CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION • CONTROLGLOBAL.COM

INSIDE:

Increased Chance of Cloud Success p2

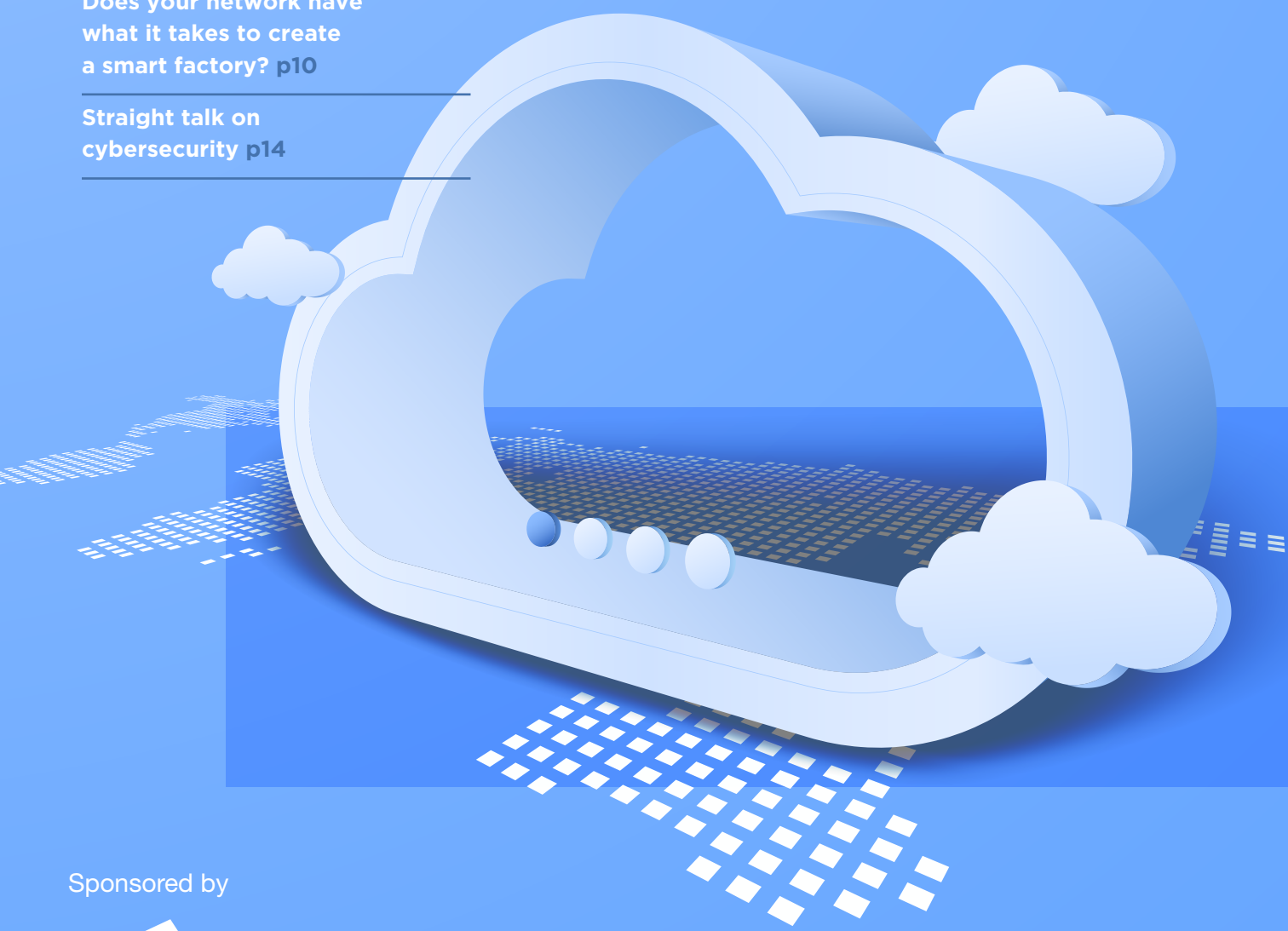
Seamlessly and Securely Connect Plant Floor to Cloud p5

Wireless moving into the mainstream p7

Does your network have what it takes to create a smart factory? p10

Straight talk on cybersecurity p14

The Cloud
TUTORIAL GUIDE



Sponsored by

WAGO

PutmanMedia®

Increased Chance of Cloud Success

By Jesse Cox, WAGO Senior Application Engineer

One of the biggest trends we are seeing in our industry is a way to make operations primarily cloud-based, especially in manufacturing. When many factories were built, they were dependent upon manual data gathering and machine operation. In today's world, many machines still operate by human hand, but the way to gather data and run a plant efficiently through automation has changed.

Manufacturers are attempting to make their facilities cloud-based and are running into complications. Machinery and, most often, the overall infrastructure of the building are not equipped with the right connections to make this possible. With MQTT and OPC UA protocols acting as the de-facto standards for cloud-based operations, we must find the proper gateway for them to gather information from the industrial fieldbus.

It is our job to have engineers and product managers work with these businesses to find the right connections to facilitate the cloud-based applications that they are looking for. With the correct complement of interconnections, we can make wiring easier, connections stronger and processing faster.

In today's world, many machines still operate by human hand, but the way to gather data and run a plant efficiently through automation has changed.

And while many larger and mid-sized companies have the in-house resources to implement IIoT on a broad scale, I believe that, over time, smaller companies will also seek to benefit from the advantages IIoT can offer. Naturally, they need to contract outside hep.

As more open protocols like Sparkplug are adopted, the implementation and management process will get easier. This will happen rapidly in the coming years. Similarly, machine learning and data analytics will continue to become more ubiquitous, as will implementing data streams into business strategy with services such as Azure Stream Analytics & AWS Kinesis Data Streams.

In short, the solutions at the ready will become more understood and more widely adopted. And that means our processes will become more widely successful.

IT + OT
IN ONE
DEVICE

EDGE DEVICES

COMPUTERS & CONTROLLERS

- Concurrent analytics and real-time control
- Data gateway between OT and IT
- Local processing, low latency
- Data aggregation for Cloud memory optimization

WAGO

www.wago.com/us/edge-devices

Seamlessly and Securely Connect Plant Floor to Cloud

By Charlie Norz, WAGO Automation Product Manager

As companies prepare for the future, the digital transformation of the plant floor is in full swing. WAGO has been helping people collect and analyze information from their plant floor for years, and we continue to enhance our technologies with exciting new tools for this digital transformation age. We have already seen companies that are gradually implementing cloud-based solutions to their plant floor, because the advantages are tremendous. Large investments are not necessary to profit from the cloud's flexibility.

BENEFITS OF IIOT

With global access to plant-floor data, dashboards of system performance can be aggregated and used for analyses including benchmark data of similar manufacturing facilities as well as helping increase equipment reliability through condition monitoring. This creates a real added value for both corporations and their customers.

CHALLENGES OF ENABLING NORTH-SOUTH DATA TRANSACTIONS

One of the major challenges that comes with IIoT is how to securely collect data from your manufacturing site's plant floors. It seems like an overwhelming task. How can data be collected when plants use multiple fieldbus protocols? Equipment on the floor is manufactured by several different vendors, so how can you cost-effectively collect information from each machine? There are all sorts of disparate machine types: conveyors, machine

Large investments are not necessary to profit from the cloud's flexibility.

tools, mills, tank farms, heat exchangers, and thousands more. How do you collect meaningful information from each? Plus, data security is always top of mind.

PRIORITIZE YOUR DATA

When getting started with adding the cloud to your plant-floor operation, project goals should start small. State your objectives to help understand what you want to get from the data to help you make a comprehensive decision. By starting small and first selecting a manageable amount of data that is the most impactful, you can easily pilot your first round and then grow your cloud tools from there.

WAGO SOLUTIONS

WAGO's PFC controllers become IIoT controllers that safely and efficiently send near real-time data from the field level to the cloud for information at your fingertips. We have embedded the MQTT protocol in our Linux-based PFCs, enabling secure data exchange between the plant floor and cloud services (Microsoft Azure, IBM Cloud, SAP Cloud and others). These same controllers also support the Sparkplug and OPC UA standards for seamless data exchange with SCADA applications. Our focus on cybersecurity tools helps users transfer this data in a secure manner with TLS security and built-in firewalls and VPNs. Manufacturers can leverage the PFC controller's fieldbus gateway features to collect data from multiple plant-floor machines and securely pipe it north to the cloud.

Wireless moving into the mainstream

Mike Fahrion of MultiTech Systems shows how Wi-Fi, LoRaWAN, and 4G and 5G cellular can simplify and streamline wireless applications

By Jim Montague

Far from being limited to process automation and control, wireless is making gains on all manufacturing and business fronts, just as it's taken over many consumer and mainstream applications. However, just like all forms of networking, wireless is still driven by its users and their innovations and requirements. And, despite its gains in all these areas, common-sense considerations and studies are still needed to determine what each user, application and site needs.

"OEMs want to make their devices smart and connected, often motivated by field service productivity and flexibility gains. They want connectivity with field assets, such as distributed solar generation, without a big investment in backhaul networking. And they want end-to-end solutions that integrate into their existing business processes and applications," says Mike Fahrion, CTO at MultiTech Systems Inc.. "Wireless technology has matured to the point where it can be integrated into most any application with rapid adoption where there is a high field service requirement. Pest control, medical sharps disposal units and even paper shredders are becoming smart, connected products."

In the commercial and enterprise spaces, Fahrion reports that MultiTech is seeing three wireless technologies becoming standard:

- Wi-Fi for smart spaces like campuses, stadiums and oil and gas plants using it to extend the reach and mobility of Ethernet, but focused on networking of IT type assets, not mission-critical processes;
- Long-range wide area network (LoRaWAN) is becoming the norm for wireless sensor networks. LoRaWAN has a mile or better range, sensing nodes can be battery powered lasting five to ten years when configured to report-by-exception; and
- Private cellular networks using 4G and 5G provide high data throughput, low latency and mission-critical reliability bringing the benefits of wireless connectivity to applications that previously required wired connections.

"Privately managed LTE cellular is hosted by the user instead of a carrier. It's totally private and managed, and lets users deploy only the devices they want, including managing their own bandwidth," explains Fahrion. "For example, due to COVID-19, schools are giving out Chromebook laptops, and putting private cellular antennas on the school's roof, which lets local students log in for remote learning, even if they don't have Wi-Fi at home. The advancement of standards based wireless technologies i displacing older, proprietary radio frequency (RF) wireless. The shift is to standards-based wireless drives down cost and provides users interoperability."

While he agrees that full site surveys haven't gone away, Fahrion adds fewer being done because users can put in wireless devices and simply validate it to see if it works. "LoRaWAN has remarkable receive sensitivity and operates at 900 MHz bands. Its high link budget makes it easy to pick up a good signal, even without line of sight, so they often get by without a site survey" says Fahrion.

Despite these advances and the fact it's easier to use, Fahrion reports that users still have to think through how they're going to use wireless. In wired solutions, we tended to send a lot of extra data because there were few consequences. "Wireless applications often imply battery power so we should think differently about the cost of data. Do you need to report every minute, every 15 minutes, or just when values change?," asks Fahrion. "People are transitioning to wireless without shifting their mental paradigms, so they're often paying for more than they need, both in power and bandwidth. Many users don't need a report every 100 milliseconds, so they should only send a message when a threshold is reached, such as going over 100 °C, which uses a lot less battery power. They also need to decide on a format to get their information into real-life values."

Even though LoRaWAN's physical and network layers are common, its sensor data payload hasn't been standardized yet,

so configure or code systems to decode payloads from different devices. “This is one part of LoRaWAN that’s still messy,” says Fahrion. “Some vertically focused application groups, such as smart metering are driving more standardization to include data payloads.”

Fahrion concludes many users are mixing and matching wireless technologies based on the needs of their applications. “Some users are putting Bluetooth beacons on tools,” he says. “This can to indicate proximity to a receiver and battery status, then they’re adding LoRaWAN bridges to send their tags from tools up to a database.”

ABOUT THE AUTHOR: JIM MONTAGUE

Jim Montague is executive editor of Control.

He can be contacted at jmontague@putman.net.

Does your network have what it takes to create a smart factory?

"Connectivity is the key word when talking about digital transformation."

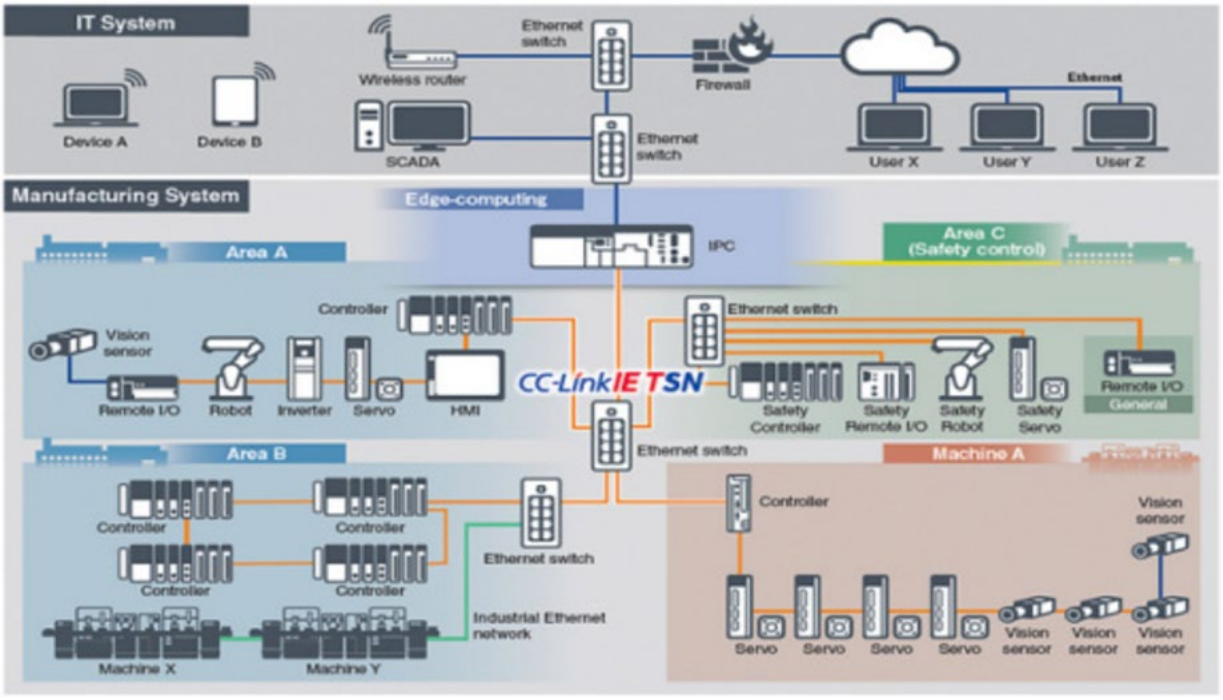
By Thomas Burke, global strategic advisor at the CC-Link Partner Association (CLPA)

Advanced-automation systems from roboticized manufacturing lines, AGVs, smart machines and integrated logistics are increasingly helping to create smart factories. These data-driven, responsive facilities can greatly enhance the competitive edge of a business. However, to realize this vision, an effective way of carrying the data and control signals is required to create an autonomous, interconnected, responsive and flexible factory.

Thus, the real protagonists are industrial networks. Let's take a closer look at how the right industrial network can jumpstart the way to a smart factory.

CONNECTIVITY—CRITICAL COMMUNICATIONS FOR DIGITAL TRANSFORMATION

Connectivity is the key word when talking about digital transformation. In fact, communication is the backbone of all the industrial components used to realize the Industrial Internet of Things (IIoT), as it brings together different entities on the factory floor, e.g., hardware devices, software tools and people, as well as higher enterprise-level systems. Connectivity enables them to collect, communicate and analyze data. By doing so, the industrial machines and the entire enterprise become intelligent systems, able to improve plant performance, productivity and flexibility.



Within this framework, a suitable network technology can go a long way toward boosting the capabilities of a factory, as it enables direct communication between manufacturing and management systems, resulting in the ability to control and make adaptive decisions based on real-time information. This is an essential prerequisite to achieving manufacturing-on-demand for a range of increasingly user-customizable products.

THE FOUNDATIONS OF A NETWORK FOR THE FUTURE

As a large volume of devices should be seamlessly interconnected in the factory of the future, keeping the costs down while ensuring good connectivity is essential. Currently, the most attractive physical layer available is Ethernet. Compared to traditional Fieldbus, this network technology is economical and faster. Therefore, industrial Ethernet provides a better price/performance ratio. In addition, industrial Ethernet offers the possibility to create different plant topologies and is generally easier to configure and scale, which are crucial considerations when defining an enterprise's automation strategy.

Not every kind of industrial Ethernet is sufficient, though. In order to establish an IIoT-enabled manufacturing line, large amounts of data from multiple devices need to be collected and transferred in real-time. Therefore, having enough network-bandwidth capacity is critical to the successful operation of these systems. More precisely, full-gigabit networks are becoming the standard for industrial automation.

In addition, the networking solution should be able to address different standards, as factories tend to adopt field devices and machines from different manufacturers to satisfy their production needs. As a result, open networks are key, as they provide the only solution to accommodate products from multiple vendors.

To address this aspect, it is best to use a network specification with increased openness, interconnectivity and compatibility with other solutions. For example, one that allows CC-Link IE and PROFINET to communicate with one another and allows individual devices to be connected to either network. Also, it could be beneficial to use a companion specification for machine technology and OPC UA that can enable further communication options.

TIME-SENSITIVE NETWORKING

Today, it is safe to assume that, in many cases, the network of the future will be a 1 Gbps Ethernet-based solution in line with the latest advances in technology, such as Time-Sensitive Networking (TSN). As well as offering real-time, deterministic communications, an open-protocol structure allows collaborative future development and, hence future-proofing.

Currently, there is only one industrial network that combines gigabit Ethernet performance with TSN functionalities to meet all these requirements.

SEAMLESS COMMUNICATION ACROSS ALL LEVELS OF AUTOMATION

An open architecture is a must for networks to accept devices from a number of manufacturers. However, this is not enough for the network of the future, which should maximize its compatibility on different fronts.

Not all installations are new and compatibility with legacy systems and devices is often required in 'real world' applications. Plus, there is always a transition period when updating an existing plant and machinery, which can include 100Mbit only connections. Yet there is only one network specification that supports these 100Mbit devices in addition to 1Gbps equipment and is easily implemented on devices or master controllers by software alone. It is a competitive advantage for a company to be able to add compatibility to its existing products without any hardware modification. Such a compatibility feature broadens the practical options when implementing upgrades or new equipment.

Secondly, the ideal system should support the convergence of information technology (IT) and operational technology (OT). It is essential to ensure that the data generated on the plant floor is accessible across all higher-level systems, from the control, supervisory and enterprise levels. This requires seamless vertical network integration, which can be obtained by using

a single protocol that can span across all levels of the enterprise.

This means that, in addition to having a large bandwidth, the industrial-communications network needs to be able to schedule different types of data traffic in a highly effective manner. In particular, time-critical control data should be prioritized to support determinism and reliability on the factory floor.

These requirements are best addressed by utilizing highly accurate traffic scheduling/prioritization capabilities. As a result, time-critical control data can be shared in a timely manner and congestions can be minimized, if not eliminated.

In addition, it is important to establish reliable communications between the field devices and the enterprise level by easily integrating with network layers such as Supervisory Control and Data Acquisition (SCADA) systems or Manufacturing-Execution Systems (MES). This enables the ability to fully monitor, manage and report plant-production processes.

A FUTURE-ORIENTATED & SCALABLE NETWORK TECHNOLOGY

The key design principles for digital manufacturing are real-time information-transfer capabilities as well as data transparency and availability across the enterprise for advanced analytics. To implement these functionalities, it is essential to select the right industrial network, one that can accommodate different types of traffic generated by a broad range of devices while ensuring the timely delivery of each data packet.

By providing combined openness, gigabit bandwidth and TSN capabilities in an industrial-network specification, businesses can succeed in the creation of advanced digital-manufacturing strategies that enhance productivity and competitiveness.

Straight talk on cybersecurity

Experts from Acquired Data Solutions, Emerson and Rockwell Automation provide practical advice on establishing and maintaining cybersecurity protections

By Jim Montague

Much of the useful news, historical context and practical advice on cybersecurity comes from end users and system integrators who've already run the gauntlet. However, most recovered from cyber-probes, -intrusions and -attacks by implementing effective new tools and software from process control and automation suppliers, who have plenty of helpful recommendations on how to protect process operation and facilities. Here are a few of the latest.

ACQUIRED DATA SOLUTIONS

Steven Seiden, president of Acquired Data Solutions, reports it addresses cybersecurity by making it part of an overall risk management framework based on NIST 800-53, which it uses to make its automation testing products secure. It's also made cybersecurity part of its engineering lifecycle as it's continued to emerge in the past three to five years. ADS is a system integrator and industrial automation testing firm in Rockville, Md., and member of the Control System Integrators Association.

"We help users develop risk profiles based on NIST 800-53, mostly for aerospace and critical infrastructure applications, and conduct penetration testing of development, security and operations (DevSecOps) to address ransomware," says Seiden. "This is crucial because one of the major trends we're seeing is a systematic mining of potential attack surfaces. Unfortunately, during and after COVID-19, many of the network boundaries that used to be

limited to the organizational boundary have disappeared, and now everywhere is becoming an attack surface. Consequently, we need user-defined and dynamically defined boundaries, along with smart security applications that can see them."

To enable more intelligent cybersecurity, ADS reports it recently partnered with Assert Security (www.assertsecurity.io), which provides security test automation solutions, such as its Vinari software. This partnership will enable ADS to make sure its users' Internet-linked devices and presences are secure, and conduct continuous, automated cybersecurity testing of software, which is increasingly required by governments and other organizations.

"These functions can only be done with smart security software," says Seiden. "In the future, we may also add mobile apps, so users can determine the locations of ports they want to keep open."

EMERSON

"When users set up industrial networks, they must also look at hardening and protecting them by changing passwords, finding open Ethernet ports, closing unused ports, encrypting communications, checking that networks are operating normally, and turning on time-synchronization functions," says Eric Braun, product security officer for Emerson's Measurement Solutions division. "It's also crucial to compartmentalize and segregate networks with firewalls and other defensive layers, and establish procedures for examining logs and quick remediation. To identify where probes and intrusions occur, network forensics can be carried out by an in-house or outsourced team that blends IT and OT experts, but it's likely best to call in a third-party for remediation."

Based on the content you've read, we recommend these articles just for you!

- Integrators make cybersecurity approachable
- Overcoming (human) inertia for cybersecurity
- Cybersecurity? Just another process control job

To address similar and growing concerns about device-level cybersecurity, Braun reports that standardized network protocols will be needed. "The lower levels of the Purdue model for industrial control system (ICS) security used to be isolated, but they're becoming more vulnerable, too," says Braun. "You can make a regular device-level protocol like HART more secure, but the result is it can't interface and loses its interoperability. Consequently, we need to use more open protocols that can also provide device-level security. These include HART-IP that supports native security; OPC UA that can adjust to its own security model; MQTT that can add security functions; and Ethernet Advanced Physical Layer (APL) that provides interoperability

and security. Open protocols can also publish details that can be reviewed, and use encryption algorithms and private software keys. Former proprietary protocols are less open and less able to be reviewed, which makes them weaker."

Braun adds that Emerson has implemented OPC UA and a secure version of HART-IP in its products, and "bakes in" cybersecurity at all stages of its design, development and testing processes. "We also use threat models, perform vulnerability assessments, and conduct penetration testing," says Braun.

ROCKWELL AUTOMATION

"Cybersecurity starts with best practices like performing asset inventory and risk assessment, then identifying vulnerabilities and applying things like network segmentation to mitigate risks," says Tim Mirth, PlantPAx platform leader at Rockwell Automation. "We're seeing an increase in attacks, such as ransomware, since many cybersecurity best practices aren't in place. Sometimes it's the use of outdated equipment, exposed networks or a lack of sufficient backups that safely restart operations. That means having securely stored and tested backups of things like servers, controller configuration files and even historical data."

Along with protecting assets, Mirth reports more insurers are requiring process industry companies to establish and maintain robust security postures. This includes aligning with standards and partnering with security competent companies. "Once you identify your assets and any vulnerabilities, trusted partners can provide guidance to help mitigate those vulnerabilities," says Mirth.

Because security is multifaceted, Mirth explains that product-only security isn't enough. He adds that network segmentation is necessary due to growing use of remote access. Segments and functional zones can be separated by logical segmentation, using virtual local area networks (VLAN), firewalls, demilitarized zones (DMZ), encrypted tunnels and other network strategies depending on the company's risk posture. "Segmentation planning involves multiple steps. First, identify process zones requirements and risks, such as functionality, efficiency and criticality. Next, make judgement calls on the risk posture of each zone. From there, separate critical production processes and their network from less-critical, higher-up administrative and enterprise areas to reduce the threat landscape," explains Mirth. "Then the main question becomes how to control communications between areas if they need to share data? This where we need to apply authentication, authorization, firewalls and cryptography."

Mirth concludes that cybersecurity must be continually updated over the lifecycle of the process system. "All users, system integrators and the like have to be authenticated

and authorized to access information, and that list of users needs to be updated, just as software patches are updated. Users and patches that are OK today may not be tomorrow," says Mirth. "ODVA CIP Security and other protocols are beginning to define ways to gain end-to-end and device-to-device capabilities that will lead to a zero-trust and zero-touch security landscape. This is an exciting premise. We're not quite there yet, but development continues for OT-based applications and users.

"Likewise, there are other promising technologies, such as software define networking (SDN), that could allow another layer of defense by restricting data flow and improving network availability. For example, SDN enables micro-segmentation from one device or area to another – almost like their own personal network. SDN can also be used to increase availability by providing multiple network paths, all of which can be obfuscated to the user, so that they can focus on running their plant. SDN still needs proven for OT demands but has been used in the IT space for a few years now. The technology is promising as security strategies continue to evolve."

ABOUT THE AUTHOR: JIM MONTAGUE

Jim Montague is executive editor of Control.

He can be contacted at jmontague@putman.net.