New Security Technologies for New IoT Threats
The industry requires a high level of protection in its processes because of the importance that its information represents. That is why CC-Link IE has the necessary safety certifications implementing corrective measures, control methods and safety curtains to generate confidence and efficiency. CC-Link IE is the future in communication technologies today.
CONTENTS

— 04  New Security Technologies for New IoT Threats
— 11  IIoT Applied: Predictive Maintenance on a Compressor
— 19  Cisco Uses IoT-Based Systems for New Innovation Center
— 26  How IIoT and E-Commerce Are Redefining Customer Value
— 33  Chinese Tire Manufacturer Upgrades to Industrial Ethernet
— 42  Discover the Power of Connected Assets
— 49  Future-Proofing Your Industrial Network
New Security Technologies for New IoT Threats

BY THOMAS NUTH
Director of product marketing, Nozomi Networks

Knowing how to assess the ability of cybersecurity technologies to handle the ever-changing threat landscape facing industry is critical to making the right technology decisions.

Industrial control systems (ICSs) have grown increasingly connected to the Internet over the past decade—a trend showing no signs of slowing down. Though accelerated connectivity of the ICS has helped to optimize automation, it has also exposed new operational risks and cyber threats. As evidenced by the recent appearance of Industroyer/CrashOverride and Triton, we are clearly experiencing a rising tide of targeted attacks on ICSs and operations technology (OT) networks.

To develop a truly comprehensive approach, it’s important for industrial companies to heighten capabilities for real-time visibility and threat detection within their OT environments that complement IT processes.
and existing cybersecurity infrastructure. As a user seeking world-class operations, continuous improvement and risk management, you must be able to evaluate the best solution for your needs.

The first step in this assessment process involves the recognition that the typical ICS environment is multi-tiered—consisting of various network segments, such as Ethernet TCP/IP, cellular, LAN, serial control and remote/intelligent I/O. The disparate and often proprietary nature of OT networks means that some segments—and the communications between them—cannot be monitored using traditional network and cybersecurity tools.

To address this, leading ICS cybersecurity solutions extend the visibility of IT cybersecurity into OT environments. These solutions generally deploy non-intrusively and provide visibility and detection across all corners of complex OT networks. For example, when an engineering workstation sends data to remote terminal units (RTUs), Nozomi Networks’ SCADAguardian discerns between a case where the RTU is being communicated with directly vs. when the RTU is being used as a gateway to a physical device. In this direct communication circumstance, a conventionally secured industrial network would be exposed to attackers through a nested node without the network security personnel being aware that these connections even exist.
A hybrid approach to threat detection

New forms of malware are emerging on a weekly basis. This reality requires a multi-faceted approach to threat detection, empowering users to be attentive, responsive and proactive in their ICS cybersecurity posture. To achieve this, the best choice of ICS cybersecurity solutions offers a hybrid approach to cyber threat detection, comprised of both behavior-based anomaly detection and rules-based analysis.

Behavior-based anomaly detection is foundational to any ICS cybersecurity approach. The ability to non-intrusively learn and monitor all traffic within an OT network enables the user to identify would-be cyber threats, with context, that would otherwise go unnoticed using conventional active cybersecurity approaches, such as industrial firewalls and agent-based security information and event management (SIEM) systems.

Achieving a useful level of contextual analysis is what separates behavior-based anomaly detection from conventional cybersecurity. The difference relies on a solution’s ability to support the correlation and covariance-testing of many anomalies across a geo-distributed,
CONTINUED

New Security Technologies for New IoT Threats

multi-tiered network. Often, a common root cause can be attributed to thousands of cyber incidents, so understanding the underlying culprit is critical to achieving fast forensic analysis and remediation.

Utilizing rich analytics engine and artificial intelligence (AI) techniques, SCADAguardian identifies both process and communication anomalies, including correlations with process data readings and critical state awareness. Examples of anomalies detected include modified and/or added devices within the network, or irregular commands and communications like bandwidth and latency variances. This concept of contextual correlation allows SCADAguardian to rapidly organize, aggregate
and assess anomalies according to threat category, risk level and location within the network.

Rules-based analysis provides a proactive threat-hunting component to ICS cybersecurity strategy and posture, allowing users to leverage deep packet inspection to help uncover malware cyberattacks on their network and to initiate a response prior to the initial infection phases. Rules-based analysis is a key component to Nozomi Networks’ hybrid threat detection approach, which uses both external rules (such as Yara rules and packet rules) and proprietary rules inherent to SCADAguardian’s unique and customizable analysis toolkit. Both forms of rules-based analysis are effective for proactive threat hunting.

An integrated IT/OT cybersecurity posture
A final discerning factor to define successful cybersecurity strategies is how well the solution scales and meets the demands of a large, geo-distributed enterprise. For scalability, ICS cybersecurity solutions must integrate seamlessly with existing IT-oriented security infrastructure, working with firewalls, SIEMs and other enterprise IT components. ICS cybersecurity solutions should scale laterally across geo-distributed networks and vertically between multi-tiered levels of supervisory and operational control.
With these factors in mind, application programming interface (API) openness, protocol support capabilities and product segmentation define the key integration and scalability capabilities of ICS cybersecurity solutions. Here’s what to look for in those three areas:

- An API is a set of defined functions and methods for interfacing with the underlying operating system; it is essentially a software gateway that makes it possible for applications to interact and share data. Not all APIs are equal and should be tested in the evaluation phase of ICS cybersecurity solutions. The API will dictate how easily and effectively a solution integrates with existing applications and adapts to the future direction of the overall enterprise architecture. For example, the API should be tested to support secure bi-directional flows that will allow sharing data with other applications and ingesting data from other sources for valuable real-time analytics, such as the aforementioned contextual correlations, when anomalies are detected.
New Security Technologies for New IoT Threats

- A protocol software development kit (SDK) allows for the parsing and analysis of various OT and IT protocols and gives the user the ability to dissect protocols that are proprietary and require anonymity, including secrecy from the ICS cybersecurity solution provider. Nozomi Networks’ protocol SDK allows the user to maintain secrecy, as required, while still taking advantage of all the integration capabilities provided by an open API.

- The ICS cybersecurity vendor of choice should support expansion and adaptability to future additions and changes to the enterprise architecture in a cost-effective and secure manner. To evaluate the readiness of an ICS cybersecurity solution provider to adjust and scale, evaluate the sourcing and segmentation of its product offering to determine how much of the complete stack—from hardware to operating system—the company owns and controls. Find out if they segment their solution physically or virtually. Also ask how they can effectively deploy their solution to support various application scenarios that require different bandwidth requirements.

Assessing these future-proofing, total-cost-of-ownership questions will help you select an ICS cybersecurity solution that best fits your current and future requirements.
You may have been thinking about doing an Internet of Things (IoT) application that could help your company, but embarking on your first industrial IoT application might seem daunting.

I’ve heard Benson Hougland, Opto 22’s vice president of marketing and product strategy, tell people to “start small” or “just get started.”

But how do you do that? My advice is to think of a desired outcome first and go backwards to what technology it would take to achieve that outcome.
INDUSTRY 4.0
WELCOME TO THE FUTURE...WE’VE BEEN WAITING FOR YOU.
A future-proof industrial network is one that provides performance for today and flexibility for tomorrow. PROFINET is the only industrial Ethernet standard built to handle the requirements of the shop floor while supporting multiple protocols like OPC UA for the top floor.

Are you ready for Industry 4.0?
For more information visit http://us.profinet.com.
Monitoring a compressor
I decided to see how I might do this for a simple example: a compressor. Compressors are very common in most industrial facilities and buildings, can be instrumented fairly easily, and are great candidates for predictive maintenance—one of the terms you hear a lot in the context of IoT.
CONTINUED

IIoT Applied: Predictive Maintenance on a Compressor

So, my desired outcome would be to move from preventive maintenance to predictive, as well as to eliminate the unnecessary costs that often result from scheduled maintenance (yes, there is such thing as too much maintenance).

The compressor I looked at is a 40 hp rotary screw compressor, and a great example of legacy equipment you might want to get data from. It has visual analog gauges for some parameters, but no connection of these values to the outside world.

The facilities manager responsible for this compressor told me they perform preventive maintenance about once a year, and we found a report from the most recent service. I verified with the manufacturer’s documentation that these items lined up with yearly service recommendations. There were also other checks and maintenance items recommended at weekly, monthly and three-month intervals.

What values to monitor?
To move from this periodic compressor maintenance to predictive maintenance, the three parameters I decided to monitor were motor temperature, vibration and motor current.
IIoT Applied: Predictive Maintenance on a Compressor

These parameters are good indicators of compressor health, are simple to start with, and can be instrumented without much effort or cost—and without taking the machine apart.

Tracking differential pressure across the compressor’s fluid would also give us great data to trigger filter replacement, but measuring it might require pipework. It was decided that tracking motor current and, perhaps, adding temperature sensors on the fluid pipes would suffice for now.

For temperature, all we’re looking for is a trend, so a simple Type J or K thermocouple could be mounted on the motor housing. This would be wired to a SNAP-AITM thermocouple input module.

Next, we would need a vibration sensor with a 4-20 mA output. These sensors are widely available, inexpensive and could be mounted on the motor and other areas. We would need 12-30 VDC to power the loop, and the 4-20 mA signal would be wired to a SNAP-AIMA module.

Next, we could measure the motor’s three-phase current by using three split-core current transformers installed at the compressor
IIoT Applied: Predictive Maintenance on a Compressor

disconnect switch. The motor is rated at about 90 A, so we’d select appropriate current transformers (CTs) with an adequate inner diameter to accommodate the feed wire. Many CTs have a standard 5 A secondary, so we would wire these three signals to two SNAP-AIARMS modules.

To complete our monitoring system, we would need:
- A four-position I/O rack, SNAP-PAC-RCK4, to mount our modules.
- A rack-mounted controller such as the SNAP-PAC-R2.
- A power supply to power the monitoring system. Since we will need DC power for the vibration sensor, we could select a SNAP-PS5-24DC.

I noticed an Ethernet switch close by with an available port, so we could put the monitoring system on the plant network. Configuring the I/O modules and points is easy with the free PAC Manager tool.

Getting data where it needs to go

At this point, we would be ready to start getting the data somewhere where we could log it, visualize it and get notifications on anomalies.

This “somewhere” could be on the same network as the monitoring system (that is, at the edge), using something like a groov device. Or it could be in the cloud, using one of the many third-party IoT platforms out there, such as IBM’s Watson. Watson has a basic rules
IIoT Applied: Predictive Maintenance on a Compressor

engine for notifications, and the data could also be shared with other Bluemix services for more advanced analytics.

With this simple, inexpensive IoT application of condition-based monitoring built on these three parameters, we should have enough data to move from preventive maintenance to predictive for the compressor.

The project is also scalable. After some experience and insights are gained, additional sensors and instruments could be installed on other pieces of equipment and the monitoring system expanded. It could even include controls to react to actionable intelligence derived from the collected data.
Top-down OT Cyber Security Management Simplified with ICS Shield®

Top-down cyber security for multi-vendor OT assets. With more than 6000 installations at industrial sites globally, ICS Shield® is Honeywell’s field-proven top-down operational technology (OT) cyber security management platform for securing connected Industrial Control Systems (ICS)/SCADA environments.

For more information, visit www.hwll.co/ICSShield

© 2018 Honeywell International Inc.
Cisco Uses IoT-Based Systems for New Innovation Center

BY CHARLIE NORZ
Product manager, Wago-I/O-System

Though not an industrial example of an Internet of Things technology application, Cisco’s use of IoT to communicate with traditional building systems using Wago’s BACnet Controller provides useful insights for industry.

With the opening of its openBerlin Innovation Center, Cisco is writing a new chapter in building technology to provide the company with an idea factory and innovation platform for the Internet of Things (IoT). With a research focus on manufacturing, transportation and logistics, the purpose of the openBerlin Innovation Center is to draw in researchers, developers and representatives from leading institutions, customers and partner firms. Cisco’s initial plans include collaboration with companies like azeti, Bosch and Intel.
Networking technology partners

Cisco set the technological bar extremely high for the openBerlin Innovation Center, which is located in a former manufacturing facility that was operational until 2014. The 1,000-square-meter space, designed as an open work environment and equipped with about 100 workstations, will be outfitted with more than 10,000 sensors...
Cisco Uses IoT-Based Systems for New Innovation Center

and high-tech communication units to detect the most detailed information about current conditions, as well as the movement of people within the building. Data collection in the center will extend from lighting and climate conditions to facial recognition.

Use of open source standards and ease of communication were of critical importance to Cisco in its selection of technologies to be used for the building. This meant that, when it came to identifying technology partners, “we needed partners who believed in our vision, were open to new concepts and could bring with them the flexibility to implement this project under time pressure,” says Mitko Vasilev, co-founder and CTO of openBerlin.

The team was given just three months to complete the design and installation of the building automation.

For the IP-based aspects of the project, Cisco turned to relayr, Berlin-based IoT experts. The system integration specialists, Hosch Gebäudeautomation (Teltow, Germany), and its technology partner, Wago (Minden, Germany), provided the designs and implemented the building technology.
Cisco Uses IoT-Based Systems for New Innovation Center

Wago’s 750-831 BACnet/IP programmable fieldbus controller with Codesys forms the core of the system installed at the openBerlin Innovation Center. Serving as the link between the IP-based sensors and the conventional building technology, it handles control of room automation—for example, control of all pumps and fans for room temperature regulation—as well as the facility’s lighting technology.

No need for building management systems

The modular design of the BACnet Controller, part of the Wago-I/O-System 750, offers an extremely high level of flexibility in the compilation of the necessary I/O modules, which provides it a high degree of scalability. It also allows for the incorporation of different protocols—such as LON, KNX, MP-Bus, EnOcean and SMI—to be united into one system. For example, the meters in openBerlin’s tap electrical consumption and hot water use M-Bus, while the lights are controlled via DALI.

Wago’s controller communicates with the facility’s IoT-based control system using BACnet. There is no building management system.

The building’s multifunctional sensors, around 3,000 of which have thus far been installed, unite eight sensors in one device and transmit their data via Wi-Fi and Bluetooth. The data from these sensors are
Cisco Uses IoT-Based Systems for New Innovation Center

collected, filtered in a fog gateway located in the building, and can be accessed via the cloud using a web application. This allows users with a smartphone or tablet to individually regulate environmental conditions in the building, such as lighting scenarios that include light intensity settings and color options.
Though customizable as described above, openBerlin’s building automation is designed to automatically set lighting and the indoor climate control to optimal comfort conditions without outside intervention. This includes handling light intensity and color change according to the season or time of day, so that the best conditions exist. To create optimum indoor climate conditions, the sensors detect temperature, humidity and CO2 content, which the BACnet controller then processes. For example, if more people gather in one space, the system registers this and automatically lowers the room temperature.

“At the moment, we record 26.5 GB of data per day,” Vasilev says. “Of that, we probably use only about 5 percent.” This usage level is expected to change as the system is expanded with artificial intelligence to integrate, for example, proactive measures in building automation.

In terms of the investment cost and energy efficiency of this project, Cisco notes that, in comparison with other Cisco properties, using the IoT-based approach employed for openBerlin saved the company about 30 percent in costs. Energy savings amount to about 60 percent, due in part to the need-based temperature and lighting control.
“We are highly satisfied with the results of the project,” Vasilev says. “The IoT-based building automation, which we developed with our partners, is the most innovative and modern open-source system. At the same time, it relies on components that are available in series production.”

The openBerlin project will serve as a global model for other Cisco innovation centers and projects.
Every day, technologies are blending in new and exciting ways that profoundly change our personal and professional lives. Just last week, my car sent me an email alerting me that its tire pressure was low. Last month, I met the leader of an 11-person manufacturing company who replaced a stubbornly traditional supplier with a collaborative robot on her own shop floor because the robot delivered much faster. Perhaps you too are sitting side by side with an artificially intelligent device right now. (Hi, Alexa!)
BEHIND EVERY GREAT PROCESS IS A GREAT HMI.

Since 1983, Maple Systems has been a global leader in industrial control products. Perfect for any machine or industry, our powerful HMI and IIoT solutions have you covered.
However, few such convergences are as promising for today’s manufacturers as a more accessible Industrial Internet of Things (IIoT), an increasing buyer preference to buy direct online, and the connected infrastructure to make it possible. These factors have brought us to an inflection point—where customers want more information about the manufactured products they buy and manufacturers can collect and understand more information about their products than ever before. The crux of it all is elegantly transforming that vast amount of raw data—not just into better business decisions—but into true customer value.

This is a trend already taking shape as manufacturers lead the way in the world of connected devices. According to a report by IDC in December 2017, the industries expected to spend the most on IoT solutions in 2018 are manufacturing ($189 billion), transportation ($85 billion) and utilities ($73 billion). By supporting manufacturing operations with more complete information collected in real time, organizations are producing higher-quality products at a more rapid and predictable pace with a more cost-effective use of resources.

What’s more, the IIoT provides a nearly untapped world of transparency into the supply chain. More and more connected devices switch on every day and share up-to-the minute information...
CONTINUED

How IIoT and E-Commerce Are Redefining Customer Value

about all kinds of players in the supply chain—like how long a ship has been out to sea, conditions of machines on the factory floor, or exact compositions of metals. This type of data has the potential to unveil all sorts of information about a manufacturer’s end product that can influence a purchasing decision or years of brand loyalty. It’s
the kind of authenticity that is not for the shy business leader, but it’s exactly what a growing majority of buyers want and for which they are even willing to pay a premium.

The 2017 Forrester Research report “A Brand New Day in B2B Commerce” revealed a staggering opportunity for brand manufacturers. More than 85 percent of B2B buyers will visit a brand’s site when they research online, 54 percent of B2B buyers trust a manufacturer site for best information, and 20 percent are even willing to pay slightly more to buy direct. Buyers are seeking authenticity and trust, and they (rightfully so) perceive that the most reliable source for accurate product information is the group of people who make those products. Whatever your online presence, buyers are visiting your website. It’s up to you to capture them before they jump away to Amazon or another competitor.

But e-commerce as an evolving technology comes with its own business challenges and rewards. B2C and B2B customers alike expect you to enable a pleasant customer experience. They expect to find 100 percent accurate and complete product information on your website, compare products side by side, see inventory levels, access discounts and personalized pricing, configure products to
their liking, check out in a totally secure environment, and the list goes on and on. As a consumer that presumably buys online, too, I’m sure you can relate.

But, as a manufacturer, how do you enable IIoT and e-commerce in a meaningful way that creates new revenue opportunities and drives business growth? Advances in cloud applications have made it easier than ever for manufacturers to consume this type of innovation. “Manufacturers upload more data to the cloud on average than any other industry, and are second only to high tech in how many cloud services they use,” according to the 2016 Skyhigh Research, “Cloud Adoption and Risk Report.” No other software deployment model than the cloud offers the scalability or global presence to accommodate the incredible numbers of devices connecting into the IIoT every day. Cloud-based enterprise resource planning (ERP) systems with integrated e-commerce solutions and fully responsive websites have the power to connect customers with the most accurate account and product information available, however and whenever they wish.
Nozomi Networks Takes the Lead in ICS Cybersecurity

The Indductroyer and Triton attacks in 2017 clearly signal that industrial control hacks are real and growing in sophistication. For critical infrastructure, ICS cybersecurity is no longer an option. Nozomi Networks is leading the charge with proven technologies that leverage artificial intelligence and machine learning. Our solution continuously monitors operational technology (OT) for cyber threats and process anomalies, providing real-time protection for critical infrastructure and ensuring industrial reliability.

PROVEN 3RD GENERATION SOLUTION

- First AI-powered ICS anomaly detection
- Industry’s only hybrid threat detection (behavior + signature)
- Easy and effective deployments and integrations
- Flexible and responsive ICS experts
- First ICS cybersecurity platform for MSSPs
- ISO 9001: 2015 Certified

SUPPORTING

200,000+ DEVICES

200+ INSTALLATIONS

~$24 MILLION IN FUNDING

5x CUSTOMER GROWTH

4x EMPLOYEE GROWTH

DEPLOYMENTS IN 5 CONTINENTS

SERVING CUSTOMERS IN

ENERGY  OIL & GAS  MANUFACTURING  CHEMICALS  MINING  PHARMA

nozominetworks.com
With the Chinese tire industry undergoing a period of massive growth—the total volume of tires produced in China increased from 112.4 million in 2000 to 630 million in 2014, accounting for more than one-third of the total global output—the rapid deployment of modern automation technologies has played a critical role in enabling this growth and positioning the industry to meet future market demands. Of all the equipment involved in the tire manufacturing process, composite extruders and four-roll calenders (a series of hard pressure rollers used to form or smooth a sheet of material) and their associated lines are the areas where networking...
communication lengths are the longest and where the greatest volume of communications data and number of stations reside.

The precision with which an extruded, semi-finished tire is produced plays a decisive role in the ultimate quality of the finished tire. Consequently, a great deal of attention to the control and drives systems of extruding equipment is required. This is why the application of a CC-Link IE network on a project at a leading Chinese tire manufacturer not only helped this manufacturer improve its production operations, it laid the foundation for the company’s ability to meet its planned annual production of 20 million semi-steel radial tires.

The automation project at this tire manufacturing facility combined the Mitsubishi Electric A800 variable-frequency drive’s speed and tension control system (floating roller function) with the CC-Link IE network. Another key technology coupling used in this project was the Mitsubishi Electric QJ71MES96 module (an energy source monitoring module) along with the CC-Link IE Energy option. The CC-Link IE Energy Management Communication feature optimizes detailed energy consumption monitoring. This function facilitates the collection and monitoring of energy data at the device/equipment level to realize significant energy savings throughout the facility.
Get your business set for growth.

To grow your business, you need to not only streamline operations and expand into new markets, but act on opportunities to enhance the customer experience. Epicor provides industry-specific, tailored ERP solutions to get your business set for growth and scale with business demand, fast.

Together, we are the Grow Getters.

Get your business set for growth at:
epicor.com/getsetforgrowth
Extruding and calendering

On an extrusion line, the stability of feeding materials is the most important influencing factor. Therefore, the feeding process is controlled by a pressure sensor in the extruder's nose. Every time a change in pressure is detected in the channel of an extruder nose, it can be proportionally fed back to the extruder and compensated for by adjusting the screw speed. Since every extruder is controlled independently, if the pressure inside the extruder nose is kept stable, the stability of the distribution of the rubber output and the semi-finished extrusion product can be guaranteed. Moreover, by using a continuous weighing system to monitor and check deviation in the quality of the semi-finished product, if any deviation from the tolerance set for the continuous quality of the semi-finished product is detected, the change is fed back to the production line drive and the speed is adjusted accordingly.

The main requirements of calendering are that distribution of tension should be stable and in accordance with process requirements. Calendering tension is mainly determined by the difference in the transmission speeds of the two machines. Therefore, the electrical system plays a determining role in tension adjustment and requires that the speed of each electric engine be automatically aligned on the basis of conveyor speed, with fine-tuning automatically
performed on the basis of actual tension. In addition, during the continuous production process, roller spacing is automatically calculated, maintaining conformity with the designated width. This means that the power and drive systems must have high-performance calculation and response speeds as well as high-speed, stable network communications.

**Network technology assessment**

Other automation suppliers looking to win this project also provided the tire manufacturer with solutions based on Ethernet network protocols. But when the performance and features were compared, CC-Link IE was shown to be superior to others in meeting the customer’s requirements. The biggest differentiators were network structure, speed and bandwidth capabilities.

One of the other proposed network protocol models used TCP/IP communication with a star topology structure, supporting a maximum communication speed of 100 Mbps. A maximum of 64 TCP/IP connections and 128 controllers were permitted for each module on this network. The distance between stations on this network was not specified, although expansion could be achieved with fiber-optic repeaters. The other proposed network for this project used Cat5 cable, with a maximum distance of 100 m and speed of 100 Mbps.
using TCP/IP communications. Topology structures for this network included star, tree, linear and ring. The input/output data volume for one series of interface modules in this architecture was 256/256, and it was expandable to 63 stations. A maximum of 256 stations could be connected with a second series of modules.

CC-Link IE’s communication speed is 1 Gbps, with a token-based communication technique providing for inherent deterministic communications. The maximum number of stations connected on a single network is 120 and the maximum number of networks is 239. Using multimode optical fiber, the maximum distance between stations is 550 m. When dual-loop topologies are used, the maximum transmission capacity is 1,920 bytes.

CC-Link IE uses tokens to control data transmissions and network shared memory for real-time data communications. Real-time requirements are high for composite extruders and four-roll calenders and their lines. Therefore, carrier sense with collision detection commonly used in general-purpose Ethernet cannot meet these requirements very well. The use of Ethernet tokens in CC-link IE to control the access time for each station to network shared memory means that only stations with tokens can read and write network shared memory, providing a level of security as well as determinism.
As a token is transferred to each station in a network, the station can separately complete its reading and writing of network shared memory. In this way, there can be no collisions when data is transmitted in the network. Since CC-Link IE uses Gigabit Ethernet technology, the transmission speed of tokens in the network is very fast, making connection scan time short. Plus, the CC-Link IE network can not only operate the current network configuration in a loop, thereby minimizing the probability and impact of communications faults, it can also support star and linear network topologies, as well as topologies combining them. This Gigabit Ethernet technology also provides the bandwidth to expand the communications and network data transfers without affecting the control of the network.

Matching drives with network capabilities
With the decision to use the CC-Link IE network made, this Chinese tire manufacturer then chose the Mitsubishi Electric A800 series variable-frequency drive (A800-R2R) due to its proven ability to control floating rollers and tension in composite extruders and calenders and their lines.

The cooling and winding equipment located at the end and back end of the composite extrusion production line is a crucial link in the entire production line. The quality of its operation does not only
have an impact on the condition of every operational segment of the line, but also impacts the finished products. Speed matching on these lines requires high-precision speed control. Winding control, in particular, requires good stability, high precision and constant tension control. In essence, line speed matching and winding control must ensure that the products are not stretched, no matter what changes might occur to the line speed or how the reel diameter of spools might change.

Mitsubishi Electric’s A800 variable-speed drive combines the required level of speed matching and reeling functions via speed tension control (floating roller control), torque tension control (with tension testing), constant tension control (without tension testing), roll diameter calculation compensation/preliminary roll diameter calculation/roll diameter memory, taper control, automatic adjustment of speed gain, short line detection, inertia compensation and materials length recording function. Since the external analog signals and operational controls are all completed within the variable-frequency drive, the application of the A800 variable-frequency drive in composite extruders and four-roll calenders and their lines mitigates the load of PLC operations and network communications while also avoiding human uncertainty.
When winding begins, the automatic arbitrary roll diameter calculation function can calculate the current roll diameter when starting, as the floating roller moves from its lower position to its target position. This facilitates winding with an arbitrary roll diameter. When winding is interrupted, the A800 can automatically adjust speed gain as the diameter continuously changes, thereby providing high system performance and safety. In addition, the inertia compensation function can reduce the phenomenon of tension lag resulting from increased deceleration. When winding operations have finished, the broken line testing function automatically detects the product tail to prevent excess speed.

The superiority of a CC-Link IE network has given the tire manufacturer a comprehensive solution featuring automation, energy management and information meeting the requirements of Industry 4.0. With the aim of ever-increasing partner satisfaction, the CC-Link Partner Association (CLPA) provides an industrial Ethernet network with an appropriate integral solution while providing Industry 4.0 customer needs.
Discover the Power of Connected Assets

BY DAN O’BRIEN
Strategy and marketing director, Honeywell Connected Plant

Are your critical assets performing their best? Is unplanned downtime draining the bottom line? Has the organization been chasing asset and process efficiency improvements? Stop reacting. Start predicting. Reexamine traditional approaches to asset performance management.

We all recognize that asset availability and performance, balanced against controlling maintenance costs and planned downtime, are essential for better productivity. The real challenge is knowing what the right balance is.

Understanding your strategy is the first step. Having an asset performance management (APM) strategy is the right direction when compared with the traditional, reactive approach of “run to fail.”
Traditional APM has focused on asset risk, reliability and maintenance cost reductions—largely based on conventional methods of asset monitoring. Implementation of traditional APM is considered complex and expensive and, as a result, is typically deployed only on capital-intensive assets. In addition, keeping such a system up to date and secure requires a significant investment in both IT and operational expertise and often involves multiple vendors. Furthermore, despite the valuable data generated by these systems, they are often disconnected and don’t help plant managers make confident decisions about how to operate.

**Smarter APM**

Though most plants operate efficiently, there are opportunities for improvement, especially when production is asset-intensive or capacity-constrained, or margin improvements aren’t optional. To assess your situation, ask yourself these questions:

- How easy is it to understand the economic impact of suboptimal equipment performance?
- Is it better to reduce throughput to extend the life of critical equipment? Or should the equipment be stressed to maximize current production demands?
• Is there excessive inspection of certain pieces of equipment that can be reduced to save maintenance budget?
• Can the potential maintenance cost savings be offset by the expected (statistical) losses of possible unplanned downtime?

Connecting three technology aspects—enabling secure connectivity to a wider set of assets, continuously monitoring both asset health and process performance, and combining predictive analytics with industry expertise—results in smarter APM and assures confident decision-making. A digitally transformed and connected APM strategy improves production certainty and outcomes by eliminating silos and effectively closes the loop between operations and maintenance.

Increasing uptime requires asset data, process data and operational settings to be brought together in a connected, secure environment. In this setting, asset and process experts can use analytics to find better ways to eliminate unplanned downtime and optimize equipment maintenance.

While assessing your situation, it’s important to realize that process and equipment are inseparable. Equipment failures can’t be completely analyzed, predicted or reduced by just looking at asset measurement data. Reliability of an asset is dependent on understanding how
Discover the Power of Connected Assets

a process is being operated and if that asset is being optimally maintained. After all, operation and maintenance-induced equipment failures account for the majority of unplanned downtime.

The best performance and equipment effectiveness comes from combining process knowledge with equipment expertise in a collaborative and connected software ecosystem.

Essentials of a connected asset performance strategy

There are several factors to keep in mind when planning a connected asset performance initiative:

• Realize that APM is rapidly undergoing a digital transformation. Traditional APM capabilities need large capital investment projects, many handcrafted interfaces and duplicated data sets. They also are often accompanied by complex system administration, upgrades and lots of end-user training. This combination can be a deterrent to improvement and strain plant resources.

• Leverage the simplicity and speed of connected software by working with a vendor possessing deep industry expertise to accelerate the APM deployment. Deployment time should be measured in days
or weeks instead of months or years. Consider an approach that blends secure connectivity, advanced analytics and automated software configuration for a solution that is as easy to live with as it is to sign up for and get running.
Discover the Power of Connected Assets

• Cybersecurity is not optional. Cybersecurity threats are pervasive and ever-growing. There can be no exceptions—every asset’s performance, operation or automation initiative must involve comprehensive and vigilant security methods.

• People are your most important investment. The best APM software in the world can only guide you in what to do. Improvements don’t happen without supervisors, engineers and operators trained to maintain and operate the equipment. Our next generation of process industry professionals will manage plants very differently, leveraging connected software in new ways that improve operations beyond what could be accomplished until now.

The bottom line is that you can avoid critical asset failure and unplanned shutdowns and improve bottom-line results by implementing a connected asset performance management strategy. With the proper technologies in place, plant personnel can more effectively collaborate to monitor and proactively manage production. Deploying a smart and connected APM initiative simplifies implementation, eliminates silos and effectively closes the loop for optimizing operations and maintenance.
PLC WITH BUILT-IN VPN & FIREWALL

PFC Series Performance Class Controllers

- VPN technology with IPSec and OpenVPN security protocols
- IIoT-ready application security with SSL/TLS encryption
- Firewall with whitelisting for increased network security

www.wago.us/PLC-VPN
Industrial networks are the humble foundation upon which an automation system is built. Often taken for granted, once a network is designed, installed and commissioned, there are other tasks engineers must tend to, not least of which include keeping their plant running at optimum efficiency. This reality means there are two points in the life of an industrial network where it gets the most attention: first, during specification, and later, if something goes wrong.

Concepts like the Industrial Internet of Things, Big Data and IT/OT convergence are making headlines and the race is on for companies to leverage each to gain a sustainable competitive advantage. It’s important to understand how industrial networks play a key role in turning these concepts into reality.
Choosing a network

Choosing an industrial network is only a trivial task if it is allowed to become one. Many questions arise when a new automation system is specified. “Which suppliers am I familiar with?” “What new technologies are out there?” “How much is all of this going to cost?” But rarely does someone ask: “Which industrial network should I choose?”

The answer to this question should be easy, but often isn’t because even deeper questions then arise. “What speeds and determinism are needed?” “Will other protocols run on the same network infrastructure?” “Are extras like functional safety or wireless relevant?”

Facing such questions underscores the fact that now, more than ever, the question of which industrial network you choose cannot to be overlooked. The reason these questions have become so important is because industrial automation is on the cusp of a transformation with the Industrial Internet of Things (IIoT). With so many IIoT possibilities available to industry, the focus for industry should be on future-proofing. After all, no one knows how all of this IIoT business will shake out. But like a home, future renovations made to the house won’t matter if the foundation is solid.
Since the winners and losers in the race to IIoT dominance remain uncertain, a future-proof industrial network will allow you to have your cake and eat it too. This means that the network should be robust, yet flexible. Robustness means an industrial network can handle whatever timing requirements are thrown at it, no matter
how demanding. Flexibility means an industrial network is not just a network unto itself (like traditional fieldbuses), but an infrastructure for other protocols as well.

This is a key point when it comes to IIoT uncertainty. As IT and OT networks converge, IT protocols are increasingly finding their way onto OT networks. Though this may seem to create an array of new questions about how to prepare your industrial network for the integration of certain IT protocols, the reality is that as long as the IT network protocols and your OT network protocols are based on open standards, it shouldn’t matter to a future-proof industrial network.

If something breaks

The other point in the lifecycle of an industrial network when it receives attention is if something goes wrong. Nine times out of 10, the root cause of network downtime is due to poor policies and procedures. For example, in some companies, the control engineers are responsible for the entire automation system, including network installation. In others, it is up to the electrician or the IT department to install the cabling. Without knowledgeable workers performing the network installation, proper procedures will likely not be followed. This can lead to wires without shielding, insulation being cut off,
Future-Proofing Your Industrial Network

bending radii limits exceeded, poor grounding, etc. This is why we at Profibus/Profinet International (PI) continue to put so much effort into our design, installation and commissioning guidelines for Profinet.

Another example of following poor procedures is how people treat the network. OT networks are not the same as IT networks. Take security, for instance. In IT networks, the priorities, in order, are: confidentiality, integrity and availability. In OT networks, the priorities are reversed: availability, integrity and confidentiality. Proper training is required to ensure that industrial networks are not only designed, installed and commissioned correctly, but that they are also treated properly.

Proof of being future-proof

If robustness and flexibility are the keys to a future-proof industrial network, there is one technology on the horizon that stands to make a big impact: Time-Sensitive Networking (TSN). The IEEE organization is taking many of the concepts formalized in Profinet IRT (Isochronous Real Time) and standardizing them in a new version of Ethernet called TSN. Therefore, companies looking to truly future-proof their industrial networks should choose a network that plans to utilize TSN from the device level to the machine level, up to the plant...
Future-Proofing Your Industrial Network

level. This technology will not be available tomorrow, but look for it in the coming months and years. It will provide future converged IT/OT networks a harmonized footing and ease possible pain points by providing robustness and flexibility.

The robustness and flexibility in Profinet to handle new developments like TSN is nothing new. From the outset, the protocol was created to be not only fast and deterministic for control, but an open network for other standard protocols that can handle anything from the need for microsecond-level speeds to providing an open infrastructure for TCP/IP or OPC UA.