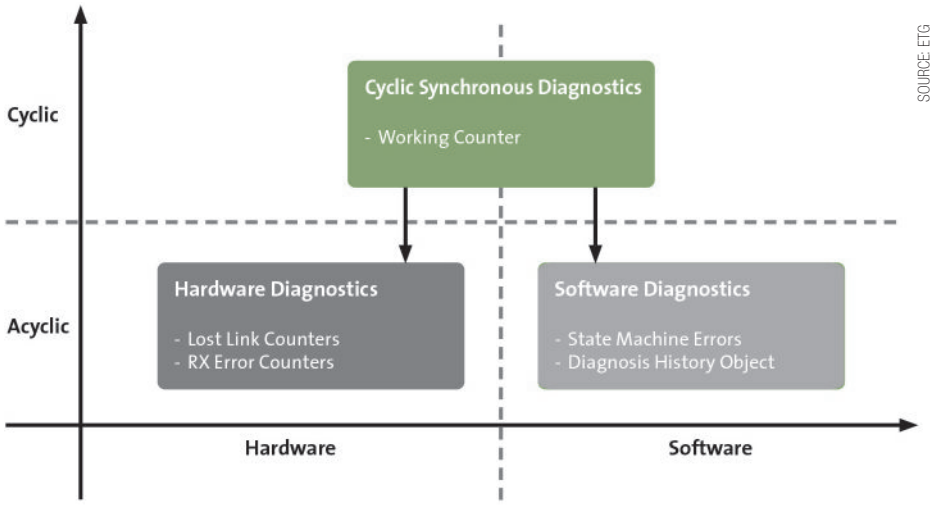
EtherCAT datagram

Each EtherCAT datagram ends with a 16-bit Working Counter field, which is expected to be incremented by all slave devices addressed by the datagram itself. A mismatch between the expected and the received value of the Working Counter means that not all slave devices successfully processed the datagram, and that they are therefore not working with consistent data in the current cycle. This can trigger an immediate error reaction on control (master) side; by default, input data carried by the datagram is discarded in this case.

Additional information can be acyclically retrieved by the master and enables to investigate the location as well as possible causes of the communication issue. At hardware level, each EtherCAT Slave Controller monitors and detects link loss as well as signal corruption on each port and increments in case the corresponding lost link counter or RX error counter, respectively.

Communication errors at software level, like the expiration of the watchdog on the cyclic data or a loss of synchronization within the network, can instead determine an unexpected state transition in the EtherCAT State Machine. They are displayed by means of the AL Status Code value, which is returned by the software stack whenever the unexpected state transition occurs.

All the necessary diagnostic information to monitor the network state as well as to detect and locate errors is therefore available to the master in all EtherCAT networks. Yet, this "raw" information needs to be provided to diagnostic tools and to end users in order to be interpreted and used. With the ETG.1510 specification "Profile for Master Diagnosis Interface", the ETG has defined a solution enabling external tools to access the diagnostic information provided by EtherCAT



SOURCE: ETG

Summary of EtherCAT diagnostic functionalities

networks in a way that is independent from the specific master vendor and software implementation.

The ETG.1510 enhances the ETG.1500 "EtherCAT Master Classes" specification. The diagnostic information is mapped into the EtherCAT Master Object Dictionary defined in the ETG.5001, which is extended for this purpose. In particular, objects in index range 0x8000 describe the network structure as expected by the master based on the "offline" configuration, while objects 0x9nnn report the current network topology as detected by an online scan. The diagnostic information itself is mapped in index range 0xAnnn in the form of consistent, cumulative counters summarizing the network state from its start up to the present. Thanks to this, the diagnostic interface can be accessed with a frequency which is independent from the cycle time of the EtherCAT network, and no real time performances are required to external tools.

The access to the diagnostic information takes place via the well-established CAN application protocol over EtherCAT (CoE).

The CoE services are routed to and from the Master Object Dictionary in the controller through the standard Mailbox Gateway functionality, which is described in the ETG.8400 specification.

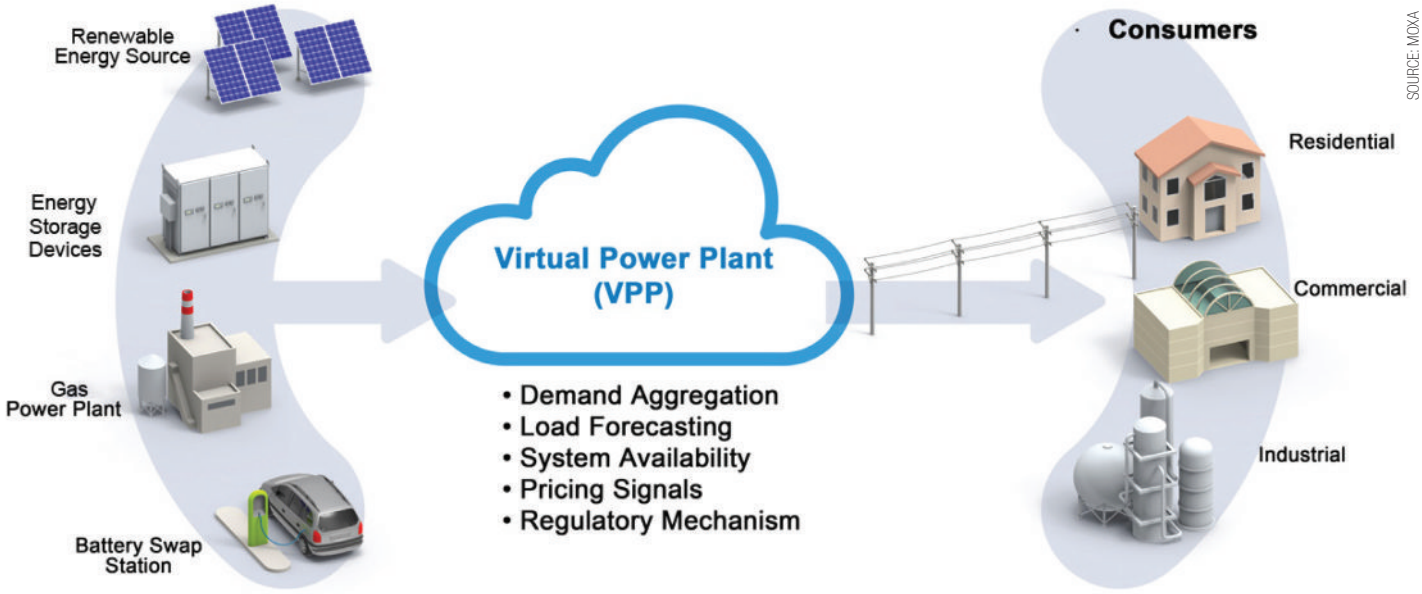
Being based on already existing and fully standard protocols and functionalities, the diagnostic interface can be easily implemented as lean software extension on top of any standard master implementation. The amount of resources required by such a software extension is very small, what makes the implementation of the diagnostic interface feasible for all master solutions including simple and compact embedded systems.

Thanks to the EtherCAT diagnosis interface, introduced with the ETG.1510 specification, providers of machine and network diagnostic tools can use a general purpose, universal interface for collecting diagnostic data from EtherCAT networks. They are able to report this information to technicians and engineers in a user friendly, graphically intuitive way, without the need to change their behavior according to the specific master manufacturer or to use a vendor proprietary access protocol for each different master implementation.

*Alessandro Figini, EtherCAT Technology Expert, **EtherCAT Technology Group.***

Enabling IIoT connectivity for virtual power plants

Leveraging IIoT connectivity for virtual power plants requires high data speeds and quick response times. In this ecosystem, a key to the stability of the system is zero network downtime. 4G-LTE and now 5G technologies are helping build stable networks, so that they can connect to remote sites and assets.



SOURCE: MOXA

The idea of virtual power plants sounds very encouraging. However, deploying the devices and technologies that are required by a virtual power plant is an uphill task. Even if the technology is in place, a change in the mindset of the stakeholders is required to make virtual power plants work.

DECLARATIONS OF CLIMATE EMERGENCIES in many countries around the world have created awareness for the need to switch to clean energy sources, which in turn has prompted the power industry and governments to take action or set definite goals.

Many governments around the world now provide incentives to individuals, industries, and communities who are interested in generating and using power from renewable energy sources such as solar and wind energy. The power grid has seen many changes that have enabled the integration of power from distributed energy sources (DERs).

In the new power economy that is emerging, virtual power plants (VPPs) are showing the way by making it possible to aggregate power from different DERs and providing an efficient platform for energy trading.

Catalyzed by these developments, a new "prosumer" class is emerging that consists of consumers who not only consume power from the grid but also produce their own green power and might have excess power to sell. In this article, we discuss the challenges faced by the introduction of virtual power plants and how IIoT connectivity can help them overcome these challenges.

Predictable power

A virtual power plant (VPP) works remotely to combine a number of independent energy resources from disparate locations into a network that provides reliable power 24 hours a day. VPPs are a departure from the traditional power plants in that they do not solely rely on a centralized power source. Unlike the traditional ones, they combine a number of distributed renewable energy resources with traditional energy.

Aggregating power from different energy resources can help meet the spike in energy consumption during peaks; the utility company does not need to build additional power plants, which is neither efficient nor economical, to achieve demand-supply balance.

Software-based technologies are being deployed to plan, schedule, monitor, and bid for distributed energy resources to make the power grid more reliable. In many geographies, this has translated to infrastructure and process improvements that have facilitated the integration of distributed energy resources (DER) into the main grid. Another goal of virtual power plants is to make it easy for producers to use clean energy portfolios comprising of grid-scale and behind-the-meter renewable energy resources.

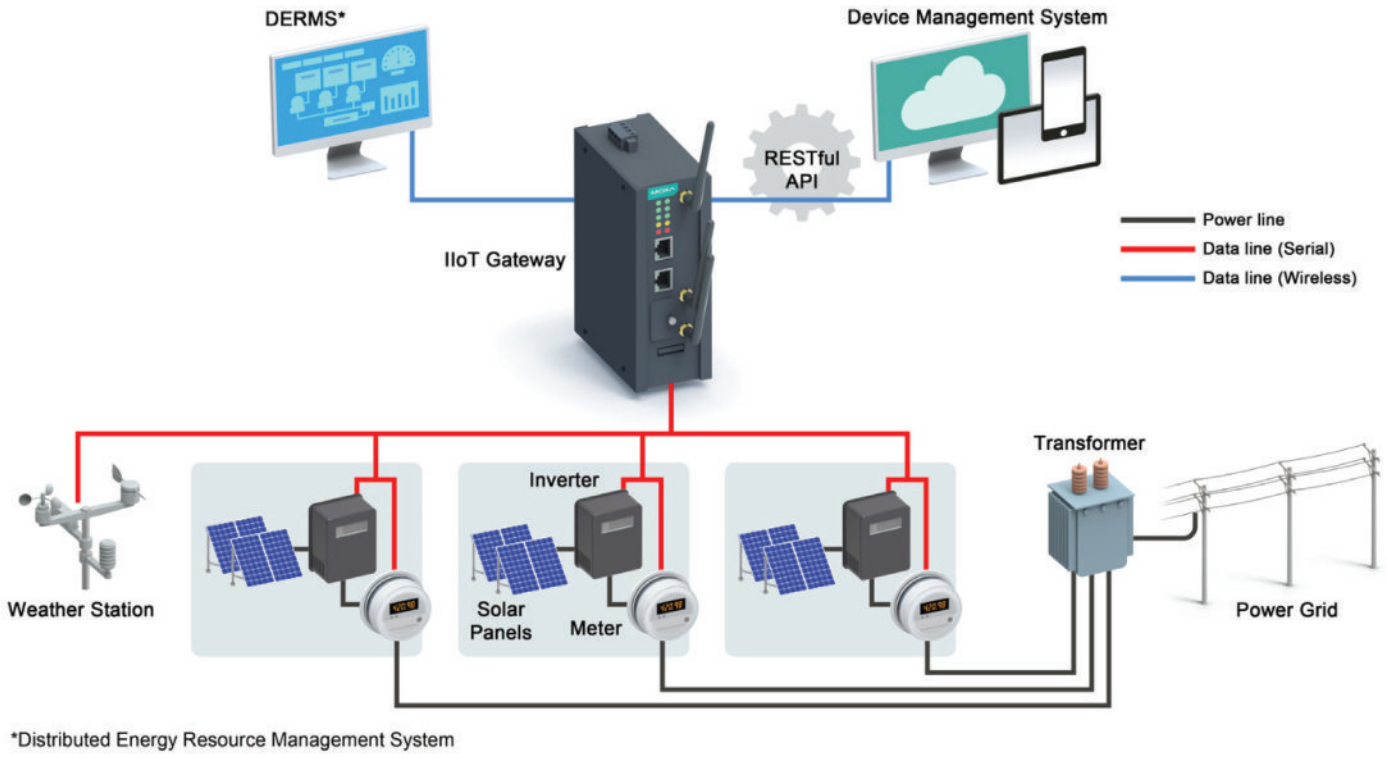
Challenges in virtual power plants

The idea of virtual power plants that are able to solve all power issues of the future sounds very encouraging. However, deploying the devices and technologies that are required by a virtual power plant is an uphill task. Even if the technology is in place, a change in the mindset of the stakeholders is required to make virtual power plants work. Some of the challenges faced by operators are discussed below.

Integrating Distributed Energy Resources (DERs) Into the Grid: Integrating power generated from distributed energy resources into a grid is easier said than done. High penetrations of DERs in the grid can introduce a variety of detrimental conditions, including voltage swings, and reverse power flow, which can cause grid instability.

Most grids have to be retrofitted to be able to integrate power from DERs, increase hosting capacity, and optimize power from DERs. Consumers also need a convenient way to buy power from DER aggregators at an economical price.

SOURCE: MOXA



Data acquired from inverters, meters, transformers, and other edge devices can be send to a DER management system to maintain the grid in a stable state and meet the energy requirements of customers.

Controlling and monitoring devices at the grid edge, especially those associated with DERs, is a major issue. Traditional substation have relied on centralized utility technologies and systems like power supervisory control and data acquisition (PSCADA), energy management systems (EMS) and distribution management systems (DMS). However as DERs have proliferated at the edge of the grid, the requirements for visibility and control of these resources have surpassed the capabilities of traditional centralized systems.

VPPs need the capability to collect and process data from the edge so that the operators know what to expect. Edge devices, such as invertors, need to be monitored for better integration of the system and to prevent grid instability. The ideal percentage of DERs in the total composition of energy sources, including traditional sources, is about 20%.

However, operators are finding it more economical to use power from renewable energy resources because of the increase in demand for green power and a steady supply from producer-consumers.

Virtual power plants require seamless communication solutions to maintain the stability of the grid: northbound communication to acquire data from power devices such as inverters and southbound communication to monitor and control the devices. IIoT gateways, with their computing power and integrated communication interfaces, can help provide the platform for seamless data acquisition and processing. Data acquired from inverters, meters, transformers, and other edge devices can be sent to a DER management system to maintain the grid in a stable state and meet the energy requirements of customers.

Estimating the Power From Renewable Energy Sources: A key factor in the success of the virtual power plant model is the ability to estimate the power from renewable energy resources that is required to meet the requirements of consumers. In addition, some countries have regulations requiring suppliers, such as solar farm operators, to provide power output forecasts for at least three days in advance to ensure demand-response balance and stability of the grid. Most operators do not have a way to gain insight into the power supply. To be able to correctly estimate the power generated, data from aggregators as well as utilities need to be combined together to get the whole demand-supply picture.

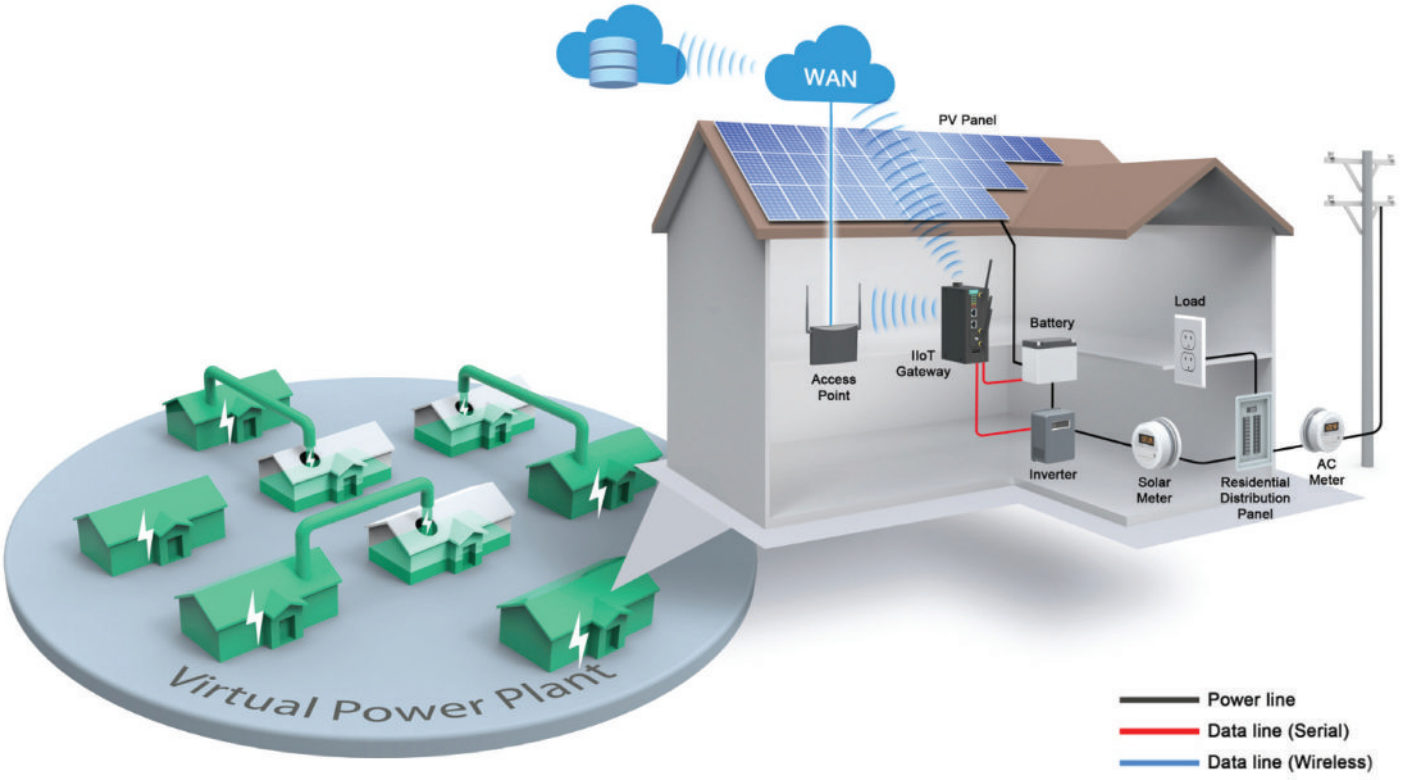
Being able to provide power output forecasts is dependent on the ability to acquire multiple weather parameter values (e.g., ambient temperature, relative humidity, and wind speed), data on the wear and tear of equipment in the field, and conversion efficiency of inverters, among other things. But, solar farms are usually spread over a large area and distributed over different locations. Each farm could return around 20 KB to 50 KB of data per minute. Existing systems may not be able to deal with the large amount of real-time data that needs to be processed and hence the response time may be slow. Other problems that the operators have to deal with include data integrity, data loss, and data security.

A solution consisting for an IIoT gateway and remote I/Os can be used to securely acquire data from various edge devices, such as PVs, located in remote and harsh environments. Solar farm operators can instantly access huge volumes of data from inverters and weather monitoring devices, and use AI technology to accurately forecast the amount of power that is required from renewable energy resources to be able to sufficiently meet the energy requirements of consumers.

Demand-response programs

Energy aggregation is a good way to connect energy producers to the grid so that the excess energy produced can be sold back to the grid. This model helps maintain the demand-supply balance. To prevent wastage, the excess energy produce can be stored in batteries and only released to the grid when required, for example, during peak consumption.

Another way of conserving energy is to shift or eliminate the peaks in energy consumption through demand-response programs, especially in heavy-load applications. For example, significant peak shifts can be achieved if there is a way to bundle industrial consumers together so that they can shift or optimize their power usage periods during the day to avoid peaks in energy consumption.



SOURCE: MOXA

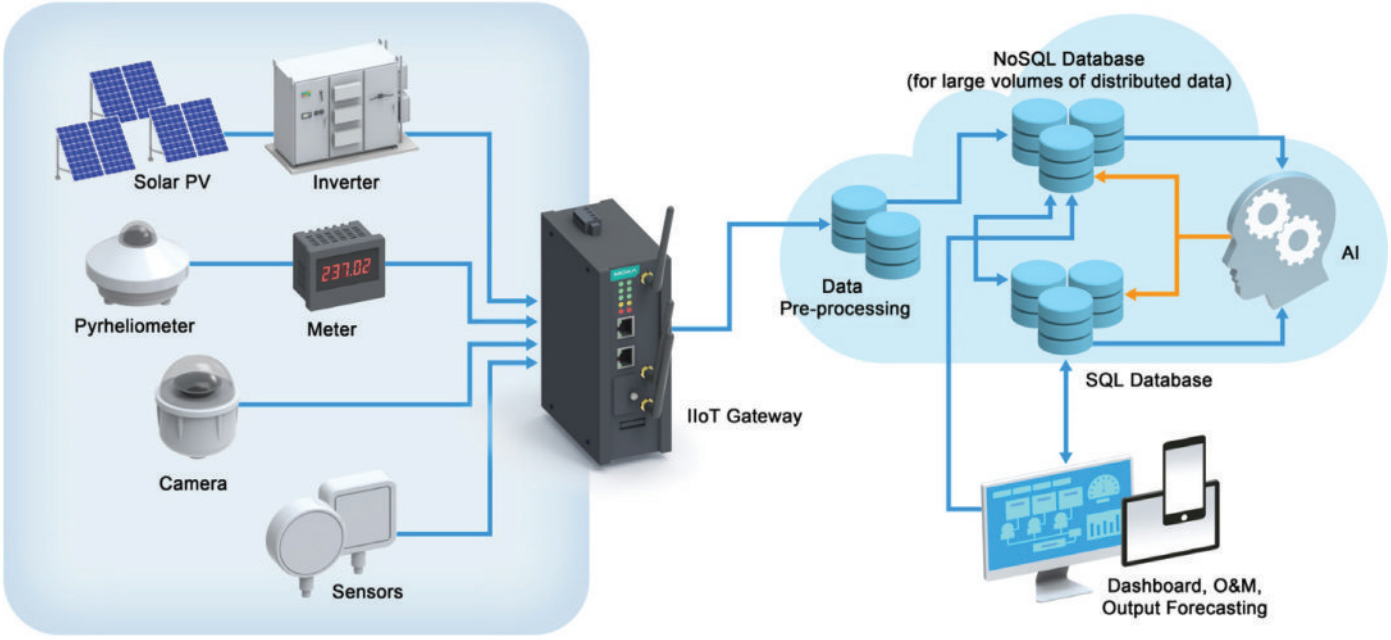
A community of solar energy "prosumers" (consumers and producers of a product) can use the infrastructure provided by the grid to trade excess energy with each other or sell the excess energy back to the grid.

Demand response (DR) can be defined as the incentive payment received by consumers (or demand aggregators) to reduce their electricity consumption during high energy rates and increasing the electricity consumption at times of low energy rates. However, one needs to be cautious and avoid disrupting critical industrial processes.

Monitoring power consumption is key to maintaining the demand-supply balance. In order to provide an efficient platform for energy trading, virtual power plants require advanced metering solutions. IIoT gateways, with their built-in communication and computing capabilities and multiple interfaces, can enable advanced metering solutions in virtual power plants, thereby maintaining demand-supply equilibrium.

Self-sufficient energy communities

Although the idea of creating a virtual network of power resources that is equivalent to the capacity of a power plant is still in the works, there are several examples of communities that



SOURCE: MOXA

Being able to provide power output forecasts is dependent on the ability to acquire multiple weather parameter values (e.g., ambient temperature, relative humidity, and wind speed), data on the wear and tear of equipment in the field, and conversion efficiency of inverters, among other things.

have adopted the virtual power plant model to become self-sufficient in energy. For example, a community of solar energy "prosumers" (consumers and producers of a product) can use the infrastructure provided by the grid to trade excess energy with each other or sell the excess energy back to the grid.

A solar panel manufacturer could be part of this arrangement such that the manufacturer installs solar panels free of cost in each household and in return the householders agree to buy the solar energy generated for a nominal price.

For this business model to work, a reliable network is important to ensure that the solar energy company can monitor the end users energy consumption in real time to ensure accurate data billing.

Furthermore, the solar energy company needs a way to monitor and balance demand against supply through flexible pricing and other options. IIoT gateways installed in the solar energy system can play an important role in acquiring energy production and consumption data from batteries and inverters via Modbus communication, and then transmit the data to a Cloud with a ready-to-run data acquisition platform via wireless networks. IIoT gateways enable the solar energy company to retrieve data related to solar energy storage and consumption, in real time, from sites spread over a large geographical area.

In order to prevent loss of data, the IIoT gateways need to have a failover mechanism whereby the network communication will switch automatically to the secondary transmission method (cellular) if the primary transmission method (Wi-Fi) fails.

When a failure occurs, the solar energy company can fix and update the Wi-Fi settings remotely via their self-developed maintenance applications that use RESTful APIs, which means operators can do all of the maintenance via their mobile devices. If this model works well, the community can be self-sufficient in energy and reduce their dependency on the power grid for their energy needs.

Leveraging IIoT Connectivity

High data speeds and quick response times are very essential in any modern production facility. This is true for virtual power plants and the ecosystem that consumes and supplies power.

In this complex ecosystem where the roles of producers and consumers are often interchanged, a key to maintaining the stability of the system is zero network downtime. 4G, LTE and now 5G technologies are helping build stable networks for virtual power plants so that they can connect to remote sites and assets. On the other hand, cloud connectivity is enabling the use of cloud-based energy management systems for better management of resources and maintenance of demand-supply balance. In addition to instrumentation, virtual power plants are highly dependent on computing and communication technology to facilitate smooth procurement of power from DERs and integrate it into the main grid without endangering the stability of the grid.

In order to acquire large volumes of data in real time and send this data to the cloud for processing and storage, reliable northbound and southbound communication is critical. IIoT gateways are industrial-grade computers that provide reliable data acquisition and computing capabilities at low power consumption, without maintenance complexities, and with the capability to reliably perform at a temperature range of -40 to 70°C in harsh environment.

Remote I/Os make it easy to acquire data from edge devices, such as sensors, for further analysis.

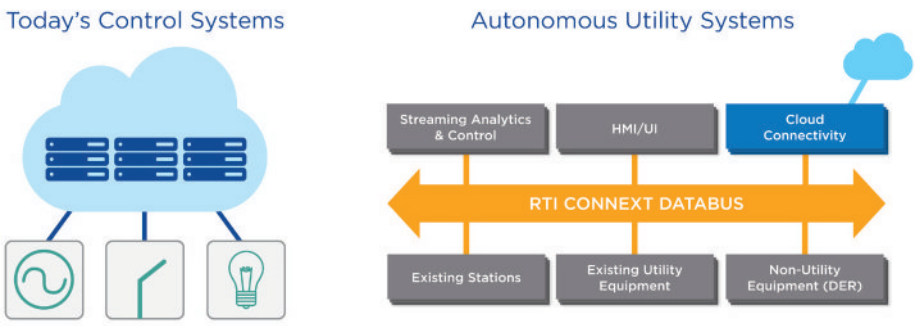
Daniel Lai, Solution Manager, Charles Chen, Solution Architect and Sean Wang, Business Development Manager, ***Moxa.***

Visibility and control over Distributed Energy Resources

A data-centric databus is the structure that enables disparate Distributed Energy Resources (DERs) to work together as an integrated ecosystem. The software databus enables independent DERs to function as a secure, scalable and cohesive ecosystem.

THE ENERGY SECTOR IS UNDERGOING an unstoppable disruption in traditional power generation sources and processes. For over a century, the industry has owned energy generation plants.

Now, power generation from Distributed Energy Resources (DER) sourced from solar, wind, natural gas and water are increasingly supplementing (and even replacing) these power plants. Hundreds, thousands, and even millions of endpoints from Distributed Energy Resources are entering the market and connecting to the grid.



SOURCE: RTI

Architectural comparison of traditional vs. autonomous utility systems.

Powerful opportunity

Many view this as a welcome new business model and opportunity. DERs have the potential to demonstrably affect the economics of power production; research from Navigant predicts a 12% compound annual growth for DERs from 2015 to 2024.

In addition to the economic impact, DERs also upend the monolithic "hub and spoke" operations model that has bben used for over a century. DERs are highly decentralized and consist of an extremely large number of endpoints, ranging in size from individual homes to large scale wind farms.

Today, the vast majority of DERs are grid-connected but for the most part, are not owned by utilities. This is a sea change for the energy industry. The ownership and power is, literally, shifting.

Even power utilities that have not yet incorporated DERs must prepare for their impact. And as the numbers increase, so too does the need to monitor and control these grid assets. In addition, there is a growing opportunity and need for regional coordination of the assets.

Incorporating DERs into the grid requires a new level of integration of new and legacy equipment. Utilities need a technical solution that integrates dynamic, dispersed DERs and provides secure interoperability to legacy systems without disrupting them.

This article discusses how utilities can use data-centricity and a software databus to mesh the old with the new.

This approach is based on the well-established Data Distribution Service (DDS) set of standards, which is used by industrial companies to solve problems exactly like the challenges that DERs present in the era of the Industrial Internet of Things (IIoT).

Data that plays by different rules

Changes are occurring on the traditional electric grid. One change that is rapidly gathering steam is the emergence of DERs. A DER is any resource on the grid that produces electricity and doesn't fit the formal NERC definition of the Bulk Electric System (BES).

DERs are becoming a more persistent and increasingly urgent topic with external policy makers and consumers. This sense of urgency is based on multiple factors, including:

- Local and global interest in clean, renewable energy production
- Improved economics for renewable energy sources, often more cost effective than fossil fueled generation
- The demand for increasing transparency for energy consumption data by technology-savvy consumers
- A shift in economics due to rising costs of traditional power generation (fuel costs, etc.)
- These factors are making DERs more attractive and inevitable, yet there are hurdles to widespread adoption.

One major consideration is that the majority of DERs are not owned by utilities. They contribute energy to the grid, but the utility has limited ability to see or control these individual power generation sources. DERs are proliferating at a rate that no one can accurately predict. Therefore, it's difficult to predict the impact on operations.

As in any industry, there are forward-thinking companies that are boldly embracing new business models and approaches. There are also utilities that continue to take a wait-and-see attitude toward DERs. Regardless of how utilities are individually approaching DERs, one thing is clear: The industry is rapidly moving beyond questions of "if" to "how."

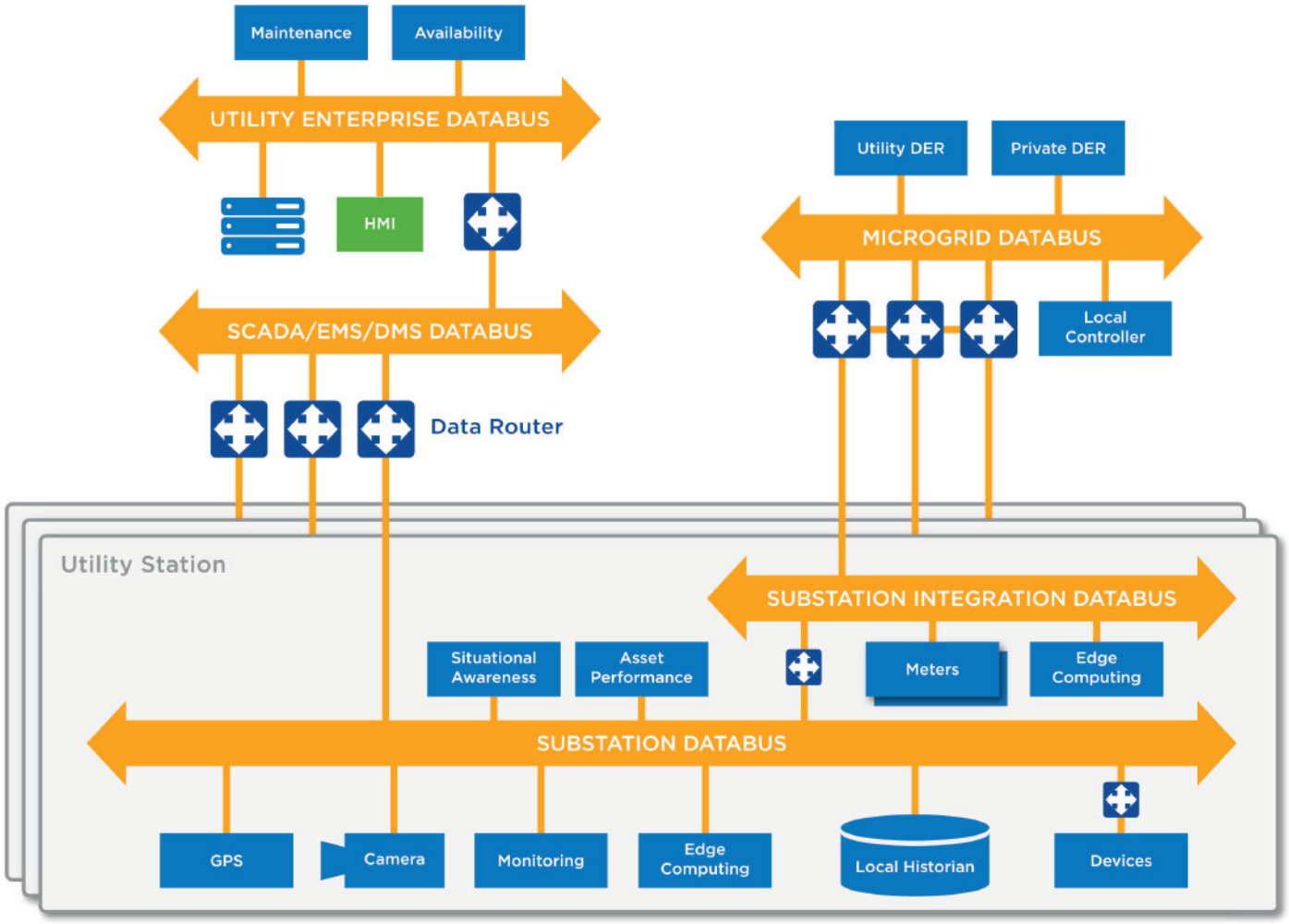
Integrating data provided from DERs into decades-old legacy systems presents numerous technical challenges. DERs are largely incompatible with traditional utility systems and processes. If utilities can manage or neutralize these differences, all of the necessary information can be visible. Gaining visibility is the first step to convert DER data into actionable information.

"Plug-and-play" ecosystem

As described above, and in terms of volume of discrete endpoints, DERs already outnumber traditional energy- generation sources. These endpoints are also likely to be incompatible with traditional systems in terms of protocol, platforms, operating systems and more. In short, they simply don't have the characteristics to act like traditional systems and fit neatly into the traditional hub-and-spoke model.

Many can't afford a lengthy hand-holding process to connect and integrate each new DER that connects to the grid. PnP functionality such as users experience when purchasing a new mobile phone today (very automatic) will be necessary. Further, instead of working with individual DERs, utilities should look at developing a holistic collection of DERs as an ecosystem. An ecosystem is usually characterized by diversity. It is also dynamic, constantly growing and changing.

SOURCE: RTI



The data-centric databus manages data from DERs and legacy utility systems. It can link to other databuses in a layered architecture pattern to accommodate information demands throughout the utility's operations.

This certainly fits the characteristics of DERs.

The technical challenge is to create an ecosystem of DERs that can easily interoperate with traditional systems and processes. With PnP capabilities, users can onboard new DERs automatically and at scale. The data generated from the DERs such as energy produced, frequency, voltage, etc. can then be collected, analyzed and utilized by traditional systems.

This requires a new communications framework to handle the flow of data between the expanded ecosystem and legacy systems. This data-centric framework is based on DDS, the highly-reliable industry standard that manages communications of disparate, high-volume endpoints that define the Industrial Internet of Things (IIoT).

Developed by the Object Management Group, DDS is widely deployed across multiple industries under the IIoT. DDS provides a proven way to manage high volumes of data for industrial applications, through an open integration data-centric framework for software applications. It is proven and used in thousands of deployed use cases, ranging from robotics in healthcare to autonomous vehicles. With its heritage in reliability and security, combining intelligent software with DDS serves as both a control bus and edge-to-cloud connectivity framework.

Data-centricity & software databus

A data-centric communications architecture connects DERs to the databus, not to each other, using a publish/subscribe process. The data is gathered from the different DER (both utility owned and not) and shared on the connected DDS databus. In turn, databuses can be layered and data can be routed while fully secured, to the appropriate databus.

From there, it is available on owned/run computers for analysis. The DDS architecture protects the legacy systems from externally-generated data, through a series of publish/subscribe rules and security protocols. It also protects the utility from an overload of data. In a data-centric model, data and services aren't tightly coupled to a specific device, setting the stage for a decoupled, PnP architecture. DDS is not dependent on servers or brokers; it is a true distributed system with no single points of failure.

The easiest way to understand a databus is to compare it to a database. A database is a repository in which data is stored (short- or long-term) and from which data can be extracted. In contrast, a databus is a shared space for data in motion (rather than standing/stale data). The databus distributes data in motion from device, machine and applications based on opt-in, authorized communications. The data serves as the interface between devices but isn't necessarily stored anywhere. Messages do not need to be sent through brokers to access or process that data. In the databus structure, information from the utility's database/historian is attached and leveraged.

Because all data and services are available on the databus, the only information needed by the application is the domain ID, the topic (or service) name, and the key that identifies the specific data object (or service instantiation). Applications are not expected to connect to any servers or specific nodes. They just send their request to the databus, which takes care of: (1) discovering applications that are connected to it and (2) securely getting information to the right place(s).

In a complex, data-intensive DER ecosystem, this means that data discovery is automatic. Data and services can flow to multiple locations. Applications can join, leave or change locations and IP addresses, and so

on. The databus automatically manages the correct flows.

With a databus, utilities can accomplish a number of tasks:

- Offer plug-and-play functionality for each DER
- Seamlessly operate with multiple protocols (e.g., Modbus, DNP3.0, GOOSE) and support any language, device or transport type
- Provide interoperability with any hardware, software, OS or network
- Create a true peer-to-peer publish/subscribe network
- Secure individual data as well as work with the network-layer security (TLS)
- Perform language/measurement conversions automatically (such as Fahrenheit and Celsius temperature)
- Enable scalability through automatic discovery for third-party data streams

Interoperability with legacy systems

When considering adding DER power sources, the highest imperative is safeguarding existing operations. This encompasses multiple non-negotiable requirements, including:

- Non-disruption of existing operations
- DDS installation/operation on the actual legacy equipment or a small gateway, with no dependence on hardware, software, language, protocol, network
- Minimal (if any) risk of exposing existing systems to security breaches through backdoor communications or data hijacking
- No risk of flooding or overwhelming existing systems with too much or unnecessary data
- The databus accommodate those requirements, enabling designers to utilize legacy, current and future equipment/devices. There's no need to rip and replace existing systems.

Handling volume

A significant benefit of the databus is its scalability to accommodate changes in size/scale. Three attributes of the databus make rapidly escalating volume manageable:

- The databus is infinitely scalable
- There is no single point of failure
- It connects applications to data, not to each other
- The databus eliminates the need to send messages through brokers or other intermediaries, providing a very clean and efficient way of handling high-volume information flow.

Prioritizing data

The DDS databus is more than a pipeline for collecting data from a myriad of disparate sources. It also embeds intelligence to identify and prioritize data on a very fine-grained basis. Without the ability to differentiate and prioritize, the cost of handling fast-growing, fast-moving data streams becomes astronomical. Scalability becomes cost-prohibitive.

The DDS databus provides efficient filtering based on virtually any set of criteria, such as high priority and low priority data, thresholds and priorities. However, filtering and prioritizing data is not going to be a static or fixed requirement. The need for information can change in the moments before or after a power failure. Efficient data filtering and prioritization uses bandwidth more efficiently. Instead of investing in bandwidth that doesn't get used, the databus has the ability to balance the flow of data using filtering. For example, the utility can define rules to limit traffic to only necessary or critical data. It can add policies for peak volumes.

Safeguarding existing systems

Bandwidth and security have a lot in common: adding more of either one is usually expensive but not always more effective. In the case of security, a lot of layers and mechanisms add management complexity, which translates to increased operational costs. Complexity can also introduce unintentional, exploitable gaps.

Extending the existing networks and security models that protect centralized legacy systems today to new/future DERs is impractical. The scale (and corresponding cost and complexity) is simply too large. The DDS databus is designed for highly distributed, high-volume, highly diverse environments. Because the databus deals with data, not applications, it's possible to apply fine-grained security at the data level. For example, if the data is confidential, it can be encrypted, authenticated and checked for data integrity, whereas non-confidential data may only need authentication.

High-stakes mandate for change

An electric utility is faced with a mandate to shift to clean energy. The economics make renewables attractive, and policy makers have updated a previous mandate on carbon-free emissions. The new mandate calls for an accelerated timetable from ten to five years.

The challenge is to identify an approach that doesn't derail programs related to keeping the lights on, which means a response that:

- Meets the accelerated timetable
- Doesn't in any way adversely affect the legacy infrastructure
- Doesn't require an investment that takes away from other high priority projects
- Is built on proven technologies

The solution using a DDS databus to create an ecosystem of DERs that allows users to:

- Gain knowledge with a standard-based approach that puts the utility ahead of competitors and future issues
- Proactively protect the grid while enhancing grid resilience
- Reduce escalating demands on already-strained operational resources
- Accelerate development time through a standard-based, proven approach

By using a DDS databus, the utility can:

- Move from 'after the fact', reactionary operations to optimized and well-orchestrated data management
- For both the utility and the DER owner, DER would be available for "solid state control" of the grid
- Incorporate data/controllability from new IIoT type devices — even behind the customer's meter — securely, with tremendous data "fidelity"
- Communicate and optimize across devices and platforms without the need for "rip and replace"
- Avoid vendor lock-in through adoption of DDS, an open standard solution that enables full interoperability, pluggable security and maintenance of other Quality of Service (QOS) functions
- Fully deploy and promote the PnP scenarios needed in utility operations

Conclusion

A year from now, the number of DERs will have grown. That's a given. However, the rate of growth for each utility's coverage area is unknown. The types of endpoints are also unknown. By implementing a DDS databus connectivity framework, utility companies can incorporate new functionality into their legacy operations — one that delivers secure, interoperable information flow, at scale. It provides utilities with the ability to create an ecosystem out of unowned DERs. Utilities can create this ecosystem without changing their legacy systems; DERs can plug into this platform without changing their systems.

What every utility gains by putting a standards-based databus in place today is easy response today and preparedness for whatever comes tomorrow. The databus is a forward-looking platform that assumes growth. It allows utilities to start with a goal of visibility and move rapidly toward more strategic, multi-faceted use of a broader DER-based ecosystem.

Through this data-centric approach, utilities will have a wealth of information they didn't have previously about these unowned DERs. This data can be incorporated into the analytics for long term planning. It can add immeasurably to accurate modeling and studies. With this real world data, utilities are in a position to have more fruitful discussions with policy makers, potential partners, the public and others. In this way, leaders will demonstrate that knowledge truly is power.

Erik Felt, Market Development Director, Future Grid at ***Real-Time Innovations.***

industrial ethernet book

The journal of Industrial IoT and Industry 4.0

Since 1999

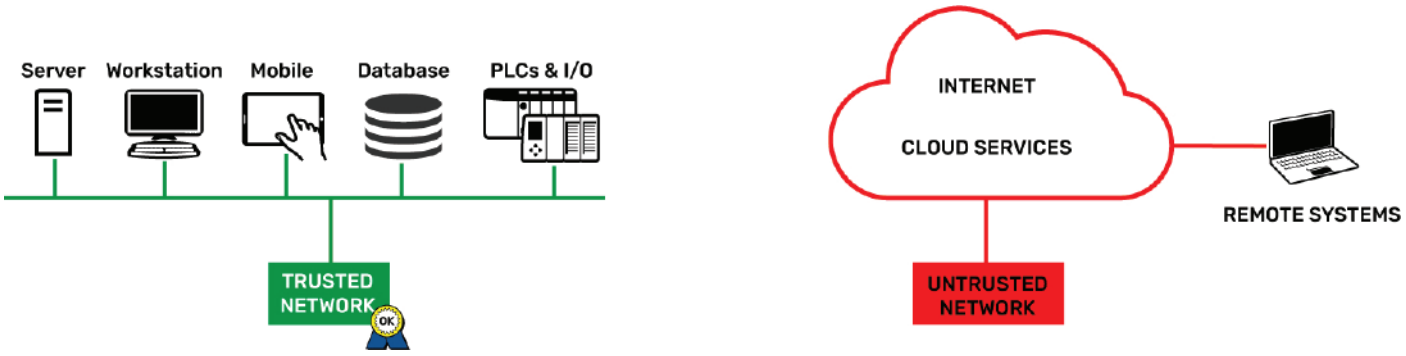
Subscribe to the magazine: iebmedia.com/service

Follow us on Facebook: facebook.com/IndustrialNetworks/

Follow us on Twitter: twitter.com/IEBook

Industrial edge control security design and best practices

To address security's complex, changing nature, system designers need to understand security risks and their environment, along with the security tools they have to work with. Security experts recognize several elements of system security including physical security, policies and procedures, and network security.



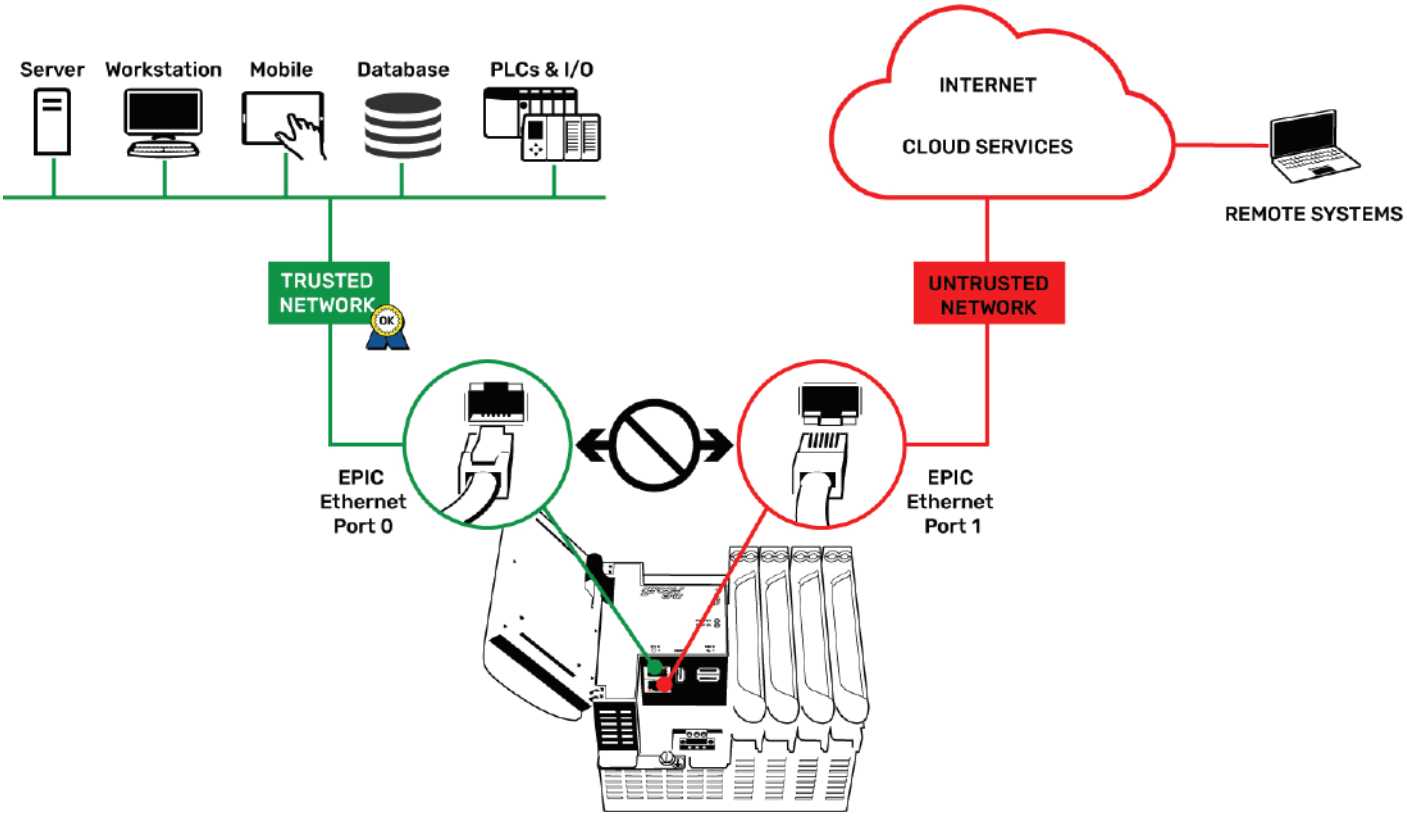
SOURCE: OPTO 22

A trusted network is any network where you know exactly who has access to it. An untrusted network is any network where you don't know who has access, like the Internet.

THE LATEST GENERATION OF EDGE CONTROL technology has been designed from the ground up to help system designers build a secure system for gathering, processing, and sharing useful data from industrial equipment. The result is industrial real-time controller technology that has been designed to maintain a high level of cyber security features and configurable options.

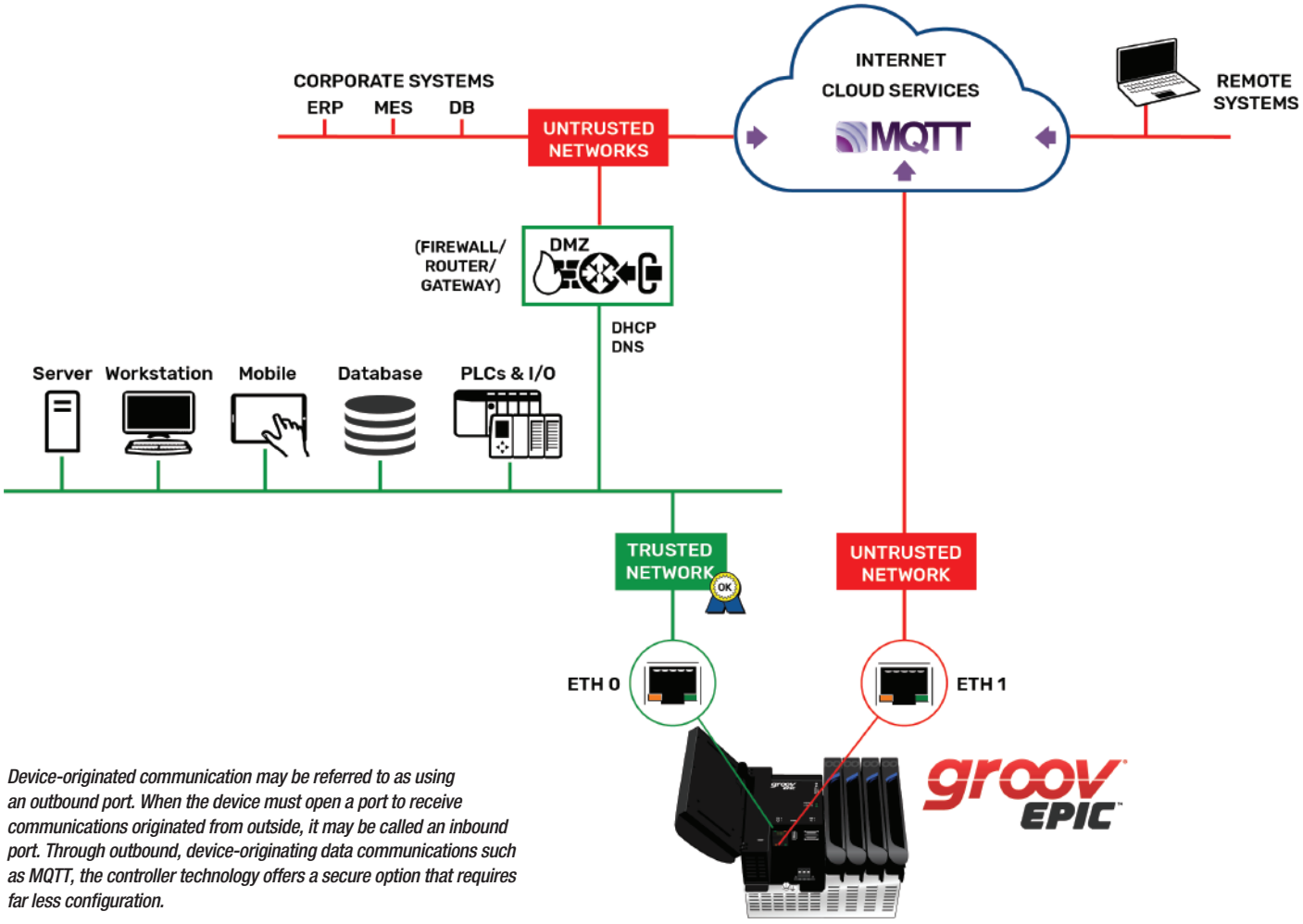
For all digital systems, security is a complex issue with different implications depending on the organization and systems. Security system requirements constantly change as the control system evolves, and building security into the system design is key to success. As Bruce Schneier wrote in 2000, "Security is a process, not a product."

To address security's complex, changing nature, system designers need to understand security risks and their environment, and the security tools they have to work with. Security experts recognize several elements of system security, including physical security, policies and procedures, and network security. Technology such as Opto 22's *groov* EPIC has been designed to address network security requirements as a primary goal.



SOURCE: OPTO 22

A WiFi network (a WLAN) can be added to the edge controller using an approved USB WiFi adapter connected to the EPIC processor's USB port.



Device-originated communication may be referred to as using an outbound port. When the device must open a port to receive communications originated from outside, it may be called an inbound port. Through outbound, device-originating data communications such as MQTT, the controller technology offers a secure option that requires far less configuration.

The objective is to provide tools and methods necessary to make the system as secure as possible from a network access standpoint, while maintaining flexibility for a variety of implementations.

The ultimate security of the system depends on adhering to system best practices and organizational discipline. This article describes security features and lists best practices for setting up a secure system along with an update on the latest technology.

Operating system

Unlike traditional controllers and computers typically used in automation or industrial internet of things (IIoT) applications, the *groov* EPIC processors have an open-source Linux operating system. Contrary to conventional wisdom, an open-source OS is in many ways more secure than a closed one (especially a well-known and often-attacked OS such as Microsoft Windows).

By design, this edge control technology includes only the operating system components necessary for its purpose, which reduces attack vectors. Contrast this limited vulnerability with Windows, for example, which includes components for all kinds of purposes. "The easiest vulnerability to address is the one you don't include," noted Ryan Ware, Security Architect at Intel, in 2017.

In addition, open source means crowd sourced. Because of the number of developers working on Linux, vulnerabilities tend to be addressed very quickly—far more quickly than they can be at an individual software company with a limited number of developers.

And most importantly, the Yocto build of EPIC Linux technology is cryptographically signed with a Private Key. That means that any firmware or software package a hacker might try to upload to the EPIC processor will not be accepted; only firmware and packages that are cryptographically signed can be loaded.

Network interfaces

The controller architecture includes two independent Ethernet interfaces that segment trusted networks (ETH0) from untrusted networks (ETH1). A trusted network is any network where system managers know exactly who has access as with, for example, an IT-managed corporate network. An untrusted network is any network where managers don't know who has access to it, like the internet.

The underlying *groov* EPIC technology and controller architecture is not a router, which functions to join two networks together. Instead, it works by keeping trusted networks isolated from untrusted networks by not routing network traffic between its network interfaces.

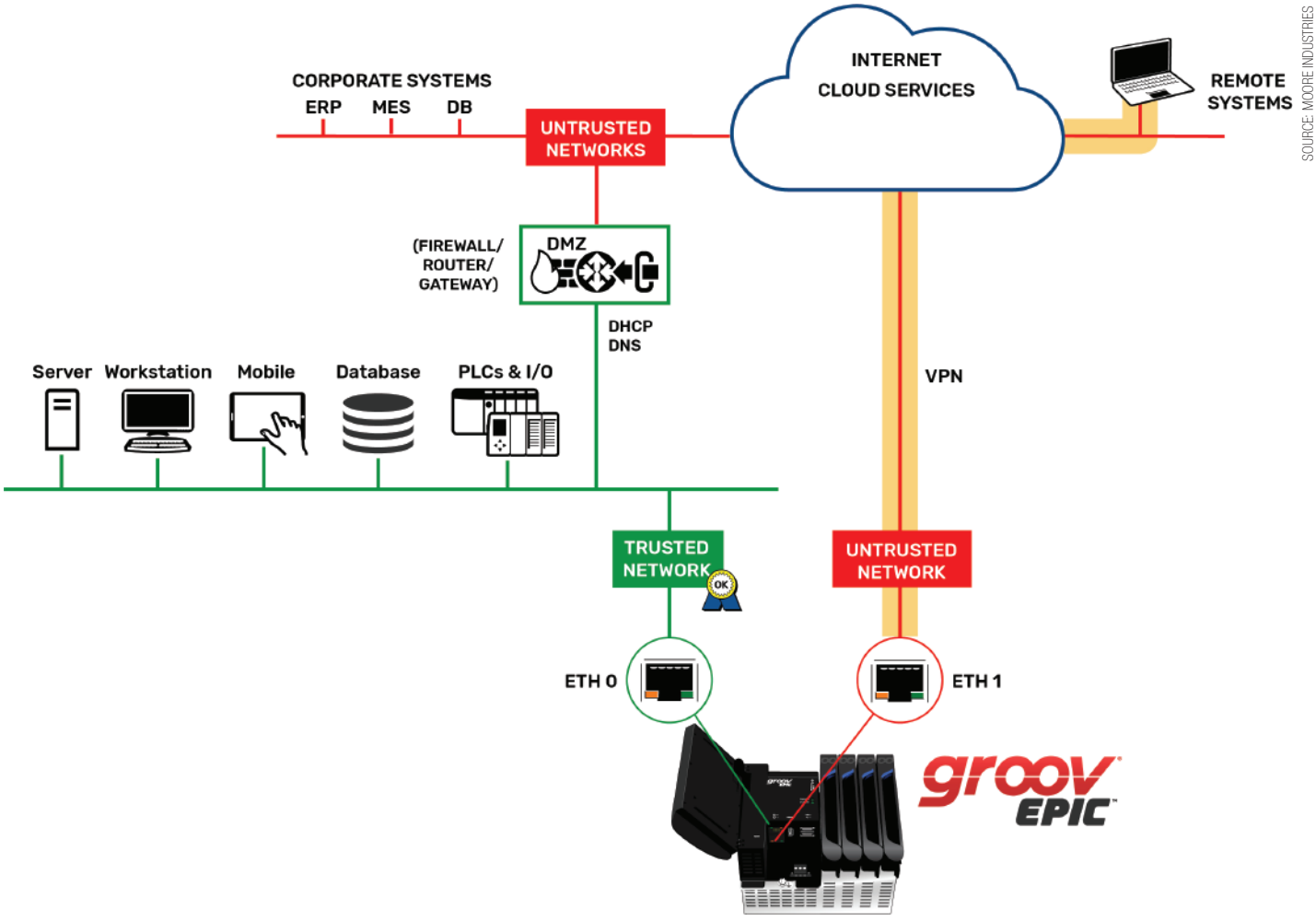
In addition, users can add a WiFi network (a WLAN) using an approved USB WiFi adapter connected to the processor's USB port. The wireless network interface is independent from both Eth0 and Eth1, and does not route network traffic between any of its network interfaces.

Networking tools

On all network interfaces, the controller technology uses standard network services like DHCP which can be configured to use optional static IP configurations, if necessary, but the default is DHCP and DNS. For name resolving and outbound, device-originating access to other networks, a software management tool can be used to choose standard DNS and Gateway addresses and automatic or manual configuration.

Firewalls

Firewalls are critical in securing data communications. The EPIC processor and system design offers a configurable firewall, which is critical in addressing system security. Generally speaking, firewalls help provide security by stopping unsolicited traffic from accessing the network or device/host.



SOURCE: MOORE INDUSTRIES

Offsite user can use software management tools to create secure VPN tunnels from the edge controller to externally configured VPN servers.

Typically the only traffic they allow through is responses to traffic that originated from the inside. Device-originated connections are considered trustworthy because their origin is known. Most firewalls—including corporate firewalls (network firewalls) and the firewall in *groov* EPIC technology (a device or host firewall)—permit devices or services behind the firewall to originate communications outbound to external servers or services.

At the same time, these firewalls generally block all inbound connection attempts originating from devices and services outside the firewall. However, a firewall may allow inbound connections when a specific port has been configured open to allow them.

Default firewall configuration

The EPIC processor's internal firewall default configuration assumes that users are implementing the two wired network interfaces as designed to segment trusted and untrusted networks. On the Ethernet trusted network interface (ETH0), it allows network communications through necessary but unsecure industrial protocol ports that are configured open. These ports allow communication with software and protocols in the EPIC processor, for example: PAC Control and CODESYS development tools, OptoMMP (protocol used by EPIC's I/O) along with Modbus/TCP and Ignition Edge Designer for communication with PLCs and other devices.

On the Ethernet untrusted network interface (ETH1), the controller technology opens secure port 443 and permits only authenticated access over secure, encrypted connections. This network interface provides authenticated, encrypted access to additional software components including *groov* Manage, *groov* View, and RESTful APIs.

All other inbound connection ports on the ETH1 Ethernet network interface are blocked by default. In the system's software tool, users can manage the configuration for each network interface is shown by application, so users can clearly see which applications are allowed access and which are denied.

Users can configure the EPIC's firewall for each network interface to suit specific applications. For example, the default configuration can be changed to close ports for any services that won't be used. If the system is not using Modbus/TCP, port 8502 can be closed to not allow any traffic, even on the trusted network interface.

Clients and servers

The technology has been designed so that individual controllers can act as both a client (a device that originates connections) and a server (a device that listens for requests to connect). Firewall configuration varies based on how the controller acts.

For example, MQTT and Node-RED running on the system are clients that originate communications. MQTT originates communications to MQTT brokers, and Node-RED originates communications to SQL servers, cloud-based services, and so on. No firewall configurations are needed for MQTT or Node-RED. Their communications are outbound and by default are allowed by the firewall.

The *groov* View software running on EPIC is a server that listens for connection requests from PCs or mobile devices running browsers. By default, its firewall is configured to open the secure port used to allow incoming connections. These connections are encrypted and must be authenticated by users.

Whether the edge controller technology is acting as a client or a server, once communications are established, data can flow in both directions as long as the connection is active.

Accounts

This edge controller technology has been designed so that users must create an administrator account with a username and password before doing anything else. The system processor does not have a default username or password that someone might be able to guess. The administrator account credentials a user creates is not recoverable.

Users can create administrator, developer, operator, REST API, and other accounts, and assign those user rights to authorized people or software services. Authentication (over an encrypted connection) is by either username/password or API token. All users can create long, complex passwords consisting of numbers, capitalization, punctuation, spaces, phrases and words in any language, and even emoticons.

Virtual Private Networks

For offsite users, the system can be used to create secure VPN tunnels from *groov* EPIC to externally configured VPN servers or Opto 22 product support. If a user contacts product support for assistance, it's possible to open a VPN tunnel so a product support engineer can temporarily access the device and help resolve the issue.

Security certificate management

Built-in certificate management provides a way that machines can identify themselves to other machines, so that when one machine tries to connect to another, it can be assured it's communicating with the correct machine and not an impostor. The controller technology supports X.509 PKI standard certified connections to servers and from clients using SSL certificates, which can be device generated, self-signed, or registered publicly through a Certificate Authority (CA).

Data communication options

As noted in the Firewalls section, a device is inherently more secure and requires less security configuration when it initiates data communication on a port, rather than having to open a port to receive connection requests.

Publish/subscribe (pub/sub) is a communication technology that takes advantage of this greater security by using device-originated communications only. Controllers can use MQTT, a pub/sub protocol, to report status (authenticated and encrypted) to a central broker. Once connected to the broker, the connection persists, so the controller can also subscribe to any new commands for it or to status messages from other devices.

Because MQTT data flow is device originating, the firewall allows the data out, keeps track of the session status, and allows any packets coming back from the broker to pass through. With MQTT, this persistent connection acts as the critical mechanism for the MQTT broker to determine the state of client connections at all times. In a pub/sub model for supervisory control and data acquisition (SCADA) or industrial communications, users always want to be sure that clients are still connected. If a data publisher's persistent connection is broken, the broker notifies all subscribers, so that the state of the system is known to all.

In contrast, in request/response communication, connections do not persist unless the client maintains them. For example, if Node-RED (a client) connects to a SQL server, once data is sent from the client to the server and the server responds, the connection is closed. Subsequent data transfers must be initiated by the client each time. Using the *groov* View software tool, the client's browser keeps the connection open to the server (*groov* View) only as long as the client software is active.

Device-originated communication may be referred to as using an outbound port. When the device must open a port to receive communications originated from outside, it may be called an inbound port. Through outbound, device-originating data communications such as MQTT, the controller technology offers a secure option that requires far less configuration.

Security design for developers

The system's design gives developers optional Secure Shell access (SSH) for developing custom applications, while maintaining security. Again, available tools help users design a secure system. A license is required to activate Secure Shell. Once users have the license, they can:

- Manage SSH access and restrict it to the trusted network only.
- Configure specific network interface ports on the controller firewall as required by custom applications.
- Install cryptographically signed packages from Opto 22's git repository.
- Compile applications, monitor server log files, start and stop applications or services, and facilitate file transfers.

Best practices for security

Every application and situation is different and practitioners know best what access an application will need and what network architecture to use. However, as mentioned throughout this technical note, *groov* EPIC technology is designed to help create a secure system. Based on a specific application, users should keep these the following best practices in mind as they develop applications and deploy projects.

Networks

Best practices include:

- Configure the controller to use the ETH0 Ethernet network interface as a trusted network.
- Use ETH1 for any untrusted network. Configure exceptions in the system's firewall only if required by the application.
- Configure the system's firewall in *groov* Manage to close all unneeded network ports on all network interfaces.

Accounts

- Have all users create long and difficult passwords, and instruct them not to write them down anywhere. Consider using a password manager where appropriate.
- Use a VPN if there is a requirement for remote unencrypted network connections over untrusted networks.
- To prevent unauthorized access to the *groov* EPIC processor, always log out of any account that has administrator privileges.
- When running the *groov* View HMI software on an external monitor, always put it in Kiosk mode so that only *groov* View is accessible.

Other best practices

If the system requirement is a completely closed system (for example, an OEM using the controller in a machine), after development is completed disable all ports in the firewall and unplug any Ethernet cables.

If someone attempts to connect an Ethernet cable to the controller to try to access the system from their computer, the ports will be closed and network access will be denied. Only an authorized user with administrator privileges can access *groov* Manage through the built-in display to reopen needed ports and gain network access.

Whenever possible, use authenticated and encrypted outbound, device-originated data connection methods. For example, use MQTT to publish data to an MQTT broker. Device-originated data communication methods help reduce open inbound network ports, eliminate man-in-the-middle exploits and prevent exposing sensitive credentials over the network.

Best practices for developers

If the system uses secure shell, configure SSH access with a unique and difficult username and password, different from *groov* Manage, *groov* View, or any other software running on the controller. Enable shell access only to configure and program the unit. Once the system is commissioned, disable shell access in *groov* software tools, so that no one else can get in. Never leave SSH access enabled once the system is in production.

*Technology report by **Opto 22**.*

Cybersecurity challenges in discrete manufacturing

Network, cybersecurity, and automation control professionals in discrete manufacturing and similar operations can work to optimize profitability with the most sophisticated automation solutions driven by the advent of the IIoT, while maintaining optimum, best-in-class cybersecurity levels on the plant floor.

LIKE OTHER INNOVATIVE INDUSTRIAL organizations around the world, many discrete manufacturing facilities such as those in the automotive, aerospace and electronics sectors are strongly benefiting from access to real time production data flowing from the plant floor, strategically applying this intelligence to increase yields, improve quality, reduce waste and more. Further, many such organizations are poised to cull even greater benefits as the Industrial Internet of Things (IIoT) continues to evolve, and new and more powerful technologies and subsequent opportunities emerge.

However, with this increase in connectivity comes a resulting increase in risk. Previously isolated control networks are now potentially accessible to outsiders through increasing numbers of touchpoints, including the global Internet itself. This can open up the production environment not only to the danger of hacking attacks and malware of many kinds, but also equipment failures, human errors, malicious internal events and other cybersecurity related incidents that can significantly impede production and even degrade safety performance on the factory floor. Such issues can be especially impactful in the discrete manufacturing environment, where unscheduled downtime can often be calculated at a cost of hundreds of thousands or even millions of dollars per hour or higher—and excessive waste or product recalls can add even more.

Fortunately, discrete manufacturers have many options to significantly reduce the potential for cybersecurity issues at their facilities, and minimize the possibility of suffering from the type of events that have had huge negative impact on productivity, quality, safety, profitability and even brand reputation in untold production operations around the world.

This article is intended to educate the reader as to the true extent and diversity of cybersecurity threats that are being experienced in today's discrete manufacturing environment, as well as introduce the possibilities that exist to limit exposure. These include practicing good cybersecurity hygiene; optimizing the strategic use of smart cybersecurity configurations in existing network equipment; understanding and initiating cybersecurity best practices such as Tripwire's comprehensive three step "Visibility-> Protective Controls-> Continuous Monitoring" solution; and deploying innovative third party tools specially designed and proven to optimize cybersecurity performance at your facility.

SOURCE: BELDEN

Discrete manufacturers have many options to significantly reduce the potential for cybersecurity issues at their facilities, and minimize the possibility of suffering from events that have had huge negative impact on productivity.

Indeed, today's operations technology (OT) professionals can readily enjoy the best of both worlds: maintaining and expanding the use of data-driven technologies that enhance production goals, while simultaneously proactively protecting against the vulnerabilities that threaten the integrity of the operation.

Vulnerable to cyber incidents

In a discrete manufacturing facility, operations professionals are charged with meeting challenging objectives and quotas, taking a diversity of raw components from a multitude of sources, transforming them, and getting large quantities of finished product out the door on time and in the highest quality, with minimal variation and optimum on-target specifications. To do so, they rely upon the data that they are receiving from networked components at each step of the production process all the way through final quality control inspection. However, what if any of this data has been compromised?

Further, the typical discrete manufacturing plant floor contains myriad dangers to human life and safety, with light curtains, motion detectors, sensors and other technologies ever vigilant to help ensure that everyone gets home at the end of the day. What if any of these fail safes have been compromised? Can we trust them if they are responding inappropriately to data or responding to false data?

Greater connectivity=greater risk

These alarming scenarios are not uncommon today, with the increased connectivity found in modern discrete manufacturing automation

industrial ethernet book

Reader Service Card

IEB issue 116 - February 2020

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

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

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

Please enter your contact details below:

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

I want to:

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

Signature: _____

Date: _____

Company Activity (select one)

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

Job Activity (select one)

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

SOURCE: BELDEN

In a discrete manufacturing, operations professionals are charged with meeting challenging objectives and quotas. To do so, they rely upon the data that they are receiving from networked components.

systems clearly creating a double-edged sword. Indeed, industries as diverse as automotive, aerospace and electronics have been highly successful at utilizing diverse automation equipment including controllers, robots, motors, sensors, HMIs, VFDs, I/O blocks and process- specific machinery of all kinds on the production floor. While these vital components had long operated independently, they now often proactively share streams of real time data, communicating in line to allow finer control of processes for accuracy and quality improvements.

In addition, many strategically generate and disseminate data for analysis that can allow further fine tuning of processes as well as archival of production data for overall equipment effectiveness, audit, vendor accountability and other purposes. With the continuing evolution of the IIoT, which promises even greater connectivity, utilization and value for connected devices and shared data, this trend can only accelerate, increasing opportunities for greater yields, faster cycles, reduced waste, improved quality, greater safety of personnel and equipment and more.

However, with these benefits comes a very real threat to the efficacy of the production environment. Isolated for years, these control networks are now, potentially, directly linked to the outside world from other areas of the factory to the IT-led enterprise side of the business to the global Internet itself.

This creates a new world of threat vectors, opening up the plant to a host of potential cyber-related incidents, malicious and unintended alike. Many of these threats are new territory for OT personnel, including ransomware, malware, employee cyber sabotage, network failure, user error and more. While these issues have been familiar and costly to the IT side of the organization, their accelerating emergence into the OT side can be even more damaging due to the fact that, in discrete manufacturing industries, producing and shipping product is the lifeblood of the business.

Productivity and process integrity

In a discrete manufacturing environment, production lines are often run at maximum capacity, and downtime—with its high costs related to lost yields, increased waste, missed commitments and more—is calculated in many industries at a cost of hundreds of thousands or even millions of dollars per hour or more.

Further, with dozens, hundreds or even thousands of assembly processes that must be in tight specification, there are myriad opportunities for a key subassembly such as a door panel, a motherboard or even a final product to be ruined by a single out-of-spec operation, even something as simple as a bolt or other fastener applied with insufficient torque value. The production instructions for any one of these can be impacted by an inappropriate change in a device configuration or production requirement, whether it comes from an input error, a purposely malicious input change, failing components or other undesired modification to the network. While discrete manufacturers theoretically have the advantage of reworking out-of-spec subassemblies down to component parts, such refabrication is often considered laborious and time-inefficient, with out-of-spec parts often reclassified as scrap, and relegated to the waste stream for costly disposal.

Additionally, for many discrete manufacturers, when out-of- spec products are not caught in time, this can lead to costly product recalls, a degradation in brand reputation or even litigation if there is a product-related injury down the line.

Variety of cyber culprits

As suggested, cybersecurity incidents are not only those perpetrated by malicious actors, such as hackers and malware developers—although these are more likely to grab the headlines. As incident responders can tell you, a cyber event is considered anything that negatively impacts the network and impedes the ability to view, monitor, control or maintain the availability of an industrial process, including safety systems—whether malicious, accidental or the result of natural wear and tear.

This includes hacking attacks such as denial of service, malicious mischief, corporate espionage and more; malware attacks such as ransomware and viruses; innocent human error by otherwise valued employees that can still ruin broad swaths of production; disgruntled employees who can wreak production havoc from inside the network; quietly failing equipment and components that can slow processes or produce operational issues like off-spec conditions—all these, and more, regardless of source or intention.

Common cyber incidents

As the potential benefits of connectivity increase, and the threat of cyber incidents increases in tandem, it seems timely for today's plant floor network professionals to fully educate themselves on their risks. Operations personnel must begin tapping into available cybersecurity techniques and technologies, many long familiar to IT, in order to protect their OT production environments. Indeed, it may be that the stakes are even higher because threats to the discrete manufacturing environment can strike the integrity of production, the creation of products that are the heart of a manufacturing enterprise as opposed to vital but non-specific administrative functions.

This starts with the basics, which, for many in the OT environment, might not be as second nature as they have become in IT. This includes good cyber hygiene practices such as disabling unused ports, separating the OT and IT environments with firewalls, initiating onboard security settings on all devices so equipped,

and, perhaps most importantly, disallowing connectivity between production devices and the global Internet. And, while these are all important, the key to cybersecurity in both IT and OT environments is establishing and continually maintaining optimum insight into network operations minute by minute in real time.

It is important to note that, while cybersecurity in IT can often be viewed as primarily "defensive," proactively driving cybersecurity in the OT environment can actually increase process integrity and improve the ability of personnel to manage processes in increasingly granular ways. Indeed, for controls professionals, cybersecurity is often not just about security; the increased visibility and monitoring capabilities that provide cybersecurity can also be integral to the drive toward process stability and optimizing quality and yields. To better understand how, let's look at a host of common scenarios and how they might manifest in a typical discrete manufacturing production environment. These examples will illustrate how the ability to "see" any of these scenarios as they occur, rather than be blindsided by them, is key to optimizing OT cybersecurity— and OT process integrity as well.

SOURCE: BELDEN

Not all cyber events are malicious—unintentional mistakes play a role in detrimental network impacts in a discrete manufacturing environment.

Unauthorized malicious entry

Hacking is perhaps the most "dramatic" of malicious attacks as it is usually a "hands-on" event. This is opposed to, for example, an actor sending a piece of malware out into the world and being unaware of the locations where it might end up. By contrast, hacks often consist of an actor personally getting into a network, and then spending time in "reconnaissance" trying to see what information and resources might be exploitable. As noted, this is the time that they can be seen and thwarted, if adequate provisions are made in advance to gain the visibility that will immediately reveal their digital footprints and alert network operators to take action.

Hackers take many forms; they could be nation state actors looking to sabotage a strategically important organization, competitors or their agents looking to gain organizational intelligence such as bills of material or production data or plans, or even simply random purveyors of criminal mischief.

Of significant note: the hacking victim might not be the ultimate target. For example, perhaps a hacker enclave wants to ultimately attack a well-protected organization such as a major automotive manufacturer. Small suppliers to that organization are immediately targets because they might have a poorly protected entry into the major company's systems through a billing or ordering link. Further, if the smaller organization has a particular device, such as a specific model of PLC that the larger company also uses, a hacker will often hack that device at a smaller company as a "test bed" to learn about its firmware operation and vulnerabilities before trying to access it and exploit it at a larger company. Another reason for targeting a smaller company is to enslave computer resources, using their captured capacity along with that of others to launch "denial of service" or similar attacks on bigger players.

You should be aware that the IP addresses of many controllers, cameras, machines and other networked devices—perhaps yours—are available right now, on the Internet for anyone who cares to look. Professional research sites such as Shodan provide this information; what might be on the dark web for more illicit purposes is anybody's guess.

Anyone can literally use this readily available information to view the inside of factories through the facility's own cameras. It is quite shocking, but enlightening, and effectively illustrates that basic security protections, such as closing ports, installing firewalls and looking for and eliminating these unnecessary and dangerous Internet access points have not been established at these facilities.

Inside hackers

Even among those OT environments more experienced with cybersecurity protections, much is often done to thwart the outside hacker, but the possibility of malicious actions by an employee—often far easier to implement and more likely to occur—are overlooked and not anticipated or protected against. Building a robust perimeter does little if the attacker is already "inside the gates." Further, employee hackers are already familiar with OT processes and equipment and can be even more damaging than the outside hacker.

Reasons for employee cyber-attacks can run the catalog of lower aspects of human nature—disgruntlement and desire for revenge due to real or imagined company slights; betrayal driven by bribery or monetary gain; becoming reluctantly compromised due to threats or blackmail; cheap thrills; psychosis; boredom; or "just because I can." Goals can be tied in to the above, including sabotaging production by purposely modifying specs or work orders, stealing and providing proprietary information to a third party or selling on the black market, or sabotaging safety systems to cause injury to perceived enemies and the organization.

Another flavor of inside "hack" is that performed by a perpetrator who is spoofing a trusted employee using stolen credentials. For example, even if they are checking the logs, operators may turn a blind eye and not be suspicious of changes made to production specs initiated by the boss, not realizing that the changes were being made by another employee illicitly using his credentials. Even if such changes were flagged, related pieces of suspicious information (Why are these changes being made at 4:00AM? Why is there communication to foreign IP addresses?) Theses are usually not consolidated to create a complete picture unless additional tools are deployed.

Amazingly, people often wonder how someone "knows" their password, the same password written on a sticky note and placed under their engineering workstation keyboard. Common cracking techniques such as password brute forcing, psychographic guesswork (kid's names, birthdays), implanted keystroke emulators, accessing unencrypted password databases, or snooping the credentials off of network traffic are highly effective, but are often not even necessary.

No matter the source, protection against "insider" cyber events starts with visibility. If every time a change is made, an alert is sent to the operator, then every change can be verified to authorized work orders, and unexpected, unauthorized changes, whether with malicious intent or not, can be immediately reverted back to the expected, operational configuration.

Malware, viruses, trojans, worms

Malware describes a number of manmade code-based phenomena that can infect the OT network and wreak havoc on production in a number of ways. The impacts of malware can vary from silly and annoying (announcing "Star Wars Rulez" on every screen) to completely shutting down production indefinitely. Reasons for doing so can include spite, sabotage or even ransom. Ransomware, which first came to light attacking the IT environment, would seem to be an even more effective attack

in the OT environment, where downtime is often so much more costly and time sensitive.

Unfortunately, with many current ransomware schemes such as WannaCry and (Not) Petya, even paying the ransom does not guarantee that the data or system operation would be returned to user control—and, ironically, it has nothing to do with the relative "honesty" of the perpetrators. Often, authorities immediately shut down the Bitcoin wallet or other electronic payment channel assigned by the criminals, leaving the victims without even this access to a potential "solution." In these cases and others, the only solution is reimaging devices along with accepting the process downtime and loss of data.

SOURCE: BELDEN

Protective controls can help prevent or lessen the impact of cyber events.

Malware can include viruses, which are attached to a file and need to be opened by a user in order to spread—hence the constant warnings to never open unfamiliar attachments or files. Worms are more insidious, duplicating themselves and acting behind the scenes, without the need for user "launching." Trojan Horses are perhaps the most insidious of all, often disguising themselves as a useful application and causing damage when opened, locking or deleting files, or opening up a backdoor allowing the malicious actor access to the network.

Malware can be introduced to the OT network in a number of different ways. Infecting user PDF manuals and schematics is a favorite channel, so that when a contractor opens such a file on the plant floor to attend to a device, the malware is launched and spreads throughout the OT network. Malware can enter through an attachment opened in an email—another reason why Internet-connected devices should not be allowed to connect to plant floor devices.

Even if correctly unconnected to the outside world, malware can get in through the purposeful or ignorant complicity of inside personnel, through someone connecting an Internet-enabled laptop, or plugging in a found "free flash drive." The latter was reportedly the source of Stuxnet, the malware which infiltrated the supposedly air gapped plants in Iran by presenting false values to PLCs and making centrifuges malfunction. Again, good cybersecurity hygiene best practices would lead one to avoid some of these scenarios through disabling the use of USB ports or denying connection of unauthorized devices to the network.

One highly unexpected source of malware is having it piggyback in on a duly purchased device. Sometimes a device manufacturer's production environment can be infected, and the malware could be riding in the device firmware, infecting the production environment of each purchaser facility it is installed in. Often, visibility saves the day as the proper tools can flag these devices secretly doing things they were not meant to do, such as performing port scans or attempting to phone out.

Of vital note, malware is often not an end in itself, but the first step in a hacking attack, with the malware designed to change configurations, "phone home" captured passwords, disable firewalls or perform some other hidden function to allow a hacker to gain access for their primary purposes. In a proactive, cybersecurity aware operation, it is these changes that are its undoing. Similar to hacking attacks, malware implementation leaves evidence of changes in the network that can be immediately identified and alerts triggered if the proper visibility is put in place.

As noted, many pieces of malware were originally created to compromise the IT environment, and yet are causing "collateral" damage in OT environments due to the fact that there are often IT devices and services—such as Windows, Linux, SQL databases, and web servers—running in plant environments as well. They can be infected independently, and, without proper separations between these environments, infections in the enterprise can spread to the OT production side as well. In recent years, however, more and more malware is being deployed that has been created with OT attacks in mind using protocols specific to the controls environment such as IEC 101, IEC 104 or Step7. One particularly appalling piece of what is suspected to be nation state driven malware, Triton, was written specifically to target Triconex, a safety instrumented system (SIS) manufactured by Schneider Electric. It seems to have the infliction of injury rather than monetary gain as its primary purpose.

Human error

Not all cyber events are malicious; unintentional mistakes play a role in a high percentage of detrimental network impacts in a discrete manufacturing environment. Think how easy it is for a busy operator to type in 60 psi instead of 6.0 psi to a torque value, or accidently set the networked PLC on line 1 with the values for the PLC on line 2, creating huge issues on the line. Consider how often a maintenance worker might weaken firewall rules in order to make a repair or create a testbed—and nobody ever changes them back. Fortunately no matter what the intention, changes to the network can be flagged using the right monitoring solution— and operators can quickly determine if these changes were appropriate and take immediate action when necessary.

Failing equipment

Another common, non-malicious scenario that can impact the integrity of the production network stems from an imminent failure in physical infrastructure, such as a cable, a switch or a device like a PLC or HMI. Production instructions can start to become garbled, lost, incomplete, or slowed, causing an impact on quality and yields in the discrete manufacturing environment.

Often, the system might be giving some indication, from measurable changes in response times of robots or conveyors to an increasing amount of cyclic redundancy check (CRC) or other errors or diagnostic information that may be generated in operation logs that are not looked at in timely fashion. Automatically monitoring this diagnostic information and deploying proper alerts is another form of preventative maintenance and is critical to help pinpoint events before they have the potential to impact production process in a negative way.

One protective strategy

As suggested by every example above, any change to the network—whether purposeful, accidental or malicious; benign, frivolous or highly detrimental—immediately leaves evidence of its inputting. Problem is, by default, such evidence is often incomplete, isolated and "hidden" somewhere in device logs or not even collected in the first place. If it is not searched out at the exact moments when an incident is occurring, it will continue invisibly and unabated until the damage has been done and the costly impacts on your facility and production are in full swing.

That's why operators consider implementing specialized solutions that are designed to provide continuous real time visibility into their network operations. Generally speaking, these have a three part strategy—inventorying what you have and what it does, putting in all the protective controls possible, and then monitoring for changes against the baseline, i.e. any abnormal network behavior. In this way you can gain control over everything that you can possibly control.

Although the idea of securing an insecure plant from "square one" can seem daunting, in fact, you can quickly gain a significant amount of protection fairly readily. There are foundational cybersecurity controls that you can begin right now to help reduce operational risk and help you detect and avoid the impacts of all the threats discussed above. These foundational controls are fundamental techniques that provide the most visibility and protection against malicious activity. In fact, they are the basis of most formal industry cybersecurity frameworks, such as IEC 62443, American Water Works Association Process Control Network Guidance, NIST SP–800-82 and NERC CIP. However, whether or not your organization chooses a specific standard to adopt, you can start with fundamental actions such as:

- Asset Inventory and Discovery of Hardware and Software
- Network Segmentation
- Vulnerability Management
- Change Management
- Network Management
- Centralized Log Management

These are all included in the comprehensive three part strategy. The philosophy and driver behind it is, as we often say, "How can you protect something if you don't know what you have or what it does, or what 'normal operation' even looks like?" The strategy remedies that. A comprehensive cybersecurity strategy can be implemented using three steps.

Step 1. Gain Visibility

Immediately, you can take the guessing game out of the equation. You can know what you have and therefore what you need to secure. When you have holistic visibility into your control network, you can create and maintain asset inventory (vendor, make, model, serial number, firmware version and more), as well as manage communication patterns between devices, see network topology variations, identify rogue assets on the network, outline configuration changes, provide vulnerability context, and other environmental elements—by fact, not guesswork. Visibility capabilities include:

1. Understand and document all network communication between the industrial control network and the corporate enterprise IT network.
2. Understand and document all remote access into the industrial control network, i.e. vendor access with dial-up modems, VPN and cellular connectivity.
3. Create and update asset inventory information for both hardware and software, including vendor, make, model, serial number, firmware version, and versions of installed software.
4. Create and maintain a network topology diagram.
5. Understand what industrial protocols are communicating and between what assets, such as HMIs to PLCs.
6. Understand how assets and devices are configured and if those configurations are changing.
7. Identify what vulnerabilities (weaknesses) are present in the environment.
8. Implement a centralized log management solution.

Step 2. Use protective controls

Protective controls are controls that help prevent or lessen the impact of cyber events. However, it is often wasteful to implement protective controls blindly. You have to implement the right protective controls for the industrial process you are trying to secure and manage. What may be appropriate for one application may not be appropriate for another. Ensuring network segmentation between the corporate enterprise IT network and the industrial control network is a great first step. This denies all unauthorized network communication through the use of firewalls or access control lists on networking devices.

Another often effective protective control is system/device hardening by which:

1. All services are disabled that are not explicitly needed to run the industrial process, i.e. disable insecure protocols like telnet which does not encrypt traffic;
2. Cybersecurity features such as logging, SSH, SNMPv3 and other features are enabled; and
3. Device/system is checked for proper configurations, i.e. change default passwords and enable password

Step 3. Continuous Monitoring

The third step is to implement continuous monitoring. Just like you have a SCADA to help optimize and control your industrial process, you need a "SCADA"-like cybersecurity solution to help optimize and control visibility to industrial cybersecurity events and ensure the protective controls you have implemented are operating correctly. This is not a one-and-done activity—it needs to be performed continuously.

Industrial cybersecurity "SCADA" monitoring helps continually answer the "How do I know" questions, such as:

1. How do I know if my device/asset configurations are changing, and do those changes put the device in an insecure state or misalign to my build specification?
2. How do I know if my operational baselines (the configuration of a device or system that is specific to the environment it is running in) are changing?
3. How do I know if one of my devices is at the brink of a failure?
4. How do I know if a rogue asset or protocol is now present on my control network?
5. How do I know if my vulnerability risk profile has changed?

If you are able to answer all of these "How do I know" questions, you will be able to keep your industrial process running without interference from cybersecurity events.

Unfortunately, you do not get to make the decision as to whether you are a target for either an external or internal malicious intent. So know your network. If you don't, someone else with a different motive will. Fortunately, control networks are defendable.

Further, as noted, cybersecurity can be an enabler to the key performance indicators of the industrial process: safety, productivity, and quality. The important thing is to take action and to come up with a strategy that is driven by executive management and sets a proactive tone from the very top of the organization.

The time to implement visibility, protective controls and continuous monitoring is now—every minute that you don't is a minute that leaves your network vulnerable to a host of costly threats.

Conclusion

The production function is the lifeblood of every discrete manufacturing business, with professionals working round the clock to get high quality product out the door on time and within increasingly tightening operations budgets. Advances in operational technologies and factory floor networking are giving OT professionals powerful tools to boost yields and reduce waste, but such tools cannot in good stewardship be implemented without an understanding of the resulting cybersecurity risk they open up.

Fortunately, with this awareness—and subsequent action—network, cybersecurity, and automation control professionals in discrete manufacturing and similar operations can work to optimize profitability with the most sophisticated automation solutions driven by the advent of the IIoT, while maintaining optimum, best-in-class cybersecurity levels on the plant floor.

Gary DiFazio, Director of Marketing, Industrial Cybersecurity, ***Belden Corporation.***

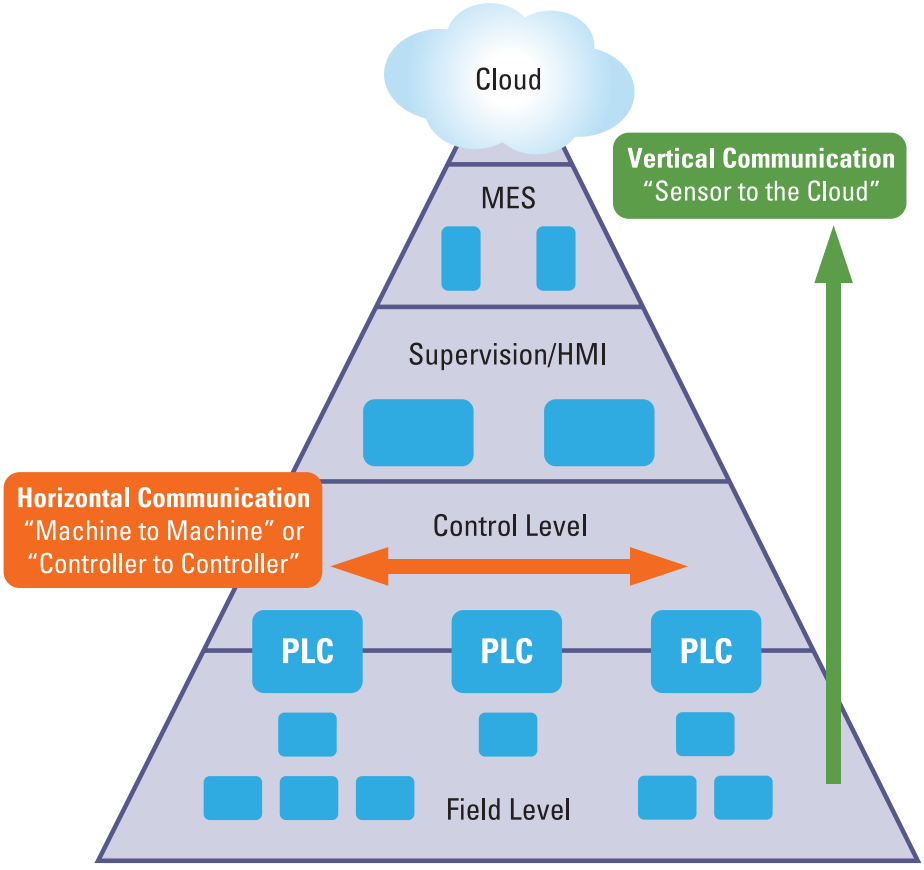
Application scenarios for Time Sensitive Networking (TSN)

TSN is an important building block in meeting the targets set for Industry 4.0. But TSN-based solutions have not yet really arrived in the portfolio of automation companies. The reason for this lies in the current discrepancy between the actual goals of TSN introduction and those currently achieved.

TIME SENSITIVE NETWORKING (TSN) has become well established in the vocabulary of the automation industry. All leading companies in this market have started activities for evaluation or even for the introduction of TSN. But what are the goals for application of TSN technology in industrial and process automation and what has already been achieved today that can be used concretely by customers? What is still missing?

Many manufacturers, consortia and TSN testbeds are exhibiting TSN demonstrators showing concrete applications of this new technology with components already available today. For example, Renesas is demonstrating a Profinet PLC with IO-Link master connection via TSN based on a current chip. Depending on the requirements to be fulfilled, the implementation of such TSN-based solutions based on available hardware is rather simple.

Protocols such as Profinet or Ethernet/IP can utilize TSN just by extending the Ethernet Layer 2 and without interfering with the higher protocol layers. Scheduled traffic is the most common method here, because this mechanism has already been sufficiently tested and widespread in industrial automation. Well-known systems such as EtherCAT, Profinet IRT or SERCOS III are successfully using this method, which was generalised in the course of TSN development, for years. However, TSN-based solutions have not yet really arrived in the portfolio of automation companies. The reason for this lies in the current discrepancy between the actual goals of TSN introduction and those currently achieved.



SOURCE: RENESAS

Automation pyramid and consistency.

The goals

TSN is an important building block in meeting the targets set for Industry 4.0. The technology has the potential to break down the boundaries that currently exist between proprietary real-time solutions by establishing a unified standard. This makes data sharing within individual sections of a production facility simpler and transparent. Different domains can share information directly via a uniform network infrastructure, without the need for gateways or other adaptations (horizontal communication).

As an example, machines from different manufacturers can be flexibly combined into production lines or exchanged between different domains without having to consider communication standards that are still incompatible today. In addition, customers can implement the complete continuity of the information flow in the vertical direction, in a "Sensor to the Cloud" manner that enables new business models.

A further objective is the standardisation of automation equipment and its components, which will reduce the cost of developing, manufacturing and stocking spare parts, as well as the maintenance of the production facility. Specialists personnel in design and maintenance can be deployed more flexibly, warehousing for spare parts is limited to one device type and standardised hardware components become cheaper due to the resulting higher quantities.

Requirements

This abstract goal allows for several possible solutions, which differ particularly in the lowest level of the automation pyramid. Basically, we can distinguish between coexistence and compatibility. Coexistence or convergence means that devices can share a common network segment and communicate over it without affecting each other. Compatibility means that in addition devices can "understand" each other, i.e. share information among themselves.

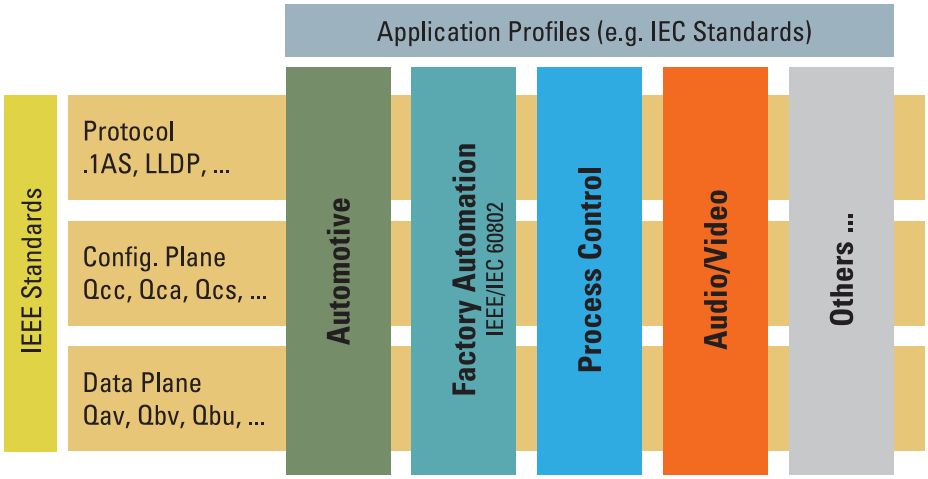
The real-time networks available today are predominantly neither coexistent nor compatible with each other. TSN as a uniform network standard can meet the demand for coexistence. In fact, IEEE only develops horizontal network standards that describe basic functions.

For example, for "Scheduled Traffic" (IEEE802.1Qbv-2015, now adopted in IEEE802.1Q-2018), only the principle and mechanisms are defined for controlling the transmission times of Ethernet packets. However, a concrete application requires

specific definitions, such as the cycle time, the concrete sequence of the time intervals, the definition and handling of the priority classes, the type and method of network administration and much more. This represents the application-specific profile or vertical standard. Without this agreement, different devices that use TSN mechanisms differently would still not be able to coexist in a heterogeneous network. Consequently, TSN-based networks would be fragmented again. Even the use of the same semiconductor chips might be inefficient in this case if the hardware requirements of the profiles differ too much.

Since 2018, a joint working group IEEE/IEC60802 has been dealing with this problem. Its task is to define a uniform TSN profile for Industrial Ethernet applications and to close any gaps in the IEEE specifications. The success of this working group, to which many experts and consortia are contributing, will make the interoperability of future industrial TSN applications take a decisive step forward. The profile is expected to be adopted in 2021.

The second aspect of the Industry 4.0 objectives concerns the compatibility of automation devices. In addition to coexistence in the same network, this also requires a common language and similar management and planning of the automation application ("engineering"). The common language has already been found. This is OPC-UA pub/sub, the real-time extension of the established OPC-UA standard. At SPS IPC Drives 2018, a new initiative was announced to define a uniform OPC-UA pub/sub-based fieldbus standard under the umbrella of the OPC Foundation, in which all leading manufacturers participate in the same way as to IEEE/IEC60802.



SOURCE: RENESAS

Horizontal and vertical standards.

OPC-UA pub/sub enables real-time communication at the level of established protocols with cycle times of less than 1 ms, such as Profinet or EtherNet/IP. OPC-UA pub/sub uses multicast frames that a publisher sends cyclically to one or more subscribers. This enables real time connections down to the machine level (controller to controller).

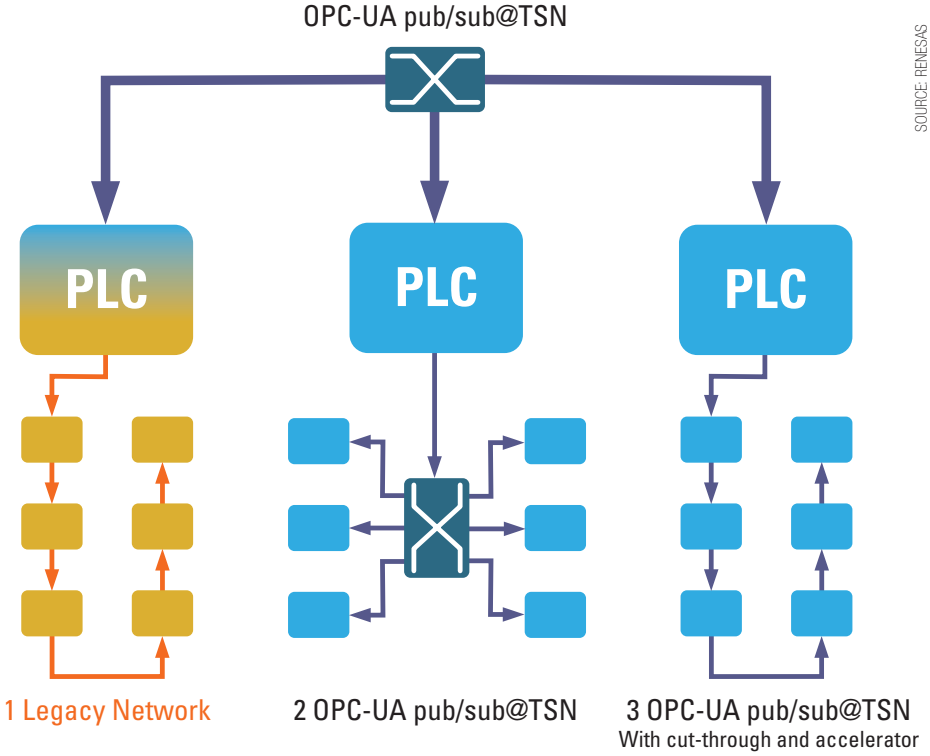
At the lowest level of the automation pyramid, the field level within a machine or production unit, smaller cycle times of less than 100 µs are sometimes required. In its classic form, the Publisher-Subscriber process cannot be used to implement longer device chains with these cycle times, as is the case with EtherCAT or SERCOS III, for example. In practice, there are three possible solutions.

The PLC at the lowest control level communicates only with the higher layers via the TSN network and OPC UA-pub/sub protocol, so that interoperability between system parts or machines is simplified. Communication at field level continues to be based on established standards. The advantages are the proven technology and devices at field level, so new developments are not necessary. However, as before, the field level will not be connected transparently, and support for "Sensor to the Cloud" remains complex.

The current line structure is being avoided and flatter hierarchies are being increasingly adopted in order to reduce the number of switches to be passed from the PLC to the most distant field device. Depending on the application, this increases the cabling effort and requires a larger number of switches. On the other hand, end devices no longer need an integrated switch. The PLC then must evaluate a large number of short Ethernet frames within the network cycle instead of an aggregated frame. The performance of the network stack is particularly critical here.

For OPC-UA pub/sub, field devices use familiar mechanisms such as aggregated frames and data sharing during cut-through to support very short cycle times. It will be crucial that this concept can be applied consistently within the standards currently under discussion. The replacement of a proprietary standard by a new one with comparable performance would be difficult to justify.

Whichever technical solution will ultimately prevail, network administration and engineering will always remain a major challenge. With the activities ongoing in IEEE/IEC60802 and the OPC-UA Foundation, the chances have greatly increased for the hoped-for Industry 4.0-capable overall solution for a uniform, real-time TSN network.



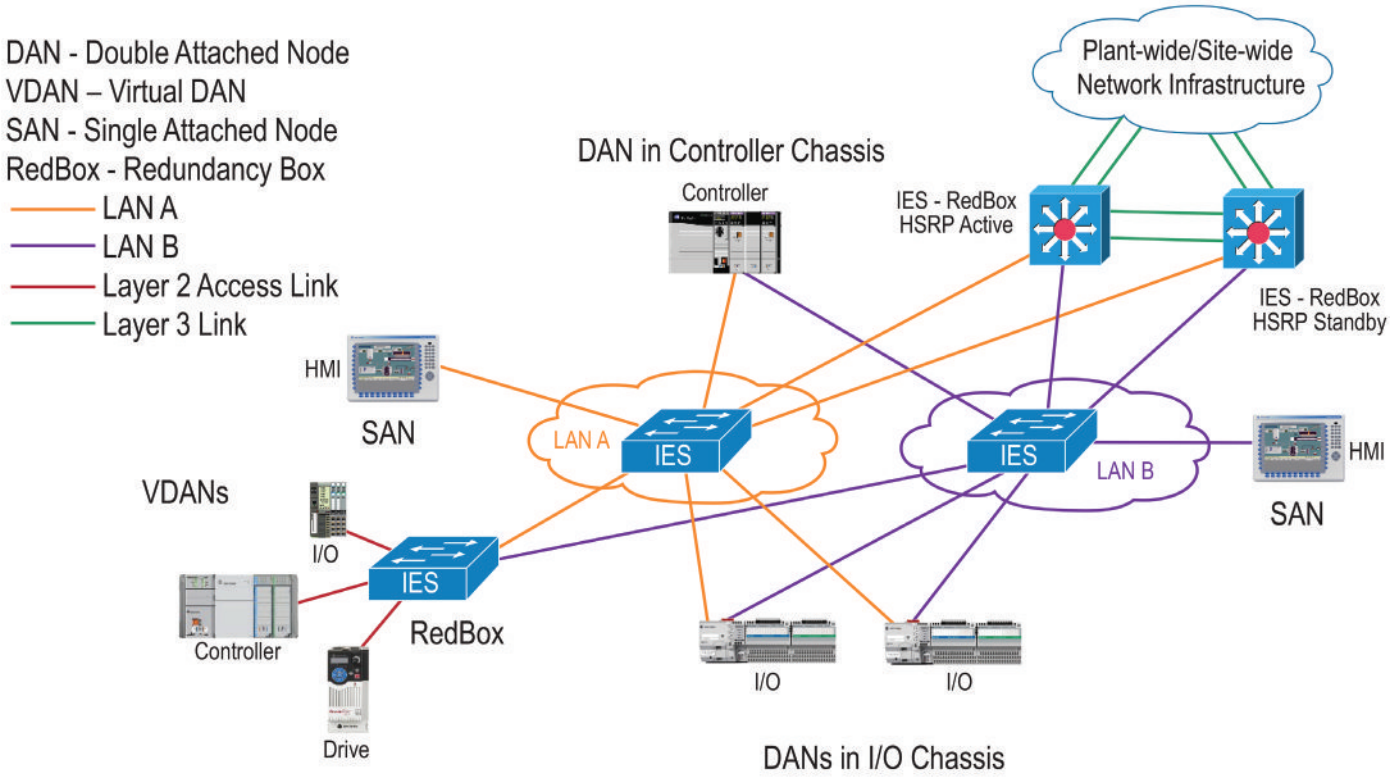
SOURCE: RENESAS

Solution variants for field level. At least initially, all three variants will probably find application.

Arno Stock, ***Renesas Electronics.***

Parallel Redundancy Protocol in CPwE Ethernet architecture

The Parallel Redundancy Protocol (PRP) is a standard defined in IEC 62439-3, and is adopted in the EtherNet/IP specification. PRP technology creates seamless network redundancy by allowing PRP-enabled IACS devices to send duplicate Ethernet frames over two independent Local Area Networks (LANs).



SOURCE: ROCKWELL

One of the challenges facing industrial operations is the industrial hardening of standard Ethernet and IP-converged IACS networking technologies to take advantage of the business benefits associated with IIoT. A high-availability network architecture can help to reduce the impact of a network failure on a mission-critical IIoT IACS application.

THE PREVAILING TREND IN INDUSTRIAL Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, through the use of standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A highly-available converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

Business practices, corporate standards, policies, industry standards, and tolerance to risk are key factors in determining the degree of resiliency and application availability required within an IACS plant-wide or site-wide architecture, e.g., non-resilient LAN, resilient LAN, or redundant LANs. A highly-available network architecture within an IACS application plays a pivotal role in helping to minimize the risk of IACS application shutdowns while helping to maximize overall plant or site uptime.

A holistic resilient plant-wide or site-wide network architecture is made up of multiple technologies (logical and physical) deployed at different levels within the plant or site. When selecting a resiliency technology, various plant or site application factors should be evaluated, including the physical layout of IACS devices (geographic dispersion), recovery time performance, uplink media type, tolerance to data latency and jitter, and future-ready requirements.

For more information on resiliency technology, refer to Deploying a Resilient Converged Plantwide Ethernet Architecture (CPwE Resiliency) Design and Implementation Guide (DIG).

Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture (CPwE PRP) Design and Implementation Guide outlines several use cases for designing and deploying PRP technology with redundant network infrastructure across plant-wide or site-wide IACS applications. CPwE PRP is an extension to CPwE Resiliency and was architected, tested and validated by Cisco Systems and Rockwell Automation with assistance by Panduit.

CPwE Overview

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures were architected, tested and validated to provide design and implementation guidance, test results, and

documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

- *Smart IIoT devices:* Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP)
- *Zoning (segmentation):* Smaller connected LANs, functional areas, and security groups
- *Managed infrastructure:* Managed Allen-Bradley Stratix industrial Ethernet switches (IES), Cisco Catalyst distribution/core switches, FactoryTalk Network Manager software, and Stratix industrial firewalls
- *Resiliency*: Robust physical layer and resilient or redundant topologies with resiliency protocols
- *Time-critical data:* data prioritization and time synchronization via CIP Sync and IEEE-1588 Precision Time Protocol (PTP)
- *Wireless:* Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- *Holistic defense-in-depth security:* Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (e.g., OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- *Convergence-ready:* Seamless plant-wide or site-wide integration by trusted partner applications

PRP use cases

An industrial automation control system is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, pulp and paper, oil and gas, mining, and energy. IACS applications are made up of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations.

One of the challenges facing industrial operations is the industrial hardening of standard Ethernet and IP-converged IACS networking technologies to take advantage of the business benefits associated with IIoT. A high-availability network architecture can help to reduce the impact of a network failure on a mission-critical IIoT IACS application.

Parallel Redundancy Protocol (PRP) is a standard defined in IEC 62439-3 and is adopted in the ODVA, Inc. EtherNet/IP specification. PRP technology creates seamless network redundancy by allowing PRP enabled IACS devices to send duplicate Ethernet frames over two independent Local Area Networks (LANs). If a failure occurs in one of the LANs, traffic continues to flow through the other LAN uninterrupted with zero recovery time.

An IACS device enabled with PRP technology has two ports that operate in parallel and attach to two independent LANs, e.g., LAN A and LAN B. This type of IACS device is known as a PRP double attached node (DAN). During normal network operation, an IACS DAN simultaneously sends and receives duplicate Ethernet frames across both LAN A and LAN B. The receiving IACS DAN accepts whichever frame arrives first and discards the subsequent copy.

IACS devices that do not support the PRP technology can utilize a PRP Redundancy Box (RedBox) to connect to the two independent LANs. The RedBox functions similarly to the DAN; a PRP enabled IES is an example of a RedBox.

IACS devices that connect to both LAN A and LAN B through a RedBox are referred to as a PRP Virtual DAN (VDAN). A single attached node (SAN) is an IACS device without PRP support that only resides on either LAN A or LAN B.

PRP supports flexible LAN topologies including linear, star, redundant star, and ring topologies. If both LAN topologies are resilient and single-fault tolerant, PRP architecture can recover from multiple faults in the network.

In contrast, other resiliency technologies are typically single-fault tolerant, are a single LAN, and utilize redundant path topologies (e.g., ring and redundant star). A resiliency protocol is used to forward Ethernet frames along one physical path while blocking the other physical path to avoid Ethernet loops. Network convergence times vary across resiliency technologies. Convergence time disruption is defined as the time it takes to discover a failure (e.g., link or device) along a path, unblock the blocked path, then start forwarding Ethernet frames along that unblocked path. For example, the convergence time for the ODVA, Inc. Device Level Ring (DLR) protocol standard is 3 ms.

CPwE PRP outlines the concepts, requirements, and technology solutions for reference designs developed around a specific set of priority use cases. These use cases were tested for solution functional validation by Cisco Systems and Rockwell Automation with assistance by Panduit. This helps support a redundant converged plant-wide or site-wide EtherNet/IP IACS architecture.

The CPwE PRP Design and Implementation Guide includes:

- Parallel Redundancy Protocol technology overview
- Design and configuration considerations for plant-wide or site-wide IACS PRP deployments. Includes topology choices; RP devices (e.g., DAN, VDAN, SAN, and RedBox); distribution switch selection.
- Selection of Industrial Ethernet Switches (IES)

Resilient architecture overview

Protecting availability for IACS assets requires a defense-in-depth approach where different solutions are needed to address various network resiliency requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit and Rockwell Automation CPwE Cisco Validated Designs (CVDs) and Cisco Reference Designs (CRDs) that address different aspects of availability for IIoT IACS applications.

The Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several use cases for designing and deploying resilient plant-wide or site-wide architectures for IACS applications, utilizing a robust physical layer and resilient topologies with resiliency protocols.

The Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide outlines several use cases for designing and deploying DLR technology with IACS device-level, switch-level, and mixed device/switch-level single and multiple ring topologies across OEM and plant-wide or site-wide IACS applications.

Summary

CPwE is a collection of architected, tested, and validated designs. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site-wide industrial network infrastructure.

CPwE can also help industrial operations and OEMs achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology.

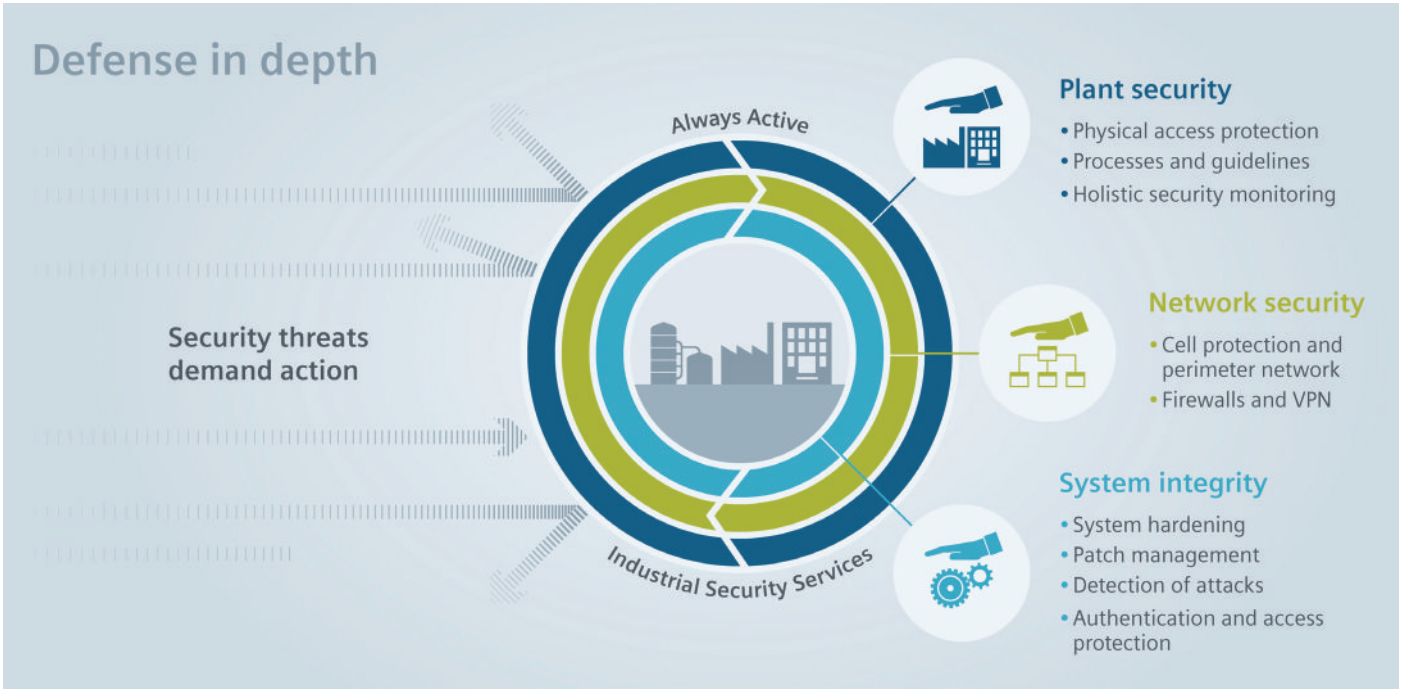
The Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Design and Implementation Guide outlines several use cases for designing and deploying PRP technology and topologies throughout a plant-wide or site-wide Industrial Automation and Control System (IACS) network infrastructure.

CPwE PRP highlights the most important industrial automation control system application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases and applications using the CPwE framework.

*Technology report by **Rockwell Automation, Cisco and Panduit.***

Network management enables greater network security

A modern network management system is an important part of maintaining plant availability in threat situations, as part of defense-in-depth in conjunction with firewalls and other security components. Especially against increasing cyberattacks, a network management system can deliver a decisive advantage.



SOURCE: SIEMENS

The defense in depth concept relies on comprehensive and effective protection against cyberthreats through various measures and mechanisms on multiple levels. Transparency and detailed information about the participants of a network are key factors in order to deploy security measures effectively and in a targeted fashion.

EACH SECURITY UPDATE IS FOLLOWED by new software vulnerabilities, and each protective mechanism by new attack vectors. This race has existed since the first appearance of a malware, and often the question is raised how an effective protection against the "unknown" can even be established. The answer can be found in the seamless interaction of several measures.

Just a few years ago, one of the most famous malicious software worldwide made headlines with these words: "Oops, your files have been encrypted!". Although neither the nature of the threat nor the technology used was characterized by great innovation, this malware achieved notoriety within a few days.

Other well-known worms and viruses, such as Blaster, Sasser, or MyDoom, have already caused billions in damage over 15 years ago. Even Stuxnet, which kept operators of industrial installations on their toes because of its primary infection target became widely known.

If you ask for famous malware today, many will probably recall the ransomware WannaCry. And this despite the fact that other worms either infected significantly more devices, caused greater economic damage, or employed even more sophisticated attack vectors. So, what was different? What helped WannaCry reach such prominence?

The answer to this question is quite complex. Crucial aspects were probably the rapid spreading and the type of devices infected. Within just a few hours, the ransomware spread across many computer systems in over 150 countries and encrypted the data stored on them.

As not only private users and industrial companies were affected, but also public facilities such as hospitals or display boards in long-distance traffic, this incident unforgivingly exposed the vulnerability of our networked infrastructures.

And although its spreading could be stopped relatively quickly, the negative connotation of those easily attacked systems and fears of new, perhaps even more effective, threats remained. But how can one effectively protect oneself against new, still unknown attacks?

Defense in depth

Certainly, the most important step is to also address cybersecurity in industrial environments and to lose the fear of the "unknown." Thus, with professional support, an effective approach to more security can be established via so-called defense in depth. The principle behind it states that a wide range of different, independently working protective measures should be utilized to fend off a possible attack. With these, the attack is either to be stopped immediately or enough time should be gained collaboratively for appropriate countermeasures to be taken. If also the automation components already sufficiently account for security aspects during their development phase, the concept can be anchored to a solid foundation. For this reason, the secure product life cycle in accordance with IEC 62443 is a fixed and certified component of the development process at Siemens Digital Industries. Since these process requirements and the concept of defense in depth – including prevalent mechanisms such as firewalls or further

SOURCE: SIEMENS

With a cell protection concept and by using industrial security appliances, individual production areas can be effectively separated from the plant network and protected.

applications for attack detection – are already extensively described in the IEC 62443 standard or relevant literature, a detailed listing of these possibilities will be omitted at this point. The focus is instead placed on a scenario that shows which additional means can be used to protect production systems from new, previously unknown attack waves.

Although it can be speculated about all possible attack vectors and exploitable vulnerabilities today, some aspects of the chronological sequence of most attack waves continue to follow a familiar pattern. After the first infections have surprisingly struck, security experts worldwide become active.

They begin to analyze the behavior and functioning of the malware as quickly as possible and initiate effective countermeasures. These range from, for example, initial recommendations for containing infected systems to new signatures for virus scanners or deep packet inspection firewalls to security updates for affected user programs.

However, as those specific countermeasures can only be rolled out after the malware has been detected and analyzed, the existing defense in depth measures continue to be relied on to ward off the initial infection.

Before the attack pattern changes, as is common with so-called polymorphic attacks, or if, despite preventive protective mechanisms, an infection of individual systems has occurred, local propagation paths must be suppressed, and vulnerabilities exploited be permanently closed. In both instances, the use of a centralized Network Management System (NMS) exhibits clear advantages and helps to achieve the required transparency in the network.

Identify vulnerabilities

After the first analyses by the security experts, well-known product manufacturers such as Siemens publish corresponding security alerts that inform whether products are affected by a vulnerability.

As the first step, with the aid of the network management system, the assets – the components and participants of the network – can be listed with little effort and compared with the information of the security alerts.

In the case of possible matches, further containment measures can now be taken in the production network until security updates by the product suppliers for the affected components become ultimately available.

The identified, vulnerable components must be especially protected from the threat by limiting the spreading of the malicious software over open ports of various protocols and network services in the local network. Consequently, the next step would be to block those protocols and network services via firewalls.

While this procedure can be implemented relatively effortlessly at the zone transition from the office to the production environment, the cell firewalls already present a certain complexity.

The additional rules must be applied to many firewalls and may only be activated temporarily or not at all for some cells so as not to influence the production process. If, as a further measure within an emergency policy, secondary systems such as archiving servers are to be temporarily disconnected completely from the plant network by deactivating entire interfaces in addition to the ports at the switch or router, the extent of the complexity quickly becomes apparent.

Combining firewall and network management into a single system then offers the user simple and flexible options for limiting the communication relationships between the network cells and for keeping the production running, e.g., with limited diagnostic or access options.

Security updates

SOURCE: ANALOG DEVICES

For a sustainable protection, the vulnerable components must ultimately be permanently protected from this specific threat. To do so, the software and firmware updates provided by the manufacturers must be installed in a timely manner. Depending on the network and system architecture, this can already be done during operation or a maintenance cycle within the production department.

In both cases, this can be associated with enormous effort. For computer systems in closed domains, therefore, a central variant via so-called update servers has established itself. To take advantage of these qualities with industrial infrastructure components such as switches, routers or firewalls, a central network management is required once again, with which firmware updates can be centrally deployed.

Once the vulnerability has been remedied on all components, the previously activated restrictive firewall rules as well as the decoupled systems can be restored to normal operation. The entire production network can then be used to the full extent again as usual with data archiving or further diagnoses. Reflecting the knowledge gained on the spreading of WannaCry, one very clearly recognizes the potential of a network management system.

While the initial infection would not have been prevented, the spreading in the local area network could have been sufficiently contained until the existing security update would have been deployed on the vulnerable systems.

A modern network management system is therefore not just for purely administrative or diagnostic purposes. Rather, it also helps to maintain plant availability in threat situations as part of defense in depth in conjunction with firewalls and other security components. Especially against the background of continuously increasing cyberattacks and constantly varying attack scenarios, a network management system can deliver the decisive advantage.

As a competent partner for industrial communication and Industrial Security, Siemens provides comprehensive consulting services, integrated solutions, and end-to-end concepts to prepare production networks against future threats.

Peter Schönemann, System Management Industrial Security, ***Siemens.***

Securing OT networks with unidirectional gateways/diodes

Data diodes offer a hardware-enforced solution to defend OT networks and safety systems, using one-way flow of data without allowing returning threats. As always, defensive strategies must still combine people, processes, and technology all working together to support OT network security.

CYBERSECURITY INTRUSIONS INTO OT (Operational Technology) networks, from malevolent groups are gaining more and more attention. Attacks against safety and critical systems are a growing concern and solutions to secure these systems are becoming critical. Ensuring the safety and availability of these networks are paramount in protecting our modern way of life.

There are mitigations to protect such systems, and this article will present a potential solution leveraging the use of Unidirectional Gateways and Data Diodes.

OT (Operational Technology) networks, also referred to as ICS (Industrial Control Systems) are a unique environment that houses and control systems critical to our modern way of life. OT security engineers have the unique responsibility of maintaining, protecting and securing critical safety systems and infrastructure.

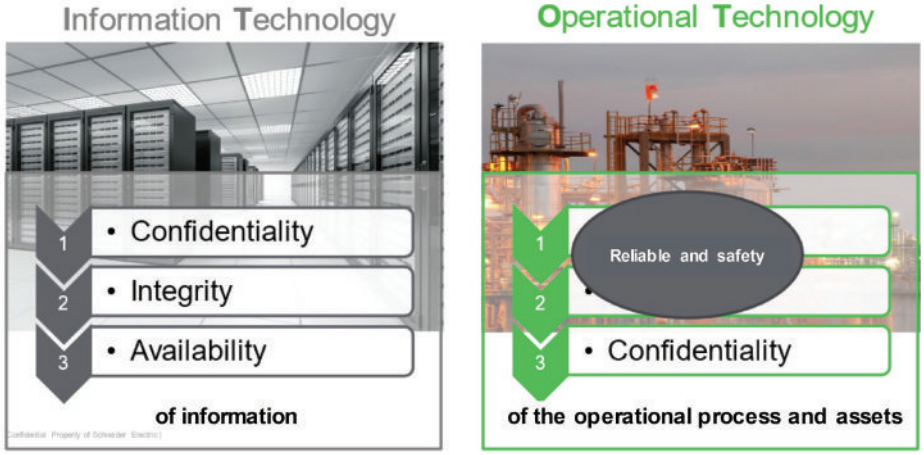
These systems provide comfort, convenience, and functionalities for a high standard of living. Media headlines describing the Ukraine Power Grid attack, the cyber-attack against a German steel mill where serious damages were incurred are illustrations of the need to secure safety systems, devices, and OT networks.

Traditional Information Technology networks or IT use the paradigm of Confidentiality, Integrity, and Availability. The OT world is primarily concerned with safety and reliability.

Unlike IT systems, rebooting a PLC (Programmable Logic Controller) that is controlling and monitoring the protection of a nuclear reactor could cause serious safety issues if an unscheduled reboot were to occur. Such use cases are not realized in IT environments.

Firewalls and routers with properly configured ACLs (Access Control Lists) are widely used to support a defense-in-depth strategy in both OT and IT networks. However, firewalls can be circumvented due to incorrect or badly written rules.

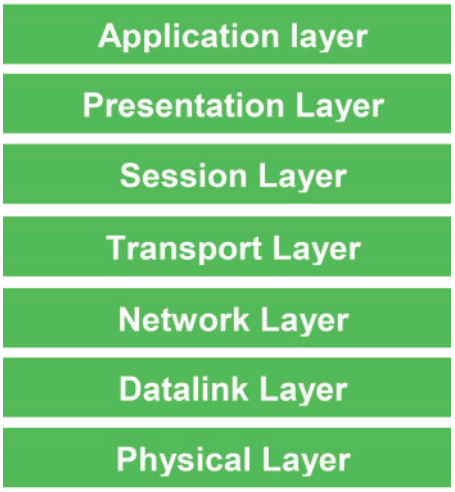
NGFWs (Next-Generation Firewalls) provide greater granularity in rule sets to filter specific applications signatures that go beyond the OSI (Open Systems Interconnection) model layers 3 and 4. They also include anti-virus protection, intrusion detection prevention systems, URL filtering and important proxy capabilities.



SOURCE: SCHNEIDER ELECTRIC

Automation pyramid and consistency.

OSI Model



The seven layers of the OSI model.

The OSI model is a conceptual model developed by the International Organization for Standardization demonstrating a standard for computer and networking communications. The OSI model is a conceptual model developed by the International Organization for Standardization (ISO) demonstrating a standard for computer and networking communications.

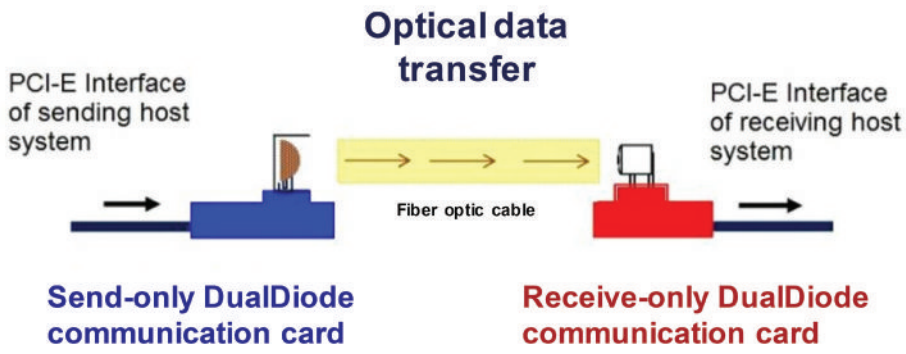
Physical layer: This layer provides electrical functions whereby mechanical and electrical functions can be enabled or disabled. This layer includes copper and optical cabling. The physical layer translates communications requests from the datalink layer to the hardware operations affecting the electronic transmission and reception of these signals.

Datalink layer: The datalink layer is responsible for handling issues resulting from bit error transmissions. The layer makes sure that data flows without overwhelming the sending and receiving components on the network. This layer also sends transmission data to Layer 3 (Network layer) to be routed. It moves data into and out of a physical link in a network. The Media Access Control (MAC) and Logical Link Control (LLC) are sublayers within the datalink layer.

Network layer: Layer 3 is where routing takes place. The routing of network protocols allows for packet communications across multiple networks. ICMP (Internet Control Message Protocol), OSPF (Open Shortest Path First), and RIP (Routing Information Protocol) are a few examples of protocols operating at the network layer.

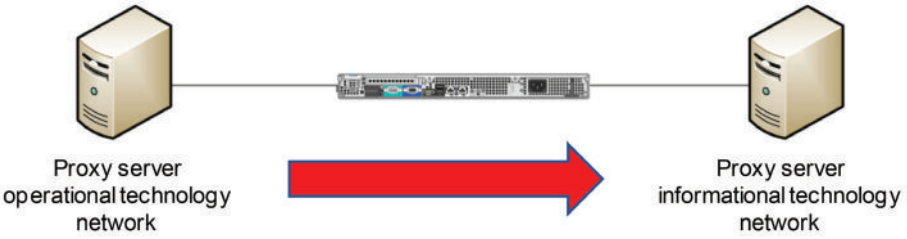
Transport layer: This layer provides the transfer of data and communication services for applications. Some of the protocols found in the transport layer are TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ATP (AppleTalk Transaction Protocol), and FCP (Fiber Channel Protocol).

Session layer: The session layer provides the network mechanism that opens and closes mapping communication sessions for applications and processes. Examples of protocols used in this layer are NetBIOS (Network Basic Input/output System, RPC (Remote Procedure Call Protocol), PPTP (Point-to-Point Tunneling Protocol), and PAP (Password Authentication Protocol).



SOURCE: SCHNEIDER ELECTRIC

Data diodes provide a level of security stronger than other network appliances, such as firewalls.



Example of a Data Diode placed between an OT and IT proxies.

Presentation layer: The presentation layer provides for the conversion of data, encryption, decryption, compression, and character code transition. Protocols include Telnet, NDR (Network Data Representation), X.25 Packet Assembler/Disassembler Protocol, AFP (Apple Filing Protocol), and LLP (Lightweight Presentation Protocol).

Application layer: The application layer provides support for applications and end-user processes. Layer 7 protocols include FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), and SMTP (Simple Mail Transfer Protocol), HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure), NFS (Network File System), POP (Post Office Protocol), SSH (Secure Shell), NTP (Network Time Protocol), and RDP (Remote Desktop Protocol).

Application layer attacks

Attacks against the application layer can come via web browsers, software applications, and email clients. If application signature updates on NFGWs are not properly maintained, attackers can exploit such vulnerabilities before developers can create a patch. Zero-day attacks find flaws in applications such as this. Some examples of famous zero-day attacks are Stuxnet, Sony Zero-Day Attack, and the DNC hack to name a few.

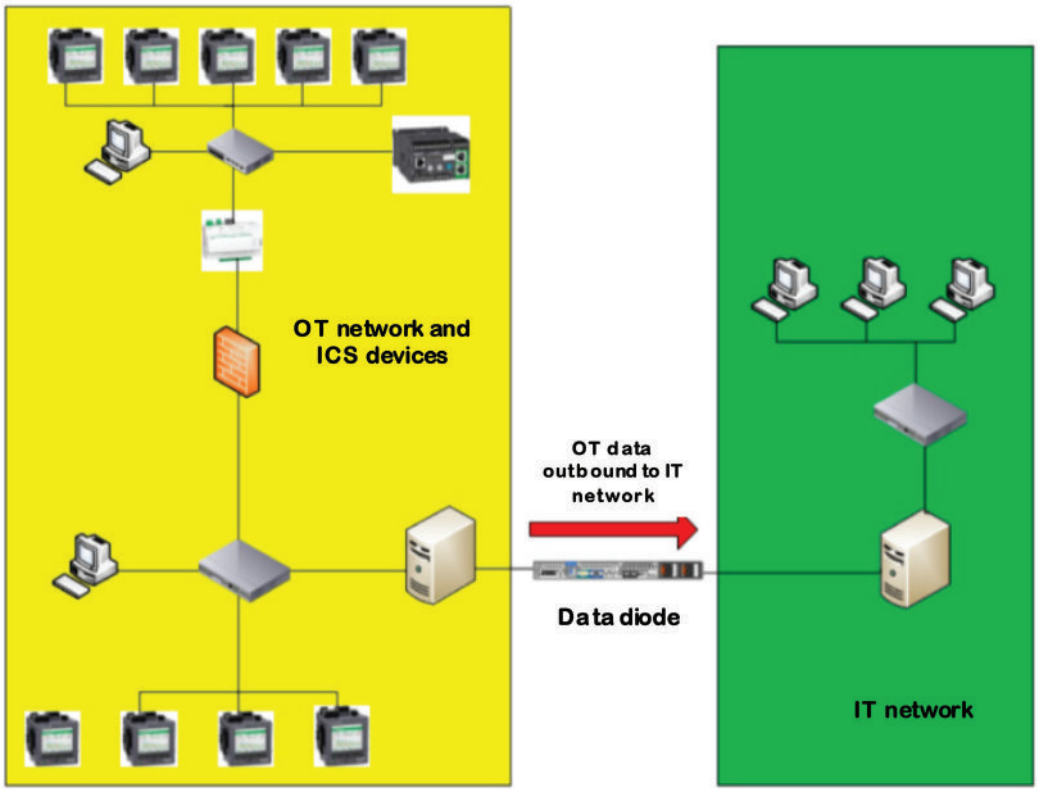
Firewalls, routers, intrusion detection, and intrusion prevention systems do provide a certain level of protection for networks and network subnets and are a key component in a defense-in-depth strategy as well as securing zones and conduits for OT networks.

The air gap theory between OT and IT networks is at best a myth. More and more OT networks are being connected to IT networks and once that connection is made, the security and impact on safety systems on the OT side have been eroded. The 2015 cyber-attack against the Ukrainian Power Grid demonstrated how the attackers got into the IT network, and from there entered into the OT network resulting in the de-energization of half the Ivano-Frankivisk region.

The attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies. They demonstrated the capability to gain a foothold and harvest credentials and information to gain access to the ICS network. Additionally, the attackers showed expertise, not only in network connected infrastructure, such as Uninterruptable Power Supplies (UPSs), but also in operating the ICSs through supervisory control system, such as the Human Machine Interface (HMI).

Finally, the adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-Ethernet convertors, inoperable and unrecoverable. In one case, the attackers also used telephone systems to generate thousands of calls to the energy company's call center to deny access to customers reporting outages.

However, the strongest capability of the attackers was not in their choice of tools or



SOURCE: SCHNEIDER ELECTRIC

Example of a Data Diode placed between OT and IT networks.

Firewall properties	Data Diode properties
Configurable software to enforce security via policies	Hardware device enforcing the one-way flow of data via the physical layer from the OSI model. No policies required to operate
Bi-directional or one-way via software	One-way only hardware enforced
Network-based administration	Local authentication
Routable to other destinations across a network	Communications are configured locally at local administrator's discretion, i.e., one-way direction
Constant maintenance of rules and updates required	No updates for rules or software patching required

in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multi-site attack.

Unidirectional gateway/ data diode

NIST (National Institute of Standards and Technology) describes the following: "A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction."

Unlike firewalls, routers and layer 3 switches, data diodes prevent return communications over the physical layer (Layer 1) of the OSI model. An example of a high-level illustration shows the internal mechanism of a data diode where the traffic entering the device from the OT side converts data from copper to the optical fiber. The device then sends the data to the IT side and reconverts that data from the optical fiber to copper then sends it out to the IT network.

Data diodes provide a level of security stronger than other network appliances, such as firewalls. These devices are configured to allow traffic to be transmitted one way only. The following table illustrates some of the differences between firewalls and data diodes.

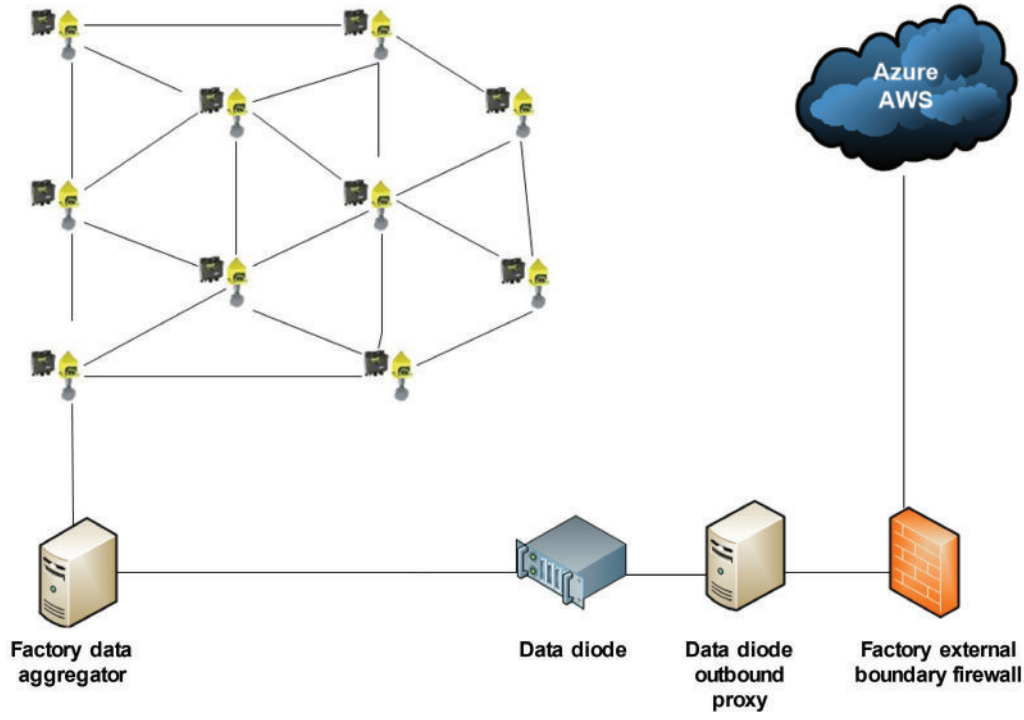
Data diodes can use a combination of hardware and proxy computers running software on the source and destination networks. Most manufacturers of data diodes support the writing of customized software for various SCADA applications to allow specific information to go through the data diode. The hardware portion of the data diode enforces the direction, for example allowing traffic to travel across the data diode from the OT network to the IT Network. The software running on the proxy computers can replicate databases as well as several ICS protocols.

Data diodes can present a level of network complexity despite being a simple concept to understand. Data diodes provide defense against malevolent agents, negligent users, malware, and viruses. Before installing a data diode, a concise strategy must be incorporated. The objective can be to protect either an entire OT network or a specific safety system, for example, requiring information to be sent out to the IT network for reporting or analysis.

IIoT and Data Diodes

Data diodes can be used for securing networks requiring connectivity to the cloud. A use case requirement would be to have factory information sent to the cloud for advanced analytics, the status of production, and the uptime of process and devices. The data diode would be placed behind the boundary firewall with the outbound proxy forwarding the required information to the cloud. The outbound proxy should be configured with the proper certificates and encryption mechanism to forward the required information in a secure and authorized manner.

From the cloud, authorized personnel can view the information to make any decisions concerning factory operations. One use case, deploying sensors throughout the factory forwarding information to a data aggregator, then forwards the data through the data diode to the outbound proxy, which forwards to the cloud. The firewall is there to filter and route all traffic, with the data diode preventing any inbound traffic from the outside world into the factory.



SOURCE: SCHNEIDER ELECTRIC

Example of data diode protecting factory external boundary while forwarding data to the cloud.

Conclusion

Data diodes provide a hardware-enforced solution to defend OT networks and safety systems. They allow the one-way flow of data without allowing returning threats into the OT network or safety system.

As always, defensive strategies must still combine people, processes, and technology all working together to support OT network security.

Daniel Paillet, CISSP, CCSK, CEH,
Schneider Electric.

Enabling robust condition-based monitoring for Industry 4.0

To meet the demands of Industry 4.0, condition-based monitoring (CbM) of robotics and rotating machines, such as turbines, fans, pumps, and motors, offers a method for record real-time data related to the health and performance of machines to enable targeted predictive maintenance, as well as optimized control.

SOURCE: ANALOG DEVICES

Predicting and diagnosing a machine's health before it becomes problematic requires insights that can only come from having accurate and reliable data.

GOVERNMENT INITIATIVES, SUCH AS GERMANY'S Industrie 4.0 and China's Made in China 2025, are accelerating the trend towards ubiquitous networked automation in manufacturing. In addition, automation is being enhanced by smart sensor systems with more data available to monitor and control production processes.

In particular, Made in China 2025 aims to rapidly develop high tech industries, including electric vehicles, next-generation information technology (IT) and telecommunications, and advanced robotics and artificial intelligence. With more advanced systems there is a need for more advanced ways to ensure system reliability.

Condition-based monitoring (CbM) of robotics and rotating machines, such as turbines, fans, pumps, and motors, records real-time data related to the health and performance of the machine to enable targeted predictive maintenance, as well as optimized control. Targeted predictive maintenance, early in the machine life cycle, reduces the risk of production downtime resulting in increased reliability, significant cost savings, and increased productivity on the factory floor.

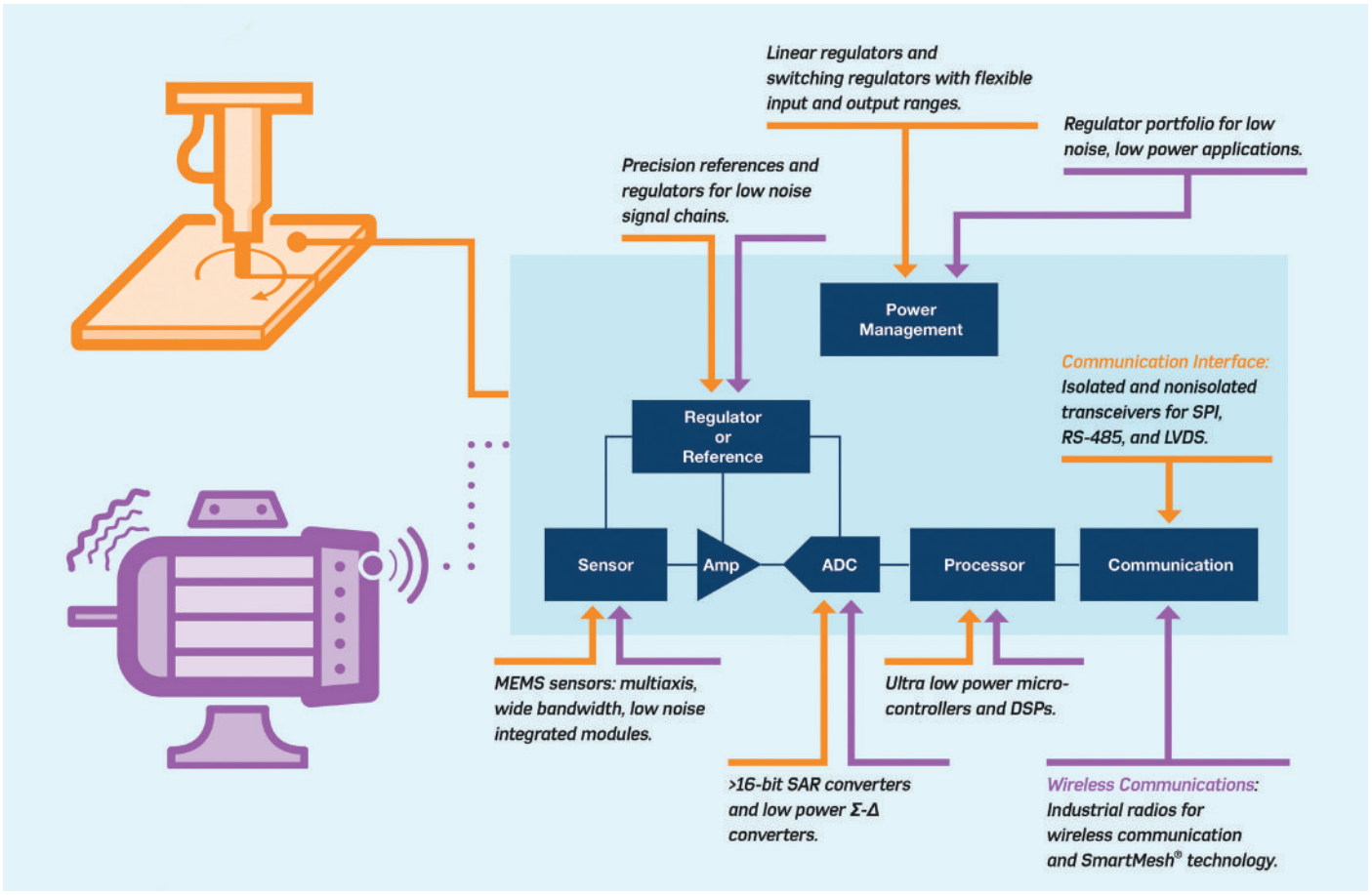
Condition-based monitoring

Condition-based monitoring of industrial machines can utilize a range of sensor data, such as electrical measurements, vibration, temperature, oil quality, acoustic, and process measurements such as flow and pressure. However, vibration measurement is the most common by far, as it can provide the most reliable indication of mechanical issues such as imbalance and bearing failure. This article focuses on the use of vibration sensing, but the methodology is equally applicable to data from other sensors.

The transmission means of the sensor data from the sensing node to the main controller or the cloud is highly dependent on applications. In many applications, some local data processing is implemented at the edge node, with summary data being subsequently transmitted wirelessly to a network gateway, or directly via a cellular link to the cloud or analytics server. In these situations, the amounts of data transmitted are typically rather low, and there is often a requirement for low power as the edge node can be battery powered.

In other applications, raw sensor data transmission is required. For example, aligning and fusing data from multiple sensors may be required prior to analysis. Raw data transmission is also required in applications where data is utilized for real-time control. In these applications, a wired interface is a more likely solution for data transmission.

CbM of industrial applications can leverage Analog Devices' optimized signal chain of Micro-ElectroMechanical Systems (MEMS) accelerometers, low power microcontrollers, and wired iCoupler isolated interfaces to



SOURCE: ANALOG DEVICES

Wireless Signal Chain Example for Motor Monitoring: *Monitoring of factory equipment in difficult to access locations requires wireless solutions that eliminate the need for extra cables while providing critical information over a robust wireless link. Low power components coupled with high performance sensors in compact form factors create new condition monitoring opportunities for a wide variety of factory applications, while minimizing the complexities of integrating into existing and new factory equipment.*

extract, condition, and reliably communicate machine health data from a remote CbM slave back to a master controller for analysis. Over time, machine health data can be used to create software-based models to determine changes in machine behavior and proactively maintain machine health. In some applications, such as CNC machines, the data can also be used to optimize the performance of the system in real time.

The challenges with implementing a wired CbM interface include EMC robustness when operating over long cables, data integrity with transmitting at a high baud rate (for real-time CbM data streaming), and communication physical layer/protocol mismatches. Analog Devices' signal chain and system-level expertise provides several possible options to implement a wired CbM interface.

RS-485/RS-422 design solutions

Wired interface solutions reduce customer design cycle and test time, and enable faster time to market for industrial CbM solutions. Several aspects for discussion include selecting a suitable MEMS accelerometer and physical layer, as well as EMC performance and power design. Potential design solutions include performance trade-offs. This article focuses on design considerations for SPI to RS-485/RS-422 design solutions.

Common challenges in implementing a wired physical layer interface for MEMS include managing EMC robustness and data integrity.

However, when extending a clock synchronized interface such as SPI over long RS-485/RS-422 cables, along with combining power and data on the same twisted pair wires (phantom power), several additional challenges are presented. This article discusses the following key considerations and provides recommendations for designing the physical layer interface:

- Managing system time synchronization
- Data rate vs. cable length recommendations
- Filter design and simulation for shared power and data architectures
- Passive component performance trade-offs for phantom power implementation
- Component selection and system design window
- Experimental measurements

Time Synchronization/Cable Length

When designing an SPI to RS-485/RS-422 link, the cable and components affect system clock and data synchronization. Over a long cable run, the SCLK signal will incur a propagation delay through the cable, approximately 400 ns to 500 ns for a 100 m cable. For a MOSI data transfer, the MOSI and SCLK are equally delayed by the cable.

However, data sent from the slave MISO to the master will be out of sync with the SCLK by twice the cable propagation delay. The maximum possible SPI SCLK is set by the system propagation delay, which includes cable propagation delay as well as master and slave component propagation delays.

System propagation delay can lead to inaccurate SPI MISO sampling at the SPI master. For a system without an RS-485/RS-422 cable, MISO data and SPI SCLK will be synchronized with little or no delay. For a system with a cable, MISO data at the SPI slave is out of sync with SPI SCLK by one system propagation delay.

MISO data arrives back at the master out of sync by two system propagation delays. As data is shifted right due to cable and component propagation delays, inaccurate data sampling occurs.

To prevent inaccurate MISO sampling, one may reduce the cable length, lower the SPI SCLK, or implement an SPI SCLK

compensation scheme (clock phase shift) in the master controller. Theoretically, the system propagation delay should be less than 50% of the SCLK clock period for error free communication, and in practice a limit of system delay of 40% SCLK can be used as a general rule.

An SPI SCLK vs. cable length guideline for the two SPI to RS-485/RS-422 designs is needed. The non-isolated design uses Analog Devices' high speed EMC robust and small form factor RS-485/RS-422 devices (ADM3066E and ADM4168E). The isolated design also includes Analog Devices' iCoupler signal and power isolated ADuM5401 device, which provides additional EMC robustness and noise immunity for SPI to RS-485/RS-422 links. This design adds additional system propagation delay, which limits operation at higher SPI SCLK rates.

Over longer cable runs (greater than 30 m) adding isolation is strongly recommended to help mitigate against ground loops and EMC events such as electrostatic discharge (ESD), electrical fast transients (EFT), and high voltage surges coupling to the data transmission cabling. When cable lengths extend to 30 m or greater, the SPI SCLK vs. cable length performance of the isolated vs. non-isolated design is similar.

Background

Phantom power combines power and data on a single twisted pair—enabling a one-cable solution between master and slave devices. Combining both data and power on a single cable enables a one-connector solution at space constrained edge sensor nodes.

Power and data are distributed on a single twisted pair using an inductor capacitor network integrated into the design. High frequency data is coupled to the data lines through series capacitors, which also protect the RS-485/RS-422 transceiver from dc bus voltages.

High-Pass Filter

For the purposes of this article, it is assumed that the phantom power inductor-capacitor network is added to two wires, which route the RS-485/RS-422 conversion of the SPI MISO signal. The filter circuit is high pass, and requires that the data signals being transmitted do not have content at dc or at very low frequencies.

Using a second-order high-pass filter circuit, the voltage output at the transmitting RS-485/RS-422 device is noted as VTX, with R1 15 Ω output impedance. The R2 30 kΩ is a standard input impedance for the receiving RS-485/RS-422 device. Inductor (L) and capacitor (C) values can be selected to suit the desired system data rate.

When choosing the inductor (L) and capacitor (C) values, the maximum RS-485/RS-422 bus voltage droop and droop time need to be considered. Standards exist, such as single twisted-pair Ethernet, which specify the maximum allowable voltage droop and droop time.

For some systems the maximum permissible voltage droop and droop time may be larger, limited by the signal polarity crossover point. The voltage droop and droop time can be used paired with a simulation to determine the system high pass frequency.

When adding phantom power to an SPI to RS-485/RS-422 communication system, it is clear that the minimum possible SPI SCLK rate will be limited by the phantom power filter components.

To achieve reliable communication without bit errors, one need consider the minimum SPI SCLK in a worst-case scenario—for example, where all SPI MISO sampled bits are logic high.

If all sampled MISO bits are logic high, then this results in a bit rate lower than the system SPI SCLK. For example, if the SPI SCLK is 2 MHz and all 16 bits are logic high, then the phantom power LC filter network will see an equivalent SPI MISO bit rate of 125 kHz.

As noted in the section "Time Synchronization and Cable Length," longer cable lengths require lower SPI SCLK rates. However, phantom power limits the lowest possible SPI SCLK rate. Balancing these opposing requirements involves careful selection and characterization of passive filter components, particularly inductors.

Passive Component Selection

When selecting a suitable power inductor, a number of parameters need to be considered, including sufficient inductance, rated/saturation current, self-resonant frequency (SRF), low dc resistance (DCR), and package size.

The rated current needs to meet or exceed the total current requirements for the remotely powered MEMS sensor node, and the rated saturation current needs to be much larger.

The inductor will not present high impedance to ac data above its quoted SRF, and at a certain point will begin to have a capacitive impedance characteristic. The chosen inductor SRF will limit the maximum SPI SCLK that can be used on the SPI to RS-485/RS-422 physical layer.

When operating over long cables the inductor SRF may not be reached; for example, reaching SPI SCLK rates of 11 MHz (part number 744043101's SRF) over 10 m of cable may not be possible. In other cases, when operating over long cables the inductor SRF may be reached for lower SPI SCLK rates (2.4 MHz, 1.2 MHz). As noted previously, when used in a phantom power filter network, an inductor will also limit the lowest possible SCLK rate.

The constraints in choosing a suitable dc voltage blocking capacitor are limited to the transient overvoltage rating and dc voltage rating of the system.

The dc voltage rating needs to exceed the maximum bus voltage bias. During a cable or connector short, the inductor currents will become imbalanced and will be dissipated by termination resistances. DC blocking capacitors need to be rated for peak transient voltages in the event of a short. For example, in lower power systems, with inductor saturation currents of about 1 A, the corresponding dc blocking capacitor should be rated to at least 50 V dc.

Design and component selection

When extending a clock synchronized interface such as SPI over long RS-485/RS-422 cables, along with combining power and data on the same twisted pair wires (phantom power), the minimum possible SPI SCLK is set by the phantom power filter components, which high-pass filter data on the SPI data line. The maximum SPI SCLK is set by either the phantom power inductor self-resonant frequency (SRF) or the system propagation delay (whichever SPI SCLK is lower in value).

Experimental Setup

A CbM evaluation system (Pioneer 1) uses SPI to RS-485/RS-422 design solutions. Pioneer 1 also includes the ADcmXL3021 wide bandwidth, low noise, triaxial MEMS accelerometer, which combines high performance with a variety of signal processing to simplify the development of smart sensor nodes in CbM systems.

The SPI to RS-485/RS-422 slave extends the ADcmXL3021 SPI output over 10 m back to the master controller for vibration data analysis in the system. The SPI to RS-485 designs use phantom power 100 µH inductors and 3.3 µF capacitors to minimize the size of the slave interface solutions, which measure 26 mm × 28 mm (excluding interface connector).

Voltages measured at the SPI master and slave, and on the RS-485/RS-422 differential voltage bus were measured using a sample application setup.

The analog signals 1 and 2 are the differential bus voltage representation of the MISO signal, as measured at the SPI slave output. The digital signal 4 shows the MISO sampled at the master controller. The MISO signal at the SPI master matches the polarity and phase of the MISO at the SPI slave, with little propagation delay.

Analog Devices has developed the Pioneer 1 wired system evaluation solution to support the ADcmXL3021 triaxial MEMS accelerometer. The Pioneer 1 evaluation kits can also support MEMS devices with the help of the expansion board described in the wiki guide.

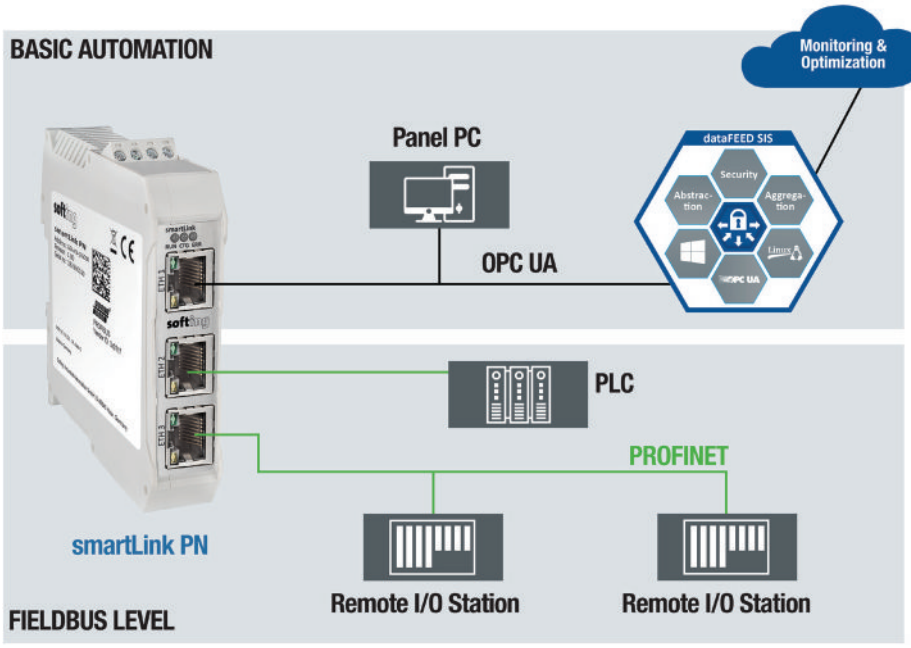
Richard Anslow and Dara O'Sullivan, ***Analog Devices, Inc.***

Smart devices leverage PROFINET and OPC UA

Smart devices provide operators not only with I/O data but also with a wealth of information about industrial plant operation. Information collected from field devices such as diagnostic data, status information on devices and specific device parameters can also help plan predictive maintenance programs.

SMART DEVICES IN MODERN PRODUCTION environments and processing plants provide operators not only with I/O data but also with a wealth of information about the state of the entire plant. The information that management systems are able to collect from these field devices, such as diagnostic data, for example, status information on the devices and specific device parameters, can help the organization plan its predictive maintenance program.

This information helps to prevent unplanned stoppages, reduces downtime and lowers maintenance costs. To enable plant operators to make the most of this potential for process optimization and cost reduction, the data delivered by all the installed devices must be transparent and, most importantly, standardized.



SOURCE: SOFTING

Sample application for smartLink PN.

Use case network monitoring

As networks continue to expand, more and more additional TCP/IP communication is taking place in parallel with PROFINET communication. Continuous information about the current state of the network, the communication processes within the network, and their quality is therefore becoming increasingly important.

In the IT market there are already sophisticated monitoring systems for this purpose that are continuously managed by administrators. But network monitoring systems are also finding their way into the automation environment. High network availability is just as important in OT as in IT. Unplanned downtimes caused by non-compliant functions can lead to production stoppages and, in a worst-case scenario, damage to the system. This can result in huge costs and lost profits.

If the automation network is continuously monitored, however, errors can be detected at an early stage and resolved before they have a chance to do any damage. With serial bus systems like PROFIBUS, the main focus is on bus physics, e.g. the quality of cables, circuits and connectors. In Ethernet systems, including PROFINET, the physical structure is unlikely to contribute to downtime. In fact, the growing complexity of devices and networks requires the qualitative assessment of a large number of parameters at a logical level. Nowadays, modern network diagnostics means obtaining as much information as possible from active requests by participants and from the analysis of frame traffic. There are basically two use cases:

Asset management

Certified PROFINET devices provide a variety of information about themselves, about the configuration of modules and submodules, and about adjacent devices. This data enables a complete picture of the assembled system to be generated. By cyclically querying this data, all changes, such as firmware updates, swapping switch ports or changing modules, can be precisely logged.

Diagnosis

Certified PROFINET devices provide detailed status information about the devices themselves and about the sensors and actuators to which they are connected. They record all faults, such as connection breakdowns or malfunctions, as well as statistical variables in the network such as frame repetition and increased jitter. This information is sent to the controller and stored in a device-specific database which can then be queried.

Common goal, no common standard

Because more and more manufacturing companies are starting to recognize the significant benefits offered by smart plant monitoring, requirement specifications of new plants increasingly often also include the necessary tools. This trend has helped the various providers of network monitoring and diagnostics systems to establish themselves on the market. Most of the systems on offer take the form of an additional device that is connected to the network and collects diagnostic and asset data. The data is clearly displayed on a variety of dashboards via an integrated webserver. Since PROFINET defines the framework within which the data is made available, the functional differences between the tools are relatively small.

The other common characteristic relates to the transfer of collected data to higher-level IT systems: it is simply not possible. Although the values are always the same and are displayed similarly, there is no standard enabling the non-proprietary exchange of data. This is where OPC UA comes in.

The OPC UA companion specification

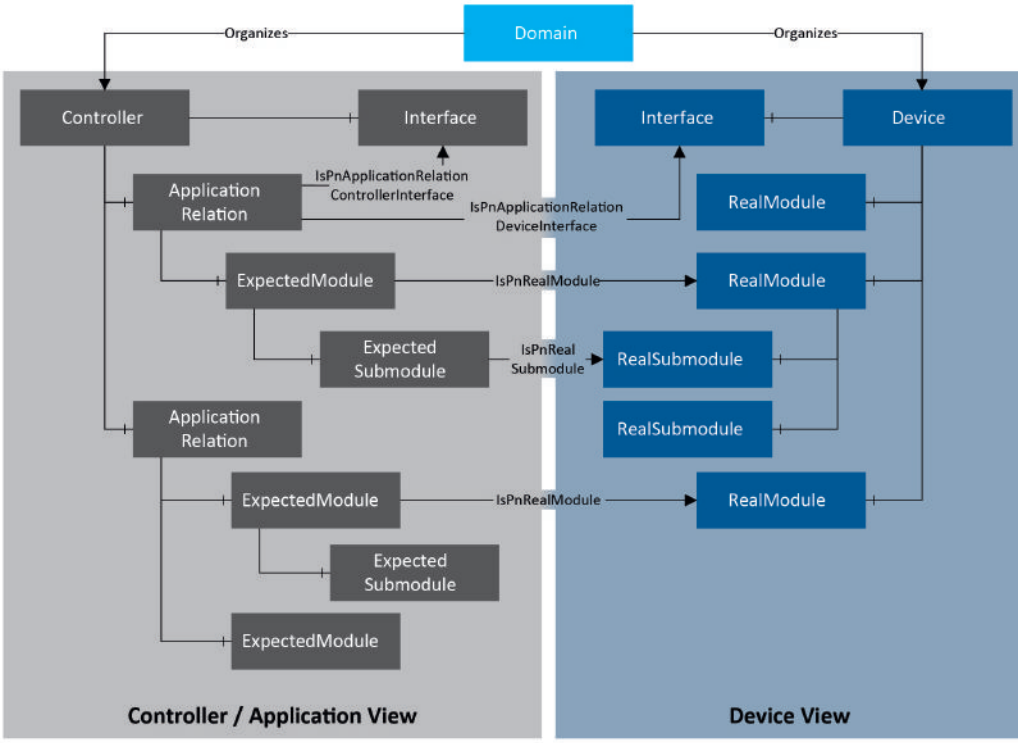
In June 2017, the PNO established the "OPC UA I4.0@PI" working group. The aim

was to create a "Joint OPC UA Companion Specification" for mapping PROFINET to OPC UA. The "OPC 30140 - UA Companion Specification for PROFINET" has been under review since July 2019 and will probably be released in December 2019.

This first version of the specification focuses on use cases in the areas of asset management and diagnostics. An OPC UA server that implements the specification can run on a controller, edge gateway or IO device.

The OPC UA information model contains two views of a PROFINET network: the controller/application view and the device view. The controller/application view contains the PROFINET connections (application relations), the modules and submodules configured in the PROFINET controller. The device view consists of the PROFINET devices and their physically available modules and submodules. Both views are linked via OPC UA references. Depending on where the OPC UA server is running, only parts of the views are available. An edge gateway provides both views of the PROFINET network.

The information model also contains a map of the PROFINET network's physical topology. The OPC UA information model therefore contains precise details PROFINET devices' wiring, their Ethernet interfaces, ports and cables, all of which can be used for network diagnostics. The submodules that provide the PROFINET interface and ports are connected via references.



SOURCE: SOFTING

The OPC UA information model contains two views of a PROFINET network.

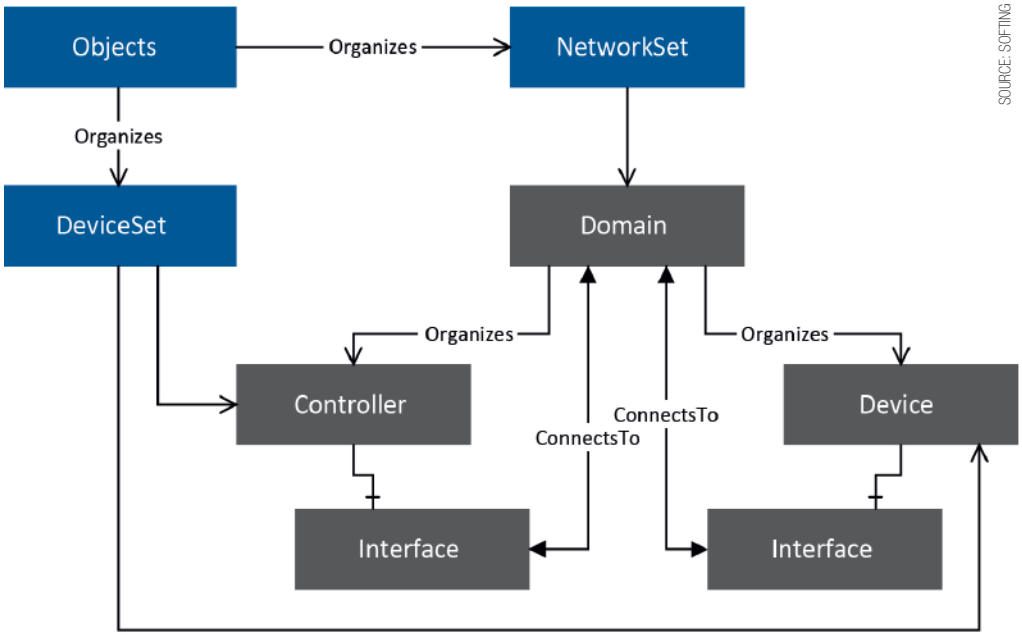
The OPC UA information model is based on OPC UA specification V1.04 and uses OPC UA V1.04 Amendment 7 "Interfaces and AddIns".

A useful annex to the specification provides an excellent description of how to use the information model with the "OPC UA Part 100 - Devices" V1.02 specification. A server offers entry points to the PROFINET OPC UA information model via the standard objects "DeviceSet" and "NetworkSet". The PROFINET Controller and PROFINET IO Devices are contained in the "DeviceSet". The "NetworkSet" contains the PROFINET domains.

Implementing the specification

Softing will provide the smartLink PN, an edge gateway that collects data from PROFINET networks and makes it available via OPC UA in accordance with the companion specification. The smartLink PN will have two 100 Mbit PROFINET switch ports, which allow asset and diagnostic data to be established via both active requests and passive frame analysis. As a result, the entire spectrum of available information defined by the companion specification is covered by a single device. The data collected will be supplied via a Gigabit interface that is separate from the automation network.

It will be possible to connect smartLink PN to a system without interfering with normal operations. When used with Softing's dataFEED Secure Integration Server, which provides external applications with unilateral access to the data, PROFINET diagnostic and asset data can be exported securely and transparently to any system both inside and outside the company's own network.



SOURCE: SOFTING

Using the information model with the "OPC UA Part 100 - Devices" V1.02 specification.

Thomas Rummel, Senior Vice President Engineering & Product Management and Thomas Schwarzenböck, Product Manager, ***Softing Industrial Automation GmbH.***

OPC UA over TSN: Frequently Asked Questions

The automation community is continuing to champion the introduction of OPC UA (Unified Architecture) over Time Sensitive Networks (TSN). B&R Automation provides its take on the importance of the technology, benefits for applications and how it fits with POWERLINK and other fieldbus technologies.

IT SEEMS EVERYONE THESE DAYS IS TALKING about OPC UA and TSN. For many machine builders and plant operators, however, it remains unclear what specific advantages stand to be gained from using these technologies in their own equipment and facilities.

To shed some light on the matter, here are answers to some of the most important questions about OPC UA over TSN and its role in the future of Industrial IoT communication.

SOURCE: B&R AUTOMATION

OPC UA over TSN seems poised to play an important role in the future of Industrial IoT communication.

Why is OPC UA over TSN necessary?
OPC UA over TSN is supported by all major automation suppliers. It ensures vendor-independent interoperability for all relevant industrial use cases, today and tomorrow.

OPC UA over TSN enables secure-by-design modular machine concepts and flexible production architectures on the shop floor. These will help users streamline their machines and plants for economical batch-size-one production.

Additionally, it offers secure insight into manufacturing processes for ongoing performance optimizations and predictive maintenance – without disturbing machine operations.

OPC UA over TSN is 100% open, significantly faster and secure. It can increase the ability to innovate, maximize Overall Equipment Effectiveness (OEE), Total Cost of Ownership (TCO) and streamline commissioning and maintenance.

What are the technical benefits of OPC UA?
Today's proprietary fieldbus systems communicate using raw data – just zeros and ones. Without the corresponding tables, devices on the network don't know how to interpret that data. That makes it impossible to achieve the kind of seamless communication required in the Industrial Internet of Things (IIoT).

With its information model, OPC UA enriches the raw data with semantic descriptions. These give it context and meaning, so any device or person that receives the information can correctly interpret it without any further explanation.

OPC UA offers so-called methods that enable direct interaction with assets. Machines can query each other to find out what kind of services, interfaces and capabilities they provide – which enables them to interact more efficiently and autonomously.

Why is it necessary to combine OPC UA with TSN?
TSN's determinism allows machine-to-machine OPC UA communication to better synchronize a multi-vendor plant floor. The same holds true for device-level communication within the machines themselves.

OPC UA provides a standardized way to structure data. It adds semantics for any kind of asset and provides it in a secure manner. TSN is the infrastructure, the highway that OPC UA drives on in a deterministic way.

Without the interoperability provided by OPC UA over TSN, these multi-vendor communications would have to be hard-coded – adding exorbitant development costs and canceling out any gains in flexibility. On top of that, OPC UA over TSN guarantees continuous insight without disturbing machine operations.

What role does OPC UA over TSN play in Industrial IoT applications?
Industrial IoT applications are data driven; information is their lifeblood. OPC UA over TSN adds a vast array of sensors, actuators and other automation devices to the available pool of information by extending the semantic self-description of the OPC UA information model down to the field level.

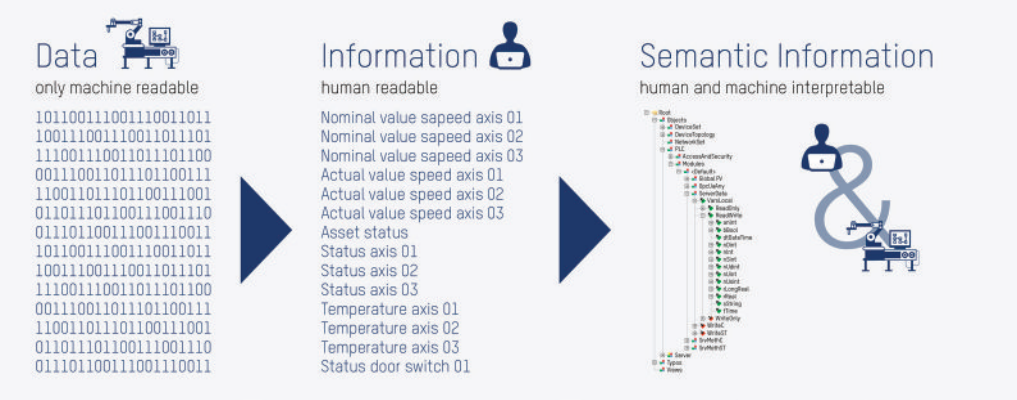
The Industrial IoT promises us an ability to design efficient and effective production processes that are at the same time cheaper and easier to commission and maintain. It also promises to allow profitable mass customization of products.

To achieve these aspirations, today's production lines will need to be transformed into flexible production units that allow continuous insight into their internal workings. This insight, combined with

clever algorithms, even artificial intelligence, will be the fuel that powers ongoing performance optimizations and predictive maintenance.

Why the sudden importance of network interoperability after twenty-plus years without it?

It is true that we have gotten this far without it. Yet, to take automation to the next level, with ready exchange of information, digitalization of manufacturing and the rise of the smart factory and autonomous operations – interoperability is an essential stepping stone.



OPC UA Information model provides semantic information which is human readable and machine interpretable.

Interoperability brings added speed, flexibility and cost-efficiency, without which it is impossible to implement the advanced data acquisition, analysis and optimization required for the IIoT.

How does the system provide interoperability all the way from the sensor to the cloud?

As a framework for thinking about communication systems, the OSI reference model divides them into seven conceptual layers – from the connectors and cables up to the user interface.

To ensure seamless interoperability on a network, you need interoperability on all seven of these layers. OPC UA delivers secure information interoperability on layers 5-7, allowing secure vertical communication from the sensor to the cloud. Interoperability on layers 3 and 4 is ensured through common IT standards. Layer 1 is covered by the Ethernet standard.

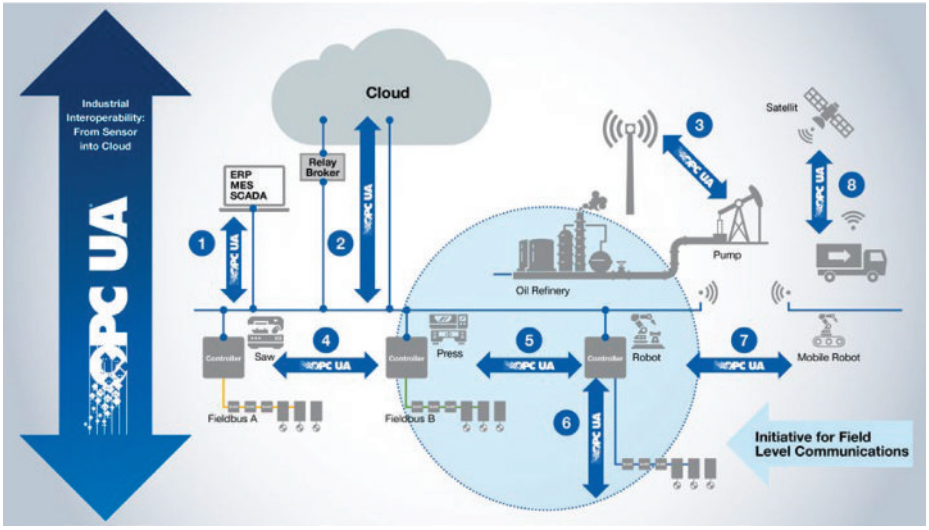
As the final piece in the puzzle, Time Sensitive Networking (TSN) brings interoperability to layer 2, the data link layer. This makes it possible to use OPC UA for precise real-time applications in converged OT/IT networks with unprecedented performance.

Who is responsible for standardization of OPC UA over TSN?

OPC UA itself is developed and standardized by the OPC Foundation. The TSN standards are the responsibility of the IEEE 802.1 working group. To ensure a cohesive, open approach to implementation of OPC UA together with TSN and associated application profiles, the OPC Foundation has launched the new Field Level Communications initiative. The director of the working initiative is Peter Lutz, who will lead and drive forward the development of the initiative and specifications.

The technology will bring vendor-independent, end-to-end interoperability into field-level devices used in all areas of industrial automation. Integrating field devices and the shop floor will further solidify the OPC Foundation's role as the driver for a worldwide industrial interoperability standard. Standardization efforts for unified functionality currently taking place at the OPC Foundation include I/O, motion and safety applications.

The OPC Foundation's steering committee for field-level communications consists of 24 leading technology providers from the automation industry, including ABB, Beckhoff, Bosch-Rexroth, B&R, Cisco, Hilscher, Hirschmann, Huawei, Intel, Kalycito, KUKA, Mitsubishi Electric, Molex, Omron, Phoenix Contact, Pilz, Rockwell Automation, Schneider Electric, Siemens, TTTech, Wago and Yokogawa. More and more companies are joining all the time, with recent additions including Moxa and Murr Elektronik.



System architecture diagram for OPC UA (Unified Architecture) over Time Sensitive Networks.

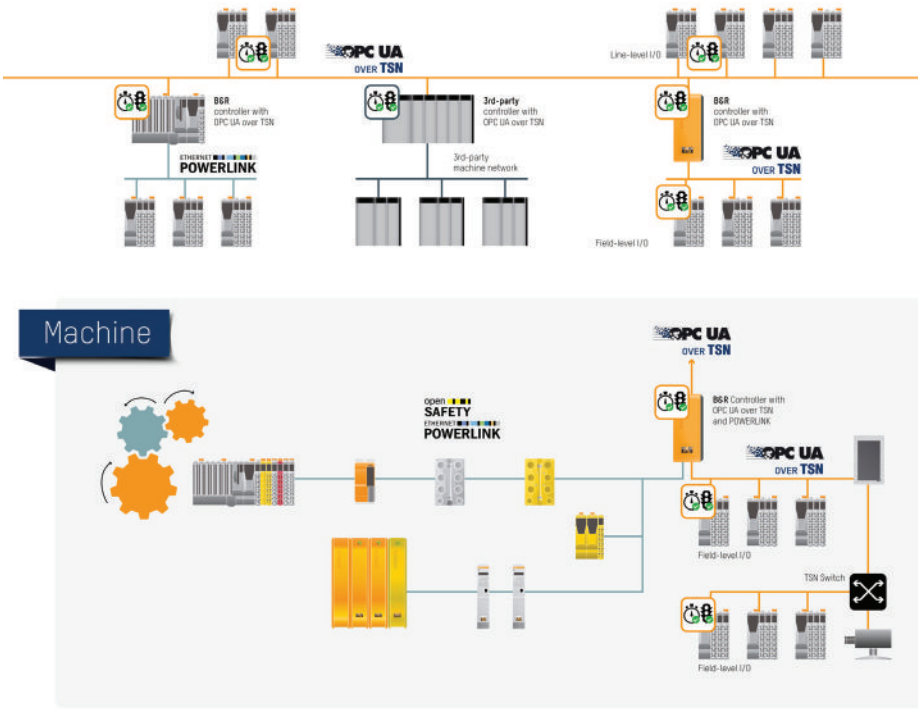
How do applications benefit from TSN being part of the IEEE 802.1 standard?

Real-time communication is critical for industrial automation capabilities such as device-level control, motion control, machine vision and machine-to-machine (controller-to-controller) control. Yet, standard Ethernet was never designed to be a deterministic network, so proprietary fieldbus systems each implemented their own mechanisms to achieve deterministic behavior. TSN now extends IEEE 802 Ethernet to include real-time communication, providing a unified standard that meets the requirements of industrial automation.

TSN also enables the possibility of converged networks, allowing the same network to manage both non-deterministic IT communications and deterministic OT communications, such as machine control and safety. In the future, the TSN standard will be a standard feature of mainstream Ethernet chips.

What kind of performance can I expect from OPC UA over TSN?

The technology is capable of addressing more than 10,000 network nodes, scalable from 10 megabits to 10 gigabits and beyond. Testing conducted by B&R achieved cycle times below 50 microseconds with a jitter of less than ±100 nanoseconds in a network of 200 remote I/O bus couplers totaling 10,000 I/O points. This is consistent with claims that OPC UA over TSN is "18 times faster than today's fastest solution."



OPC UA over TSN and POWERLINK can be combined into effective machine control architectures.

This level of performance makes proprietary fieldbus networks obsolete. OPC UA over TSN allows high-performance motion control traffic and bandwidth-intensive IT traffic on a single cable without interference between them.

Since 2017, B&R has been thoroughly testing the performance of OPC UA over TSN. In the test setup, 200 network nodes are synchronized with a cycle time under 50 µs, while five HD streams are transmitted over the same network.

Will OPC UA over TSN help integrate factory and machine networks with our IT requirements?
OPC UA was designed to communicate with IT systems. OPC UA over TSN will enable convergence of OT and IT networks without disturbing machine operations. This is thanks to TSN and the use of OPC UA security mechanisms familiar to IT departments today, including user authentication and authorization, encryption and certificate handling.

My plant is standardized on an existing fieldbus; is there any advantage to switching?
The main advantages are openness, consistent semantics, security and performance. The performance aspects include high bandwidth and guaranteed real-time system-level communication.

Whereas a machine builder would otherwise need to support every major fieldbus over TSN, the combination OPC UA with TSN mechanisms for real-time field-level communication provides a single vendor-agnostic network and protocol all the way from the sensor to the cloud.

An end user may be concerned with converged networks, for example, and need the ability to use OPC UA to connect to the cloud over MQTT. Cloud, ERP and DCS platforms today support an OPC UA connector, simplifying communication.

Regardless of the manufacturer of a machine, OPC UA companion specifications allow the machines to describe themselves in a consistent manner, with standardized semantics. The VDMA robot companion specification, for example, provides a standardized information model which is capable of presenting all robot related information and functionality regardless of manufacturer or location in a uniform manner.

What topologies does OPC UA over TSN support?
The topologies commonly used in industrial networks are all supported – including line, star, tree and ring. TSN includes a standard mechanism for seamless, real-time redundancy implemented through cable redundancy, ring or mesh topologies.

How do I configure my OPC UA over TSN network installation?
The supplier's development suite will provide everything to make configuration simple and automated. For those who choose not to use the supplier's tools, necessary configuration interfaces are open standards and additional third-party network tools are available.

Can TSN and non-TSN OPC UA or normal IP devices be used in the same network?
Yes, because TSN is an evolution of standard Ethernet. TSN simply enhances standard Ethernet with real-time capabilities, so it is possible to have standard Ethernet devices and TSN devices present in the same network.

Standard Ethernet devices would not need any interface or gateway to connect to a TSN network. However, only TSN-capable devices will be able to communicate in real time.

Will universal acceptance of OPC UA over TSN mean an end to POWERLINK support?
B&R has always followed a sustainable product strategy ensuring long-term availability of products and technologies. This will not change with the market introduction of OPC UA over TSN. B&R will support POWERLINK parallel to OPC UA over TSN in its product portfolio. Customers will be able to select the best communication solution to suit their needs.

What B&R controllers can I buy today that will be compatible with OPC UA over TSN?
TSN capability is already built into the majority of B&R's newer Automation PCs and will be supported in all new PLCs to come. The TSN and Ethernet port will be the same one.

What about running existing fieldbus protocols such as EtherNet/IP, Profinet, EtherCAT or CC-Link IE over TSN?
The legacy fieldbus protocols would share a common TSN network, but the devices would not be interoperable as OPC UA devices would be. These protocols also lack the semantics and methods that OPC UA provides. OPC UA has built-in security and is recognized an international standard for communication from sensor to cloud with new developments being added all the time.

The key difference is system interoperability: without it, you are locked into one vendor and one automation solution, with no ability to communicate or synchronize with other systems. In a multi-vendor plant, this means you are unable to secure your communication and implement advanced functionality such as condition monitoring, line balancing, predictive maintenance, machine optimization and plug-and-produce startup and maintenance. As a machine builder, this means you are limited to the level of innovation offered by your chosen vendor.

When will commercialized OPC UA over TSN solutions be available on the marketplace?
The first products have been announced by suppliers in late 2019 and available in early 2020.

*Technology FAQ by Stefan Bina, networking specialist at **B&R Industrial Automation.***

Industrial 4G router

Westermo: Critical infrastructure systems rely on communication devices to provide reliable and secure networks. To support this requirement Westermo has launched the MRD-455-NA, a 4G router designed to provide resilient, secure high-speed remote access across cellular networks. Offering an industrial design and a broad range of connectivity features, the MRD-455-NA ensures reliable machine to machine communications.

The MRD-455-NA is well-suited to industrial control applications where reliable machine to machine communication is vital. It has a compact design with all interfaces and LEDs at the front, DIN-rail mounting, isolated power supply and an operating voltage range spanning from 10 to 60 VDC. This industrial cellular broadband router offers a broad range of connectivity options, supporting many mobile standards including 3G and 4G LTE. A GPS antenna port enables customers to track remote assets by location which can be helpful in order to reduce the time it takes to locate equipment in an area. It offers Virtual Private Network (VPN) functionality, enabling secure tunnels to be created over insecure networks, such as the Internet. Dual SIM support ensures that connectivity is not dependent on a single carrier.

Gigabit Ethernet switch

Red Lion Controls: The new NT328G Layer 3 Ethernet switch offers 28 high-speed ports (24-Gigabit, 4-10 Gigabit) and reliable wire-speed switching performance. The NT328G offers performance and reliability is designed to meet the current and future needs of the oil & gas, water & wastewater, energy, transportation, and video and security sectors, as well as other bandwidth-intensive industrial applications.

NT328G Layer 3 industrial Ethernet models feature a flexible mix of copper and fiber ports, allowing for a vast variety of connection options, with Layer 3 routing that provides the ability to route across VLANs or subnets—versatility that ensures scalability. The industrial-grade NT328G's robust feature set includes network redundancy, advanced, integrated security, policy-based traffic control and easy-to-use configuration and management—reducing operating costs while providing continuous monitoring of network activity.

Its sleek but rugged IP30 rackmount metal housing is constructed for long-life use in harsh industrial environments, including wide operating temperature conditions and hazardous locations—durability that ensures reduced downtime.

Single port Ethernet transceiver

Analog Devices: New industrial Ethernet physical layer (PHY) products will help manufacturers address key Industry 4.0 and smart factory communication challenges surrounding data integration, synchronization, edge connectivity, and system interoperability.

The ADIN1300 is a low-power, single port Ethernet transceiver with high power and latency specifications primarily designed for time-critical industrial Ethernet applications up to Gigabit speeds. As industrial automation increases the adoption of Ethernet and pushes the boundaries of data rates, the ADIN1300 is designed to operate reliably in harsh industrial conditions over extended ambient temperature ranges.

Position sensors

MTS Sensors: A POWERLINK version of its Temposonics R-Series V position sensors for industrial applications broadens the range of applications which can now be supported by this new generation of magnetostrictive position sensors.

The R-Series V POWERLINK starts measurement synchronously with the master clock, which is an essential prerequisite for processes requiring

simultaneous actions. The sensor is also able to read out a resolution up to 0,5 µm, which is a first for a magnetostrictive POWERLINK sensor.

POWERLINK is a software-based solution that complies with IEEE 802.3 Ethernet standard. Available in rod style (RH) and profile style (RP), the R-Series V POWERLINK sensor has several special features that make them suited for a variety of applications. With 250 µs, the sensor achieves the same minimum cycle time as the R-Series V Profinet.

In addition, the extrapolation of the new sensor enables the output of a new position value for each polling cycle, regardless of the sensor's stroke length. The sensor also supports multi-position and multi-velocity measurement with up to 30 magnets. Backward compatibility based on proven electrical connections and mechanical designs allows for seamless integration into existing applications.

Analytics software

Beckhoff: TwinCAT Analytics offers automated functionality for converting analysis configurations into executable PLC code, and now also includes dashboard generation. With One-Click Dashboard (OCD), all it takes for users to generate an entire HTML5-based analytics dashboard based on the PLC code and to load it into a selected Analytics Runtime container is a simple mouse click.

When the process completes, users receive a network address that they can then use to access the dashboard in a web browser. This ability to generate dashboards without the need to write a single line of code or design graphics is a huge time-saver within the engineering process.

Based on TwinCAT 3 HMI, the new functionality provides at least one HMI Control for every TwinCAT Analytics algorithm, each with an up-to-date tile design that follows the latest web standards.

High performance firewall

Belden: The Hirschmann EAGLE next-generation industrial firewall is designed to meet the evolving cybersecurity demands of today's industrial automation networks.

Together with the Hirschmann Security Operating System (HiSecOS), the EAGLE40 firewall offers a comprehensive solution to securely monitor communication flow. Specifically designed for operational technology (OT) applications, the device hardens networks at the factory floor, especially those requiring high-performance support, such as within industrial and process automation systems.

Designed with a convection-cooled metal housing to meet a variety of industrial ratings, the device provides a ruggedized cybersecurity solution to the factory floor without compromising network performance. This is especially pertinent to OT teams seeking to optimize cybersecurity under the harsh conditions present in machine building and general manufacturing environments.

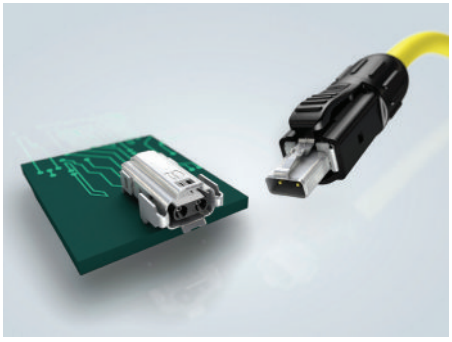
CC-Link IE TSN products

CLPA: Gigabit Ethernet with Time-Sensitive Networking (TSN) capabilities are key tools for Industry 4.0 applications.

CC-Link IE TSN compatible automation products from Mitsubishi Electric include a range of solutions PLCs, the iQ-R and iQ-F series, FR-A800 inverters, MR-J5 servos, GOT HMI as well as remote I/O modules.

These products can deliver TSN-based high performance solutions, even for high-speed and accurate motion control applications. Integration of a Cognex TCP/IP machine vision system into the network demonstrates how CC-Link IE TSN can handle both time-critical control data and non-time-critical network traffic while ensuring deterministic communications. In this way, the open network technology from the CLPA is designed to support the merging of information technology (IT) and operational technology (OT).

T1 industrial interface



HARTING: A fully standardised interface for industrial $M_3I_3C_3E_3$ applications (IEC 63171-6) will be released this year, creating an established interface for Single Pair Ethernet applications in the industrial sector. HARTING had begun developing the interface as far back as 2016.

In addition to the standardisation of the mating face, an international selection process saw both the international and the American standardisation bodies (ISO/IEC JTC 1/SC 25/WG 3 and TIA TR42) establish the T1 Industrial style as the SPE mating face for industry and industry-related applications in 2018.

This decision is further supported by the important Ethernet standard IEEE802.3. Hence a broad consensus exists within all the major standardisation bodies: ISO/IEC, TIA and IEEE. Consequently, the future SPE interface for industrial applications has been finalised and has a name - the T1 Industrial.

Industrial switches

Lapp: New ETHERLINE ACCESS switches are available in different versions with four to 16 ports, also in combination with ports for fibre optic cables and as a Power-over-Ethernet variant. All switches have robust metal housings and are designed for DIN rail mounting. Special highlights includes units claimed to be the smallest Profinet switches on the market.

This switch is used where there are conflicts due to multiple IP addresses. It has three LAN ports and one WAN port that connects the switch to a higher-level corporate network. The NAT functionality translates the same IP addresses at machine level into different IP addresses at company level. The switch translates different external IP addresses into a different address range for the machine-level network. Port forwarding and routing mode are also on board.

In addition to the eight RJ45 ports, each of these two managed switches also has two SFP ports for connecting fibre optic cables, with the ETHERLINE ACCESS M08T02GSFP for fast Gigabit Ethernet. The switches withstand temperatures between -40 °C and +75 °C, implement IP40 protection against the ingress of foreign bodies and can be supplied with redundant power. SFP standard modules are available for converting optical into electrical signals.

Industrial Network Defense

Moxa: An Industrial Network Defense solution, specially designed to secure industrial networks from both an Operations Technology (OT) and Information Technology (IT) perspective is designed to better address the surging market demand for a comprehensive cybersecurity solution for industrial networks.

Moxa's Industrial Network Defense Solution includes critical IT cybersecurity technologies such as an Intrusion Prevention System (IPS), a key component for defense-in-depth strategies, that has been specifically tailored to protect OT networks from cyberthreats without disrupting industrial operations.

As system availability is often the most important consideration for OT systems, network operators are seeking a more effective and less-impact approach to prevent operations from being affected by cyberthreats and attacks to ensure maximum system availability. Nowadays, the prevelance of cybersecurity incidents have urged governments to pass laws that require industries such as power, energy, transportation, and critical manufacturing to implement cybersecurity countermeasures into their industrial control systems, especially for critical network infrastructure.

Furthermore, companies in the manufacturing sector have started to enhance the security of their industrial networks to avoid loss of revenue or damage to their reputations. To that end, industrial network security has become a major concern that has driven OT and IT departments to work together to find a holistic solution.

PoE injectors with ATEX

Phoenix Contact: PoE injectors supply remote PoE-capable devices, such as cameras, with data and power via the same cable. ATEX approval means that these devices can now be installed in Ex zone 2 without restrictions. Cameras are increasingly being used in the process environment for monitoring critical processes and for condition monitoring. The injectors supply the camera systems for system monitoring and for monitoring devices, assets, and passageways.

The PoE injectors are dimensioned for standards IEEE 802.3 af (15.4 W) and at (30 W), and there is also an option for PoE++ with a supply of up to 60 watts. The electrically isolated power supply unit has an extended input voltage range of 18 - 57 V DC. In addition to the RJ45 socket, the INJ 2000 series devices are equipped with various connection technologies, such as Push-in, for the PoE-feeding cable. This enables easy cable connection without the need for connector assembly or special tools. The devices also feature integrated surge protection.

Microcontroller EtherCAT support

Renesas Electronics: The RX72M Group of RX microcontrollers (MCUs) feature an EtherCAT slave controller for industrial Ethernet communications that offers a high-performance, single-chip MCU solution with large memory capacities for industrial equipment requiring control and communication functions such as compact industrial robots, programmable logic controllers, remote I/O, and industrial gateways.

The use of EtherCAT in industrial Ethernet is growing fast, and is currently used on dedicated MCUs, ICs, and high-end system-on-chip (SoC) devices specialized for EtherCAT communication. The new RX72M Group achieves the performance of a 1396 CoreMark score at 240MHz as measured by EEMBC Benchmarks, and it is capable of both application processing and EtherCAT communication. Combining a motor-control MCU with on-chip EtherCAT slave functions allows industrial application developers reduce their bill of materials (BOM) and support the miniaturization levels required for industrial equipment design.

The RX72M Group is the first RX MCU group to include an EtherCAT slave controller featuring the RX family's highest SRAM capacity – 1 MB of SRAM – and 4 MB of Flash memory.

Automation control platform

Bosch Rexroth: The new ctrlX AUTOMATION platform enables centralized and decentralized automation topologies. Using a Linux real-time operating system, open standards, app programming technology, web-based engineering and a comprehensive IoT connection, ctrlX AUTOMATION is designed to reduce engineering time and effort by 30 to 50%.

The new ctrlX platform encompasses engineering software technologies for all PLC and motion tasks. Software functions are combinable in any number of ways with ready-made, customized and customizable apps. These apps can be created in a variety of programming languages such as C++, script languages such as Python, or new graphical languages such as Blockly.

Configuration and commissioning of the automation components is completely web-based, eliminating the need to install software. Within minutes of switching the system on, the software is programmed. A completely virtual ctrlX AUTOMATION system environment is available, enabling programming without hardware.

Automation digitalization solution

Siemens: Industrial Edge is a digitalization solution that adds machine-level data processing to automation devices, by taking the intelligence of Edge computing and thus, sophisticated analytics securely to manufacturing level.

Industrial Edge offers users the opportunity to execute a wide range of descriptive, diagnostic, predictive and prescriptive analytics applications. Cloud connectivity is used in conjunction with Edge apps, from third-party providers or from users themselves in an integrated hardware and software ecosystem for automation components.

Users have the opportunity to close the gap between conventional local data processing and Cloud-based data processing, depending on individual requirements. With Edge computing, large volumes of data can be processed locally almost in real time. A broad spectrum of applications for this include data processing, data visualization via web server, data transmission to the Cloud or IT infrastructure and fast innovation cycles for app development. In addition, storage and transmission costs are reduced for users because large volumes of data are preprocessed, and only relevant data is then transmitted to a Cloud or IT infrastructure.

Field device mobile solutions

Softing: The combination of Softing's mobiLink interface with the Field Xpert SMT70 or SMT77 Tablet PC from Endress+Hauser offers users a simple and safe system solution for configuring and parameterizing field devices for a wide range of important process automation protocols--including HART, PROFIBUS PA and FOUNDATION Fieldbus.

The bundle includes a Field Xpert SMT70 or SMT77 tablet with pre-installed CommDTMs (HART, PROFIBUS PA and FOUNDATION Fieldbus), a mobiLink interface that establishes the connection to the tablet via Bluetooth, and optionally a license to use mobiLink for the configuration of FOUNDATION Fieldbus and PROFIBUS PA field devices.

IP67 Managed Ethernet switch

Turck: The new TBEN-L switch with a GBit high-speed backbone guarantees short cycle times and secure operation in IIoT applications.

Thanks to its very high data rates up to 1Gbit/s, the TBEN-L-SE-M2 makes it possible to considerably speed up applications, such as for tool changing. Thanks to its suitability for decentralized installation directly in the field, the switch also reduces the wiring required between the control cabinet and Ethernet stations on the machine. The TBEN-L switch clears the way for consistent modularization in machine building.

The manageable switch offers several functions for the secure and efficient organization of industrial Ethernet networks. The integrated firewall offers bidirectional protection from unauthorized access and thus reliably increases security in IIoT. Its NAT routing function enables stations to be represented under alternative addresses in higher-level networks.

The device thus reliably prevents the doubling of IP addresses in the network of the user. The port-based IP address assignment allows station addresses to be allocated via the web browser of the switch.

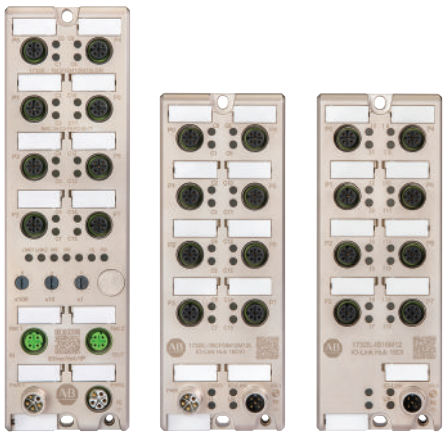
PROFINET I/O system controller

WAGO: The company has extended their family of PFC200 Generation 2 controllers with the release of the new 750-8215. The 750-8215 is IIoT-ready, comes with two Ethernet ports, two PROFINET ports, and is programmable with WAGO's e!COCKPIT software (CODESYS 3.5).

The PROFINET ports are switched for use as a line configuration enabling the controller to function as an I/O device connected to a PROFIBUS master. The two Ethernet ports can be used in a switched configuration or separated, and support other protocols such as EtherCat and Sparkplug (with additional licenses).

Other features of the controller include: USB-A port with removable memory to extend memory capabilities of the controller; high speed processor for complex applications; large on-board memory plus SD card slot; built-in web server and a CANopen port that allows connection to other devices on a CAN network.

Machine I/O modules



Rockwell Automation: Manufacturers can simplify the design and leverage productivity benefits using on-machine I/O modules on smart machines used in harsh applications. New Allen-Bradley ArmorBlock I/O modules operate in a wide range of temperatures and offer up to IP69K protection in applications like automotive, material handling, packaging and welding.

The new ArmorBlock I/O options can be mounted anywhere on a machine for shorter cable runs and lower wiring costs. They use nickel-plated zinc die-cast housing, have QuickConnect functionality and offer diagnostics in an EtherNet/IP universal digital I/O block to reduce commissioning and troubleshooting times. Three IO-Link hub blocks help reduce design complexity by allowing more devices through the IO-Link master. And an M12 L-coded power connector on selected blocks supports higher current, allowing more blocks to be daisy-chained and resulting in lower wiring and installation costs.

For companies with separate I/O blocks for digital input and output, the ArmorBlock I/O modules are an option. They provide 16-channel self-configurable digital I/O with flexibility to be used as the digital input or output depending on the application needs.

IoT edge gateway

Eurotech: A new multi-service IoT edge gateway, the ReliaGATE 10-14, features LTE connectivity for industrial and lightly rugged applications.

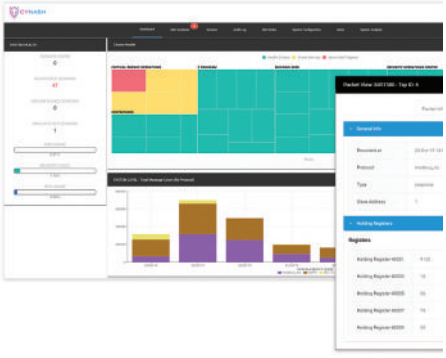
The ReliaGATE 10-14 is the natural evolution of the ReliaGATE 10-12 that now embeds a more powerful core bringing more computational capabilities and memory. With this evolution addressing the more and more demanding industrial-grade IoT applications will be easier and faster. An extra feature such as the video output capability is also available.

The ReliaGATE 10-14 has a very compact mechanical enclosure with a small profile, suited to be installed on DIN rails, reducing both the cost of installation and the mounting space required, allowing an easy retrofit in existing cabinets and other type of applications.

Given the focus on end-to-end security for the deployment of IoT services, the ReliaGATE-10-14 is designed to meet the new cybersecurity standards set by IEC 62443-4-1/2 including an anti-tamper mechanism to detect and report unauthorized access to the device, secure boot and the TPM 2.0 for secure storage and device identification.

An input power monitoring technology will allow to check regular operative conditions and detect operation anomalies, facilitating preemptive maintenance and further enhancing the device security.

Control system cybersecurity



Cynash Inc.: A new release of the Cynalytic analytics appliance acts as an intrusion detection system and behavioral monitoring tool for serial communications-based ICS/ SCADA networks, now includes advanced alerting such as logical

operators and other new features.

The enhanced appliance builds on Cynalytic's suite of data visualization and dashboard tools to help users monitor and make sense of historically unmonitored and unprotected serial communications.

Improvements include: Advanced alerting for serial traffic across environments; Logical operators (AND, OR, NOT) for precise multi-tiered conditions; protocol breakdown GUI to display protocol characteristics; protocol hover for easy-to-understand "byte-attribution" of protocol metrics; integration with SIEM tools (such as ELK or AlienVault) with native support for Syslog; integration with JSON and XML structured data, metrics and audit log data; configuration templates to quickly provision SerialTap sensors; and system-level analysis, providing a threat-hunting view for anomalous serial traffic.

Cynalytic analyzes serial communications data using Cynash's patented SerialTap sensors. By identifying and detecting intrusions and other operational field device issues, Cynalytic—in combination with SerialTap—helps ICS operators mitigate the risk of cyber-physical damage to industrial control systems.

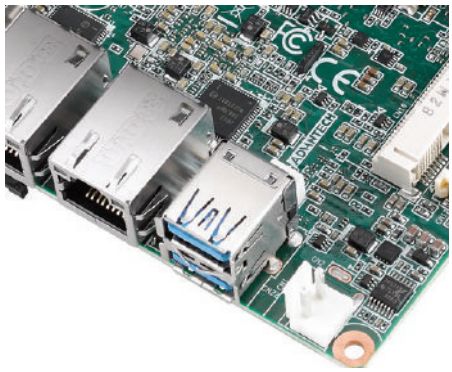
Predictive maintenance module

SIGMATEK: A new addition to the S-DIAS series is designed for predictive maintenance and cost monitoring. The compact DIN rail module is used to efficiently record energy, power and phase angle directly on the machine. With the EE 121, the voltages of the three input phases (L1, L2 and L3) can be measured. Additionally, up to 12 currents are also recorded which can be assigned to any phase. The voltage, as well as current inputs have a 16-bit resolution (ADC). The measuring range of the module is between 0-500 V AC and 0-2 AC.

In addition to current and voltage sequences, the EE 121 can be used to measure the phase position and frequency. It enables the calculation of Ueff and Ieff for each channel, as well as the energy consumption since the first activation. The module can also detect power disruptions or a phase drop and registers the zero crossing point for the application.

The main power synchronization is also possible with the EE 121. A timestamp function is provided for the zero voltage crossing points. Therefore, when using several energy recording modules, the time offset of the voltage zero crossing points of two main voltages can be determined.

Intelligent IoT systems



Advantech: MIO-2361 is the latest Pico-ITX single board computer designed with onboard LPDDR4-2400 & 32G eMMC powered by Intel Atom E3900 series/Pentium N4200/Celeron N3350 processors.

The rugged design of the MIO-2361 means typical memory (socket type) assemblies are not used. The MIO-2361 offers deep power down mode, 12V/24V +/- 10% power input, better storage capacity, M.2/mSATA, and -40° to +85°C wide temperature support.

Combined with Intelligent Management Software Integration, MIO-2361 offers various types of selected embedded OS including Windows 10 and Linux Yocto BSP for testing hardware drivers and devices to prevent unauthorized data access. MIO-2361 is also integrated with WISE-PaaS/DeviceOn IoT device management software to expedite IoT development particularly in factory automation.

IO-Link master with OPC UA

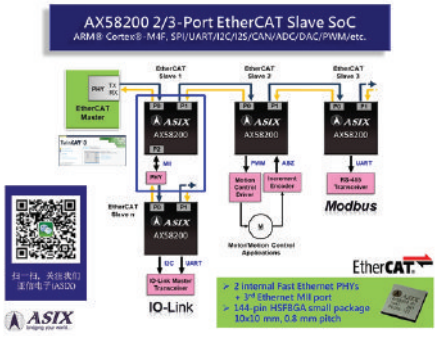
Pepperl+Fuchs: IO-Link masters with an OPC UA interface are paving the way for end-to-end, transparent and seamless communication from the lowest field level to the cloud.

OPC UA is an Ethernet-based communication protocol and provides an easy and flexible method of communication between machines or between a machine and the cloud. OPC UA is characterized by its independence, which gives customers flexibility when designing their IoT systems, and ensures that they have complete freedom, no matter which platform they choose to use.

By combining OPC UA and IO-Link, Pepperl+Fuchs has opened up new possibilities for end-to-end, transparent, and seamless communication from the lowest field level to the cloud. If IO-Link functions as the interface for the identification, diagnostics, and parameter data from the sensor technology,

OPC UA provides a solution for transmitting this data to PC- or cloud-based systems in full and in parallel with time-critical control communication.

EtherCAT slave controller



ASIX Electronics: A new generation EtherCAT Slave Controller SoC provides designers a small package size (10x10 mm).

The AX58200 is equipped with ARM Cortex-M4F core and DSP extension runs up to 192 MHz, embedded 512 KB dual bank Flash memory for supporting Over-The-Air (OTA) firmware upgrade, embedded 160 KB SRAM which includes 32 KB cache supporting eXecute-In-Place (XIP) to speed up the code execution from external SPI Flash.

Factory pre-loaded 32 KB bootloader for secure boot, built-in 4 KB Secure Protection ROM providing a convenient and safe space to save confidential program or data. The solution also supports a variety of additional communication interfaces such as 10/100Mbps Ethernet MAC with RMII and hardware cryptography accelerator, HS USB OTG, SPI/UART/I2C/I2S/CAN/PWM, etc.

This solution is suitable for motor/motion control, digital I/O control, sensor data acquisition, robotics, EtherCAT IO-Link master, and automation fieldbus applications.

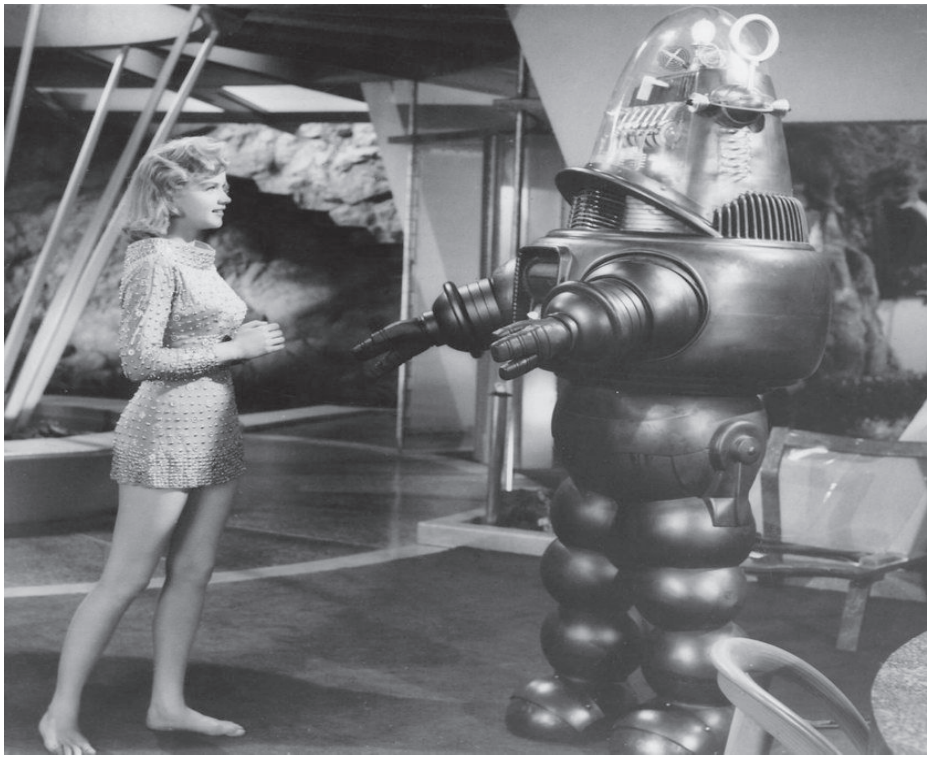
50 years later: The invasion of the robots is finally happening

In the science fiction movies of the 1960s and 70s, robots played a major – and often sinister – role. Half a century later, the invasion of the robots finally seems to be happening. But the robots that permeate our world are not terrifying war machines, but rather cute.

"THE COLOSSUS OF NEW YORK" sent a steel cyborg-robot on a rampage through the city, "Kronos" was a gigantic, box-like robot, an all-consuming, insatiable alien machine, and "Dr. Satan's Robot" was used by a mad criminal scientist to take over the world.

In the movies of the 60s and 70s, robots were often shown as mean machines trying to conquer the world with super-human strength, rockets and laser beams. Because this has not worked (yet), the robots now try a different strategy: Cuteness.

At this years Consumer Electronics Show in Las Vegas, robotics was a big theme. Here are some of the cute and sometimes bizarre concepts that were shown at CES:



FORBIDDEN PLANET

Petit Qoboo

Some people would love to own a pet but can't, because they suffer from allergies, live in a small apartment or are simply too busy.

Yukai Engineering, a Tokyo-based robotics startup, has developed Petit Qoobo specifically for this market segment. This almost-animal is designed to comfort people who cannot own a real pet. It could be described as a furry therapy pillow with an expressive tail.

Petit Qoobo wags its tail in response to one's stroking and rubbing. It waves gently when caressed and swings it playfully when rubbed.

PHOTO: YUKAI ENGINEERING

It also moves spontaneously in reaction to the sound of clapping or one's voice. "As a user, you would project your emotions onto how the tail moves, and you could get a sense of healing from that", says Prof. Nobuhiro Sakata of Dokkyo Medical University.

Petit Qoobo comes in a compact size, small enough to fit in a purse. It can thus provide comfort and emotional support not only at home, but also in a lonely hotel room or office.

qoobo.info

MarsCat

MarsCat takes the robotic pet concept one step further. It can independently perform various cat-like tricks. MarsCat walks, runs, sleeps, sits, stretches, and plays with its owner.

It is fully responsive and has sensitive interactions. Through an array of sensors it can feel a touch, hear a voice, recognize a face and play with toys. The robot feline can also express different emotions by different meows or gestures.

MarsCat comes with six pre-programmed characters which can be changed. It can be enthusiastic or aloof, energetic or lazy, social or shy. The personality develops over time. MarsCat will be more active if the owner frequently interacts with it. Else it behaves cat-like and needs to be pleased until it feels in the mood for playing again.

Built on an open source platform, users can program MarsCat easily and include new functions. In addition to a Raspberry Pi kit, it comes with integrated open source modules

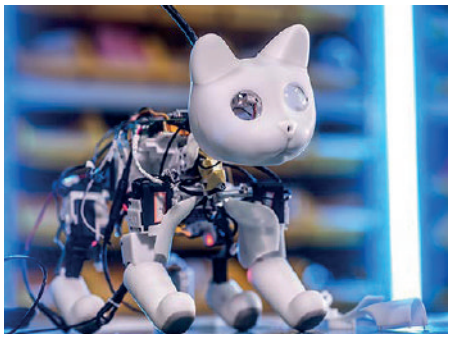


PHOTO: ELEPHANT ROBOTICS

for vision and haptic, microcontroller, gyro sensor and more. Protocol and library are open-source embedded in Raspberry PI.

The MarsCat SDK gives access to all the sensors and actuators to adjust the functions to different applications.

www.elephantrobotics.com

RollBot

Qoboo and MarsCat are essentially just sophisticated toys, but RollBot was designed to solve a very real problem. According to a survey commissioned by Charmin and conducted online by The Harris Poll, 58 percent of people ages 18-34 admit to being on the toilet before realizing they had run out of toilet paper.

PHOTO: CHARMIN GOLAB

RollBot comes to the rescue. Developed as part of the Procter & Gamble Charmin GoLab concept lab, it is a first-of-its-kind robot that, when controlled with a smartphone using Bluetooth, delivers a fresh roll of toilet paper to you so you won't have to be left in a bind ever again. According to Charmin GoLab, "its futuristic design uses self-balancing technology to give it a more bear-morphous look".

www.pg.com

Bot Chef

While RollBot lends a hand in the bathroom, the Samsung Bot Chef provides an extra pair of hands in the kitchen, sharing the burden of the laborious and repetitive tasks that go into creating meals.

It is an AI-powered chef's assistant, a so-called "cobot" or collaborative robot. Bot Chef is designed to be easy to use and highly versatile, with a sleek exterior that hides its advanced mechatronics.

This cobot is optimized for kitchen use and is capable of a wide range of tasks, from chopping and whisking, to pouring and cleaning. Based on SARAM, Samsung's multi-purpose programmable robotic platform, the lightweight robotic manipulator arm has six degrees of freedom,

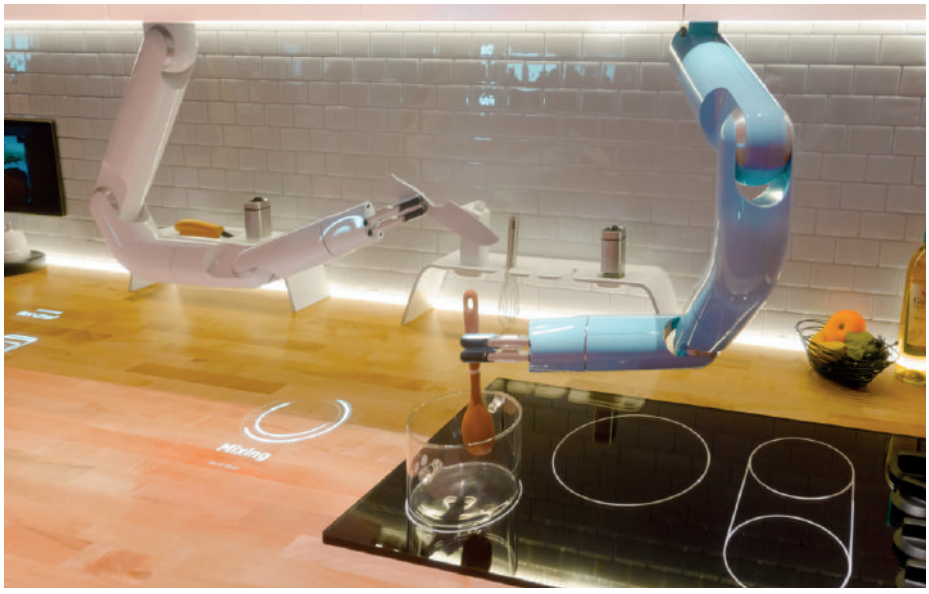


PHOTO: SAMSUNG

with the diameter, reach and safety of a human arm. This allows it to perform with a payload just enough to lift common, everyday kitchen items. With advanced internal and external sensors and AI-based planning algorithms, the Bot Chef works alongside a person safely, even when they get in each other's way.

Users can interact with the robotic arm using voice control, physical manipulation and app-based controls. Meanwhile, the underlying AI and machine-learning platform enables the cobot to learn new skills. New skills can also be downloaded, customized and shared as part of an online ecosystem, providing almost endless possibilities in the kitchen. To stir a pot of soup, for example, a user can download the "stirring" skill from the skills ecosystem. Bot Chef can autonomously understand the location of objects, so the user can tell it where to find the spoon, and which pot to stir. "Hey, Bot Chef, let's make a soup."

www.samsung.com

Misty

Misty Robotics believes that platform robots are the missing link to accelerating the use of robots in businesses, homes, research, and education.

By providing robust tools, comprehensive documentation, and extensive APIs, Misty Robotics makes it easy for developers to build on the Misty platform. Tools include a pre-built Command Center, Skill Runner, and API Explorer, which are accessible through an easy to navigate SDK interface.

Developers can extend Misty's capabilities by integrating with third party APIs such as those provided by Twilio, Microsoft, and Google. Additionally, Misty can be expanded through third party hardware such as Arduino and Raspberry Pi and physically expanded through 3D printing.

www.mistyrobotics.com

Leopold Ploner

PHOTO: MISTY ROBOTICS

CODESYS

Node-RED

ssh

groov VIEW

Ignition by Inductive automation

Sparkplug MQTT

OPENVPN™

***groov* EPIC**: it's **real-time control, connectivity, data handling,** and **visualization** in one industrial package. And it's ready for your industrial automation and IIoT applications today—and tomorrow.

- Program using tools you know: flowchart, ladder, function block, Python, C/C++, and more
- Integrate with other systems, including PLCs, databases, HMIs, cloud services, and IoT platforms
- Reduce unnecessary middleware to securely and efficiently get data where it needs to be
- Protect with built-in security, including configurable firewalls, encryption, and user accounts
- Install on plant floors and at remote sites—UL Hazardous Locations approved; ATEX compliant

Learn more now at **op22.co/thisisEPIC**

MADE IN THE USA

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

OPTO 22
The Future of Automation.