September/October 2022 132
ISSN 1470-5745

industrial ethernet book

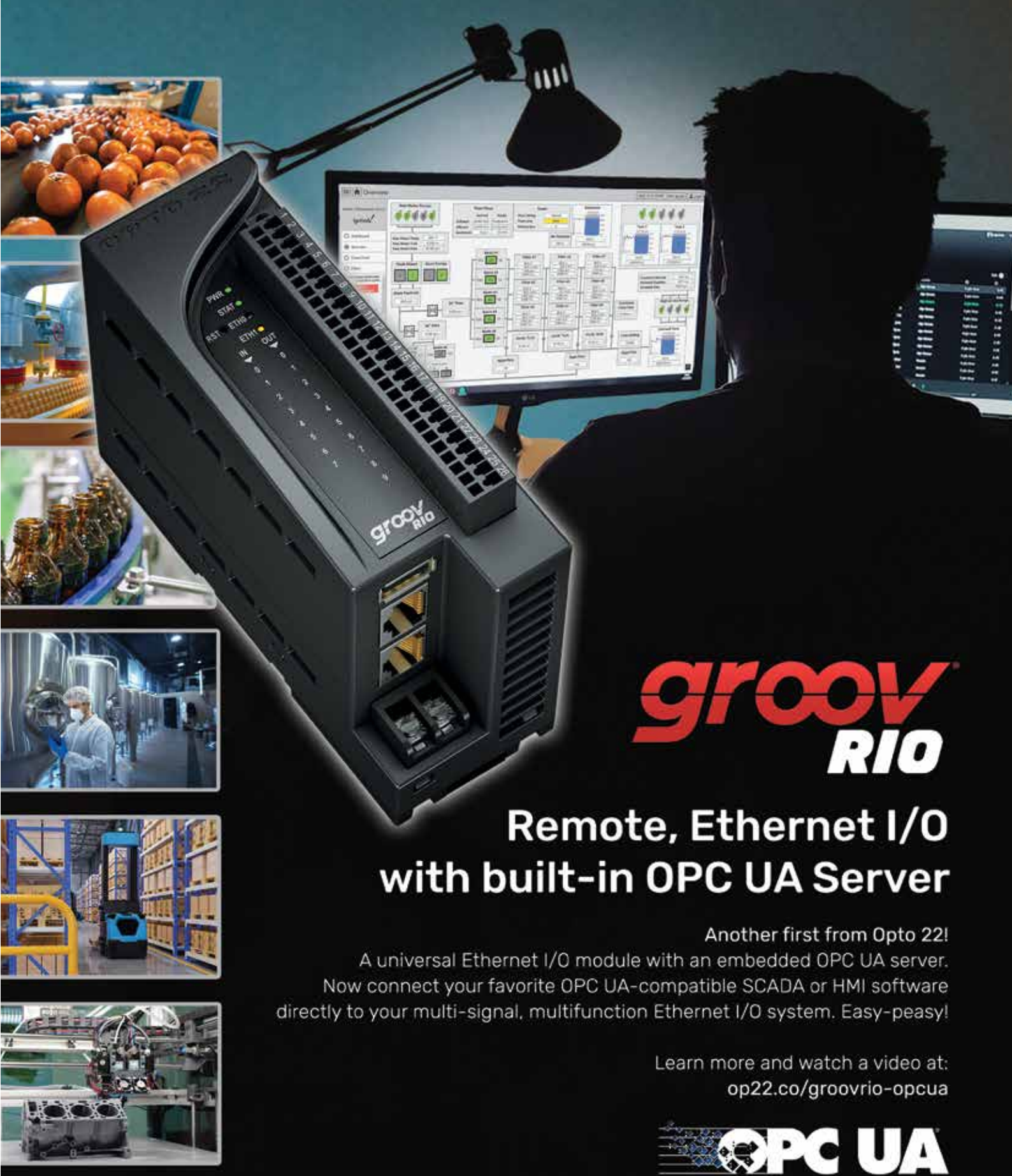
Industrial Ethernet Automation Networking & IIoT

Special Supplement

Industry Corporate Profiles

Page 37

Industrial cybersecurity: 2022 special report 6



groov RIO

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

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

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

OPC UA

MADE IN THE USA

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

OPTO 22
Your Edge in Automation.™

GET CONNECTED…

Visit our new website at: www.iebmedia.com

Rise in cyber attacks

Cybersecurity has become the number one challenge for automation control networks, given the increase in threats to networks worldwide and confirmed by recent research. With cyberattacks becoming so commonplace, technology suppliers are responding with new solutions for protecting networks.

According to the data presented by the Atlas VPN team, based on the Cyber Readiness Report 2022 by Hiscox, cloud servers are now the number one way in for cyberattacks, with 41% of companies reporting it as the first point of entry — a 10% increase from the year before.

The top cyberattack vector in 2021, corporate-owned servers, now occupies the third spot on the list. According to the 2022 survey results, 37% of businesses reported them as the main cyberattack entry method. Nearly half of companies experienced cyberattacks in the last year.

Meanwhile, the second spot belongs to the business emails. They were named as the main access point for attackers by 40% of businesses.

While the pandemic led to a shift in IT infrastructure in organizations, such as the wider adoption of cloud solutions, the security strategies of businesses fall behind the new technologies.

In total, 48% of companies reported experiencing at least one cyberattack in the last 12 months. Even with a 60% higher cybersecurity spending, cyberattacks rose by 5% compared to the year before.

Out of the surveyed countries, companies in the Netherlands suffered the most. There, 57% of companies reported having experienced cyberattacks in the last 12 months. Organizations in the Netherlands also saw the most significant rise in cyberattacks which increased by 16%.

The Netherlands is followed by France, where 52% of organizations had cyberattacks in the last 12 months. Cyberattacks targeting French businesses rose by 3% compared to 2021.

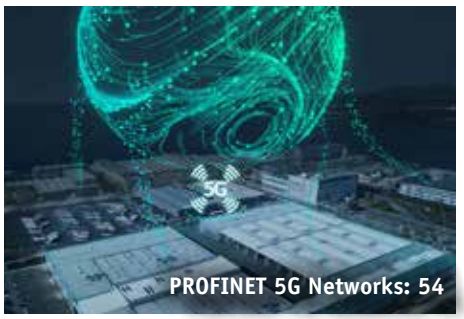
Next are organizations in Spain. Spain is the only country surveyed where cyber attacks decreased compared to the year before. Cyberattacks targeting Spanish businesses dropped by 2%, from 53% in 2011 to 51% in 2022.

Meanwhile, 49% of companies in Ireland went through cyberattacks in the past 12 months, followed by the United States with 47%. Cyberattack numbers there grew by 10% and 7%, respectively.

To read the full article, head over to: https://atlasvpn.com/blog/cloud-servers-are-now-the-most-common-method-of-entry-for-cyberattacks-at-41

Al Presher

Scalable automation controls: 52



PROFINET 5G Networks: 54

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **September/October 2022.**
Deadline for editorial: September 9, 2022 **Advertising deadline:** September 15, 2022

Editor: Al Presher, editor@iebmedia.com

Advertising: info@iebmedia.com

Tel.: +1 585-598-4768

Free Subscription: iebmedia.com/subscribe

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

Process Automation Device Information Model Standard

Collaboration promises to simplify integration of OT and IT systems by optimizing process automation end users' management of data from field devices

ISA100 WCI, NAMUR, ODVA, PI, VDMA, and ZVEI are planning to partner with FieldComm Group and the OPC Foundation to collaboratively develop the process automation device information model standard.

Major standards development and end user organizations serving the process automation industry announce today ongoing collaboration work on the specification for a standardized Process Automation Device Information Model (PA-DIM®). Participating organizations plan to share ownership of the specification and collaboratively participate in the PA-DIM working group, hosted at FieldComm Group, creating enhancements and extensions to the PA-DIM specification.

Expanding ownership to these organizations and their members will further solidify the adoption of the OPC UA-based standard model for core field device information in process automation plants today and new products going forward.

New co-owners of the PA-DIM specification include ISA100 WCI, ODVA, PROFIBUS/ PROFINET International, NAMUR, VDMA, and ZVEI.

SOURCE: ISTOCK

PA-DIM is expected to make a major impact on core field device information in process automation plants.

Statements of support follow:

Andre Ristaino, Managing Director of ISA100 WCI: "As a standards-driven organization, the ISA100 Wireless Compliance Institute has been supporting the ISA100 Wireless (IEC 62734) standard with its core mission of assuring device interoperability. The PA-DIM specification fits into our mission and we have adopted it as the foundation for standardized data exchange in our ISA100 Wireless ecosystem."

Ted Masters, President & CEO FieldComm Group: "PA-DIM helps bridge the gap between IT and OT systems in a protocol agnostic way. This coupled with the extensive use of semantic identifiers provides an ideal solution to allow end users to access instrumentation data from both the installed base and newly installed instruments. We are delighted that the major standards bodies and end user organizations in the process automation industry have agreed to collaborate on this important standard."

Michael Pelz, Vice President, Christine Oro Saveedra, General Manager, NAMUR (User Association of Automation Technology in Process Industries):

"NAMUR bundles end-user competencies for automation and digitalization within the process industry to enable more efficient, sustainable, and secure processes. NAMUR Open Architecture (NOA) aims to make stranded production data easily and securely accessible and more importantly usable for plant and asset monitoring as well as optimization. NOA enables this without compromising the availability or OT-Infrastructure of a production facility. In order to use NOA effectively, standardized information models are essential. For this reason, NAMUR, in cooperation with ZVEI, supported the PA-DIM activities at a very early stage in order to develop a common data model as an interoperable, non-proprietary interface. It is a great signal that the future development of PA-DIM is now supported and adapted by further organizations. A signal that with this broadly supported standard, investment-safe (NOA) projects can be realized in the long term."

Dr. Al Beydoun, President & Executive Director of ODVA: "ODVA is pleased to support the PA-DIM profile to enable greater information standardization within process automation, which will allow for more seamless data analysis and prognostics. End users of EtherNet/IP networks will be able to leverage PA-DIM to move data from the field to the cloud and to realize improved data standardization across networks."

Stefan Hoppe, OPCF President & Executive Director: "Digitization needs a secure transfer of globally accepted information models across industries, technologies, and applications. No single organization can achieve this alone! OPCF, as a co-owner from the beginning, welcomes to extend the ownership of PA-DIM to ensure this necessary global acceptance. OPC UA over MQTT is the only accepted field-to-multi-cloud solution - the combination with PA-DIM plus 70+ additional information models is unique."

Karsten Schneider, Chairman PROFIBUS & PROFINET International: "For us at PI, standardized information models like PA-DIM are a key enabler for the digital transformation. Since PROFINET is based on standard Ethernet, it can be used as the infrastructure in plants for all data exchange needs. With OPC UA being a perfect match for vertical communication in addition to PROFINET's powerful and rich feature set, your automation solution will be ready for Industry 4.0."

Andreas Faath, VDMA Head of Machine Information Interoperability: "Interoperability is one of the major pillars for intelligent production. The VDMA's vision is to achieve interoperability not only within the machine building industry but also across industries. VDMA will support the PA-DIM standard with its experience out of 60+ released or in development domain-specific and cross-domain harmonized OPC UA-based information models, including models for the area of process industry, for example, pumps and motors."

*News report by **ODVA, OPC Foundation, VDMA, PI International and FieldComm Group**.*

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

ADI Chronous™
SCALABLE ETHERNET TIMED TO PERFECTION

EV-RPG2

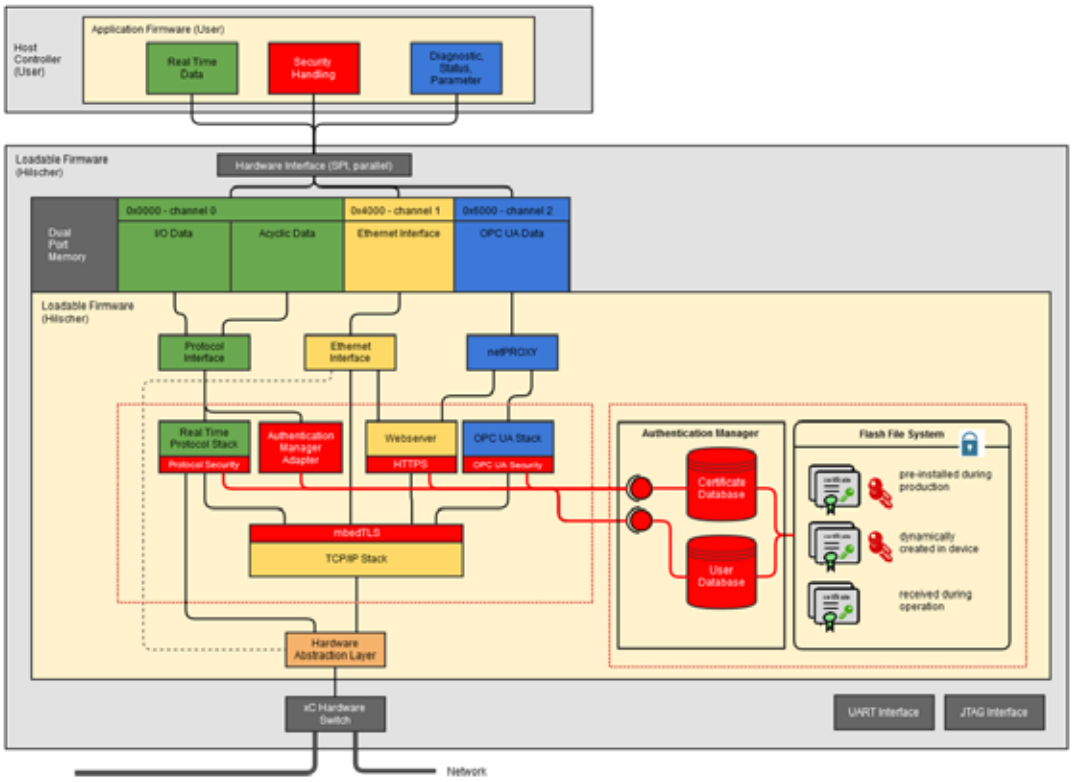
Complete Industrial Ethernet Communication Interface Reference Design Supports Multiprotocol Requirements

- Proven and verified hardware and software system design saves development time and risk.
- Precertified multiprotocol software for Ethernet/IP, EtherCAT, Modbus TCP/IP, and PROFINET.

Learn more at analog.com/EV-RPG2.

Industrial Cybersecurity 2022 Special Report

In this special report, industry experts provide their perspective on trends and innovations in Industrial Cybersecurity. Security on the factory floor is the utmost priority, with IT pushing down new technology solutions to meet networking demands, new levels of IT/OT convergence and expanding IIoT requirements.



SOURCE: HILSCHER

Industrial automation networking architectures now face a wide array of challenges from protecting the cloud down to the need for field-level cybersecurity.

INDUSTRIAL CYBERSECURITY HAS BECOME ONE of the hottest topics and a driving need for industrial automation. Security has always been a priority but the complexity of solutions required, given new and dire threats in the computing world along with the new application requirements driven by the continuing emergence of the IIoT, has resulted in an unprecedented need for new ideas, technology solutions and new levels of IT-OT cooperation and convergence.

In this special report on Industrial Cybersecurity, the Industrial Ethernet Book has reached out to six industry experts to gain their insights into the the trends in security, applications and challenges for automation engineers.

Field-level cybersecurity

Becomes a prerequisite to further open up industrial networks.

According to Dirk Fischer, Software Product Manager at Hilscher, the trends in industrial cybersecurity are focusing on the needs created by IT/OT convergence, IoT application requirements and security extensions for field-level devices.

"Historically, industrial cybersecurity in automation systems has concentrated on controller-to-controller communications and using dedicated IT/OT gateways, with systems segmented into interconnected zones," Fischer told IEB recently. "Today, integrators are primarily applying cybersecurity to the interfaces of these zones. These segments typically include operations technology (OT) industrial networks, and their device intercommunications are generally unprotected. Integrators are installing firewalls and strict, on-premises access control to increase security in this space."

"Segmentation is a good strategy to prevent incidents from spreading and it reduces risks. However, it does not solve the issues at hand," he added. "User groups, standardization bodies and technology providers are working on extensions to secure OT-level communications. These extensions include field devices, servo drives, IO-devices and small sensors, to name a few, and they are equipped with security capabilities. With new, heightened security functionalities, network nodes will be able to authenticate each other and data can be protected against tampering to ensure that only trusted devices can communicate. Furthermore, even data encryption is possible to protect confidential information."

Hilscher has already implemented such cybersecurity standards into its communication protocol stacks. Devices based on the multiprotocol netX chips that feature security-enabled hardware and firmware make use of these advantages.

Industrial cybersecurity benefits

Fischer added that field-level security is a prerequisite to further open industrial networks towards enterprise networks and the internet, and access to field-level data increases production process transparency

Highly individual: custom-designed Panel PCs and Control Panels

As a specialist for PC-based control technology, Beckhoff offers a great variety of Panel PCs and Control Panels of the highest build quality, which are also available as customized solutions. The range stretches from visual adaptations and logos in the customer's corporate design to individualized configurations with special keys such as emergency stop buttons, scanners, or RFID readers through to complete custom enclosure design. Highly available and reliable operation are assured through the continuous development and integration of electronic components, displays, and touchscreens. Beckhoff Panel PCs and Control Panels can be operated optionally as stand-alone devices, DVI/USB Extended Control Panels, or via CP-Link 4.

Whether integrated in control cabinets or installed on a mounting arm: custom Panel PCs and Control Panels meet the most varied requirements.

sps
smart production solutions

Hall 7, Booth 406

Scan to experience the complete Panel and Panel PC portfolio

New Automation Technology **BECKHOFF**

and visibility. This enables new technologies to increase productivity.

One simple application is asset management, while device condition monitoring, remote diagnostics and predictive maintenance are other potential applications that enable system operators to save time and money.

"New business models are possible when applications in the cloud can directly access the field level. Machine builders can release their products and charge customers by production quantities rather than selling a machine. This will lead to more flexibility in production processes — factories could offer individualized products down to a lot size of one," Fischer said.

Controlling physical access to industrial facilities is difficult, expensive and sometimes impossible when systems are distributed over large areas like chemical process automation systems. But, cybersecurity protected networks could make physical access restrictions obsolete. A communication channel that prevents infiltration allows a system to be exposed to the public without risks.

Fischer added that it is expected that authorities worldwide will increase mandatory requirements related to cybersecurity functions for industrial automation equipment going forward.

Device makers must follow these upcoming requirements, and can benefit from Hilscher solutions since cybersecurity functions are transparently integrated into the protocol stacks. This alleviates a lot of development-engineering responsibilities — an API interface can be used for security certificate handling.

Cutting-edge technologies

Fischer said it isn't necessary to reinvent the wheel in order to provide security functions to field devices. OT can borrow well-established security methods and standards from the IT world. One example is EtherNet/IP CIP Security, which makes use of proven SSL/TLS technology and its underlying methods, to secure IP-based real-time Ethernet communication. It uses the same cryptographic algorithms like Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) or Diffie-Hellmann Elliptic Curve Cryptography (ECC) — which are all already established in IT systems. This is similar to PROFINET security and other industrial Ethernet-based communication standards.

"However, technologies must be adapted to the unique requirements of OT networks such as determinism, guaranteed timing behavior and long maintenance intervals," he said. "But this adaptation is a difficult task, as OT devices typically have limited resources in terms of CPU performance, memory and available space."

For this reason, Hilscher includes dedicated security hardware support to its netX 90 multiprotocol communication controller. Security-enabled firmware makes use of a hardware accelerator for encryption functions to unburden the CPU and guarantee deterministic real-time behavior.

Hilscher also provides the protocol firmware as a monolithic binary, running independently on a dedicated CPU on the netX communication controller. Users won't have to hassle with library integration, enabling fast time to market.

When asked about specific application areas that the newest Industrial Cybersecurity solutions are targeting, Fischer said that field-level cybersecurity is potentially important for all segments of the industrial automation market. As discussed earlier, every system operator who wants to benefit from IT/OT convergence must consider field-level cybersecurity. Automation system operators must reduce the high-cost risks caused by cyberattacks.

"Authorities will define systems rules, beginning with critical infrastructure, and certain security levels will be mandatory in such systems. This shows there is a market demand for all kinds of security-enabled automation equipment such as servo drives, sensors, valves and IO-systems. These components, and others like them, will have to meet IEC 62443 requirements," Fischer said.

"Hilscher's solution is ideal for device makers as it provides a ready-to-use protocol firmware with integrated security functionality that helps them equip their devices quickly at a low cost."

Meeting the challenges

Real-time Ethernet protocols are common and widespread in automation systems. But Fischer said that implementing them requires constant maintenance since the compliance test specifications are constantly adjusting and expanding. Security extensions add another level of complexity, because even if device integrators are familiar with the protocol specifications, the latest cybersecurity extensions require a lot of time to build knowledge, train and implement. The Hilscher netX 90 with security protocol firmware is a solution for this problem.

Handling security certificates poses another challenge. Each device in a secure network requires certificates which must be initially deployed (transferred to and stored on the device), then updated in regular intervals. Typically, this task is the operator's responsibility and it should occur during normal system operation. But there are different approaches to address this issue.

"Operators may want full control over certificates and keys because they are using a public key infrastructure (PKI) or they might want to leave key generation and certificate signing to the device maker," Fisher said. "Therefore, component manufacturers must provide flexible solutions for their products. The security-enabled protocol firmware from Hilscher provides a flexible certificate manager which supports a variety of different uses and enables the freedom to adapt to individual requirements and use cases."

IT-like cybersecurity solutions

New functionality and solutions a necessity for users of industrial automation.

Arun Sinha, Engineer at Opto 22, said that the trend toward Industrial IoT, Digital Transformation and Industry 4.0 is a key driver behind new industrial cybersecurity solutions.

"The promise of the IIoT is that data is an asset to the enterprise. Specifically, it is not the data in and of itself but rather what actionable insights can be developed from that contextualized data," Sinha said. "The proliferation of machine learning and artificial intelligence solutions are facilitating the use of this data in applications like predictive maintenance. That said, the processing and modeling of data is often in the cloud, but the data originates at the edge."

He added that what is enabling these new industrial solutions is the move toward bringing more IT-like cybersecurity functionality and capabilities into edge of network devices. Advances in cybersecurity on industrial devices help you build a scalable architecture, while providing the tools and methods necessary to make your system as secure as possible from a network access standpoint. This can be done while maintaining the flexibility that is needed in an automation implementation.

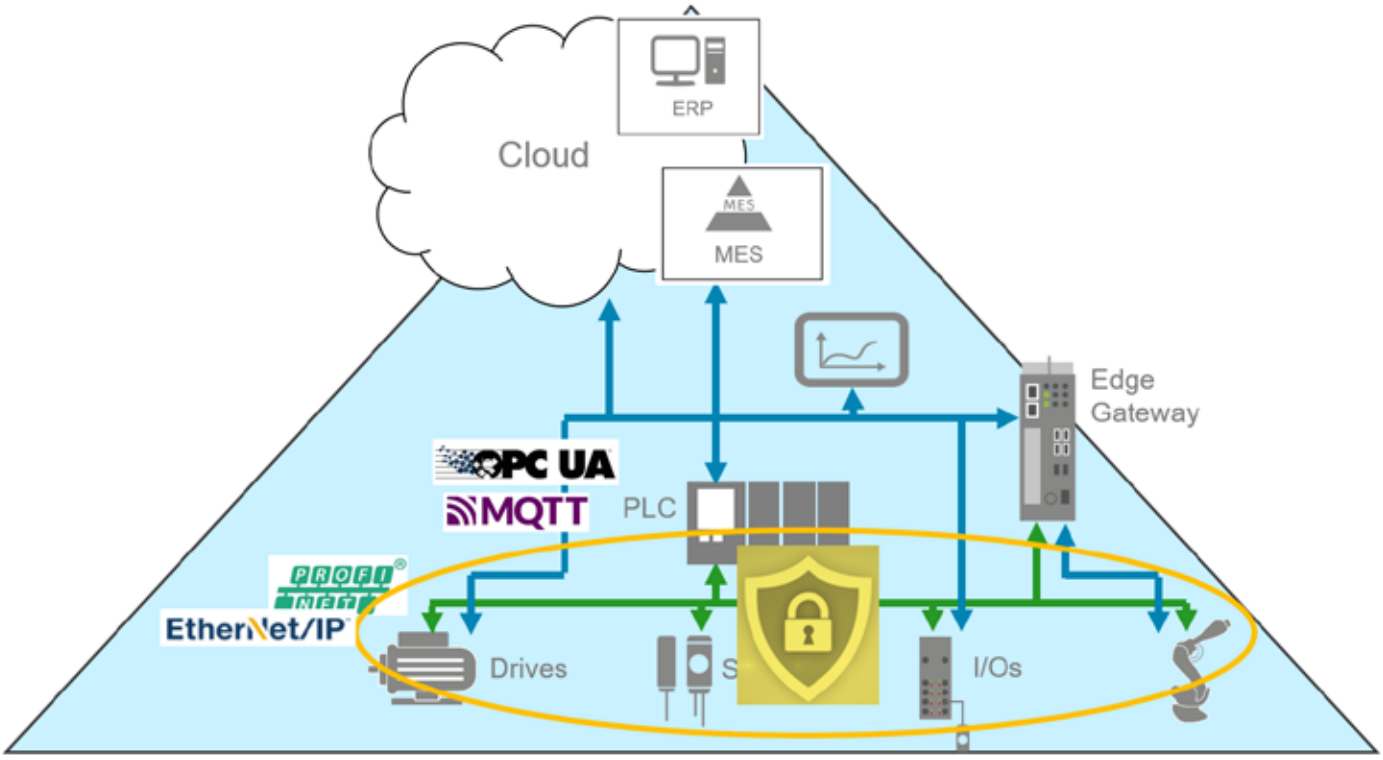
As a result, a key benefit that new solutions for industrial cybersecurity offer is interoperability with IT systems, software and cloud applications with a similar level of security. Digital Transformation is predicated on previously siloed and locked down data being made available to applications and tools outside of the industrial control system network. Traditional PLCs are inherently not secure as they were not designed to exist or share data outside of the manufacturing network.

"The fundamental idea with Digital transformation or Industry 4.0 is to bring operational data from these systems onto IT networks for where software, tools and applications reside that are related to business processes. Only then can an enterprise look to improve their business through increased efficiencies, reductions in costs and improvements in quality," Sinha added.

Bridging the gap

"Essentially this comes down to the now somewhat clichéd phrase of bridging the gap between operation technology and information

SOURCE: HILSCHER



"Segmentation is a good strategy to prevent incidents from spreading and it reduces risks. However, it does not solve the issues at hand. User groups, standardization bodies and technology providers are working on extensions to secure OT-level communications. These extensions include field devices, servo drives, IO-devices and small sensors, to name a few, and they are equipped with security capabilities." Dirk Fischer, Software Product Manager, Hilscher

technology. For this to become a reality, the systems on the manufacturing network need to be viewed from a cybersecurity perspective in the same way as those on the information technology network."

His viewpoint is that traditional control systems are unsecure, and require other measures to be implemented, such as firewalls, air gaps and other forms of protection. New cutting edge solutions for industrial cybersecurity allow industrial control systems to be managed from a cybersecurity perspective like all other IT devices on the network. What makes these new systems unique are features on board such as dual network interfaces to separate trusted and untrusted networks, a fully configurable firewall, a built-in VPN client, secure data communications options like MQTT, user account management and security certificates.

Unlike the traditional controllers, processors, and computers typically used in automation or industrial internet of things (IIoT) applications, cutting edge control systems are increasingly built upon a custom, industry-specific build of the open-source Linux® operating system. Though it sounds counterintuitive, an open-source OS is in many ways more secure than a closed one. These products might only include 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.

Best practices suggest the build of Linux on the system be cryptographically signed with the manufacturer Private Key. That means that any firmware or software package a hacker might try to upload to the controller will not be accepted. Further, 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.

Application targets

Sinha said that two specific application areas that the newest industrial cybersecurity solutions are targeting include remote asset monitoring and extracting additional value from legacy systems.

"Remote monitoring by industrial end users is not new, and is common in verticals like water and wastewater, oil and gas and mining. Over the decades we have seen communication methods in these industries evolve from things like satellite, unlicensed radios, fiber optic and cellular and then eventually to standard internet technology," he said. "With this came the need to protect these networks using IT technology such as VPNs, DMZs and firewalls. The newest industrial cybersecurity solutions include moving some of these technologies into the control system itself, thus flattening the architecture and minimizing complexity."

As digital transformation proliferates, there is an increasing need to connect to, secure and extract value from traditional control systems that were not inherently designed for cyber security, which is the vast majority. Newer secure control systems with tools on board like Inductive Automation's Ignition Edge IIoT or Telit's Devicewise can connect to these systems non-invasively and communicate with tags while at the same time adding an additional layer of security. This securely unlocks siloed data that can now be accessed by higher level applications for things like OEE, ML and AI.

Bridging OT and IT networks raises concerns about overall network performance. Next generation pub-sub communication protocols such as MQTT largely address this issue. MQTT with Sparkplug B data format is lightweight, reports by exception, uses a unified namespace and supports store-and-forward technology, securely.

"For an automation engineer that wants to gather, process, and share operational data from industrial equipment on premises or located remotely, cybersecurity is a big worry. Their systems and equipment—and the data in them—are essential and sensitive, and they need industrial internet of things (IIoT) devices and software that protect them," Sinha added. "Advances in industrial cybersecurity give automation engineers the ability to advance digital transformation projects while at the same time ensuring that their devices on the OT network are safe from security vulnerabilities."

SOURCE: MOXA

"There exists a large number of IT cybersecurity solutions like central user management, digital certificates, and endpoint detection. With increasing computer power and software and protocol support, industrial components and systems support such solutions as well and may even become integrated into solutions. This will significantly help in increasing the cybersecurity from both the technical and the organizational perspective." Dr. Lutz Jänicke, Phoenix Contact

He added that there is often a misconception that industrial cybersecurity is a product, whereas in fact it is a process. For all digital systems, security is a complex issue with different implications depending on the organization and the system. Security requirements constantly change as the system evolves, and building security into the system design is key.

"For some automation engineers, myself included, there is a bit of a skills gap with regard to IT systems, software, tools and security," Sinha concluded. "This gap though is closing, as automation and IT professionals are respectively learning each other's technical skills to the extent necessary to complete successful, cybersecure digital transformation projects."

Technical & Organizational Needs

Well-rounded perspectives shape good security practices.

According to Dr. Lutz Jänicke, Corporate Product & Solution Security Officer for Phoenix Contact, said that new technologies and process improvements need to act together to create effective industrial cybersecurity solutions.

"There exists a large number of IT cybersecurity solutions like central user management, digital certificates, and endpoint detection. With increasing computer power and software and protocol support, industrial components and systems support such solutions as well and may even become integrated into such solutions. This will significantly help in increasing the cybersecurity from both the technical and the organizational perspective," Jänicke told IEB.

He added that it should also be noted that security of industrial components, according to IEC 62443-4-1/2, is advancing. In the process industry, concepts like the NAMUR Security Gateway address the conflict to allow process monitoring without interfering with the core process automation.

"It should however be pointed out that technology is only one part. Having good security processes in place stays the most import aspect," he said.

Potential impact on manufacturing networks

"Having tools like good asset and device management definitely helps to improve operation and situational awareness. If technically feasible, zero trust concepts help with end-to-end security, a sensor on the endpoint that can be used to detect security violations will help, too. It however turns out, that endpoint security solutions become ever more complex and thus can create problems on their own," Jänicke said. "Ever seen a security tool tagging and blocking some of your applications on your PC? Imagine this happening on an industrial system shutting down a factory line. Also, cybersecurity solutions in the office environment are not real time critical beyond annoyed users. Performance impacts may not be tolerated as easily in industrial environments."

He added that applying "cutting edge" technologies is itself a challenge and may be not the best way to go. IEC 62443 typically relates to clauses like "commonly accepted security industry practices", which already expresses that maturity should be considered. When closely following implementation projects involving for example zero trust concepts with Detection and Reaction (xDR) capabilities, it quite often can be observed that unwanted side effects occur. This is especially true considering that automation equipment is not IT equipment based on some standard operating system in a default deployment but very often is individually designed.

And, indeed, basic concepts like defence in depth with zones and conduits, network segmentation with security appliances or enabled PLCs, supported by secure operating processes, is state of the art.

"Indeed, the focus should be put onto the demand side. Highest demands come from those areas having the greatest risks. There are critical infrastructures, for which cybersecurity by now is also a regulatory requirement," Jänicke added. "Electrical energy, being the basis for infrastructure services, being most prominent. Process industry is facing high risks. Large manufacturers for example in the automotive industry might face significant

damage in case of cybersecurity incidents and therefore are increasing their security posture as well."

Still, the higher the risk, the more weight is put into the maturity of the security concepts and solutions applied. In any case regulatory requirements regarding operators as well as suppliers of IT/OT components will be imposed or intensified in the future.

Automation engineering challenges

The main challenge for automation engineers is keeping track of unknown attack surfaces, which continue to increase due to the growing digital footprint of industrial companies, which can lead from a single machine standstill and an entire plant standstill to an overall standstill of business operations. A second crucial challenge is uncertainty in assessing current risks and the impact on business operations.

"A security-conscious company has an organization in which security officers and automation engineers work together conducting a business impact analysis and assessing current risks. However, building a security-conscious organization is difficult and must be mandated by top management," Jänicke concluded.

OT/IT and IoT Integration

Amplifying the need for comprehensive security solutions in automation control networking.

Franz Köbinger, Marketing Manager - Industrial Cybersecurity for Siemens AG, said that the combination of the need for IT/OT integration and state of the art security functions in automation systems is rising to meet the challenge of today's cyber threat environment.

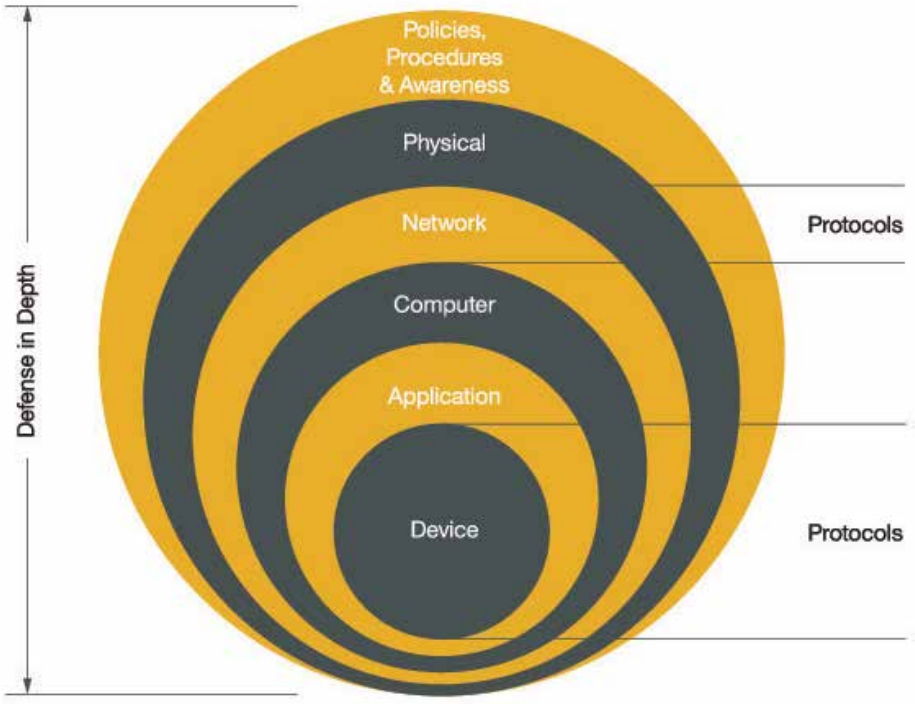
"As automation components have become part of the IoT, and due to the nearly complete OT/IT integration, it is necessary to integrate state-of-the-art security functionalities in automation systems to improve their capabilities against cyber-attacks," Köbinger said. "So, more and more IT security standards will be used in OT as they are connected and face the same cyber-threats, now. Such technologies are, for example, certificate-based secured communication like SSL or OPC UA protocol, which will be used for data exchange between controller and other systems. Another example is the use of zero-trust principles to provide immediate and secure access to the OT environment and, in combination with other measures such as cell protection, to implement an effective defense-in-depth concept."

He also cited specific benefits that new solutions for industrial cybersecurity offer, and the potential impact on manufacturing networks

Köbinger said that "the use of proven, state-of-the-art security technologies in automation systems enhances the security standards in OT significantly. And this is necessary as up to now there is a gap in between OT and IT security standards. The IT is much longer connected with the Internet or other unsecure networks while the OT was usually separated and formed often 'communication-islands'."

But he added that, with digitalization, this changed quickly and completely. Now, the OT faces the same cyber-threats as the IT, which means it also needs the same protection. And there is no alternative or way back to avoid the digitalization or connectivity as the advantages are too great. But to use and unleash all the possibilities it is necessary to have an adequate protection which needs to be kept up to date to avoid plant standstills, production losses or data theft and manipulation. It is necessary to protect all relevant levels: the network, the system integrity of automation systems like Controller, HMI or IPCs, but also the training of people and processes for e.g., vulnerability management or intrusion detection. The integration of security functionalities in automation systems is a great advantage and step forward to an effective and easy to handle holistic security concept for manufacturing."

"Cutting edge cybersecurity technologies are proven to be effective against cyber-threats and attacks. Unless there are vulnerabilities, which are not fixed and thus can be exploited by malware or hackers. Therefore, it is necessary not only to rely on the security



SOURCE: ODVA

A defence in depth strategy is more important than ever. "Since 2020 the number of cybersecurity complaints that the United States Federal Bureau of Investigation's IC3 (Internet Crime Complaint Center) receives daily has increased from 1,000 to over 3,000 today." Dr. Al Beydoun, ODVA President & Executive Director

technologies, but also to establish a multi-layered security concept which cannot be broken by a single vulnerability as it combines several independent security measures.

The application of some security technologies in industrial environments needs to be connected to IT security applications or at least this can offer advantages. For example, the user management for automation systems can be connected to a central user management in IT like active directory to avoid laborious and different management of the user. Or the use of the PKI for secured communication and authentication with certificates."

Applications & Challenges

Specific application areas are the protection of critical infrastructures like food & beverage or water/wastewater. But also, every production site and OT network needs to be secured by the newest industrial cybersecurity solutions as they were also targeted by malware and hackers.

All the time and everywhere. The contribution to the overall performance of the network depends on specific conditions and cannot be answered in general terms. But this is usually not a big problem. Much more interesting is the contribution to the overall usability and production performance. In most cases the availability is the highest protection goal in OT to keep the production running.

Therefore, the main task of security measures is to keep malware and hackers out and avoid disturbances in every way. On the other hand, security measures also decrease the usability of the automation systems. Therefore, the implementation of security measures needs to be easy to use and consider the specific requirements in OT – e.g., a configuration assistant or wizard can help the automation engineers to handle the security configurations of automation systems.

"Industrial Cybersecurity requires more coordination with IT and more knowledge and awareness of automation engineers," Köbinger added. "Also, cybersecurity is a 24/7 task and must always be kept up to date. Especially the vulnerability management is a challenge when security patches need to be installed in a running production. However, this can be supported by specific security services, for example, and a holistic security concept can enable a later update when production is still protected, and the exploitation of a single vulnerability is not possible."

Open, standard technologies

Future proof industrial cybersecurity solutions.

According to Dr. Al Beydoun, ODVA President & Executive Director, key technology trends are enabling new Industrial Cybersecurity Solutions.

"Open, standard technologies are the key to robust and future proof industrial cybersecurity solutions. The continuous updating, improvement, and reliance upon open security standards by an immense number of users located globally across industries is one of the main reasons to avoid creating proprietary solutions that still require the same level of investment and updating, but by a much smaller user group," Beydoun told the Industrial Ethernet Book recently.

He added that data transfer security standards such as IETF Transport Layer Security (RFC 5246) and Datagram Transport Layer Security (RFC 6347) are a core underpinning of automation security. Transport Layer Security (TLS) uses cipher suites that determine the algorithms used for initial key exchange, encryption of application messages, and authentication of application messages. These algorithms can be understood as highly complex mathematical problems that enable messages to be secretly coded, which can then be solved or decoded by knowing a unique key. These security algorithms are constantly being updated to become more complex over time in order to stay ahead of the efforts of bad actors.

Additional open, standard technologies such as OAuth 2.0 and OpenID Connect can enable cryptographically protected token-based user authentication, JSON Web Tokens (JWT) can be used as proof of authentication, and X.509 certificates can provide cryptographically secure identities to both users and devices.

Benefits of new industrial cybersecurity solutions

CIP Security™, which is a cybersecurity network extension for EtherNet/IP™, includes robust, proven, and open security technologies including TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security); cryptographic protocols used to provide secure transport of EtherNet/IP traffic, hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authentication to EtherNet/IP traffic; and encryption as a means of encoding messages or information in such a way as to prevent reading or viewing of EtherNet/IP data by unauthorized parties.

CIP Security also uses several open, common, ubiquitous technologies for user authentication, including OAuth 2.0 and OpenID Connect for cryptographically protected token-based user authentication, JSON Web Tokens (JWT) as proof of authentication, usernames and passwords, and X.509 certificates to provide cryptographically secure identities to users and devices.

Additionally, CIP Security can provide information assurances for resource-constrained devices by requiring fewer mandatory features. Adding device level

security provides a last level of defense for your most critical motion control devices.

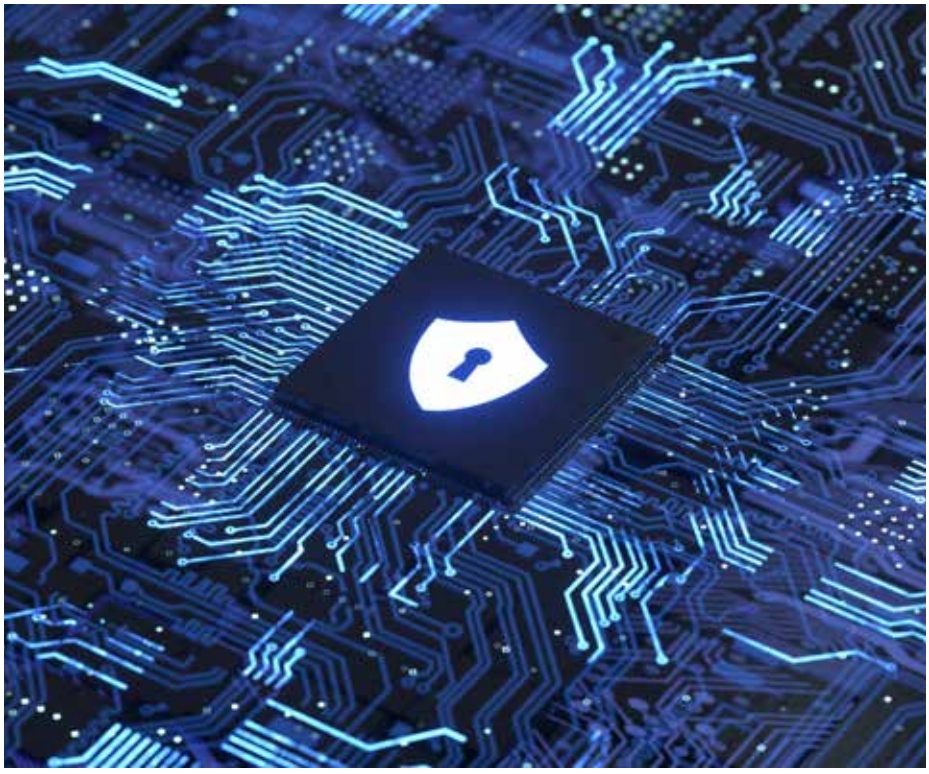
"CIP Security relies upon profiles to allow only the necessary capabilities to be added to a device. A Security Profile is a set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability," Beydoun said.

Secure Hash Algorithm (SHA)

Beydoun added that a Secure Hash Algorithm (SHA) is an interesting example of a cybersecurity technology to examine in greater detail. The original data is transformed from its original state using a hash function into a new fixed-size piece of hashed data that is completely different. The goal of the hash function is to create a one-way transformation so that the resulting values can't be changed back into the original data by a bad actor. SHA-1, SHA-2, and SHA-3 are SHA examples that are progressively stronger in encryption and require larger data outputs when moving from -1 to -3.

Security benefits of SHAs also include the avalanche effect where changing a few details in the original message will cause a massively different output message making it difficult to guess the input string along with tamper resistance given that slightly altered files result in a changed output hash that can alert security to the presence of a bad actor.

"Keep in mind though that no matter how tough a single cybersecurity technology is to defeat that it can eventually be overcome with enough time and resources. That's why a holistic defense in depth security strategy is so important to adopt. Staff training, physical lockouts, network switch firewalls and deep packet inspection, updated computer virus protection, patched applications, and device defense such as CIP Security all play a role in keeping intruders out," Beydoun said.



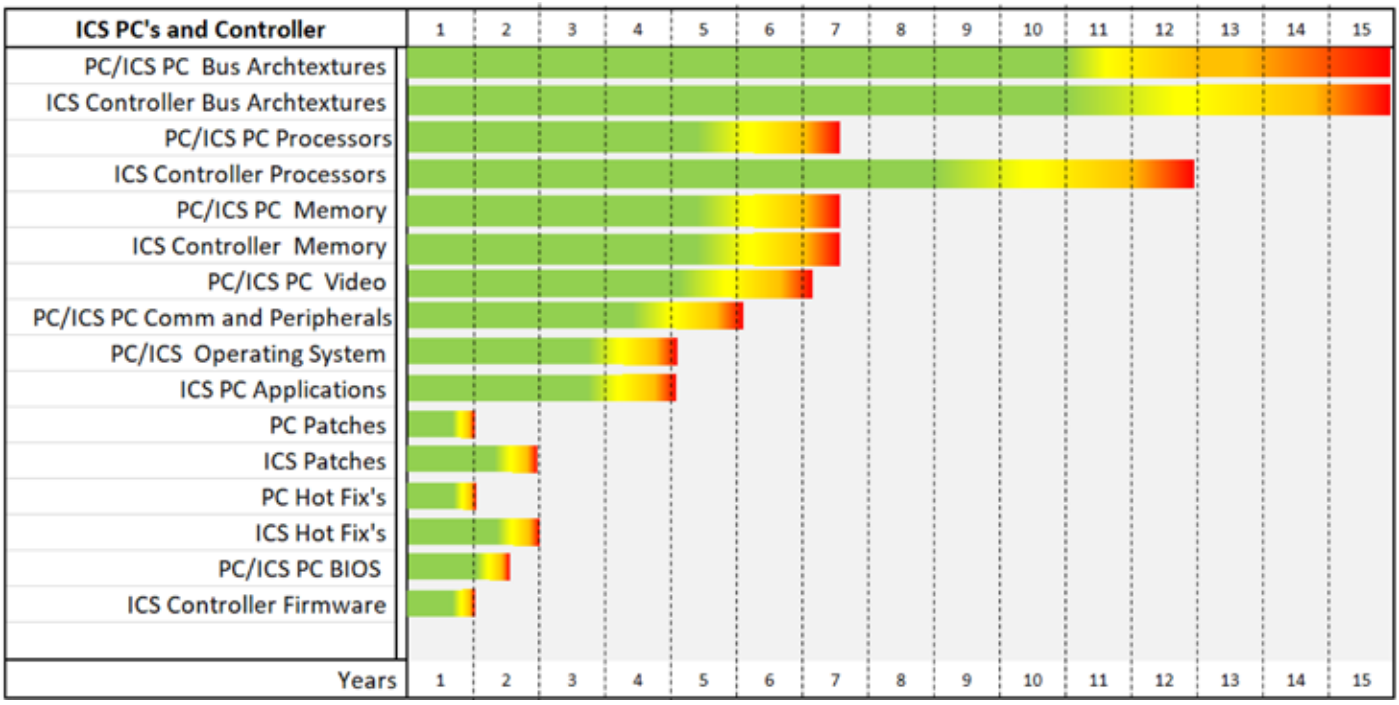
SOURCE: ISTOCK

Application areas

CIP Security is designed to be able to be used for those devices where the risk to life, property, and operations is the most critical. This means that CIP Security can be deployed in only those zones where workers could potentially be hurt by motion equipment, in devices that could reveal product recipes or manufacturing process secrets, or in lines that could cause great environmental damage. Further, CIP Security is designed so that different profiles can be applied where needed. For example, the User Authentication Profile may not be applied in a device which doesn't have strong needs for user authentication yet does have high performance optimization needs.

Network performance can be affected with the addition of both integrity and confidentiality protection of CIP Security. Specifically, it's not uncommon to see around a 15% reduction in I/O packet capacity or approximately a 45% decrease in standard message capacity. It's especially important to plan for a change in capacity when using a CIP Security proxy to add protection to an existing device. Given that the security ciphers add additional traffic to the network, it's important to assess where security is needed the most and what other network changes might need to be made to ensure adequate bandwidth for operations.

Beydoun said that another issue is that automation engineers are facing a steady



increase in the number of cyberattacks. Since 2020 the number of cybersecurity complaints that the United States Federal Bureau of Investigation's IC3 (Internet Crime Complaint Center) receives daily has increased from 1,000 to over 3,000 today.

The enhanced connectivity that less expensive and smaller chips have enabled via IIoT and Industry 4.0 has both increased the amount of valuable data that business leaders are able to access to improve their manufacturing operations as well as the vulnerability of production facilities to bad actors.

"Cybersecurity is an incredibly important business risk that can either be addressed proactively at a much-reduced cost or as a prohibitively expensive reactive measure to try to get manufacturing back online, to manage the press and customer reaction of a down facility, and to attempt to create an effective security strategy all at once," Beydoun concluded. "Conducting regular threat assessments using the STRIDE model and creating a defense in depth strategy is a best practice to ensure uninterrupted revenue growth in today's highly connected industrial environment."

Driven by Connectivity Needs

Increased use of IIoT devices and cloud systems spur innovation.

Patrick O'Brien, CFSP, CACS, Safety and Cybersecurity Engineer at exida LLC is a member of the International Society of Automation Global Cybersecurity Alliance (ISAGCA) told IEB that industrial environments are continually evolving to meet new production demands.

"Current trends include increased connectivity, increased use of IIoT devices, and increased use of cloud systems. As industrial systems are becoming more connected, this increases both the need for stronger security features and opportunities to introduce new cybersecurity solutions. This has also led to an increased focus on improving security capabilities for embedded components, including IIoT devices, devices with enabled wireless technologies, as well as traditional industrial components distributed control systems (DCSs), programmable logic controllers (PLCs) and safety instrumented systems (SISs)," O'Brien said.

"For these security features, we are seeing a major trend towards adoption of international standards, such as the ANSI/ISA 62443, which include clear requirements for embedding security features directly into these components. This is allowing not only for the systems to be built more secure from the start, but it is also providing the opportunity for newer solutions to be migrated from the traditional IT space to OT environments without resulting in a loss of system availability."

O'Brien added that building security capabilities directly into components has many benefits over "bolted-on" security measures after a component has already been developed. Built-in security features are more effective against sophisticated cybersecurity attacks, easier to implement for end users, do not have the potential compatibility issues of security measures added later and requires less ongoing support. This is a major cost saving advantage, considering the time required to implement and the cost of additional security measures.

Improved compatibility with newer protection technologies such as endpoint detection and response (EDR) or security information and event management (SIEM) are more effective than traditional measures and have the features to successfully identify and prevent malicious activity sooner.

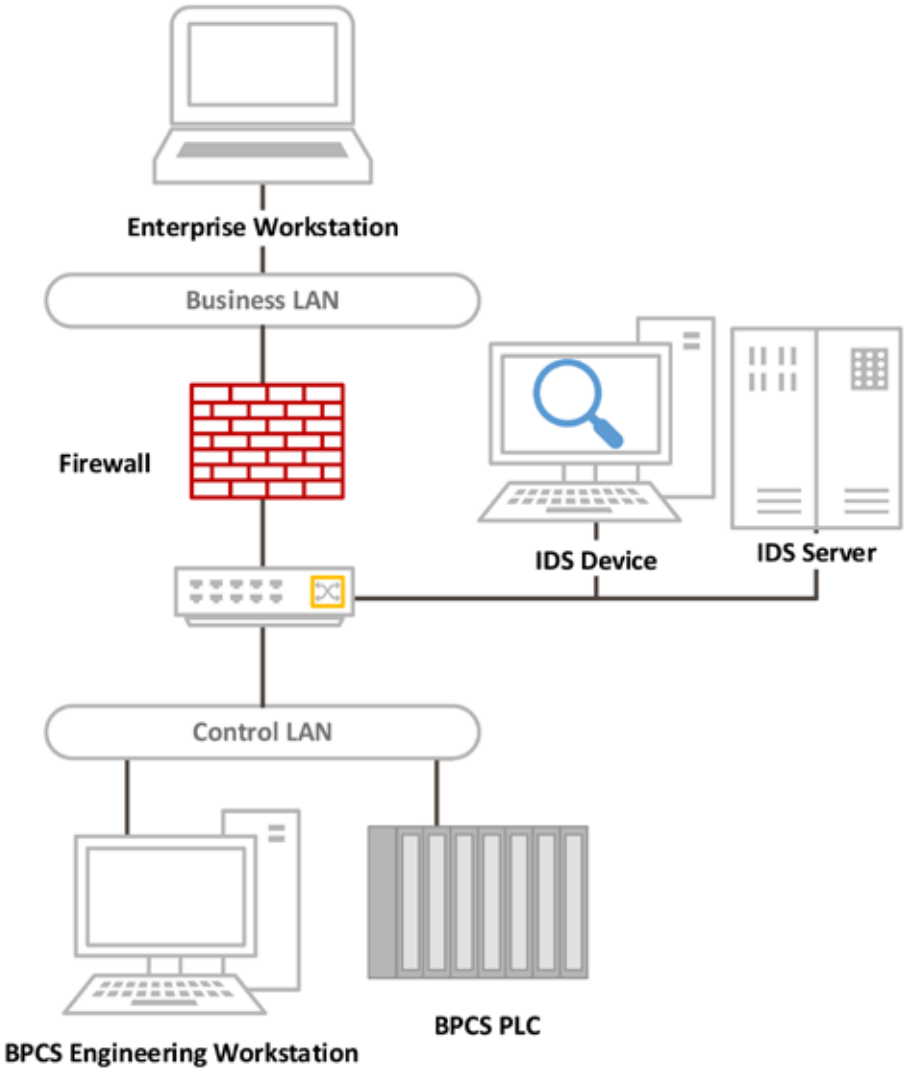
Identifying potential cybersecurity attacks sooner offers major improvements for the performance of manufacturing networks, because this allows operating personnel to respond to issues before a cybersecurity issue leads to a loss of production or physical damage. In industrial environments, where an hour of downtime can cost tens of thousands of dollars this makes an enormous difference.

When asked to explain what makes cutting edge cybersecurity technologies unique, he said a fundamental difference between traditional cybersecurity technologies and emerging technologies is the use of AI to make real-time decisions about whether a behavior is normal or malicious.

This can be applied to running software programs by EDR, to network traffic with intrusion detection systems (IDS) or next-gen firewalls, and user behavior by SIEMs.

"While traditional anti-virus is only effective against a list of known attacks and known malicious programs, EDR solutions can analyze new programs as they are run to determine if they are potentially malicious or not. Because existing anti-virus definitions are rarely updated in many industrial environments, and the constantly changing threat environment, EDR solutions are often much more effective," he added.

When deciding how to apply these



technologies to the industrial environment, the key question is: How can I improve the effectiveness of my cybersecurity protections, while maintaining the reliability and availability of my industrial network? While each of these technologies has the potential to improve cybersecurity, they can also lead to performance concerns if they automatically block programs or network traffic that are needed for the control system to run.

Industrial environments should start by applying these new technologies to monitor and alert an identified user of suspicious activity but should rarely be used to automatically block this activity.

One example from the user-behavior analysis side, would be a remote user logging on to address a critical production issue. An administrator logging in remotely outside of working hours to make a critical change to keep operations running or help start up after an issue, has all the markings of a malicious attack to a SIEM system (remote access, outside of normal working hours, administrator privileges, change to critical configuration file), but in this case the activity is completely valid. Instead of automatically blocking the action, if the system generates an alert instead, it provides time to respond in an actual cybersecurity event, without hindering the availability of critical systems.

O'Brien said that one difference between traditional IT networks and industrial environments is the widely varied use of different industrial protocols and the diverse components (sometimes with incompatible communications) that often need to be married together to create a functioning industrial environment.

"A big area of focus for industrial cybersecurity solutions is to adapt a traditional IT protection so that it can recognize the different industrial specific protocols and signatures," O'Brien said. "Without this step a technology that works perfectly well in the IT environment will have limited potential to identify specific threats to the industrial environment (e.g., malware targeting common industrial vulnerabilities or unusual network behavior)."

"Another trend that is helping in part to address this concern is the standardization of many components across different industries to a set of common cybersecurity requirements. As the ANSI/ISA 62443-4-2 requirements for auditable events are incorporated, more products are following industry standard formats for event reporting. This is a significant benefit for industrial network monitoring applications and SIEMs as it allows for a direct connection of information from the industrial cybersecurity assets themselves into the protection technology, streamlining the implementation process and making the newer technologies effective for industrial use."

Challenges for automation engineers

O'Brien said that, although much of the focus in cybersecurity issues is on the technology side, it is also a very human problem. Automation engineers often aren't provided with the necessary training to identify potential cybersecurity issues or to effectively deal with them.

Automation engineers are already extremely loaded with responsibilities for keeping the industrial system up and running, and rarely have the additional bandwidth to address the additional burden of cybersecurity concerns. Any solution for industrial cybersecurity first needs to address these issues by providing the necessary competency development and training for users on the awareness of cybersecurity concerns for industrial networks and understanding of the cybersecurity protections that will be used.

This also needs to include appropriate resource planning for the ownership of cybersecurity protections and the time required to maintain them.

Legacy systems

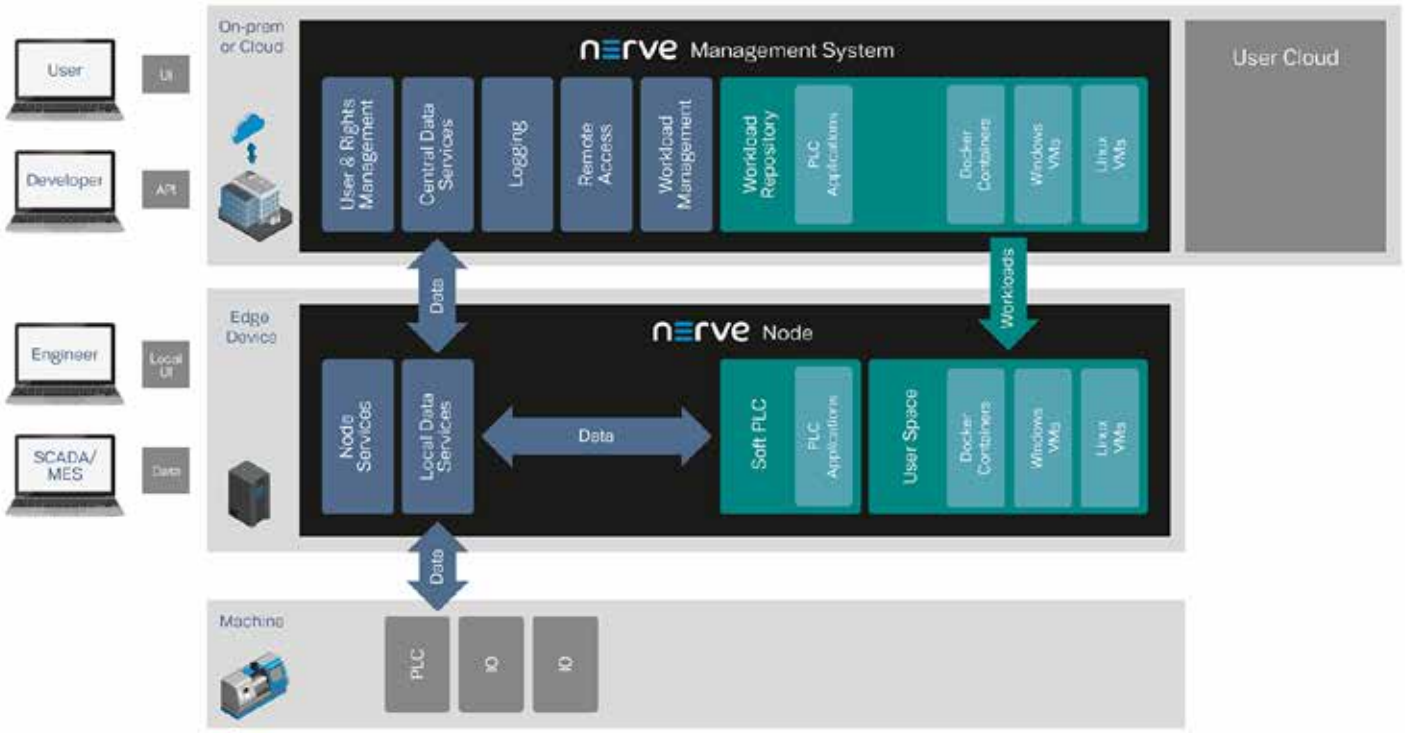
A second fundamental challenge for industrial cybersecurity is the prevalence of legacy systems. Many industrial components are expected to operate without significant change for 15+ years as opposed to the typical 3-5 year turnaround for IT equipment. The inability to make frequent changes to industrial systems due to network availability concerns, operational constraints, and abundance of legacy equipment, means automation engineer are always a step behind the latest threats.

"However, newer technologies directly combat this concern by having the capability to automatically analyze new behavior and respond, improving the effectiveness of the protection measures themselves and limiting the reliance on slow-to-update technologies. This helps to reduce the amount of ongoing support time required by automation engineers and can automate many of the activities that had to be manually completed in the past," he added.

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

Nerve: a Secure Basis for Edge Computing

The Nerve software platform serves as a secure foundation to manage software and devices in plants across the world. A lot of development time is being invested in testing to ensure Nerve is always up to date in terms of security.



SOURCE: TTTECH-INDUSTRIAL

Nerve node software runs on devices at the edge and the Nerve Management System runs in the cloud or on a local server.

CYBERSECURITY IS HIGHLY RELEVANT IN the Industrial Internet of Things (IIoT), as connectivity of machines/plants and sending data to the cloud and across the Internet increases potential risks for OEMs and end users. There are two dimensions to this connectivity – the cloud and the edge device, both of which need to be secured to protect data and minimize the risk for cyberattacks.

When it comes to the large cloud platform providers, we assume that they have mature cybersecurity in their platforms, but edge devices also have to play their part as they are where data is collected and often pre-processed before being forwarded to the cloud. There are a lot of things to consider – from legacy systems to data protection and access control issues.

"For our edge computing platform Nerve, we undertake massive cybersecurity efforts. This year, we are looking to certify our processes according to IEC 62443 and we have been implementing security features according to IEC 62443 level 2 and, in part, also for level 3 from the very beginning. And by the middle of next year, we are aiming to have a security certification for Nerve," says Herbert Hufnagl, Member of the Executive Board and General Manager, TTTech Industrial.

Nerve 2.5.0: Improved user experience and system usability

TTTech Industrial's modular edge computing platform Nerve supports machine builders and system integrators in their digitalization journey. Nerve is built as an open and modular system because industry and customer requirements differ, and the digitalization of machines or factories is not a task that can be accomplished overnight. Feedback from customers using Nerve in their plants and for different use cases is considered to further optimize user experience and features for the needs of today's industrial environments. The latest update, Nerve 2.5.0, includes updates for easier handling of workloads and remote connections in the tool, as well as improvements in security and system stability and for the user interface (UI).

Nerve includes a range of basic security features: All connections in Nerve are secured using TLS and there is regular penetration-testing on the platform. TTTech Industrial's software processes are implemented according to the industrial standard IEC62443 and Nerve provides a Role-Based Access System, so administrators have full control over the individual user access rights to the Management System. With Nerve 2.5.0, the Management System and the Local UI now also have brute force login protection in place. This helps to reduce the risk of unauthorized access in a cyberattack.

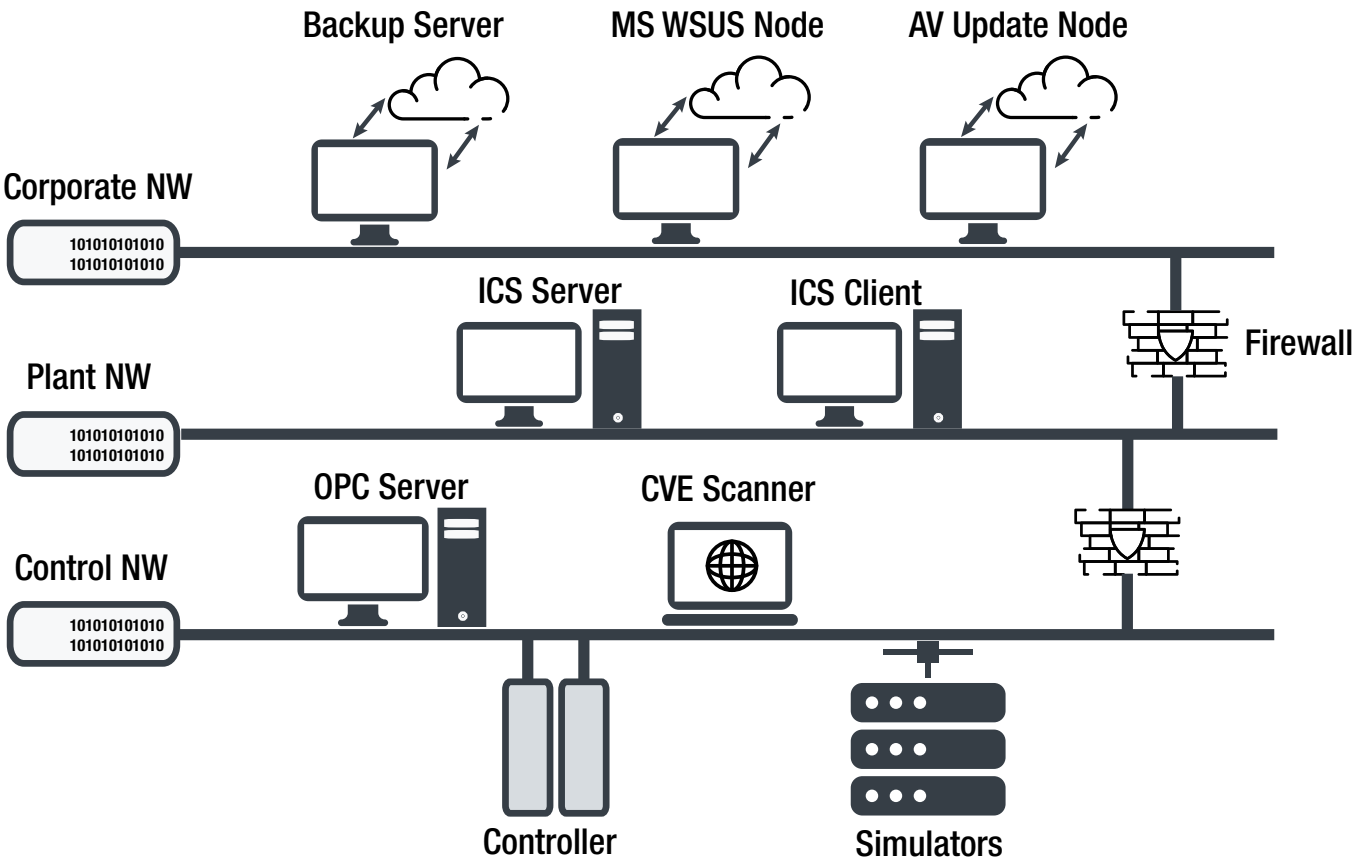
A second focus in Nerve 2.5.0 was on user experience and user interfaces, especially on features for configuring workloads and managing remote connections and edge nodes in the Nerve Management System. This is the central hub for accessing, managing, and updating devices and can be hosted either in the cloud or on a local server.

*Technology report by **TTTech Industrial.***

Learn more

ICS Cybersecurity Resilience and the Remote Laboratory

Increasing the use of information and communication technologies in ICS has exposed them to multiple threats for which they are unprepared, making them vulnerable to malicious attacks. By exploring the ever-changing field of cybersecurity, companies need to manage risks from an expanding attack surface.



SOURCE: ISA

Example of a Remote Test Lab for ICS Cybersecurity.

THE DIGITAL TRANSFORMATION IS HAVING A profound impact in industrial environments. Improvements in cost and performance have encouraged the evolution of the industrial control system (ICS) by utilizing information technology (IT) & operational technology (OT) capabilities in existing systems, resulting in many of today's "smart" systems, such as the smart electric grid, smart transportation, smart buildings, and industry 4.0. Technological advances have made possible that ICS have great flexibility, scalability, and connectivity, thanks to the intensive use of IT & OT at all levels.

However, these systems were originally designed to be isolated systems instead of connected to a corporate network or Internet, so most of them lack security mechanisms to protect them against external attacks. Replacement of such systems by IT/OT increases the connectivity, but at the same time the criticality of these systems creates a greater need for their safety and security resilience.

This evolution has exposed them to a series of threats for which they are unprepared and has made them vulnerable to malicious attacks that compromises ICS security properties (e.g., integrity, confidentiality, authentication, or availability). On the other hand, this evolution has also allowed the ICS application to not be limited to industry, such as oil and gas, power generation and distribution, transport, health, communications, etc.

Attacks on such facilities, especially those categorized as critical infrastructures, would involve extremely serious consequences. Therefore, cybersecurity should be a matter of priority to avoid incidents that interfere with its operation and cause serious economic losses, compromise the safety of people, or cause environmental disasters.

Many cyber events go undetected or unreported. However, there are notable attacks on ICS, such as the German Steel Mill Attack in 2014, where hackers had manipulated the control systems in such a way that a blast furnace could not be properly shut down which resulted in massive damage.

Another cyber-attack on the multinational pharmaceutical giant, Merck, reported $385 million in direct financial losses in their 2017 annual report. In this context, cybersecurity of ICS is one of the most important aspects to be taken into consideration. It is necessary to provide robust cybersecurity mechanisms for ICS.

Fortunately, there are some practical and effective steps that ICS providers can take to improve resilience and business continuity in the event of a cyber incident. Since it is not possible to perform the experiments on real control systems, it is therefore required to rely

Standard Procedures and Policies	Node-based Policies	Network-based Policies
User Management	System Hardening	Network Segregation
Role-based access control	Application control	Internet Protocol Security
Regular Maintenance	Antivirus & Security Update Management	Firewall Rules
Backup & (Disaster/Incident) Recovery	Vulnerability Scanning & Analysis	Intrusion Detection & Prevention

SOURCE: ISA

Table 1: Standard procedures and policies.

on labs or testbeds.

Most of the testbeds have research-oriented purposes to simulate the actual process. With remote lab, the contents should be aligned with the standards and recommendations that are generally used in the field. The system manufacturers, users, and integrators can have the most relevant standards, which defines ICS security concepts and requirements.

Cybersecurity Standards for ICS

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has published the ISO/IEC 27000 standards on IT security techniques for information security management systems and requirements. In 2017, the U.S. Security Framework Adoption Study reported that 70% of IT organizations preferred National Institute of Standards and Technology (NIST) Cybersecurity Framework as the most popular or best practice for IT Security, but also reported that it needs significant investment.

There are a range of standards, regulations, and guidelines available in the ICS field. For guidance on how to secure ICS, there is the "Guide to Industrial Control System (ICS) Security" by the National Institute of Standards & Technology (NIST). Another useful document is "Cyber Resiliency Design Principles," produced by MITRE Corporation, which provides a set of cyber resiliency design principles.

However, one of the most prominent is the ANSI/ISA99 standard by the International Society of Automation (ISA). It is an international standard on "Industrial Automation & Control Systems Security," being further utilized by IEC in producing the multi-standard ISA/IEC 62443 series.

ISA/IEC 62443 addresses the systems whose compromise can result in any of the following situations:

- Endangerment of public or employee safety
- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss and impact on national security

Though it is possible to consider recommendations at the national and international level, on top of it there are a few region or sector-specific guidelines that must be followed by security practitioners. In Europe, government authorities have increased their involvement in ICS cybersecurity. I

n March 2013, the European Network & Information Security Agency (ENISA) published a study about ICS cybersecurity called, "Protecting Industrial Control Systems - Recommendations for Europe," which details the current situation and gives recommendations for improvement.

In the United States, government organizations are also significantly active, establishing a framework to assess cybersecurity in critical sectors.

In 2016, ICS-Cyber Emergency Response Team (CERT) published a report with a total of 245 incidents, out of which energy (32% of incidents) and critical manufacturing processes (27% of incidents) were the most affected sectors. Further, North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) has planned the set of standards designed to secure the assets required to operate the North America's bulk Electric Systems.

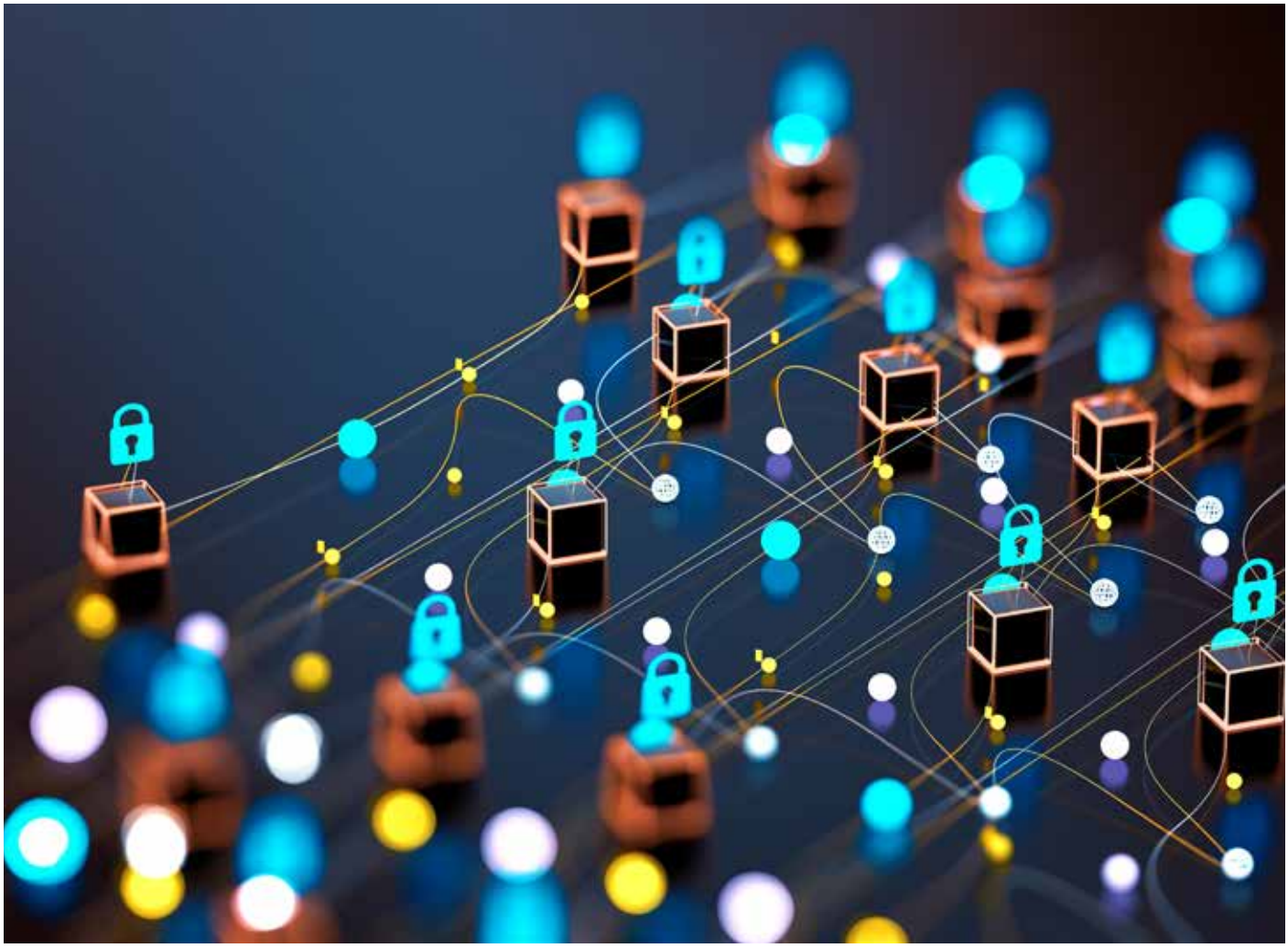
Cybersecurity Resilience Plan for ICS

ICS cybersecurity defense across all industry sectors is inadequate. Unfortunately, the likelihood of a cyber-attack is difficult to estimate. We need a complete approach that includes the relevant aspects or factors that can be categorized, as below:

- Size of the control system: Complexity of automation has been achieved in ICS (e.g., whether its simple digital systems or distributed control systems).
- Hardware and software integration: The level of third-party hardware integration has been done at the control floor or the number of enterprise resource planning (ERP) software integrations has been done at the plant floor.
- Connectivity: The dependency over legacy fieldbus devices like Modbus, TCP, or Profinet. Usage of Internet (including cloud and mobile platforms).
- Standardization: Company-wide standard processes and technology used in systems replicate both strengths and weaknesses.

In the case of software integration, ICS providers need some degree of trust with third-party original equipment manufacturers (OEMs), as it is necessary to keep the infrastructure up to date with anti-virus (AV) and security updates. However, sometimes AV and operating system (OS) patch updates can be the highest target for malware (or unintentional errors).

A real example of this is the consequences of McAfee's AV false positive detection with



SOURCE: ISTOCK

Effective industrial cybersecurity programs require system architectures that are redunndant and diverse.

the 4715 DAT update that incorrectly deleted different file types en masse (including Excel). As OEMs cannot test their updates against every ICS application, these risks can be managed by designing internal testing procedures and hosting cybersecurity services/ support within organizations.

Key elements to consider in ICS Cybersecurity Resilience Programs

Security resilience categories range from "very long downtime with high recovery cost" (due to ineffective backup and recovery strategies, unhardened system designs, lack of firewall, etc.) to "short or no downtime with very low recovery cost" (by doing regular maintenance, controlling the applications and implementing IPsec). Standard procedures and policies are shown in Table 1.

Below are four key areas and actions which are practical and effective for resilient systems:

1. System architecture: Design the system architecture with in-built resilience, which will be easy to safeguard.

2. System version/update management: Keep the system up to date with the latest version and remove the obsolescence.

3. Regular maintenance and backup: Maintain the system regularly and improve its ability to recover from any disaster.

4. Dedicated support and resource: Retain standards against pressures of cost, constrained resourcing, and workflow.

A. System Architecture

There are a few things to consider while designing the control system architecture to safeguard it from cybersecurity attacks:

1. Make it redundant: Minimize the downtime due to data loss or performance characteristics. In case of critical plants, redundancy can be achieved in many forms over independent standalone systems (e.g., hot or cold standby control systems, automatic failover, etc.). Though the design for redundancy can provide a significant level of resilience against many non-cybersecurity related risks, using identical systems for redundancy can compromise the benefits due to the likelihood of malware.

2. Make it more diverse: Minimize the potential damage from a dominant malware attack over the usage of common third-party software (e.g., operating systems, browsers, ERP solutions, etc.). This applies to all the levels of the application, but especially operating system; hence the suggestion is to use a range of different third-party software or its versions to host critical control systems (e.g., OS – Server 2019, 2016 or Browser – IE Edge, 11 or Office 2019, 2016, etc.).

Though greater usage of common software creates greater vulnerabilities, differences in software presents different vulnerabilities and have different patch cycles. Moreover, many attacks are not simultaneously launched across different platforms. There are some similarities in the threats, but not all OS are vulnerable to a common viral threat. This can be challenging for few critical applications, like supervisory control and data acquisition (SCADA), which often supports a single OS, but this recommendation is based on the concept of diversity that will increase the overall resilience.

B. System Version/Update Management

A certain degree of change is required to keep the system up to date (e.g., AV .dat files and software security patches, or system upgrades

and obsolescence). These changes need to be managed in a way that it should not weaken the system functioning.

Sometime the "fix" is the virus (e.g., McAfee's Excel false positives). "Bad" .dat files may cause a mess with such false positive observations or unqualified security patches that cause a stoppage to the control system functioning.

Recommendations to minimize risks:

1. Do internal analysis/testing of .dat files and security updates before deployment.
2. Do not use automatic update tools, as some may accidentally break the control systems.
3. Keep software and hardware within its support age as obsolete systems may contain vulnerabilities (few cannot be rectified).
4. Use of the most recent software or hardware is also not advisable as it may not be sufficiently tested against control systems.

C. Regular Maintenance and Backup

The ability to successfully recover from an attack is one of the most important aspects of resilience. An effective backup system can make the difference between downtime and not being able to recover. Virtual environments have brought many advantages in this regard, including failover replication.

The purpose of a backup is to provide a copy of the software that is enough to rebuild the system or function. In addition to regular, automated online/offline backups, it is good to periodically backup the critical information to low-cost disposable/removable media that can be write protected and can be physically relocated (e.g., Blu-ray). Some issues may go unnoticed for long periods of time, so it is important to maintain a deep history of backup data.

D. Dedicated Support and Resource

Maximum achievable resilience requires effective/relevant standards, processes, and resources. In many companies, it is a battle to retain standards against the pressures of cost, constrained resourcing, and workflow. Getting correct and immediate support is critical in cyber resilience as the cost of inadequately addressed cybersecurity will be extremely high. Excessive use of third-party software or the acceptance of irrelevant resilience workflows can collectively and unnecessarily lower the cybersecurity defense, however, the provision of diverse hardware, software, and applications will make it easier for customers to retain the system.

Recommendations to minimize risks:

1. Learn from the nature of security and integrate the relevant aspects into company standards.
2. Build cybersecurity collaboration with relevant third-party specialists and the supply chain to maximize defense.
3. Do not trust OEMs to the max, rather internally exercise managing, testing, and rolling out security-related updates.
4. Some may prefer virtual environments for offline redundancy options. Ensure that low-cost, high-capacity removable storage is available.

The Importance of Remote Lab in ICS Cybersecurity Resilience Programs

This section presents a laboratory to perform cybersecurity tests remotely for the detection and analysis of vulnerabilities in ICS. In the United States, there is a large-scale testbed program (National SCADA Test Bed-NSTB) dedicated to control system cybersecurity assessment, standards improvement, and training. The proposed internal testbed includes software, controllers, field devices and communication technologies commonly used in real ICS. Automation can work with both real industrial equipment and simulations.

Let's see a detailed description of both the physical equipment/simulations used to build testbed and the setup/tools used for vulnerability tests, AV or security update validation. We must have effective backup and recovery strategies, system hardening with firewall exceptions, and IPsec implementation. If required, we can have user management and application control policies in place.

The above testbed provides the possibility to perform remote cybersecurity tests using:

1. ICS server and client: It contains the necessary software for the configuration of the SCADA, human machine interface (HMI), and programmable logic controller (PLC). The HMI is designed to control and monitor the physical systems wired to the industrial PLC, whereas SCADA systems are designed for monitoring and storage of the process variables.

2. OPC server: An additional communication server through which the open platform communications (OPC) protocol can be implemented using a free tool developed by the Metricon group. It acts as a master, requesting data to and from the device or OPC Clients every second.

3. Controller with HART and Profibus devices: An industrial PLC connected to analog and digital modules to simulate the real system. The devices communicate with PLCs designed for this purpose using HART and Profibus protocols.

4. Simulators for Modbus TCP, DNP3, IEC104, IEC61850, etc.: A simulation tools through which the Modbus TCP, DNP3, IEC104, IEC61850 and other Fieldbuses such as the Profinet protocol can be implemented using a free tool developed by the Axon, Triangle Microworks, and Anybus groups, respectively.

5. System hardening with firewall enabled at plant and control network: Helps to limit incoming traffic to the PLC, HMI, and SCADA, guaranteeing that they cannot be reprogrammed or modified from unauthorized users or devices. Furthermore, it also blocks all outgoing traffic to isolate the testing environment.

6. Microsoft and antivirus security update nodes: Helps to overcome security vulnerabilities and fully manage the distribution of updates that are released over Microsoft, McAfee, or Symantec Update Server to computers in production environment. Microsoft updates will be automatically synchronized with Windows Server Update Services (WSUS) whereas antivirus updates will be auto synchronized with McAfee ePolicy Orchestrator (ePO) or Symantec Endpoint Protection Manager (EPM), respectively.

7. Vulnerability scanner: To reduce or mitigate the attack surface to increase the cybersecurity of ICS, it is advisable to perform vulnerability assessments periodically. This type of analysis identifies the vulnerabilities in the system to understand and patch them, for which the vulnerability scanners (such as OpenVAS or Nessus) are useful tools.

8. Backup and recovery server: A fileserver used to store server images and backups of Microsoft-based operating systems. Acronis Cyber Backup delivers data protection as well and provides fast and reliable recovery of apps, systems, and data on any device from any incident.

Conclusion

Increasing the use of information and communication technologies in ICS has exposed them to multiple threats for which they are unprepared, making them vulnerable to malicious attacks. By exploring the ever-changing field of cybersecurity, companies need to manage risks from an expanding attack surface.

There are a few practical and effective measures that companies can take together with existing standards and frameworks which will further increase the cybersecurity resilience. An approach for experimentation in cybersecurity of ICS, based on the replication of a simple ICS, is also proposed. The aim is to provide resilience for an easy definition of ICS cybersecurity. To achieve this purpose, remote laboratories can provide excellent support that companies can consolidate their experimentation with real equipment used in the industry.

Deshabhushan Chougule, software test specialist at ABB Global Industries & Services, on behalf of the ***ISA Global Cybersecurity Alliance.***

To learn more about the IEC/ISA 62443 standard, please visit Download ISAGCA's Quick Start Guide for the ISA/IEC 62443 Standards.

Visit Website

Five Key Questions about Industrial Cybersecurity

To improve security, IT security requirements for industrial communication standards and development processes must now be carefully considered to make sure that they are protected, today and tomorrow. For any company in industrial communication in the future, security will be a requirement – not an option.

CYBERSECURITY IS A CRITICAL ISSUE NOT only for internet banking and general IT infrastructure. As IT and OT converge, general factory floor automation and many industrial applications need to be prepared for both today´s and tomorrow's cybersecurity threats. Where things are going and what security measures will be needed are the big questions. And often the magnitude of the potential threats is hard, if not impossible, to estimate due to the simple fact that the threat landscape is constantly evolving.

Comparing industrial applications and systems to consumer applications presents quite different pictures and completely different outcome scenarios. A security breach in an industrial or infrastructure system can lead to so much more than just financial loss – since a more physical picture comes into play. Imagine for example a malfunction in industrial equipment like a robot, or an infrastructure system like a dam or water supply system failing. This could seriously hurt or even kill people, and on a very large scale even threaten a nation.

In an ever-developing world, more and more applications are exposed to a larger group of threat vectors, which need to be handled securely. Here we outline the current situation and discuss several key questions that are worth considering right now.

Manufacturing industires today are undergoing a significant digital transformation as Information Technology (IT) and Operational Technology (OT) communication systems rapidly converge. Industrial automation devices provide more useful information than ever before – in many cases through networks like OPC UA and MQTT transferring data to IT domains. This is combined with existing industrial Ethernet networks, that in their turn also evolves, adding features and TSN capabilities. This means that a much larger range of data is being made available and collected from the factory floor, across local enterprise IT functions, on-site storage, and into the external cloud – to give companies new competitive advantages.

The IT/OT convergence, encompassing aspects of Industry 4.0 and the Industrial Internet of Things (IIoT), allows new interconnected communication which helps factory OT equipment create greater value out of data shared with local IT applications or via a manufacturer's IoT Platforms. This cross-shared data can offer many benefits in terms of enhanced levels of production, quality and profits. It will also provide industrial processes with much better possibilities to enable predictive maintenance and analysis.

SOURCE: HMS NETWORKS

In the increasingly complex industrial world, applications and sysatems are being exposed to an expanding group of threats, all of which need to be handled securely.

Cybersecurity needs your attention

At the same time, however, these advances make industrial communication networks and manufacturing processes vulnerable to intrusion and attacks. Although large-scale IT hacking cases like Stuxnet and the Ukraine power grid cyberattack a number of years ago are more famous, attacks and intrusions are happening at industrial plants at an increasing rate. Quite recently, several paper mills in Canada were shut down by computer hackers, creating chaos and making headlines around the world.

Five Key Questions about Factory-Floor and Industrial Cybersecurity

1. How widely will the factory floor of the future be connected to higher level systems?

Extracting information from devices, machines and production lines, and passing it on to other IT systems, is a process that has been going on for quite a while. A common way of achieving this is to only use selected points of entry at certain places in a plant/factory. However, the trend and evolution is clearly going in a direction where these will open up more and more.

Without question, some factories or installations will continue to be tightly closed. But considering the advantages interconnectivity can bring – and driven by initiatives like Industry 4.0 – the market is

striving to connect industrial machines to the IT level to enhance maintenance, analysis and production effectiveness.

This likely means that a fast-growing number of industrial machines will no longer be completely isolated from the outside world. Going forward, a factory needs to consider opening selected entry points on different levels. There will most certainly be a transition period as this opening up occurs; what remains to be seen is how fast and how extensive it will be, but trying to minimize entr point is definitely a smart move to reduce attack vectors.

2. Aren't today's factories closed systems, meaning outside access is denied?

Not necessarily, but it depends on how we define "closed". If there is absolutely no connection to the internet, then yes it has a higher protection from external threats. However, a factory owner needs to consider security on different levels. For example, even if it is closed to the internet, people allowed inside the factory can make security "mistakes" that need to be considered.

Examples might be:

1. An external maintenance person, from your supplier, connects their laptop to your machine for diagnostic purposes. Via this connection you are exposed to unnecessary risks and threats – such as viruses or access to internal confidential documents and data
2. A PC being connected to an unused network port on an industrial Ethernet network, where only the machine communication is allowed.
3. Incorrect firmware being downloaded to a machine.
4. An employee making unintentional configuration changes, through tools, web or other environments not requiring authentication.
5. Someone, either an inside employee or outside contractor, bringing a non-secure USB memory stick containing a virus into a factory. Upon connecting to an internal computer or port, the virus itself enables its installation.

There are most likely numerous other examples, and this is just a shortlist illustrating some threats. The consequences though, if any of them would occur, can vary widely from downtime and system failure to risk of viruses/ malware getting into your system, causing unpredicted behavior, huge loss of money, quality issues and even potential harm of people.

On the other hand, the increasing complexity of production machines is already pushing the local team to often interact with their suppliers through remote access solutions that, if not fully secured and managed, create additional entry points to the factory. This trend will clearly continue and accelerate.

3. Who will be responsible that an installation is secure?

Everyone will eventually have to consider security aspects in both new as well as old installations, and then build systems in different levels by segmenting various parts of a factory to create a higher security level. We will also need to accommodate co-existence with older products/installations using older networks. In addition to the question stated in the headline, another interesting question is: Can device manufacturers rely on someone else's technology to solve the actual security part?

Yes, it is our belief that in many cases this will be possible, and even preferred. And when industrial manufacturers are required by their customers and end users to do this, the use of communication solutions that include built-in security features will help them do it more easily and efficiently. Thus, a manufacturer of automation equipment can meet their customers' installation requirements related to security, but without the headaches and investments needed to do it by themselves.

It is worth pointing out that security is not only meant to prevent someone from outside the factory getting access to the network. It can also be intended to protect the network, and the products on this network, inside the factory.

4. Do I need to secure all my products, or can I only secure the ones considered to be at risk? And how do I know which products those are?

This will be the key question for the people specifying a new factory or installation containing industrial network communication. The level of security will probably be decided based on numerous factors. This could be the value of the product being made, the value of the information and processes inside the factory, the consequences of a security breach (eg. a nuclear plant), the level of restricted access inside the factory (who can get close to the machines), IT/internet network connections, and type of data on the network, to give some examples.

As mentioned above, it is not totally clear at this point how and at what speed IT security in industrial communication networks will develop in the future, and what routes will be taken to achieve it. However, we do know that HMS is in an ideal position to help start to make things clearer. We are actively using our deep network communication experience to undertake numerous progressive steps that will assure that our communication solutions, and the users' automation devices and systems, will be secure as IT and OT converge further in the future.

In this context, it is important to note the difference between the meaning of a 'secure' product and a 'security' product. A Secure product is any type of product, e.g. an I/O block, a proximity sensor, or a PLC – that has been developed with security in mind, and therefore certain security methods and counter measures have been implemented to add a certain level of protection for the product's intended usage.

A Security product, on the other hand, is product developed with the sole purpose of addressing specific cybersecurity functionality, e.g. a firewall, a DPI gateway, or data diode. Naturally, those products are also secure products. Those kinds of products have been developed in order to differentiate themselves on the market and to make their customers' jobs easier when they need to implement specific security measures.

5. Is it the device manufacturer's responsibility to solve the security requirements in a factory?

The quick answer is no, it is not the device maker's sole responsibility to solve security. But, if you want to sell your devices in an international marketplace with a wide variation of use cases, you will have to meet the protection requirements of an installation, using security protocols and functions built into your product.

A secure infrastructure is based on in-depth security, which itself is built on several lines of defense – going down to the component level. But, as a device manufacturer, you have no control over the specific security policies within a factory. Therefore, by strengthening the device to handle any situation helps to provide more reliable security performance regardless of the installation conditions.

Security also depends on acceptance by users that have already a strong focus on security management. For example, if a factory demands that its webpages shall be accessible on the network, only products with HTTPS (secure web protocol) can be accepted. This, in turn, means the manufacturer/device maker needs to support this secure functionality in their product, or otherwise risk losing the order and future business.

Even though the route is not entirely clear, the journey has certainly begun and is in full motion.

At HMS, we are committed to being in the forefront within the security area, just as we always have been within the industrial communication space. We will make sure to do what it takes to ensure that our solutions are continuously future proof – both from a connectivity standpoint, but also from a security perspective. For any company aiming to work within industrial communication in the future, security is a requirement – not an option.

*Joakim Wiberg, Head of Technology at **HMS Networks, Business Unit Anybus.***

Visit Website

Threat Modeling Using CIP Security and EtherNet/IP

Threat Modeling is an important activity for the security of any system involving protected resources and communication interfaces. This article provides an overview of some of the Threat Modeling done for the CIP Security protocol within Volume 8 of the CIP Specification, as well as other additional technologies.

CIP SECURITY BRINGS A NUMBER OF IMPORTANT cybersecurity protections to CIP and EtherNet/IP communication. However, CIP Security is not meant to defend against all possible threats, but rather stands as a part of a Defense-in-Depth approach to cybersecurity of industrial equipment. It is important for vendors and users to understand what types of protections CIP Security provides, as well as limitations of those protections and areas where other technologies might be able to boost overall defense.

This article provides a sample of some of the interesting and impactful threats where CIP Security provides protection, as well as areas where CIP Security is meant to fit into a layered approach to cyber protection. This is not meant to be a full Threat Model of CIP Security, but rather provides some illustrative examples around Threat Modeling and the Defense-in-Depth approach to security in which CIP Security plays a major role in protecting important plant assets.

Introduction

CIP Security is a technology which provides robust cybersecurity protections for products and systems which use it. However, it is not enough to simply state this, users of this technology must be given an understanding of the specific protections provided by CIP Security and the threats for which it is meant to provide mitigation.

Threat Modeling is a powerful technique used by security professionals to understand the threats present within a system as well as mitigations to those threats. This technique has been applied to CIP Security and will be published as an appendix to Volume 8 of the CIP Specification. In the creation of the Threat Model the well-known STRIDE technique was used. This technique instructs threats to be analyzed from the STRIDE acronym:

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

The CIP Security Threat Model analyzes the threats on the system's protected resources via these six tenets and then analyzes mitigations provided by CIP Security. For each threat analyzed a mitigation is also described, with some mitigations involving just CIP Security Technology and others requiring additional countermeasures or protections.

SOURCE: ODVA

Figure 1: Trust boundary and data flow for CIP Security Push Model.

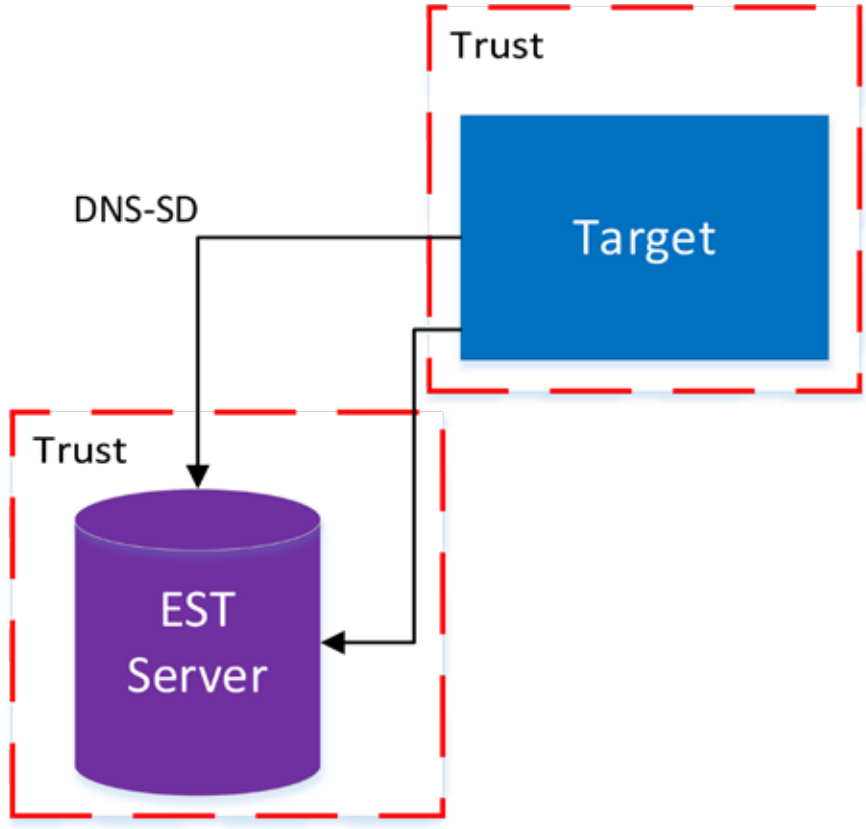
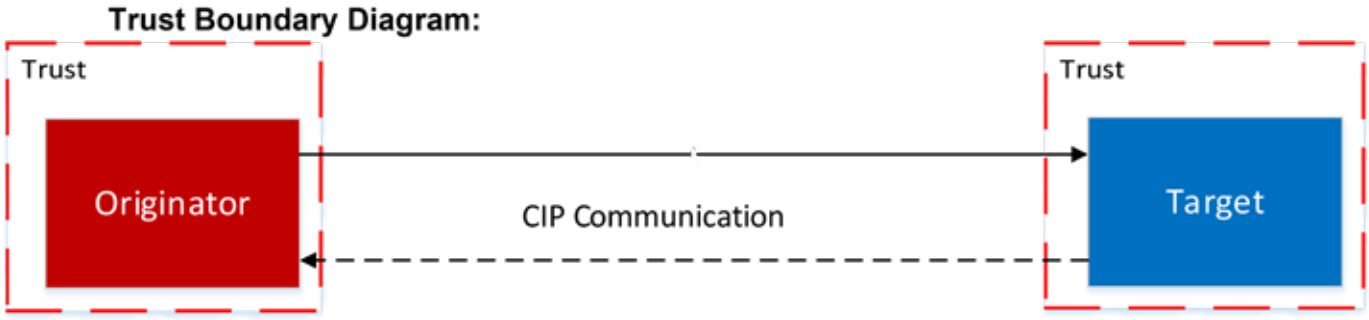


Figure 2: Trust boundary and data flow for CIP Security Pull Model.

A Threat Model relies on the idea of a "Trust Boundary". A trust boundary is a designated boundary over which information that crosses it needs additional protection (e.g. data encryption, data confidentiality, etc.). The designation of trust boundaries is somewhat arbitrary and depends on the goals of the system, but it is an important part of establishing how threats will be analyzed and mitigated. For each threat discussed with the CIP Security Threat Model, a trust boundary is denoted by a dashed red line.

Note that this article does not contain all the Threat Modeling information in Volume 8, but rather a sample of it as well as some additional discussion about threats and



SOURCE: ODVA

Figure 3: Trust boundary and data flow for general EtherNet/IP communication.

mitigations. For a more detailed analysis of threats and mitigations provided by CIP Security please see Volume 8. The Threat Modeling done in Volume 8 is meant to be very generic and as such will not cover all the specific situations that might arise. It is meant to serve as guidance for a more specific and detailed Threat Model done by vendors and/or users.

CIP Security is meant to fit into a Defense-in-Depth architecture and as such is not expected to mitigate all threats on a system. Therefore, many threats and aspects of cybersecurity fall outside of the scope of CIP Security. Although not an exhaustive list, some of the areas that are outside of the scope are:

- Non-EtherNet/IP Communication
- Security of non-CIP endpoints (e.g. Certificate Authorities, NTP servers, DHCP servers, etc.)
- Network-based Denial of Service attacks (e.g. dropped packets, data storms, etc.). In general an attacker with local network access can drop packets or cause packet storms with sufficiently powerful hardware. A secure communication protocol at the transport or application layer will not protect against these IP-based attacks, as it does not prevent an attacker from access to that layer of the network stack.

Threats and Mitigations Sampling

The following section provides a sample of some of the threats and mitigations described within the CIP Security Threat Model. More details are available in Volume 8. These threats and mitigations were chosen because they serve as good examples of a given threat type or mitigation type. A brief discussion of how a particular threat and mitigation serves as an example is given after each description.

Threats Against Provisioning (EtherNet/IP Confidentiality Profile) Background Info:
The EtherNet/IP Confidentiality Profile provides for two mechanisms for provisioning, the Push Model (where certificates and/or PSKs are "pushed" to the endpoint via EtherNet/IP) and the Pull Model (which allows certificates to be requested automatically via the EST protocol). For the Push Model a device simply waits to accept security configuration from any client which can connect to it. In the Pull Model a device will discover an EST server via DNS-SD and then request a certificate. However, the device has no information assurances for the DNS-SD exchange or the EST exchange.

Both of these mechanisms utilize a Trust On First Use (TOFU) mechanism (see RFC 7435 for a general discussion of TOFU). That is, a device in the Factory Default state will trust whatever configuration client is the first that connects to this. Note that vendors are free to further restrict this trust by vendor specific mechanisms, although the standard EtherNet/IP Confidentiality Profile provisioning is TOFU.

Being that the TOFU mechanism is utilized, there are no authenticity guarantees of the configuration software provided by the CIP Security protocol. This must be managed by securing the supply chain and/or by a vendor specific means.

Note however that in both the Push and Pull Model, the configuration software/EST server can possibly verify the device. If a device is shipped with a vendor-signed certificate, then the configuration client software or EST server can be pre-loaded with the root of trust for that vendor. The vendor-signed certificate is used for the initial TLS connection as the server certificate for the Push Model and as the client certificate in the Pull Model. This allows verification of device authenticity.

As mentioned, there is no trust pre-provisioned to the CIP Security endpoint before initial provisioning, as such there is no guarantee of authenticity for the configuration client. For the Pull Model, in general DNS-SD can be spoofed, as there are usually not any information assurances on the DNS communication.

Mitigation: This risk is accepted as a TOFU trust model is how CIP Security works by design. However, device authenticity can be provided by a vendor-signed certificate, therefore it is highly recommended for vendors to ship devices with a vendor certificate. Furthermore, vendors and users are free to include additional controls that go beyond a simple TOFU model if they deem this risk to be worth further mitigation. Examples of these types of controls could be pre-provisioning devices with roots of trust in manufacturing or using a compensating network control like 802.1X https://1.ieee802.org/security/802-1x/.

Additional Discussion: This threat and mitigation is an example of a threat which in general is accepted due to industry and product requirements. Threats of this nature are not directly mitigated by CIP Security, but can work with other countermeasures to provide additional mitigations if desired by a user. In this particular example, something like 802.1X is provided as an additional countermeasure that can be deployed. However, this also serves as an example of a threat which a user needs to evaluate within their own unique environment to make an informed decision of whether or not additional countermeasures are required.

Threats Against Data in Transit (EtherNet/IP Confidentiality Profile) Background Info:
Class 3 and Unconnected Messaging are used by EtherNet/IP endpoints for sending and receiving information in a structured, request-response manner. Without authentication of endpoints there is no guarantee that a connection is made with the correct Originator and Target. Furthermore, as the underlying transport for Class 3 and Unconnected Messaging is TCP/IP this messaging is subject to standard "Person-in-the-Middle" attacks. Similarly, Class 0 and 1 "implicit" messaging uses UDP and is subject to these same network level Person-in-the-Middle attacks.

Threat – Spoofing

A connection to a device from an unauthorized Originator represents a spoofing threat. Unauthorized Originators could affect configuration or I/O data by sending messages to the device. Like this, an Originator attempting to connect to a Target is susceptible to spoofing of the Target by an attacker.

Mitigation: Authenticators provided by (D)TLS such as certificates or PSKs provide for the authentication of both parties in the (D)TLS session. For certificates, CIP Security provides a configuration option via an attribute in the EtherNet/IP Security Object Instance that causes the Target to request and validate the

client certificate. Mutual authentication during the (D)TLS handshake fully mitigates this risk. For systems in which the user determines that Originators do not need to be authenticated the option can be selected to only validate server certificates.

Note that even with client and server authentication, there is no notion of Role-Based User Access Control; for that the CIP Security User Authentication Profile is required. Also note that proper generation, storage, and protection of private keys is necessary for mitigation of this risk, this subject is specific to a given product and therefore outside the scope of the specification and Threat Model.

Threat – Tampering

Data may be tampered with through well-known or novel Person-in-the-Middle attacks such as ARP cache poisoning/ARP spoofing. This could result in a device receiving messages which are different from the intended message, and in some cases without the sender or receiver knowing of the change.

Mitigation: The information assurance properties of (D)TLS include data authenticity. This is realized by using an HMAC and/or an authenticated encryption algorithm. With either an HMAC and/or authenticated encryption in place through the (D)TLS cipher suite this risk is low and therefore generally mitigated.

Additional Discussion: This threat and mitigation is a good example of how CIP Security can provide a very strong mitigation. CIP Security, and the backing technologies of TLS and DTLS, were designed to specifically mitigate this type of threat, and therefore are well suited to this use.

However, even with a case like this it is still important for a user to evaluate their unique system to ensure there aren't any extenuating circumstances that change their risk profile. However, most systems likely will have this type of threat sufficiently mitigated by CIP Security.

Threats Against Communication Redirection (EtherNet/IP Confidentiality Profile) Background Info:

Even in a system in which CIP Security has been set up, an attacker may be able to affect packet routing through TCP/IP based attacks on network traffic (e.g. ARP spoofing). This could allow for an attacker to re-direct legitimate communication from the intended Target to a different one.

As an example, consider the case where a controller is sending data and commands to two drives, Drive A and Drive B. There is mutual trust between the controller and drives, and yet the commands sent to each drive are different. An attacker may attempt to re- direct traffic intended for Drive A to Drive B.

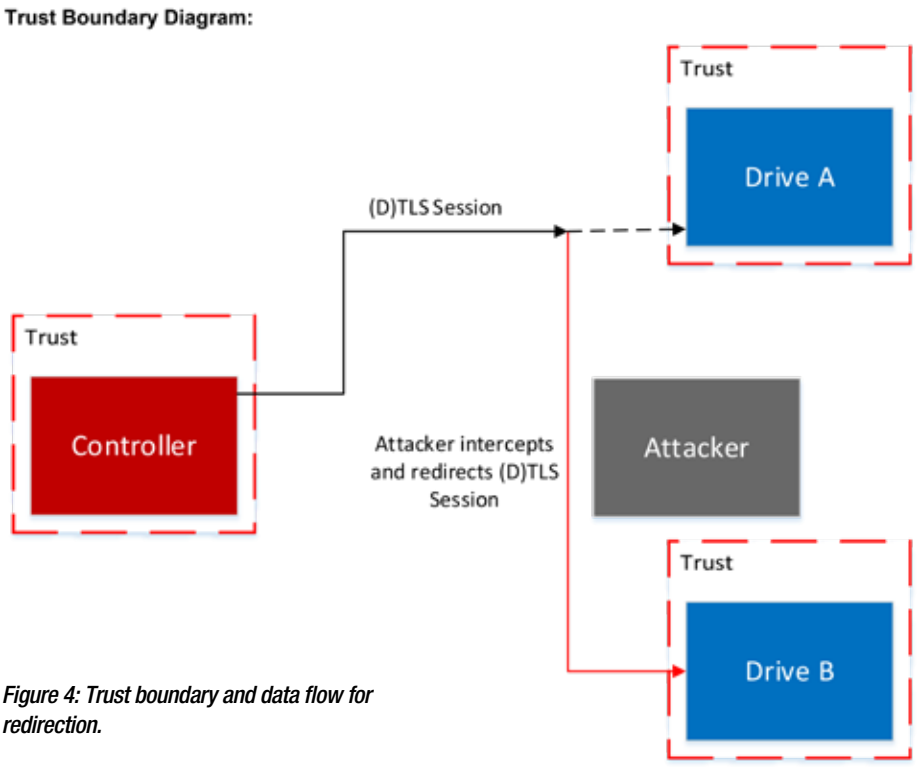


Figure 4: Trust boundary and data flow for redirection.

Threat – Spoofing and Tampering

An attacker able to successfully re-direct traffic intended for one Target to another represents a spoofing threat in that the communication, although legitimate for the intended Target, can be considered spoofed on the new Target. Depending on the contents of the communication, tampering may also occur, as data could be modified in ways not intended by the legitimate user. Note that the attacker is not able to author any of the commands, but rather just redirect existing legitimate commands to an unintended Target. Furthermore there must be trust between the Originator and both Targets for this attack to be successful.

Note a special case of this attack would be a redirection of communication from the Originator back to the Originator. This was discussed extensively in "Selfie: reflections on TLS 1.3 with PSK" (https://eprint.iacr.org/2019/347).

Mitigation: Several mitigations exist for this vulnerability. Fundamentally this vulnerability is mitigated through the use of identifying information for the Target that can be trusted and verified by the Originator. One mechanism for this would be identifying information at the application layer (EtherNet/IP). Often times there may be route information, and/or product type and code information that would prevent this attack from occurring. However, this is not always the case, and as such a better mechanism for this would be to rely on identifying information within the cryptographic identity. Any identifying information within the certificate can be used, such as the Common Name or the Subject Alternative Name.

CIP Security does provide mechanisms to set both of these, as well as to specifically check the Subject Alternative Name matches what is expected. If the Originator verifies this information as part of the (D)TLS handshake then this vulnerability is mitigated. However, PSKs do not have any such identifying information, and as such, any usage of a PSK beyond two parties may be subject to this type of redirection attack. Note the PSK usage field prevents the special case of this attacker where an Originator's communication is reflected back to itself, as PSKs are only allowed to be used for Target or Originator functionality, but not both.

Additional Discussion: This is an example of a somewhat nuanced threat and why details of the configuration are important. Simply using CIP Security is not enough to provide a mitigation to this class of attacks, but rather setting specific configuration options is necessary. This drives the point that in Threat Modeling and mitigation analysis details are often very important.

Threats Against Proof of Authentication (User Authentication Profile) Background:

After authentication occurs the Originator receives a signed Token that serves as proof of the authentication event. The Token provides proof to the Target that the authentication has occurred, as well as claims regarding the role/identity of the Originator. Several threats exist on this proof of authentication via the Token.

Threat – Spoofing

There are several spoofing threats for this data flow:

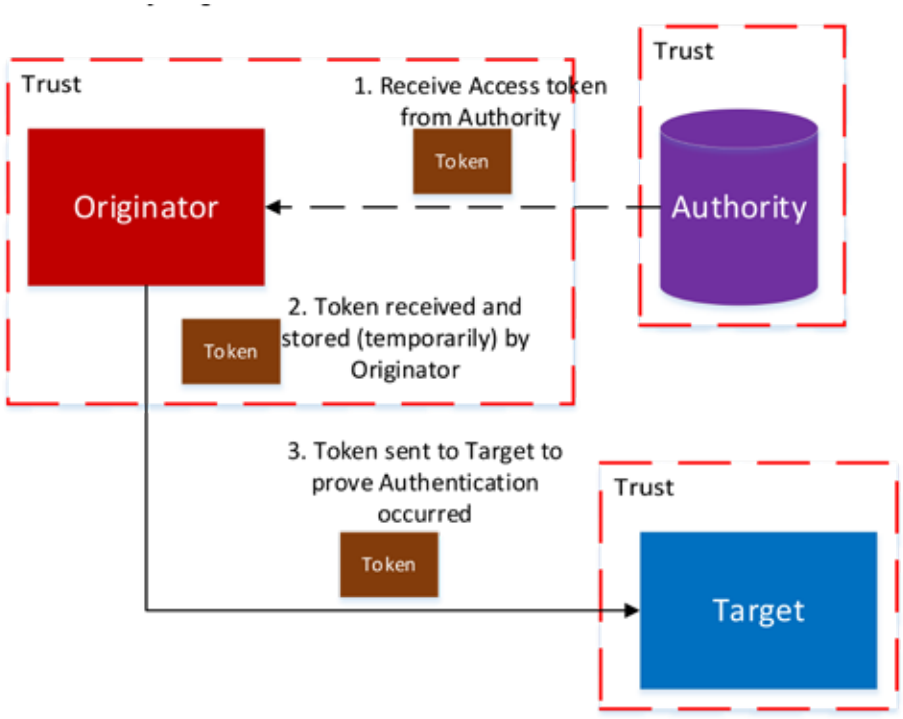


Figure 5: Trust boundary and data flow for proof of authentication via token.

- An attacker might spoof the Originator to obtain the Token (interaction #1 in figure x)
- An attacker might spoof the Target to obtain the token (interaction #3 in figure x)
- An attacker might spoof the Token itself

Mitigation: (D)TLS provides endpoint authentication of both Originator and Target when Verify Client Certificate is enabled, providing assurances against the spoofing of the Originator or Target. Tokens are produced by the Authority with a unique digital signature generated by a private key the Authority controls, which provides mitigation against an attacker spoofing the token itself.

Threat – Tampering/Elevation of Privilege

Tampering and Elevation of Privilege threats are closely related. Tampering with the token can lead to a change of role or other claim information, granting the attacker a higher privilege. Similarly, a token could be replayed after expiration in order to obtain a level of privilege that is no longer granted.

Mitigation: The digital signature of the token provides information assurance guarantees against tampering of the token.

Threat – Information Disclosure

An attacker might attempt to capture the token in order to impersonate the user; the Token is considered confidential as it can be used for impersonation. This might be done via standard network-based attacks, or via the spoofing threats discussed earlier in this section where the attacker spoofs either the Originator, the Target, or the Token itself.

Mitigation: While in transit over EtherNet/IP the confidentiality of the token is protected via a (D)TLS session with a confidentiality-based cipher suite. Note: the design of an Originator must ensure that the Token is not exposed outside of its trust boundary, although the internal structure of an Originator is outside the scope of this Threat Model and is vendor specific.

Additional Discussion: This threat is an example of a complex data flow in which a protected resource (the Token) is handled by various endpoints. Due to the complexity of this flow there are various threats, although mitigations are provided for each.

Threats Against Originator to Authority Authentication (User Authentication Profile) Background

The Originator will send authenticators to the authority in order to prove its identity. Authenticators can include confidential information such as passwords. Note for external, non-CIP authorities this communication is not within the scope of the Threat Model. However, two CIP-based authenticators are supported: username/password and X.509 certificates. The communication of these CIP-based authenticators is within scope for this Threat Model and is subject to enumerated threats. Note that threats in this section all have the same mitigation, so only one mitigation is discussed.

Threat – Information Disclosure

An attacker might capture confidential authenticators (e.g. passwords). This could be done either through spoofing the authority (described in C-3.4.2.1) or through passive network attacks where packets containing the authenticators are captured.

Mitigation A (D)TLS session between the Originator and Authority provides data authenticity and endpoint authentication. However, these assurances are only provided if bi-directional authentication is enabled (via the VerifyClientCertificate attribute of the EtherNet/IP Security Object) and if a cipher suite that utilizes confidentiality is used. Further note that non-CIP based Authorities may have other mitigations besides (D)TLS; in that case those Authorities must be evaluated against these threats.

Additional Discussion: This threat and mitigation is an example of a situation in which information assurances of one profile are used to protect resources of another profile. In this case the confidentiality assurances provided by TLS and DTLS from the EtherNet/IP Confidentiality Profile are used in mitigating risks against authenticators like passwords being exposed. This is one of the reasons which the CIP Security User Authentication Profile requires the EtherNet/IP Confidentiality Profile be supported.

Threats Against Discovery (User Authentication Profile) Background

Before any User Authentication can occur, the Originator needs to discover the Target and the Authority. Threats exist against this process of discovery.

Threat – Spoofing

An attacker might attempt to spoof the Target and send a malicious response to the Originator containing discovery information. This could in turn direct the Originator to a rogue authority, possibly leading to the leakage of authenticators.

Threat – Tampering

An attacker might attempt to tamper with the discovery information to direct the Originator to a rogue authority, possibly leading to the leakage of authenticators.

Mitigation: In the case of both the spoofing and tampering threat the mitigation is provided by the (D)TLS session over which the discovery is done. A (D)TLS session between the Originator and Target provides authentication of both the Originator and Target, if the VerifyClientCertificate option is set to true.

The (D)TLS session also provides information assurance as to the authenticity of the data in transit, which in this case is the discovery information. Through the (D)TLS session a mitigation is provided against the tampering threat.

Additional Discussion: This threat and mitigation provides another example of information assurances from one profile being used to protect data in another. However,

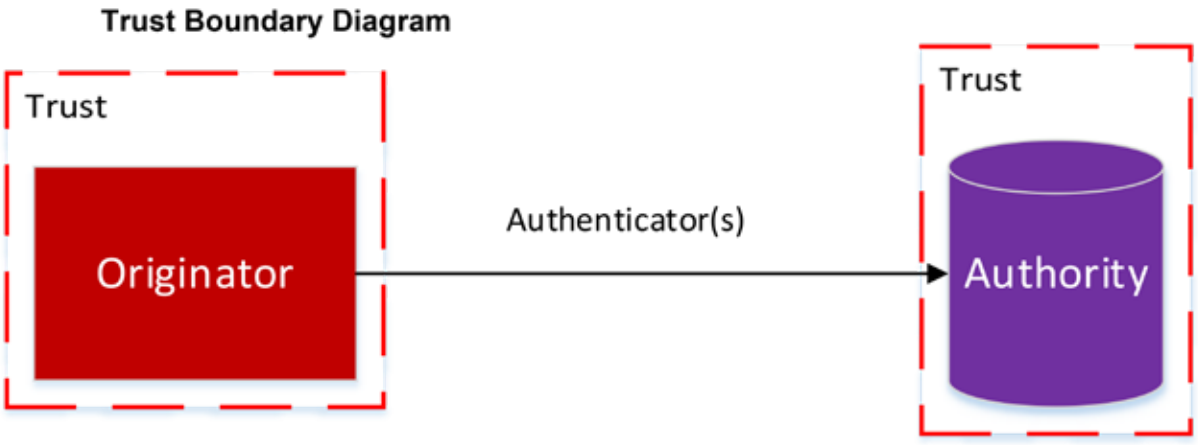


Figure 6: Trust boundary and data flow for authenticator exchange.

in this case the information assurance is not around data confidentiality, but rather the authenticity of data and authenticity of the endpoint. Again this is provided by the TLS session that is part of the EtherNet/IP Confidentiality Profile.

Best Practices

Threat Modeling CIP Security shows that CIP Security is not intended to provide a mitigation to all threats, but rather to fit into a defense-in-depth system. This section describes some of the supporting technologies for CIP Security, as well as some of the other defense-in-depth protections that can be applied to a CIP Security system. This section simply contains examples, there are other technologies that could also be used which are not listed.

Supporting Technologies

Public Key Infrastructure (PKI)

A PKI is a fundamental part of a system utilizing CIP Security. Although CIP Security can be used without a PKI (with PSKs or self-signed certificates), it is highly recommended to make use of a PKI for any but the simplest systems.

A PKI allows for unique identity certificates to be issued and revoked, as well as for trust to be managed across the entire system. CIP Security endpoints can be configured for trusting multiple Certificate Authorities which can be managed by the PKI. Policies around how a certificate is granted are the domain of a Registration Authority (RA) within the PKI and are very important to constructing a secure PKI. The RA function is outside the scope of CIP Security, but directly impacts the security of an endpoint using CIP Security. Therefore, it is important to analyze and review the RA policies to ensure that proper authorization is required for a certificate to be granted, renewed, or revoked. There are many options for using commercially available software to set up a PKI, and for many users this will be a good option. IT departments often have a PKI already in place that could be used. However, in some cases the OT system will want to utilize a separate PKI that can be used to distribute certificates and trust anchors to CIP Security devices independent of IT trust. CIP Security can work with multiple CAs and multiple roots of trust, although a compromise of one or more CAs will likely have serious consequences to the effectiveness of CIP Security. Therefore it is very important to carefully consider the security of the PKI and CAs contained within.

OpenID Connect Identity Provider

For systems which use centralized authentication, an OpenID Connect Identity Provide is the technology chosen to work with CIP Security endpoints. There are many commercially available and open source OpenID Connect Identity Providers (see https://openid.net/developers/certified/ for examples).

These Identity Providers issue the tokens which serve as proof of authentication, therefore it is very important that they are configured, used, and protected properly. Many OpenID Connect Identity Providers are available as a service, with the Identity Provider running in a cloud environment accessible over a secure Internet connection. In this case some of the protections are managed by the service provider, although it is still important for users to understand what types of protections are provided and how the Identity Providers are intended to be used. For an OpenID Connect Identity Provider running on-premise, more of the burden around configuration and protection will fall to the end user. Each particular environment will have nuanced needs which must be evaluated by the end user.

OpenID Connect Identity Providers generally support a wide range of authentication mechanisms. Many support various multi-factor authentication schemes, which may include the user of biometrics, smartcards, secure dongles, etc. It is important to understand the tradeoffs provided by various authentication schemes in terms of information assurance, ease-of-use, cost-to-deploy/maintain, etc. Systems with more advanced information assurance needs will likely want to use multi-factor authentication, although the exact details behind which scheme are important to work out through a Threat Model.

Given that the OpenID Connect Identity Provider issues the tokens which serve as proof of authentication in CIP Security it is a fundamental part of the security system. A compromise of the Identity Provider would very likely lead to a significant elevation of privilege, as tokens may be issued for an elevated role (e.g. Administrator). It's very important to ensure that tokens are only issued to properly authenticated parties, and that authentication is set up in such a way that it provides appropriate assurances of identity without causing undue burden to the users.

Secure Time Server (e.g. NTS)

System security depends on a synchronized time between endpoints in the system. Some components of the system are time sensitive, as such server and client must agree on time to ensure certificates are used within their window of validity, tokens have not expired, and events logged can be correlated. By default, expired tokens and certificates are rejected.

There are two well know abuse cases regarding time. The first is to manipulate time backwards to re- use previously expired credentials or certificates. This is a rare case as the attacker needs to compromise private keys in addition to manipulating time. The second abuse case is where the attack manipulates time to be outside of the validity window of all certificates and tokens causing a denial of service when they are rejected. Typically, time was manipulated by spoofing response messages to the NTP client with invalid time. As there was no method to authenticate the

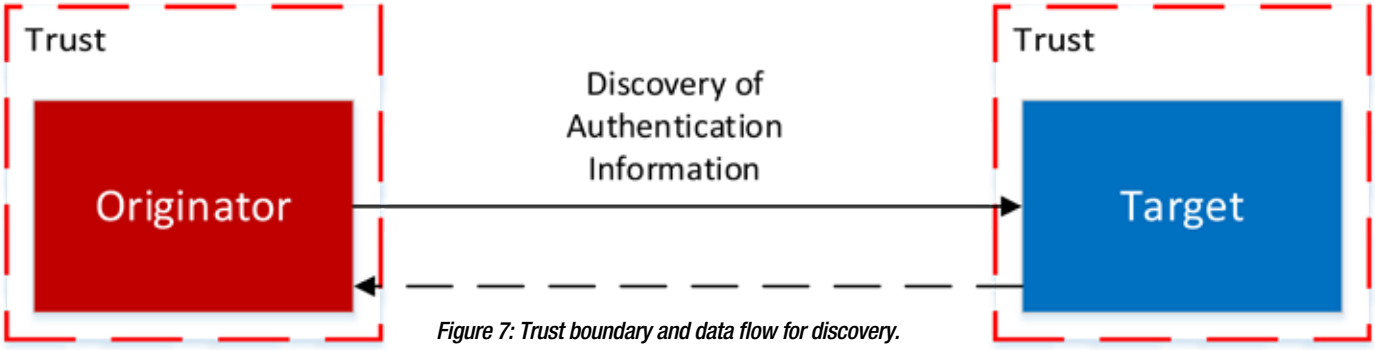


Figure 7: Trust boundary and data flow for discovery.

timestamp, the NTP client would adjust time towards the malicious time setting.

These abuse cases have been known for years, and NTPv3 included Message Authentication Code extensions to allow a client to authenticate the timestamp with a symmetric key. The key distribution mechanism was manual out of band management that posed non-trivial key management problems for implementors. NTPv4 attempted to solve the key distribution problem with the autokey protocol. Autokey included a key distribution and timestamp signing mechanism. However, autokey suffered from design flaws and was depreciated.

In 2020, the IETF released NTS4NTP (RFC 8915) to provide for uni-cast and multi-cast NTP environment an initial key agreement mechanism, and continuous update of a nonce used in MAC extension key. NTS4NTP allows automatic key distribution using a TLS channel and protocol handshake to give the NTP client the symmetric key and initial nonces used by the server. The client then uses NTP with NTS extensions in the client to request a secured timestamp. The server responds with a timestamp and Authentication extension. The MAC allows the client to verify the authenticity of the timestamp to ensure the time received is accurate.

Mitigating Technologies Firewall

A firewall is often one of the first tools that is brought to mind for cybersecurity protection. Firewalls range widely in their usage, features, and sophistication, but it is often true that a firewall can help provide additional protection for an industrial system. Firewalls often block certain types of traffic. They might block traffic based on the source or destination; for example preventing traffic from a class of IP addresses, or to a particular known-malicious domain name. More sophisticated rules might be applied dealing with certain types of traffic, for example blocking the insecure telnet protocol. More sophisticated tools can utilize techniques like deep packet inspection to apply more nuanced rules against certain types of traffic or network patterns.

Firewalls are often placed at network boundary locations as their function of blocking certain classes of traffic works well in the context of a network boundary. What constitutes a network boundary and what type of firewall to install there varies from system to system. They might be placed at the boundary between an internal network and the Internet, or between the IT network and OT network, or even between a cell or line within a plant and the rest of the plant network. Given the firewall's function at the network boundary, it typically does not interact directly with CIP Security devices and their communication, although in some cases it may. Since CIP Security is typically device to device, or computer to device, firewalls may not be blocking or inspecting CIP Security traffic. However, if they are, then it is of course important that the firewall be configured to allow CIP Security traffic. It is important to analyze the firewall configuration to ensure that it won't prevent legitimate CIP Security traffic from crossing a network boundary. Given that CIP Security uses well known ports and uses standard TLS and DTLS, writing rules for allowing CIP Security traffic should be quite achievable with most firewalls.

IDS/IPS

Another cybersecurity protection that can be applied is an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS). IDS and IPS are often grouped together as they share many similar characteristics, with the main difference being whether or not the response to a threat is active and preventative as in the case of an IPS, or passive and more logging/alerting-based, as in the case of an IDS.

Like a firewall, there is a wide range of sophistication of these tools; some are quite advanced and apply complex machine learning to determine if an attack is taking place, whereas others are quite straightforward in terms of simple packet matching for detection. One important consideration for deploying an IDS/IPS within a CIP Security system is that the CIP Security traffic may be encrypted, in which case an IDS/IPS that uses packet inspection will not be able to do any deep inspection of the CIP Security packets. That said, information can still be gleaned from the IP layer packets, such as source/destination, protocol, routing information, etc. However, if deep packet inspection is important to the security of the system then the user should consider using TLS and DTLS cipher suites which support authenticity only. Other than this consideration, IDS/IPS will likely work well with CIP Security devices, and can help bolster the defense-in-depth posture of the system.

Conclusion

Threat Modeling is an important activity for the security of any system involving protected resources and communication interfaces. This article provides an overview of some of the Threat Modeling done for the CIP Security protocol within Volume 8 of the CIP Specification, as well as some additional technologies that are used by CIP Security or can be used to increase the defense-in-depth of a system using CIP Security. However, Threat Modeling and mitigation analysis is highly dependent on the particular details of a given system, therefore the information provided here is not meant to be a "one-size-fits-all" Threat

Model for systems and devices that use CIP Security. Rather, the intention is that this paper provides an introduction to the topic and activity of Threat Modeling with CIP Security, and serves as an aid to vendors and users who are using CIP Security and are creating a Threat Model for their system. Threat Models are not static but rather continuously updated as new information, including new attacks, become known. Therefore the information here is necessarily a snapshot in time and may need adjustments as time goes on. Note that the CIP Security Threat Model present in Volume 8 of the CIP Specification will be updated as conditions dictate. This paper and the information in Volume 8 show that CIP Security provides robust mitigation for a large class of cybersecurity threats, and that its usage is important in a system where CIP and EtherNet/IP communication are used.

*David Smith, Cybersecurity Architect, **Schneider Electric**, Jack Visoky, Principal Engineer and Security Architect, **Rockwell Automation** and Joakim Wiberg, Head of Technology, **HMS Networks.***

Visit Website

Enhancing Cybersecurity for Connected Serial Devices

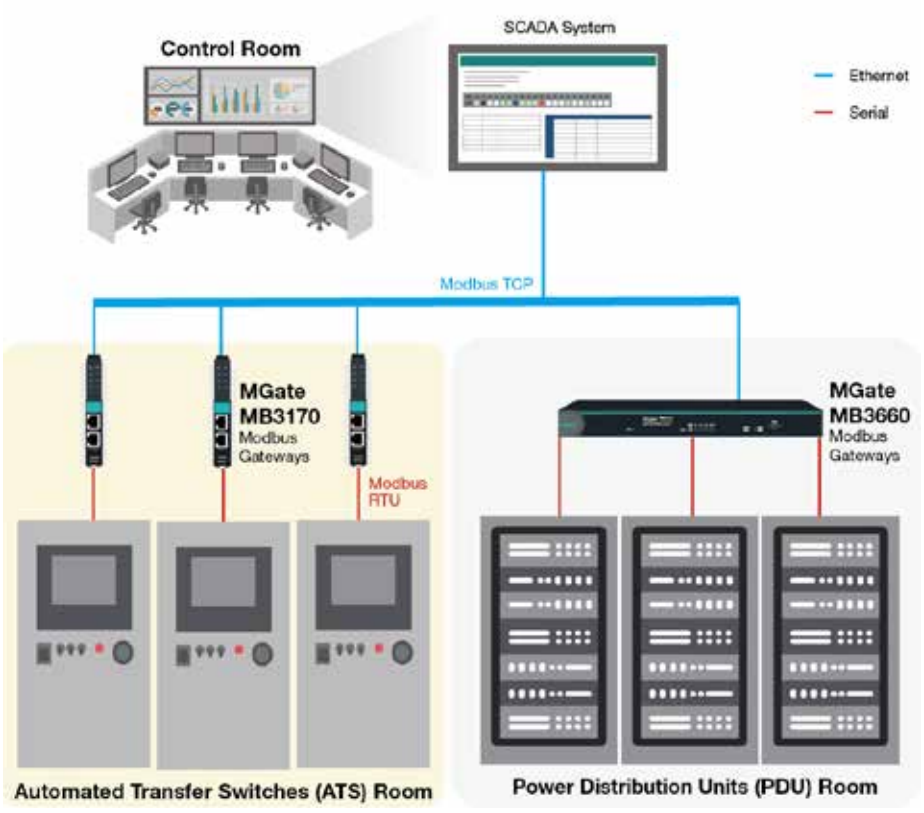
High-profile cyberattacks targeting critical infrastructure has underlined the need for industrial organizations to prioritize cybersecurity. This article discusses the challenges industrial operators face and solutions that enhance cybersecurity with minimal effort.

INDUSTRIAL NETWORK SECURITY IS NOT A luxury option anymore — it is a necessity. A spate of high-profile cyberattacks targeting critical infrastructure has underlined the need for industrial organizations to prioritize cybersecurity.

No matter which industry you are in, potential threats are everywhere. Recent incidents include hackers shutting down a fuel pipeline and demanding millions of dollars in ransom payments, and a ransomware attack against self-service ticketing machines of a UK railway company that took the machines offline.

Needless to say, these types of cyberattacks lead to tremendous cost and inconveniences to industrial operators and their end users. To make matters worse, predicting where the next cyberattack is going to strike is almost impossible, meaning that anyone or anything connected to a network can be a target.

To enhance network security, companies can replace equipment with newer models that features embedded security functionality. However, replacing equipment will be costly and involve significant efforts in deployment and installation. Besides, legacy equipment is most likely still in a good working condition. A more realistic option is to update the security patches of existing equipment. Unfortunately, some legacy equipment still use legacy operating systems that do not support the latest security patches anymore — Windows XP being one such example. In this article, the cybersecurity experts at Moxa discuss the challenges industrial operators face and the solutions that enhance cybersecurity with minimal efforts.



SOURCE: MOXA

To monitor power usage and quality, the power supply equipment including switchgears, PDUs, and UPSs connect to networks to allow operators to receive real-time information. .

Challenges to Secure Edge Networks

To improve operational efficiency, industrial operators must take advantage of the capabilities of today's networks to realize real-time remote monitoring. However, it also means that field devices can't be air-gapped any longer.

The first challenge is connecting legacy equipment that use RS-232/422/485 communications to your local area network (LAN) or the Internet, which uses Ethernet communications. Serial-to-Ethernet devices, such as serial device servers or protocol gateways depending on the application's required transparent transmissions or protocol conversions can connect serial-based equipment to Ethernet-based networks.

Once legacy devices are connected, security concerns unfortunately raise their ugly head, especially if the connection doesn't have proper protection. Therefore, it's essential to find a serial-to-Ethernet device that ensures secure connectivity without replacing existing serial devices.

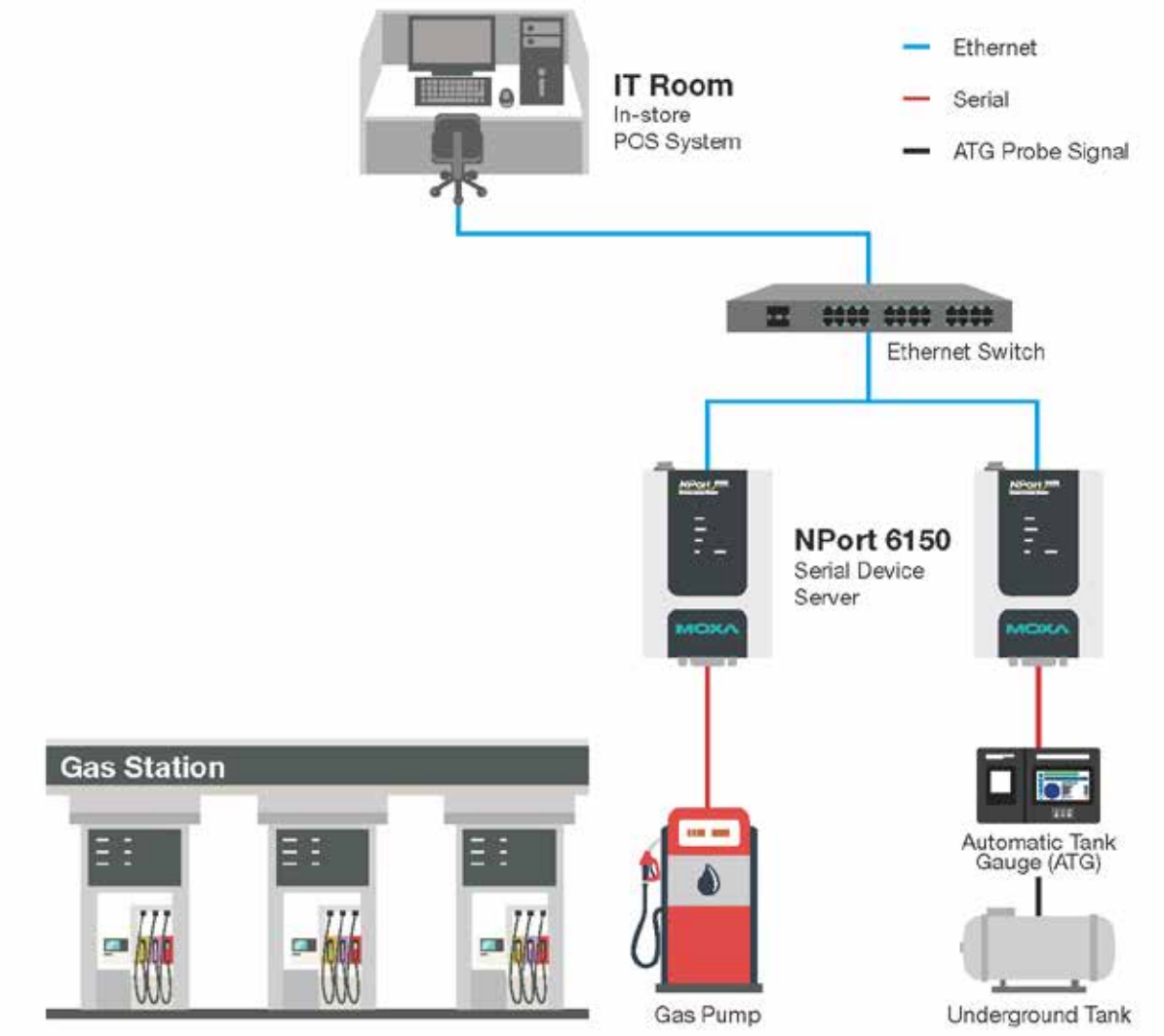
How to Choose a Secure Serial-to-Ethernet Device

Today's security standards, such as IEC 62443 and NERC CIP, are available to help secure your network infrastructure. These security standards include guidelines that help verify qualified networking devices and component suppliers. Thus, it's an easy way to find a secure serial-to-Ethernet device that complies with industry security standards. Moxa is an IEC 62443-4-1 certified networking solution provider, and the design of Moxa serial-to-Ethernet devices is based on the IEC 62443-4-2. With security embedded functions, Moxa serial-to-Ethernet devices enhance network security and reduce the chances of unwanted actors accessing serial equipment through Moxa devices.

Two Real-world Examples: Enhancing Cybersecurity

Moxa secure serial device servers and protocol gateways have helped customers ramp up their connectivity security in a variety of industrial applications. To demonstrate, here are two real-world examples showcasing how Moxa NPort 6150 serial devices servers and Moxa MGate MB3000 protocol gateways strengthen cybersecurity in the energy industry.

Problem 1: A Moxa customer with over 600 gas stations in the U.S. required real-time monitoring of the levels in their oil tanks with "ATG" -- Automatic Tank Gauge, usually



SOURCE: MOXA

Serial device servers feature basic security functions such as user authentication and accessible IP list to ramp up device security with device access control.

with serial interfaces -- to schedule inventory replenishments as needed at remote sites. They also needed data from POS terminals at gas pumps to be sent back to the store for transaction processing and records. These connectivity requirements are security sensitive.

Information regarding the tank levels needs to be well secured so that it could not to be manipulated, and the POS data contains confidential information of consumers, which needs to be further protected. To enhance connectivity security, the connection between the gas station and the in-store IT room also requires protection. In addition, to ensure the connected devices are operating at accepted security levels, IT personnel are required to execute vulnerability scans periodically to update firmware and security patches, keeping the communication systems safe.

Solution: Moxa NPort 6150 serial device servers feature basic security functions such as user authentication and accessible IP list to ramp up device security with device access control. During operations, Moxa products support a data-encryption function to enhance transmission security when sending serial data over Ethernet. To make the daily maintenance easy for IT personnel, the NPort 6150 serial device servers support tools to make the configuration and management of many devices easy.

Problem 2: A data center service provider and its data centers have been frequent targets of cyber intruders, resulting in data losses and significant penalties over the past five years. To reduce the chances of being hacked, cybersecurity has become a corporate-level initiative. Security risk assessments do not focus solely on vulnerabilities in the server rooms, but also extend to all network entry points, including the power sources that supply the server rooms.

Solution: To monitor power usage and quality, the power supply equipment including switchgears, PDUs, and UPSs connect to networks to allow operators to receive real-time information. Moxa MGate MB3000 protocol gateways bridge communication between serial-based Modbus RTU devices such as power meters used inside power supply equipment and the Ethernet-based SCADA systems in the control center. When corporate IT personnel are required to perform a vulnerability scan, they can scan thousands of MGate MB3000 protocol gateways so that they can take immediate action if they identify a vulnerability.

To make IT personnel's work easier, Moxa also performs vulnerability scans periodically and, if needed, takes necessary action, such as updating security patches and firmware to reduce potential threats. In addition, Moxa MGate MB3000 protocol gateways feature an easy-to-use configuration tool in both GUI and CLI format, helping OT and IT users easily handle mass firmware updates. Moxa MGate MB3000 protocol gateways not only allow customers to monitor power usage in their serial-based devices but also ease their security concerns and daily operation efforts at the same time.

Technical article by ***Moxa.***

Visit Website

Expanding CIP Security with CIP Authorization Profile

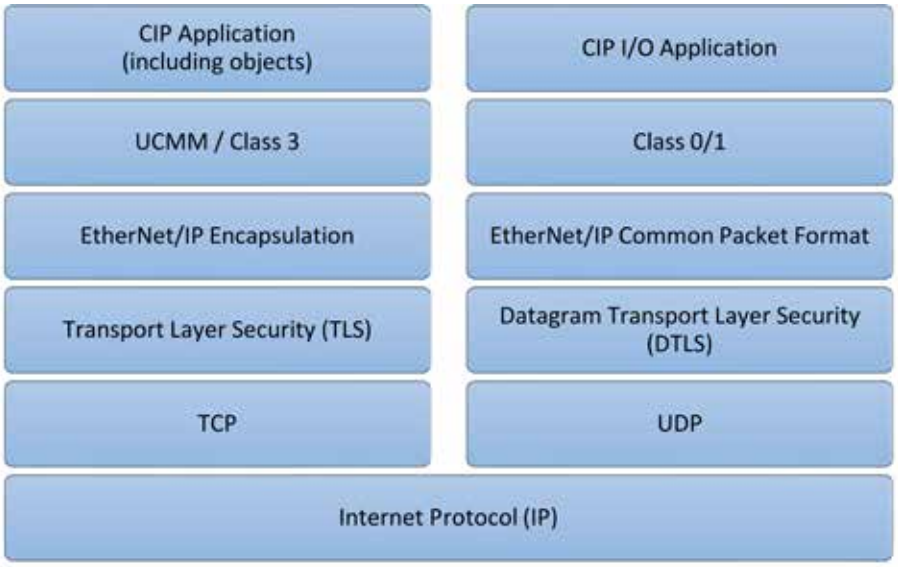
The CIP Security Authorization Profile enhances CIP to provide additional security properties such as general, flexible authorization where access policy can be based on any attribute of the user and/or system. Concepts and open systems that might serve as a basis for the CIP Authorization Profile are explored.

CYBER SECURITY WITHIN INDUSTRIAL ETHERNET has exhibited rapid growth, with CIP Security and EtherNet/IP™ emerging as a leader. End users seek to take advantage of the features provided by the CIP Security Profiles today and related open ecosystem. Benefits include data integrity and data confidentiality, device identity and authentication, and user authentication.

These features are provided by Security Profiles as defined today and serve as a base for CIP Security devices. Over time CIP Security has been extended with new optional Security Profiles targeting different applications and functionality.

Within this article the idea of a new optional profile named "CIP Authorization Profile" is explored and evaluated. The CIP Security Authorization Profile will enhance CIP to provide additional security properties such as general, flexible authorization where access policy can be based on any attribute of the user and/or system. Concepts and open systems that might serve as a base for the CIP Authorization Profile are explored.

This article will provide advanced insights regarding technology and requirements for the CIP Authorization Profile that will eventually be added to CIP Security. As the CIP Authorization Profile is officially developed within ODVA it may deviate from the scenarios described in this article. However, the general application of the CIP Authorization Profile can be understood.



SOURCE: ODVA

Figure 1 EtherNet/IP over TLS and DTLS layering.

Introduction

Volume 8 of the CIP Specification currently defines CIP Security via several profiles. These profiles provide security features like secure transport, user authentication, automatic certificate enrollment, and others as well. However, there is currently no standard profile that defines features around configurable authorization. That is, there is no standard way to define what privilege levels are required to access what resources. Defining this functionality in a standard way gives the user a powerful mechanism to define authorization in a highly flexible and configurable way. However, providing this functionality is not a simple task, there are many ways in which

Security Profile	General Description
EtherNet/IP Integrity Profile (Obsoleted)	Provides secure communications between EtherNet/IP endpoints to assure data integrity and device authenticity.
EtherNet/IP Confidentially Profile	Provides secure communications between EtherNet/IP endpoints and ensures data confidentiality for transport class 0/1 traffic. Includes the EtherNet/IP Integrity profile as a subset.
CIP Authorization Profile (future)	Provides secure communications between CIP endpoints to ensure device and user authenticity.
CIP User Authentication Profile	Provides User-level authentication for CIP communication
Resource-Constrained CIP Security Profile	Provides a lightweight version of the protections afforded by other CIP Security Profiles specifically for highly Resource-Constrained devices

SOURCE: ODVA

Table 1 CIP Security Profiles.

Security Property	EtherNet/IP Confidentially Profile	CIP Authorization Profile (future)	CIP User Authentication Profile	Resource-Constrained CIP Security Profile
Device Authentication	√	√		√
Trust Domain	Broad – group of devices		Narrow - individual device/user	Broad – option to be Narrow via Gateway or Proxy
Device Identity	√		√ (Identity of User)	√
Data Integrity	√			√
Data Confidentiality	√			**Via Gateway or Proxy**
User Authentication			√	
Change Detection (Audit)		√		
Policy Enforcement (Authorization)		Flexible	Fixed	Via Gateway or Proxy

SOURCE: ODVA

Table 2 Supported Security Properties.

this could be done technically, each with their own tradeoffs.

Before defining a profile for authorization and access control policy an investigation must be done regarding technology options, as well as tradeoffs for the user. It is important to balance flexibility against complexity and to define this profile in such a way that it is user-friendly yet powerful enough to provide options to the user. This article provides a starting point for this investigation to aid in the definition of this profile.

CIP Security and CIP Security Profiles overview

CIP Security is defined in Volume 8 of the CIP Networks Specification and includes the definition of security-related requirements and capabilities for CIP devices. Volume 8 at present is focused on EtherNet/IP, as EtherNet/IP-connected devices represent the largest risk due to enterprise network connectivity and provides a secure transport mechanism for EtherNet/IP devices.

CIP Security for EtherNet/IP devices makes use of the IETF-standard TLS (RFC 5246) and DTLS (RFC 6347) protocols in order to provide a secure transport for EtherNet/IP traffic. TLS is used for the TCP- based communications (including encapsulation layer, UCMM, transport class 3), and DTLS for the UDP-based transport class 0/1 communications. This approach is analogous to the way that HTTP uses TLS for HTTPS.

The secure EtherNet/IP transport provides the following security attributes:

Authentication of the endpoints: ensuring that the target and originator are both trusted entities. Endpoint authentication is accomplished using X.509 certificates or pre-shared keys.

Message integrity and authentication: ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS message authentication code (HMAC).

Message encryption: optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS handshake.

The following example illustrates how the secure EtherNet/IP transport would mitigate a security threat.

Consider a simple end-user application that consists of an EtherNet/IP-connected programmable controller (PLC) and several EtherNet/IP-connected I/O devices. At initial configuration time, the user configures the PLC and each I/O module with a pre-shared key (PSK) and disables the non-secure EtherNet/IP TCP and UDP ports. Subsequent EtherNet/IP communications take place over TLS and DTLS, and require that each endpoint possess the PSK that has been configured.

Assume further that an employee has unknowingly downloaded malware that sends programming commands to the PLC's IP address via EtherNet/IP. If the malware attempts to connect to the PLC without using TLS, the PLC will not accept the connection. If the malware attempts to connect via TLS,

Attr ID	Need in Implem	Access Rule	NV	Name	Data Type	Description of Attribute
1	Optional	Get		AtReference	BOOL	0 = Drive hasn't reached SpeedRef 1 = Drive has reached SpeedRef
2	Required	Get		SpeedActual	INT	Actual speed
3	Required	Set		SpeedRef	INT	Commanded reference speed

Table 3 Example Instance Attributes

SOURCE: ODVA

Name	Data Type	Description of Parameter
Engineer access	ENUM	Access rights to Engineer
Operator access	ENUM	Access rights to Operator
Auditor access	ENUM	Access rights to Auditor
Viewer access	ENUM	Access rights to Viewer
Anonymous access	ENUM	Access rights to Anonymous

Table 4 Apply_Permission_Information parameters.

but doesn't know the PSK, the TLS connection will not be established. In either case, the malicious programming commands will not be sent to the PLC.

Recognizing that every CIP device does not need to provide the same level of support for all defined security features, CIP Security defines the notion of a Security Profile. A Security Profile is a set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability. At present, three profiles are defined for EtherNet/IP devices, and two potential future profiles are identified for CIP-level security capability.

Authentication vs. Authorization

Access control is a security term that is used to reference a set of policies for restricting access, in broader terms this can be access to tools, functionality, or physical location. Though, in this paper, access control relates to restricting access to information, such as data and the software used to manipulate the data.

Software is used to access and grant authorization to users and devices that need to access the digital information. Authentication and authorization are integral components of digital information access control. Although the two terms might sound similar, they are distinct security concepts in the world of identity and access control management.

Authentication is the security practice to confirm that the user is who they claim to be. Authentication is the first step in security on logging in and gaining access to digital information. The process of authenticating a user could be accomplished by different means such as passwords, authentication apps, or biometrics. Any of these mechanisms could be used to prove that that the user is who they claim to be, thereby authenticating the user.

Once authenticated, a user can see the information that they are authorized to see and access information that they are authorized to access. Authorization in system security is the process of giving the user permission to access a specific resource or function. This could be granting access to folders on a server or starting certain applications.

Authorization strategies

After a user has been authenticated the user authorization can be determined in different ways, often referred to as authorization strategies. Over time many different authorization strategies have been developed for different purposes and use cases. Some common authorization strategies are Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Graph-Based Access Control (GBAC), and Discretionary Access Control (DAC). Within this paper the two most prominent ones, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) will be discussed and further one of them will be used as an example of how to realize a CIP Authorization Profile.

Access	Value
No access	0
Read access	1
Write access	2

Table 5 Access rights.

Role-Based Access Control (RBAC)

RBAC treats authorization based on permissions associated with roles and not directly with the user. Users are assigned to roles bases on the permissions they are supposed to have. Often times a user will have multiple roles. A role can be seen as a collection of permissions. The "Principle of Least Privilege" states that a user should be assigned the role of least access necessary for the job to be done.

This is an important principle when implementing RBAC or any other access control mechanism.

As an example, an "administrator" for a plant would have permissions to reflect this role. In this administrator role the user would be able to change any or most of the configuration, update firmware and read any data, simply put the administrator role would almost have no restrictions. On the other hand, a user possessing the "view" role would be limited to just view data.

The advantage of using RBAC is that managing authorization privileges becomes easier because system managers can deal with users and permissions in bulk instead of having to deal with them one by one.

The existing CIP Security User Authentication Profile provides for user authentication and assigning roles to specific users. The specification includes a minimum list of roles which all compliant products must support, with the option to add additional roles as needed for a user. This profile allows for user decision in terms of what users/devices to assign to a given role, as well as what authentication mechanism to use to authenticate the users/devices. However, the profile does not define an interoperable way to assign what a given role can do within a device; that is the role of the CIP Authorization Profile to be defined in the future (and the

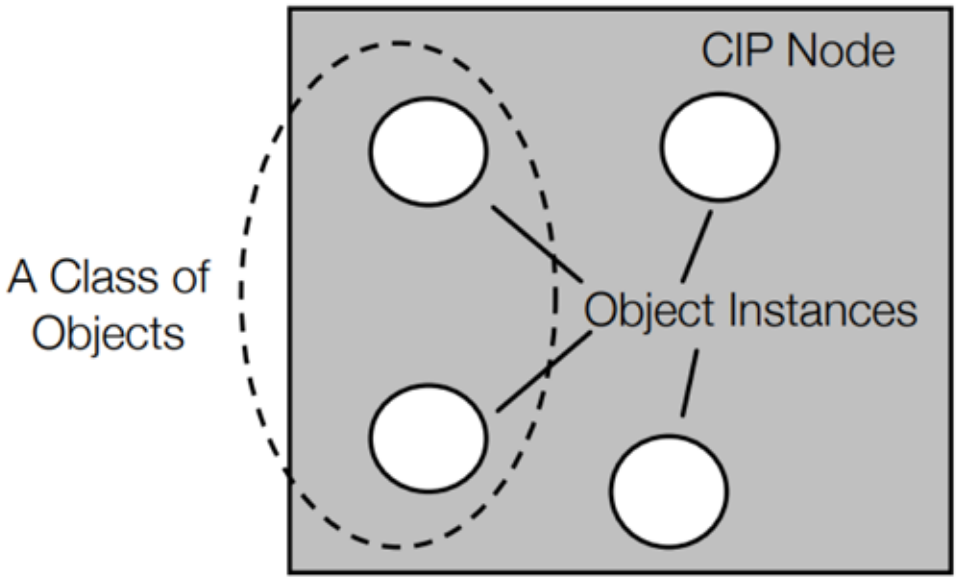


Figure 2 CIP Classes and Instances.

subject of this article's investigation).

Attribute-Based Access Control (ABAC)

ABAC provides access based on who the user is rather than what they do, for example in what organization they work and how they were hired. These attributes allow for easier control structures since permissions can be based on the user's department, location and so on. Utilizing attributes from a user, information that already exist in the HR system, permits for a rich and flexible control structure.

Using the example above from RBAC, if a user is promoted from working on the floor to become a control engineer then the person would automatically gain administrator rights when HR updates the attributes in their system.

Requirements for the CIP Authorization Profile

A few high-level requirements are defined for the CIP Authorization Profile:

CIP Endpoints must be policy enforcement points: The authorization policy will be enforced within CIP endpoints therefore the mechanism for communicating that policy must be well-suited to an embedded device. In other words, the technology cannot be prohibitively difficult to implement in an embedded device or rely on technologies rarely present within an embedded device.

Reuse existing technologies if possible: CIP Security always maintains a preference for using existing security technologies rather than inventing new ones. This is not always possible due to the unique needs of industrial protocols, but if an existing technology can be used then it should be leveraged for this profile. Note that a highly ubiquitous authorization policy technology doesn't exist within the IT world.

Support both RBAC and ABAC: Some users will prefer the simplicity of RBAC for their system, whereas others will require the flexibility of ABAC. The Authorization Profile should support both of these, although it is possible that some of the more complex features might be optional.

Provide options for both simple access policy and advanced access policy: Similar to the RBAC and ABAC requirement the access policy should support simple declarative statements such as "resource x can only be accessed by an administrator" as well as more complex logical statements such as "resource x can be accessed by [administrators OR [engineers AND time of day == 8:00 – 15:00]]. Again, more complex logical statements may be optional.

Integrate with IT systems: As much as possible the technology chosen should be integrated into existing IT systems. This is related to the idea of re-using existing technology if possible.

Existing authorization systems

There are many existing authorization schemes that allow a user to configure how authorization will be done in a system. However, it is worth noting that although some of these schemes have gained traction in particular industries or applications, none is deployed ubiquitously like TLS is for communication security.

That is, although the CIP Authorization Profile could use one or more of these authorization technologies, there is no single technology that stands out as a clear market leader. The following section provides a list of options as well as a brief discussion of the technology. Note that this list is not at all exhaustive, many options are not discussed here. This list is meant to be illustrative of some of the more popular options available.

OPA (Open Policy Agent) and Rego

OPA is a policy engine that allows a user to define an access policy via Rego, the open language for defining access policy. OPA and Rego have proven successful in cloud-based software environments and with various compute functions "as a service" (referred to as XaaS) gaining traction it has grown in popularity and usage. Rego supports a wide variety of access control policies and is not limited to simple RBAC, although RBAC could certainly be supported. Rego uses expressions written against input to determine access criteria. It provides a lot of flexibility and power for writing complex expressions, although given this it may be overly-complex for the needs of a CIP device.

Although these two pieces are meant to work together, Rego could be used by itself in CIP endpoints or could be used with OPA running within a CIP endpoint. OPA would likely be an optional component as CIP conformance test would not be mandating a given implementation of Access Control, although OPA might be useful for highly resourced environments. Given that OPA usually runs in enterprise/cloud environments, it may not be suitable for the many embedded devices which implement CIP and EtherNet/IP. Despite this, Rego may still provide a useful technology for configuring access policy within a CIP device.

XACML (eXtensible Access Control Markup Language)

XACML is an XML based language for describing access policy. XACLM has been in use for more than 20 years and as such has a lot of runtime and support within commercial and open source libraries.

XACML defines Rules as part of Policies and Policies as part of PolicySets. XACML was mainly designed with ABAC in mind, although can certainly also be used with RBAC. Rules contain conditions that are evaluated for a given access request, the result of the evaluation determines whether or not the access is permitted. Like OPA and Rego, XACML was not designed primarily for embedded systems, although it is likely a bit better structure for this use than Rego and OPA.

General Data Modeling Language

It is also possible to make use of a general data modeling/data encoding language to define a custom access policy format. For example, YANG (Yet Another Next Generation) could be used to define an access policy language. Encoding could be done in JSON or XML, or even a new format. This would of course require a significant design effort to define rules and structure of the access policy.

However, it would allow for something far more custom and better suited to CIP devices, although at the expense of extra effort both in terms of design and implementation within a device. However, this is an option that should be seriously considered.

Mapping to CIP

Every CIP node is modeled as a collection of objects. An object provides an abstract representation of a particular component within a product. Anything not described in object form is not visible through CIP. CIP objects are structured into classes, instances and attributes.

A class is a set of objects that all represent the same kind of system component. An object instance is the actual representation of a particular object within a class. Each instance of a class has the same attributes, but also has its own particular set of attribute values. As Figure 2 illustrates, multiple object instances within a particular class can reside within a CIP node.

The CIP family of protocols contains a large collection of commonly defined objects. Objects defined in the CIP Networks Library or may be Vendor specific and only used by one vendor. The objects group attributes, generally the data being represented.

In order to access the data and perform other actions with the data or behavior provided by the object, CIP Services are invoked. These CIP services are common in nature, meaning they may be used in all CIP Networks and they are useful for a variety of objects. Furthermore, there are object-specific service codes that may have a different meaning for the same code, depending on the class of object. Finally, defining vendor-specific services according to the requirements of the product developer is possible.

As a part of the CIP Security User Authentication Profile the idea of a RBAC scheme with six well-defined roles has been introduced. Volume 8 states that this scheme is defined as the minimum set of functionality to allow for interoperability between Originators and Targets. Furthermore, Volume 8 discusses the fact that there is no standardized way to make granular changes to access control policy stating that this is a future concept of the CIP Security specification. The six roles that have been defined are:

- Administrator
- Engineer
- Operator
- Auditor
- Viewer
- Anonymous

Each role has a general baseline description related to access policy. Some guidance is provided on what access levels each role enables, although specific access control policy is up to the product's vendor. As an example, Volume 8 states the following regarding the Administrator and Operator roles.

The Administrator role allows for any and all access to the product. That is, once an administrator has been properly authenticated, this role may access any protected resources on a Target. Specifically, the Administrator role is the only role that can configure User Authentication once the Target has been provisioned for User Authentication. Note that although the Administrator should have access to any resources, this does not prevent a product from limiting access due to overriding conditions such as functional safety. For example, a device can prevent changes that could put the device into an unsafe state.

The Operator role is meant to work with runtime access to equipment. An Operator role should be able to perform troubleshooting, set and interact with I/O, monitor operations, and perform limited configuration that might be necessary for device replacement. Therefore, the operator should be permitted to create or reconfigure I/O connections, although would not be permitted to perform significant configuration, such as downloading a program to a PLC or changing the screens available in an HMI.

It's suggested in Volume 8 that it is not feasible to enumerate what CIP objects, attributes, and services each role may access, although in cases where prescriptive guidance is warranted it is explicitly provided within the CIP Networks Library of Specifications. In this paper the concept of a flexible way to provide fine-grained access control to attributes (data) and permissions (services) is introduced. Two mechanisms for this are discussed, which may be implemented independently or combined for a joint mechanism for managing access control. The first of these is a CIP service-based mechanism, and the second is a document-based mechanism.

CIP Service-Based Access Policy Management

For the purpose of introducing the fine-grained access through CIP Services, a fictitious CIP object with just three instance attributes is used. The object's instance attributes are laid out as in Table 3, using the same notation as in the CIP Networks Library.

As already mentioned above and in Volume 8 it wouldn't be feasible to enumerate what CIP objects, attributes, and services each role may access, at least not in one new CIP object used for authorization management. The reason for this is that a CIP device contains multiple CIP objects and each CIP object can have many attributes. For some devices this can sum up to several hundred or even thousands of attributes. Having this in one singe authorization management object would likely end up being cumbersome and unmanageable.

An alternative way to look at this would be to allow each attribute to also carry permission information. This permission information would be additional information that would go together with the attribute data within the module. The permissions would carry the roles that would be allowed to get or set the attribute.

In order to interface with and manage permissions the already established notion of services would be used. In this case two new general services would be defined named, View_Permission_Information and Apply_Permission_Information. The former would be used to get the current permission information and the latter to apply new permission information. Both services would use a list of service parameters, View_Permission_Information would return the list of parameters and Apply_Permission_Information would receive the list of parameters. Table 4 shows the list of parameters.

Basically, this is just a list of roles and what access rights should be applied. Note that Administrator has been omitted since this role should have full access to all data in a CIP device, and it helps avoid potential risk of locking out the Administrator thus bricking the CIP device.

The ENUM data type would carry values indicating what kind of access that the specific role should have. I.e. no access at all, read the attribute, or read and write to the attribute as shown in Table 5.

Summing this up using the example from Table 3 the attribute table with the permission information added would look something like Table 6. Here the instance has been configured to prevent anonymous users to have no access to any attribute. The viewer can only access the SpeedActual attribute and only read it. The operator and auditor can read all three attributes, but not modify SpeedRef which is the only settable attribute. The engineer has read access to all attributes and access to modify the SpeedRef attribute.

With the potential number of attributes in a complex CIP device the database of permission information would be huge. One important thing to consider is that it needs to be reasonably easy to get an overview of all permission settings so an audit can be made making sure that the CIP device has been configured with the correct authorization settings.

One way to solve this would be to provide an easy to use interface to gather all permission information from a CIP Device. There are several ways this could be done. Either to have a service that provides all permission information from the whole CIP device, this likely would return a large response that in the end would be a bit unmanageable. An

Attr ID	Need in Imp	Access Rule	NV	Name	Data Type	Permission information		Description of Attribute
1	Optional	Get		AtReference	BOOL	Engineer access	Read	0 = Drive hasn't reached SpeedRef 1 = Drive has reached SpeedRef
						Operator access	Read	
						Auditor access	Read	
						Viewer access	No	
						Anonymous access	No	
2	Required	Get		SpeedActual	INT	Engineer access	Read	Actual speed
						Operator access	Read	
						Auditor access	Read	
						Viewer access	Read	
						Anonymous access	No	
3	Required	Set		SpeedRef	INT	Engineer access	Write	Commanded reference speed
						Operator access	Read	
						Auditor access	Read	
						Viewer access	No	
						Anonymous access	No	

SOURCE: ODVA

Table 6 Example Instance Attributes with permission information.

alternative way would be a service, View_All_Permission_Information, that returns all permission information for one specific instance.

Document-Based Access Policy Management

Another potential mechanism for managing access policy is to use a more document-based structure. A document that enumerates access policy can be produced in a particular language and encoding, and then distributed to CIP endpoints that will then enforce that access policy. Documents can be signed and even have portions encrypted if necessary, and the signature provides authenticity assurances regardless of the transport mechanism (or in many cases in addition to the transport mechanism).

Depending on the defined language, a document may have the ability to implement complex access policy rules that include logical operations (AND/OR/IF THEN) on various attributes and device states. Although the level of support for more complex policy statements may vary by device this would provide a powerful mechanism for defining highly flexible and customized access policy to protected CIP resources.

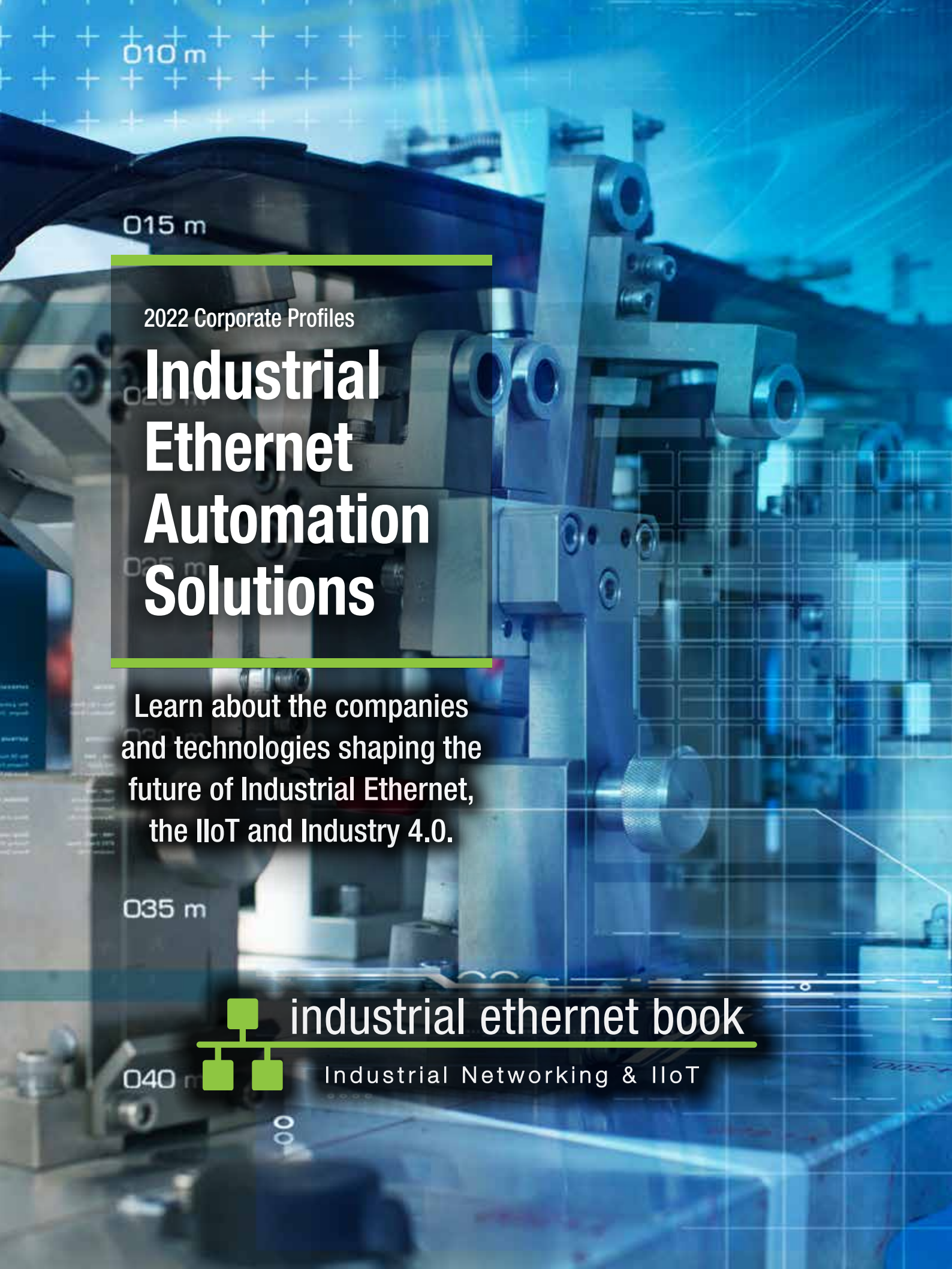
The mechanisms discussed in the "Existing Authorization Systems" section all use a document-based mechanism (Rego, XACML, and a YANG Model-based mechanism). This type of mechanism has the advantage of better integrating with many existing authorization definition technologies. However, downsides to this approach also exist. This approach would require devices to support a technology beyond CIP, which includes parsing of a given language and then translating that into policy enforcement on incoming CIP messages. These technologies may also provide more flexibility than is necessary for the average user of CIP Security, although that could also provide some opportunities for future expansion of the technology.

Conclusion

This article has explored different approaches how authorization models could be applied to CIP Security. None of these are a "one-size-fits-all" solution, rather each offer advantages and disadvantages. These "models" could be implemented with using purpose-built CIP functionality or would require use of other external well-defined standards. As such, it provides guidance on some of the characteristics of each model described.

Joakim Wiberg Head of Technology, ***HMS Networks,*** *David Smith, Cybersecurity Architect,* ***Schneider Electric*** *and Jack Visoky, Principal Engineer and Security Architect,* ***Rockwell Automation.***

Visit Website



2022 Corporate Profiles

Industrial Ethernet Automation Solutions

Learn about the companies and technologies shaping the future of Industrial Ethernet, the IIoT and Industry 4.0.

industrial ethernet book

Industrial Networking & IIoT

Beckhoff Automation: new automation technology

Beckhoff implements open automation systems using proven PC-based control technology. The main areas that the product range covers are industrial PCs, I/O and fieldbus components, drive technology, automation software as well as control cabinet-free automation.

SOURCE: BECKHOFF

PRODUCT RANGES THAT CAN BE USED AS separate components or integrated into a complete and mutually compatible control system are available for all sectors.

Our New Automation Technology stands for universal and industry-independent control and automation solutions that are used worldwide in a large variety of different industries and applications, ranging from CNC-controlled machine tools to intelligent building control.

PC-based control technology

Since Beckhoff's foundation in 1980, the development of innovative products and solutions on the basis of PC-based control technology has been the foundation of the company's continued success. We recognized many standards in automation technology that are taken for granted today at an early stage and successfully introduced to the market as innovations.

Beckhoff's philosophy of PC-based control as well as the invention of the Lightbus system and TwinCAT automation software are milestones in automation technology and have proven themselves as powerful alternatives to traditional control technology.

EtherCAT, the real-time Ethernet solution, provides a powerful and future-oriented technology for a new generation of control concepts.

Worldwide presence on all continents

The corporate headquarters of Beckhoff Automation GmbH & Co. KG in Verl, Germany, is the site of the central departments such as development, production, administration, sales, marketing, support and service. Beckhoff's presence in the international market is guaranteed by its subsidiaries. Beckhoff is represented in more than 75 countries by worldwide cooperation partners.

EtherCAT – the Ethernet Fieldbus

Selecting the communication technology is important: it determines whether the control performance will reach the field and which devices can be used. EtherCAT, the Industrial Ethernet technology invented by Beckhoff, makes machines and systems faster, simpler and more cost-effective. EtherCAT is regarded as the "Ethernet fieldbus" because it combines the advantages of Ethernet with the simplicity of classic fieldbus systems and avoids the complexity of IT technologies. The EtherCAT Technology Group (ETG), founded in 2003, makes it accessible to everyone. With over 6,000 member companies from 67 countries (as of Dec. 2020), the ETG is the world's largest fieldbus user organization.

EtherCAT is an international IEC standard that not only stands for openness, but also for stability: until today, the specifications have never been changed, but only extended compatibly. This means that current devices can be used in existing systems without any problems and without having to consider different versions.

The extensions include Safety over EtherCAT for machine and personnel safety in the same network, and EtherCAT P for communication and supply voltage (2 x 24 V) on the same 4-wire cable. And also EtherCAT G/G10, which introduces higher transfer rates, while the existing EtherCAT equipment variety is integrated via the so called branch concept: even here there is no technology break.

Beckhoff Automation at a glance

- 2021 global sales: €1.182 billion (+28%)
- Headquarters: Verl, Germany
- Managing owner: Hans Beckhoff
- Employees worldwide: 5,000
- Engineers: 1,900
- Subsidiaries/representative offices worldwide: 40
- Sales offices in Germany: 24
- Representatives worldwide: >75

Beckhoff Automation
info@beckhoff.com
Phone: +49 5246 963-0

Visit Website

Analog Devices: Accelerating Your Digital Transformation Journey

Access new insights from the intelligent edge with innovative solutions that solve the toughest industrial automation challenges.

SOURCE: ANALOG DEVICES

ANALOG DEVICES (ADI) IS A GLOBAL LEADER in the design and manufacturing of analog, mixed signal, and DSP integrated circuits. We intelligently bridge the physical and digital worlds with a cutting-edge portfolio of technologies that sense, measure, interpret, connect, power, and secure. ADI is, however, not a typical semiconductor company. It pushes the boundaries of silicon technology, investing heavily in software, systems expertise, and domain knowledge within its key markets such as industrial automation. The combination of this knowledge with that unmatched set of analog-to-digital capabilities enables ADI to approach challenges at the system-level and help its customers get to market faster, create and capture more value, and make sound investments with a roadmap to tomorrow.

Industry-leading, scalable Ethernet – timed to perfection

We turn your vision of connected factories into reality. ADI Chronous™, Analog Devices´ family of compatible and interoperable Industrial Ethernet connectivity products, enables best-in-class industrial automation solutions for the connected factory of tomorrow. From complete Time Sensitive Networking solutions for high-performance motion control in factory automation to innovative 10Base-T1L concepts for robust field instrument connectivity in process control – our market-leading Ethernet portfolio of combined software and hardware solutions are scalable and timed to perfection.

ADI Chronous encompasses a range of advanced Industrial Ethernet technologies from real-time Ethernet switches to physical transceivers and network interface solutions that include protocol stacks. Designed to support scalable and flexible system development, the ADI Chronous portfolio offers multiple port count, low power consumption, and flexible bandwidth. Being multiprotocol, these solutions are compatible with the majority of existing industrial protocols while also providing the ability to future-proof for TSN networks.

ADI Chronous solutions are designed and verified for robust operation in harsh industrial environments and offer effective security at each node point within a system. Our suite of Industrial Ethernet products includes technologies, solutions, software, and security capabilities designed to connect the real world to factory networks and beyond to the cloud.

Why ADI?

Our long and rich industrial expertise and system design knowledge coupled with advanced technologies deliver seamless and secure connectivity across the automation network, turning your vision of the connected factory into reality. ADI ensures your time-critical automation and control data is delivered perfectly on time, every time. Get to market fast by using ADI's complete solutions that provide predictable, trusted results you can depend on every time. For deterministic, verified robust, scalable and flexible solutions that simplify system design and reduce the development burden, look no further than Analog Devices.

Analog Devices
Email: EMEAMarketing@analog.com
Phone: +49 89 769030

Visit Website

Shaping the future of open, autonomous industry

TTTech Industrial develops innovative computing and connectivity solutions that help customers to modernize industrial automation systems and become IoT leaders in their field.

TTTECH INDUSTRIAL WORKS WITH ITS customers to achieve their goals of smarter automation, better data access and more flexible manufacturing with industrial IoT solutions. TTTech Industrial delivers simple and effective ways to bring IoT to industrial systems by providing product platforms that combine traditional automation functionality with secure access to IT services and deterministic connectivity.

© SHUTTERSTOCK/PAND P STUDIO

TTTech Industrial delivers simple and effective ways to bring IoT to industrial systems.

Modular platform to cover a wide range of industrial use cases across industries

Edge computing allows manufacturers to gain in-depth insights into machine performance thanks to real-time data collection and processing. TTTech Industrial's edge computing platform Nerve enables manufacturers to connect and manage their machines worldwide, with use cases ranging from the automotive and process industries to food processing and the energy sector.

Nerve is an open, modular platform solution with a set of base features that provide a secure foundation for managing software and devices. Nerve hosts applications from different vendors, supports virtualization and containerization of applications, and offers an intuitive user interface at the edge or in the cloud.

The Nerve Management System also allows for easy updates and deployment of software to machines installed worldwide. With Nerve, customers can find the best solution for their application, easily scale up or adjust as their requirements change, and only pay for the features they use. A free trial is available to help customers familiarize themselves with Nerve and find out if it is the right solution for them.

Reliable communication solutions for the energy sector

Today's highly efficient and reliable energy networks, wind turbines and energy storage solutions require increased automation capabilities.

TTTech Industrial offers a variety of solutions to support industrial automation in the energy market:

- The Flexibilis product line offers robust and reliable communication for substation automation and energy management.
- Energy storage solutions or wind turbines are often located in remote areas. TTTech Industrial's edge computing platform Nerve can provide easy real-time machine data access, better software management and offline operation capabilities that support connectivity and automation of these applications.
- In the wind energy sector, more than 10,000 Vestas wind turbines with TTTech Industrial's scalable distributed control system (DCS) have been deployed in the field and Vestas continues to integrate the DCS into thousands of wind turbines each year.

© TTTECH INDUSTRIAL, ISTOCK/AYDINMUTLU

Nerve is an open, modular edge computing platform providing connectivity from the shop floor to the cloud.

TTTech Industrial Automation AG

www.tttech-industrial.com

Social Media:
www.linkedin.com/company/tttech-industrial/

Visit Website

HARTING – Innovative connectivity for automation

Equal if big industry connectors or miniaturized I4.0 Ethernet interfaces – HARTING solutions have stood for quality and innovation for over 70 years.

QUICK AND EASY HANDLING, ROBUSTNESS, flexibility in use, a long lifecycle and, ideally, a tool-free assembly - whatever you expect from a connector – Han® won't disappoint you.

Industrial Connectors Han®

The industrial connector Han has set decades ago the standard for all modern industrial connectors. All industrial lifelines combined in one connection changed the world of industrial automation – Han connectors transmit Power, Signal, Data and compressed air to your application. The modular system allows to individualize several housing types with a personal combination of contacts, fitting to your machine.

Ethernet Connectivity

Today ethernet is the dominating protocol in the factory automation. Increasing data rates, real time communication and other challenges of Industry 4.0 needs more powerful and innovative solutions to connect industry sensors and devices with their environment. Besides well-known ethernet interfaces as the RJ45, we offer also new, smaller and more robust solutions like HARTING ix Industrial® and T1 Industrial for Single Pair Ethernet. From IP20 to IP67 we offer a wide range of connectivity solutions. All solutions for powerful data networks from one hand in factory automation and railway market – for seamless ethernet networks from the sensor to the cloud.

SOURCE: HARTING

Pushing Performance

As a slogan, Pushing Performance combines the claim with worldwide product innovations and the highest quality standards to persuade customers in a sustainable way. It is also our aspiration to drive the potential of our customers through the portfolio we offer them. The goal of HARTING is to provide consistently good services and to promote these through innovation, internationalisation and future-oriented thinking. The basis is a steady improvement of our products and solutions.

About HARTING

The HARTING Technology Group is one of the world's leading providers of industrial connection technology for the three lifelines of Data, Signal and Power and has 14 production plants and 44 sales companies. Moreover, the company also produces retail checkout systems, electromagnetic actuators for automotive and industrial series use, charging equipment for electric vehicles, as well as hardware and software for customers and applications in automation technology, mechanical and plant engineering, robotics and transportation engineering. In the 2020/21 business year, some 6,000 employees generated sales of EUR 869 million. Founded on September 1, 1945 in a small 100 m² hall, HARTING has stood for quality and innovation for over 70 years.

HARTING Technology Group

www.HARTING.com

info@HARTING.com

Visit Website

Opto 22: Your Edge in Automation

Let the engineers at Opto 22 help you build your connected automation system.

Opto 22's *groov*® family of industrial edge controllers and I/O is designed from the ground up with integrated control, connectivity, and security tools to help you connect automation, enterprise, and cloud data.

With *groov* EPIC and RIO, you can bring your brownfield systems into the next generation of industrial automation. Unify multi-vendor automation networks into cohesive OT data systems with embedded protocol conversion and OPC UA connectivity. Then secure PLC, I/O, and equipment data with mandatory user authentication, configurable device firewalls, and SSL/TLS encryption.

Whether from new systems or legacy devices, you can publish data directly into on-premise and cloud-based applications like databases, CMMS, and ERP. The included Node-RED IoT programming environment, REST APIs, and MQTT publish-subscribe communication options allow you to collect, process, transform, and transmit operational data efficiently. Store-and-forward capability and fault-tolerant file systems support highly scalable infrastructure for IIoT.

groov devices also reinvigorate traditional industrial control applications with innovative tools that reduce complexity. Develop real-time control programs in a language you know: ladder logic, function block diagram, flowcharts, Python, C/C++, and more. Build dynamic operator HMI screens directly from your controller and publish to embedded or external touchscreens, mobile devices, and browsers.

SOURCE: OPTO 22

An edge programmable industrial controller, groov EPIC® is much more than a PLC or a PAC. It can simplify and secure automation and IIoT projects, while reducing cost and complexity.

Replace costly, high-maintenance Windows PCs for HMI, OPC, and data processing with these Linux-based edge devices. The suite of free, web-based tools and software-configurable intelligent I/O allow you to rapidly prototype innovative designs for secure, connected systems and go straight into production with the click of a button.

Built on decades of field-proven experience, *groov* products are backed by lifetime guarantees on solid-state I/O, UL Hazardous Locations approval, ATEX compliance, and a wide -20 to 70 °C operating temperature range.

Count on free pre-sales engineering help and product support as well. All Opto 22 products are developed, manufactured, and supported in the U.S.A.

With 45+ years as a trusted automation manufacturer, we understand your projects and speak your protocols. Contact our engineers today. Let's talk about what you want to do.

SOURCE: OPTO 22

groov RIO® revolutionizes remote I/O by offering over 200,000 unique software-configurable I/O combinations in a single, compact, PoE-powered industrial package.

Opto 22
www.opto22.com

Visit Website

Contemporary Controls: Your Trusted Partner

Providing innovative and reliable solutions to the industrial automation industry for more than 47 years, Contemporary Controls has been a leader in innovative solutions for industrial automation.

WITH MORE THAN 47 YEARS OF EXPERIENCE, Contemporary Controls has been a leader in innovative solutions for industrial automation. Contemporary Controls' CTRLink products are designed for unattended operation in environments not conducive to office-grade equipment.

The products provide convenient DIN-rail mounting in control panels, 24VAC/DC power, UL 508, improved EMC compliance and reliability. Contemporary Controls' repeating hub, switches, media converters and IP routers adhere to IEEE 802.3 standards and more. Specialty regulatory needs are addressed in selected models.

SOURCE: CONTEMPORARY CONTROLS

CTRLink – Networking for Automation. Ethernet Switches and IP Routers.

Rugged Ethernet Switches

Whatever the Ethernet infrastructure need, a solution is available from CTRLink products. For simple systems, plug-and-play unmanaged switches provide a cost-effective method for expanding Ethernet networks. Most models include features such as auto-MDIX and auto-negotiation. For demanding applications, managed switches provide features such as VLANs, SNMP, Quality of Service, port security, port mirroring, alarming and cable redundancy.

Innovative Diagnostic Switches

For troubleshooting, diagnostic switches allows a network sniffer to attach to an unused port on a switch and observe all traffic on the network.

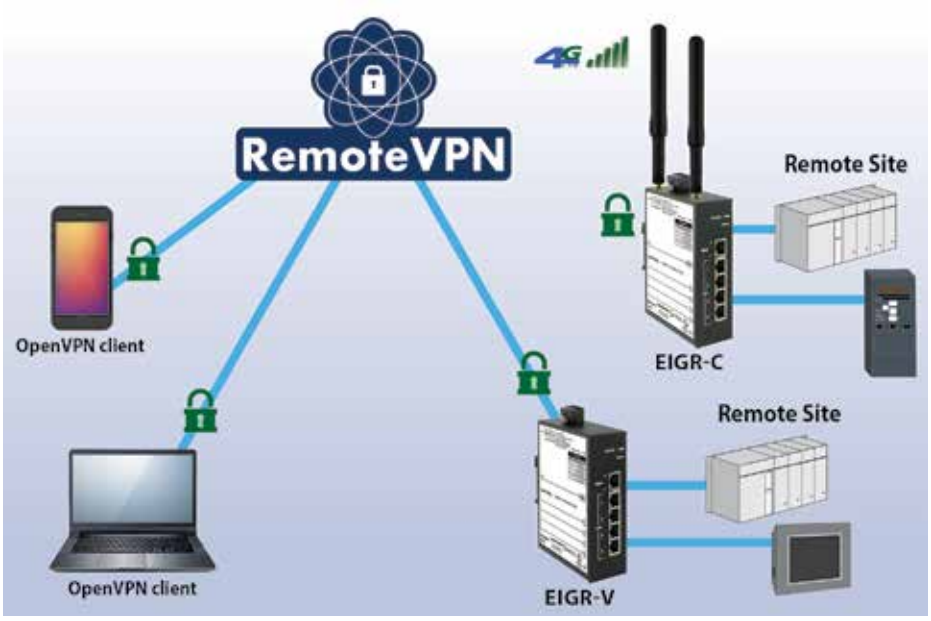
Cost-Effective, Trusted IP Routers

Contemporary Controls' Skorpion series of IP routers ease the integration of new machines into the existing network. Each machine consisting of multiple IP devices connects to the LAN side while keeping the same IP settings for the devices and the application, lowering installation cost and eliminating trouble shooting. The IP address for the WAN port on the IP router is the only setting that requires modification allowing multiple machines to reuse the same configuration on the LAN side. Skorpion routers have been successfully used in Robotics, Automated Guided Vehicles (AGVs), Packaging and Scientific Equipment.

Simplified, Secure Remote Communication

RemoteVPN is a service offered by Contemporary Controls that allows systems integrators remote access to systems from the convenience of the systems integrator's home or office.

A cloud-based VPN server hosted by Contemporary Controls provides the critical connection between two VPN clients—one installed on the systems integrator's PC and the other permanently installed on Contemporary Controls' EIPR/EIGR VPN router located at the remote location. Using this approach, two secure VPN tunnels are created with no concern for intervening firewalls.



SOURCE: CONTEMPORARY CONTROLS

The RemoteVPN service provides secure remote access.

Solutions You Can Depend On

With automation systems, applications vary and can require a special product or need. Contemporary Controls has worked with OEMs in obtaining UL 864 compliance with some CTRLink switches, and can help in other areas such as private-labeling, unique packaging or extreme environmental design.

Contemporary Controls' customers are systems integrators, contractors and OEMs seeking simple, reliable networking and control products from a dependable source. With headquarters based in the US, Contemporary Controls also has operations in the UK, Germany and China and is well suited to fulfil your application needs.

Contemporary Controls

www.ccontrols.com

Visit Website

EtherWAN: When Connectivity is Crucial

EtherWAN is a leader in the manufacture of Layer 2/Lite Layer 3 DIN-rail & rackmount industrial Ethernet switches, media converters, Ethernet extenders, PoE (Power over Ethernet) products, and wireless communications equipment.

SOURCE: ETHERWAN

ETHERWAN PRODUCTS HAVE BEEN WIDELY used in intelligent transportation systems, security surveillance, energy & utility, critical infrastructure, and factory automation.

Advancing for 20 years

Established in 1996, EtherWAN became a subsidiary of the German Phoenix Contact Group in 2017. With more than two decades of accrued expertise in hardened products, EtherWAN has developed the tools and policies needed to ensure quality.

Industrial grade wired and wireless network solutions

Our products are designed in compliance with or certified by industry standards.

- NEMA TS2 for ITS and Transportation
- IEC 61850/IEEE 1613 for Utility Substations
- IEC 61000 for Industrial Automation Applications
- UL C1D2 certified for Explosive and Hazardous environment
- IEEE 802.3at and 802.3bt for PoE needs
- IEC 62443 for Cybersecurity

Our wireless products are designed in compliance with the following specifications.

- MQTT for Cloud Connectivity
- Ready to Cloud for AWS and Azure
- Microsoft Azure Sphere Security solution (AiR GUARD)

Quality down to the smallest detail

EtherWAN has been consistently dedicated to the innovation of industrial-grade Ethernet communication equipment. With experienced software and hardware teams, solid integration verification capability, and high-quality technical consulting, the company has obtained many patents worldwide. Designs produced in-house, and manufacturing based in Taiwan, are guaranteed to maximize quality and service.

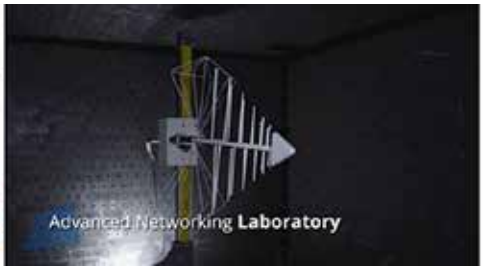
- Conduction: Stricter than industrial standards by 3db.
- Radiation: Stricter than industrial standards by 3db.
- ESD Contact: 2KV Stricter than IEC61000-6-2 standard
- EFT (Electrical Fast Transient): 10% higher than industrial standard
- Surge: Full range voltage with standard high criterion
- HALT (Highly accelerated life test): Improves overall robustness of product

Beyond expectations, EtherWAN can help.

Creating reliable, secure, and durable network solutions requires more than just manufacturing know-how and quality assurance. It requires an in-depth understanding of the requirements and constraints of specific applications. These requirements include not just data transfer speed, but support for redundancy protocols, multi-level security, and the ability to seamlessly mesh with existing systems and future expansions. Going beyond expectations, EtherWAN can help.

EtherWAN Systems, Inc.
Email to: info@etherwan.com.tw

Visit Website



Redefining Futureproof Industrial Networks

Evolved Networking Solutions That Strengthen Operational Resilience.

MOXA IS A LEADING PROVIDER OF EDGE connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things.

With over 30 years of expertise in providing industrial networking solutions that enable communication and collaboration among systems, processes, and people. Moxa knows what it takes to build seamlessly converged OT/IT connectivity for your industrial digital transformation and provide enhanced network security, scalable performance, solid reliability, and simplified management to increase your operational resilience and efficiency.

SOURCE: MOXA

World's first IEC 62443-4-2 compliant Ethernet switches certified by IECEE.

Defense-in-depth Network Security

Cyberthreats are escalating at a time when industries and companies must shift to remote and distributed operations. With a low tolerance for downtime, industrial control system networks are frequently subjected to cyberattacks. It is critical for every industry to strengthen their security infrastructure and cyber-defense against cyberattacks to ensure maximum operational uptime and safety. Following the guidelines defined by the IEC 62443 standards, Moxa combines OT-centric firewall capabilities with MXsecurity management to help you detect cyberthreats and prevent them, ensuring secure and continuous operations.

Built-in Scalability to Strengthen Your Network Resilience

Industrial networks need to evolve to support resilient operations. When integrating new network components, even small changes can face unexpected challenges, such as limited installation space.

The EDS-4000/G4000 Series industrial managed Ethernet switches consist of 68 models that feature scalable functionality compressed into one unified form factor, allowing you to effortlessly expand your network to meet changing requirements. Adding more bandwidth or more PoE power is now easier than ever. More importantly, EDS-4000/G4000 switches are certified for the latest security and industry standards to ensure robust network resilience.

SOURCE: MOXA

Real-time visibility and security management for threat protection.

Simplified OT Network Management

Leverage our new scalable industrial network management platform to extend in-depth visibility to network security and specific operations for improved uptime. MXview One helps OT engineers simplify management of converged IT/OT networks. With comprehensive, real-time visibility of wired, wireless, and IEC 61850 substation networks, MXview One optimizes operations and availability throughout all stages of network deployment, management, and maintenance.

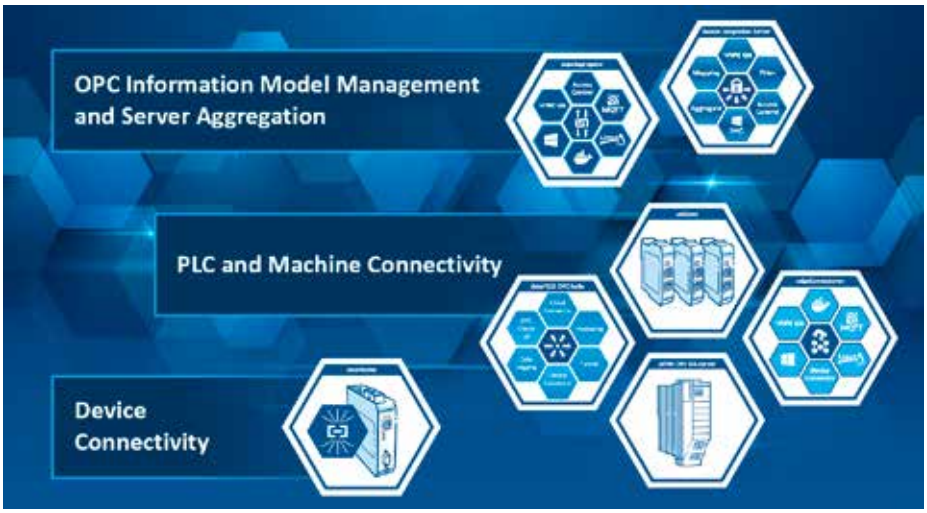
Moxa Europe GmbH
www.moxa-europe.com
europe@moxa.com

Visit Website

Softing Industrial: Data Integration for IIoT

Take advantage of the benefits offered by seamless networking of IT and OT.

DIGITALIZING AND NETWORKING YOUR enterprise data is the crucial step in getting a clear picture of your production processes. Using the collected and processed data, you can make informed decisions to optimize your production. As a recognized expert in digital data exchange in industrial applications, we support you in bridging technological gaps and in designing smooth data exchange between machines and plants, OT/IT integration, and cloud connectivity flexibly and securely.



SOURCE: SOFTING

Softing products ensure seamless data exchange between machines and plants, OT/IT integration, and cloud connectivity.

Centralized and Secure OPC UA-based Data Integration

With the products of our dataFEED family, we ensure the seamless flow of information between devices and software applications and the secure transfer of data to IoT and cloud platforms.

Our **dataFEED OPC Suite** is an integrated software solution for OPC UA and OPC Classic communication and IoT connectivity. Via the integrated OPC UA server with store-and-forward, it enables secure and reliable access to controllers from Siemens SIMATIC S7, Rockwell ControlLogix, B&R, Mitsubishi, and Modbus controllers, among others.

Our **Secure Integration Server (SIS)** acts as an aggregator, providing the required address space filtering, access control, and semantic extraction functions via OPC UA, and serves as a central OPC UA server. SIS combines all mechanisms for the management, regulation, and monitoring of data access in one central location. This allows you to control the interface between OT and IT at a single point and manage it easily and securely.

Connectivity for "Industrial Edge"

Industrial applications are increasingly taking advantage of edge computing, i.e. centralized management of decentralized data processing. Integrating connectivity and edge computing in an "industrial edge" also makes data integration centrally manageable and allows for more efficient operation of the IoT solution. Our connectivity products for the industrial edge run as Docker containers and can be deployed using Amazon AWS, Microsoft Azure, or Kubernetes.

The **edgeConnector product family** provides access to process and machine data in controllers for OEE, predictive maintenance, or machine learning. Our **smartLink product family** allows access to device data (sensors, actuators) for asset management and asset monitoring applications. Finally, the **edgeAggregator product family** provides OPC UA server aggregation capabilities as well as additional security for OPC UA-based data integration. You don't need specialized hardware and use open standards like OPC UA, MQTT, and httpREST. This way you can design your IoT solution in a simple, flexible, and scalable way.

SOURCE: SOFTING

IT/OT integration up to edge and cloud applications leads to optimized processes.

Stable Communication Networks

Robust digital communication is fundamental for the reliable provision of data which is needed to increase flexibility and efficiency in Industry 4.0 applications. Our mobile plug & play solutions provide access to a variety of protocols and physical layers for setting parameters, commissioning, and maintenance of field devices. Our network diagnostics solutions allow easy commissioning, acceptance testing, and troubleshooting, which guarantees a high-performance network.

Softing Industrial Automation GmbH
info.automation@softing.com

Visit Website

Phoenix Contact: Automation for the future

Phoenix Contact is the worldwide market leader of components, systems and solutions in the area of electrical engineering, electronics and automation. The product range comprises components and system solutions for energy supply including wind and solar, device and machine engineering as well as control cabinet engineering.

SOURCE: PHOENIX CONTACT

Image source: Robert Kneschke@shutterstock.com and Valery Brozhinsky@shutterstock.com

Today, the family-owned company employs 20,300 people worldwide and had a turnover of 2.97 billion Euros in 2021. The corporate headquarters is located in Blomberg in North Rhine-Westphalia. The Phoenix Contact Group has eighteen companies in Germany, as well as more than 55 sales subsidiaries. Internationally Phoenix Contact is on site in more than 100 countries.

Phoenix Contact produces with a high vertical range of manufacture all over the world. Besides screws, plastic and metal parts, highly automated assembly machines are also built in-house.

Wide product range

A diverse product range of modular terminal blocks and special-purpose terminals, printed circuit terminal blocks and plug connectors, cable connection technology and installation accessory offers innovative components.

Electronic interfaces and power supplies, automation systems on the basis of Ethernet and Wireless, safety solutions for man, machine and data, surge protection systems as well as software programs and tools provide installers and operators of systems as well as device manufacturers with comprehensive systems.

The automotive, renewable energy and infrastructure markets are supported with holistic solution concepts including engineering and training services and further service features according to their specific demands.

Product innovations and specific solutions for individual customer requests are developed at the locations in Germany, China and the United States. Numerous patents underline the fact that many developments from Phoenix Contact are unique in their own.

In close cooperation with universities and science, future technologies like e-mobility and environmental technologies are explored and integrated into products, systems and solutions for the market. Phoenix Contact supports the digital transformation with products, systems and solutions. Based on the experience in the in-house machine building, the company knows the requirements of the digitalization and integrated data flow from the engineering through the production and furthermore along the whole product life cycle.

360° Security

Phoenix Contact supports its customers throughout the entire process chain with standardized security. For risk assessment and threat analysis of existing or planned systems, individual service offers form the basis for implementing security concepts.

In addition, secure automation solutions are provided for various industries. Last but not least, the corresponding security components such as firewalls and secure controls of the company, which work in combination with the security functions of other components, contribute to the creation of secure networks. From the secure development process to the continuous vulnerability management of Phoenix Contact PSIRT (Product Security Incident Response Team), security is anchored in the complete life cycle of the products and solutions.

This wide-ranging competence of Phoenix Contact is also reflected in certifications: Phoenix Contact was one of the first companies in Germany to be certified by TÜV Süd according to the series of standards for IT security IEC 62443-4-1, -2-4 and -3-3.

These certifications underline Phoenix Contact's strategy of offering standardized security in products, industrial solutions and consulting services to enable future-proof operation of machines, systems and infrastructures.

Phoenix Contact GmbH & Co. KG
Email: info@phoenixcontact.com
Phone: +49 52 35 300
www.phoenixcontact.com

Visit Website

Rugged instrumentation for reliable measurement and control

Moore Industries is a world leader in the design and manufacture of exceptionally rugged, reliable and high quality field and DIN rail mounted instrumentation for the process monitoring and control industries.

MOORE INDUSTRIES WORLDWIDE SALES AND support offices provide first rate customer service and solutions for the chemical, petrochemical, utilities, petroleum extraction, refining, pulp and paper, food and beverage, mining and metal refining, pharmaceuticals, and biotechnology industries.

SOURCE: MOORE INDUSTRIES

IIoT Solutions built to Deliver Field Data to your Host Systems

HART and MODBUS industrial communication protocols have dramatically increased access to device and process information that allows you to make more effective operational process decisions. Our Remote I/O systems including the NCS Net concentrator System® and HART gateways and converters such as the HES HART to Ethernet Gateway System and HCS HART to MODBUS Converter help integrate valuable data into your monitoring and control system strategy.

Instrument Panels and Systems Engineering

Moore Industries can specify, procure, and assemble your multi-vendor electronic and pneumatic instrumentation/hardware into custom-built instrument panels, systems and enclosures. We will provide complete documentation, expert technical assistance, and the assurance that complete and thorough testing has been performed.

Complete Temperature Solutions

Moore Industries Universal PC-Programmable, Smart HART® Temperature Transmitters convert and send RTD or thermocouple signals ready for direct interface with an indicator, recorder, PLC, DCS, or SCADA system. Temperature assemblies and measurement components include The WORM® flexible RTD and thermocouple sensors, connection heads and enclosures, thermowells and fittings. Our TCS Temperature Concentrator System provides precision measurements via HART or MODBUS RTU while significantly reducing hardware, wiring, and installation costs.

Programmable Alarm Trips

Provide on/off control, warn of trouble, or provide emergency shutdown with one or more programmable alarm (relay) outputs when a monitored process signal falls outside of a selected high and/or low limit. Our SPA2 Programmable Limit Alarm Trip accepts inputs from over thirty RTD and Thermocouple sensor types, provides two or four independent and individually-configurable alarm relay outputs, and offers an analog output (-AO) option for transmitter functionality to reduce installation costs/time.

SOURCE: MOORE INDUSTRIES

Functional Safety Solutions

Our spectrum of SIL 2 and SIL 3 capable FS Functional Safety Series instruments include signal isolators and splitters, alarm trip logic solvers, temperature transmitters and more. Every instrument is built and approved for use in Safety Instrument Systems and are third-party certified by exida to IEC 61508 standards.

More Than 50 Years Designing and Manufacturing Rugged and Reliable Instruments

Moore Industries has been proudly serving the process instrumentation needs of global manufacturers and automation companies since 1968. Designing, building and supporting more than 170 products across 14 product lines with unmatched systems support and services expertise. Watch the video to learn more.

Moore Industries Worldwide

www.miinet.com

Visit Website

Leading the way in Time-Sensitive Networking

The CC-Link Partner Association was the first to introduce an open industrial Ethernet technology combining gigabit bandwidth with Time-Sensitive Networking.

SOURCE: CLPA

THE CC-LINK PARTNER ASSOCIATION (CLPA) IS an international organization dedicated to the technical development and promotion of the CC-Link family of open automation networks. The CLPA was founded over 20 years ago in November 2000, when it introduced CC-Link, its highly respected industrial fieldbus technology. This was followed in 2007 with the widely adopted CC-Link IE, the first open industrial Ethernet to offer gigabit bandwidth. CLPA has since grown to be an acknowledged industrial automation network technology leader globally.

Today, CLPA's key technology is CC-Link IE TSN, the world's first open industrial Ethernet that combines gigabit bandwidth with Time-Sensitive Networking (TSN), making it the leading solution for Industry 4.0 applications and providing the foundation of the converged network architecture necessary to address the ever-changing challenges of 21st century manufacturing.

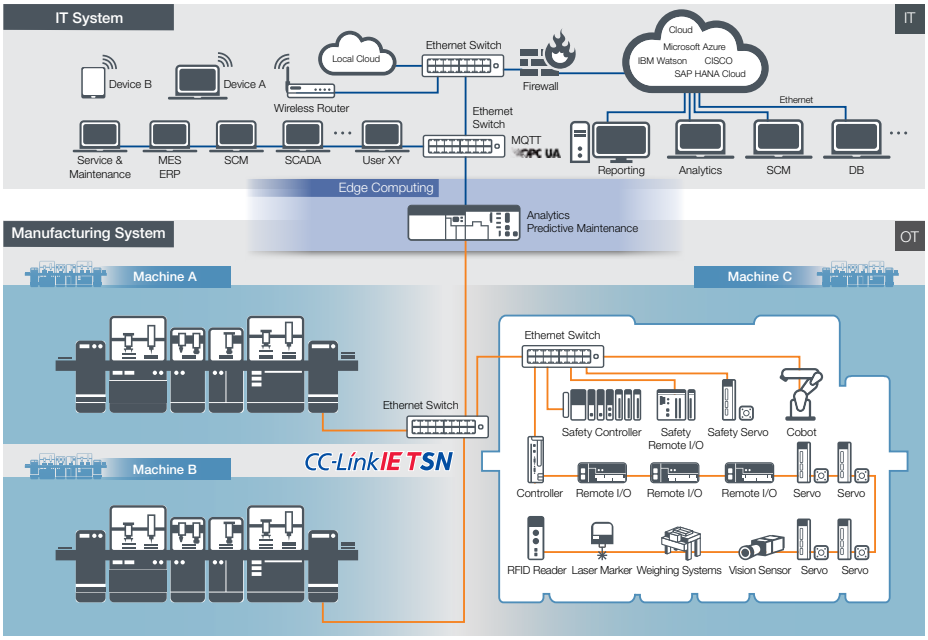
In order to meet demanding productivity and quality targets, current production trends demand cost effectiveness, better process insights, the shortest cycle times and the management of large amounts of process data. Complying to IEEE 802.1 standards, CC-Link IE TSN provides this capability by combining gigabit performance with the integration of control, safety and motion data along with general TCP/IP traffic **on a single network architecture**, all without compromising performance. This is the key to future industrial network convergence and only CC-Link IE TSN offers this functionality today. This translates to key business benefits:

- Simpler, more cost-effective network architectures and system designs
- Greater process transparency and better management
- Higher productivity
- Better integration of OT and IT systems

Currently the CLPA has over 4,100 member companies worldwide, and more than 2,600 certified products available from over 370 manufacturers. Together, these form a global installed base of over 31 million devices. The CLPA's technologies have found application in a wide variety of industries including but not limited to automotive, consumer electronics, semiconductor, food & beverage, packaging, material handling, water treatment and more.

CLPA offers development support and certification for device makers and product developers wanting to take advantage of CC-Link IE TSN's advanced capabilities in their own compatible products.

The CLPA has also been active in forming relationships with other industry leading associations such as the OPC Foundation and PROFIBUS & PROFINET International and is a member of the TIACC organisation.



SERVICES

- Open industrial Ethernet
- Time-Sensitive Networking
- Gigabit & 100Mbit bandwidth
- Support for Industry 4.0
- Open fieldbus
- Safety networks
- Motion control networks
- Product certification
- Product development support
- Product promotion opportunities
- PROFINET interoperability
- OPC UA compatibility

CC-Link Partners Association
Email: partners@eu.cc-link.org
Website: eu.cc-link.org

Visit Website

Challenging the way of automation

As a specialist for decentralized automation technology, Murrelektronik is a household name for connections and connectivity.

SOURCE: MURRELEKTRONIK

Murrelektronik is an internationally operating family business for automation technology. The company headquarters is in Oppenweiler.

THE COMPANY'S PRODUCTS DISTRIBUTE SIGNALS, data, and energy to where they are needed, thus literally bringing machines and systems to life. Murrelektronik's customers come from the automotive & robotics, warehousing & conveyor technologies, handling & packaging, machine tool and mobile applications sectors. Among them are all well-known automotive manufacturers, machine builders as well as SMEs. They are all united by the desire for greater efficiency in their processes. The influence of installation technology is often underestimated. But the early selection of the right installation concept influences the material costs as well as the flexibility in engineering, the time required for installation and commissioning, the compatibility of the products used, the degree of digitalization, the possibilities for later machine expansions, to name but the most important areas of impact.

The solutions include customized systems for both the power supply to and monitoring of the entire plant as well as for the networking of actuators and sensors with their own or any other control system - all the way to the cloud. With its innovative technologies for network installations, highly efficient I/O systems for all fieldbus and IoT protocols as well as safety technology and high-performance power supply solutions, the company accompanies its customers in the digital transformation process and the realization of new business models in the age of Industriy 4.0.

Decentralization

Murrelektronik consistently relies on decentralization to move the modules out of the control cabinet and into the immediate vicinity of the process. This saves not only resources, for example by significantly reducing the amount of cabling, but also a great deal of time during installation and commissioning. Decentralized modules can be connected with pre-assembled connectors, which is much faster and ensures an error-free, safe, and reliable connection. The use of intelligent decentralized modules enables simplified service and maintenance processes. This in turn reduces downtimes and ensures maximum productivity and high quality.

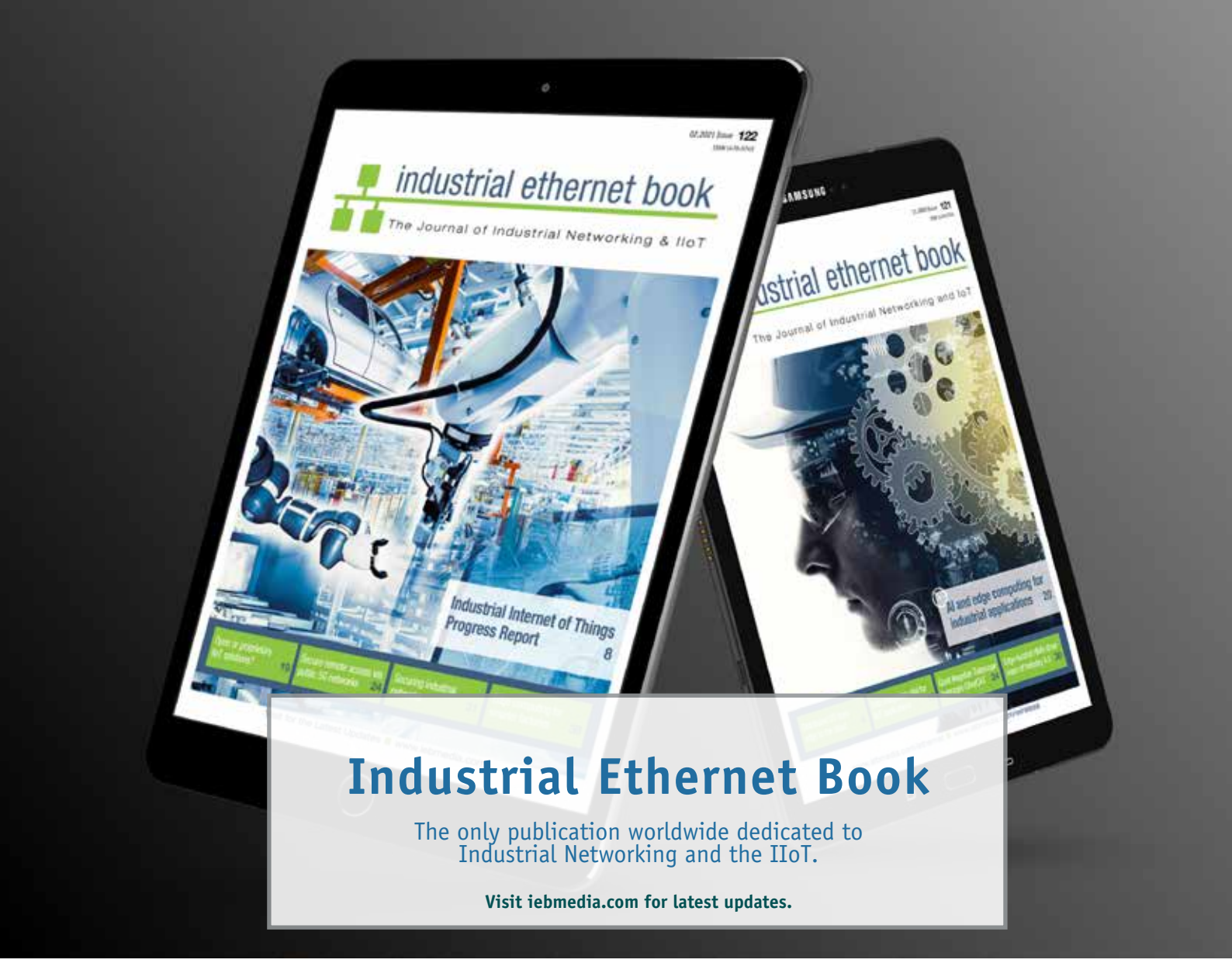
What Murrelektronik means by "We challenge the way of automation" is best summed up or proven by Murrelektronik's Vario-X automation system, which has won several awards: As a modular system, it can be put together exactly as needed, bringing all automation components to the place where they are needed.

Connection Devices

Murrelektronik offers a vast and constantly growing variety of connection devices, making it a leading supplier for literally anything connectivity and automation related: sensor-actuator cables, network and fieldbus cables, motor cables, self-connecting connectors, T-pieces, or adapters. Depending on our customers' needs, our products come pre-assembled with countless connection plugs, LED and protective circuitry integrated in many cases, and available in almost all cable lengths, cable qualities, and sheath colors.

Murrelektronik GmbH

Visit Website



Industrial Ethernet Book

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

Visit iebmedia.com for latest updates.

Offering the deepest, richest archive of Industrial Ethernet and IIoT content on the web.

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

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

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

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

industrial ethernet book
Industrial Networking & IIoT

Open and scalable controls automate process sequences

Diaphragm embossing machine for pressure sensor technology illustrates how the demanding process sequences can be automated with the aid of open control technology, which can be optimally scaled from a simple tabletop device to a large production plant.

PICTURE: © KELLER AG

The diaphragm embossing machine from Keller AG, which appears in anti-reflective red light, can be conveniently operated from all sides via the customer-specific CP3921 multi-touch Control Panel.

THE SWISS COMPANY KELLER AG FÜR Druckmesstechnik is a specialist in pressure sensor technology and offers an extremely wide range of products for a host of applications that require correspondingly complex production processes. A diaphragm embossing machine used in prefabrication illustrates how the demanding process sequences can be automated with the aid of open control technology from Beckhoff, which is optimally scalable from a simple tabletop device to a large production plant.

Winterthur-based Keller AG für Druckmesstechnik was founded in 1974 by the inventor of the integrated silicon measuring cell, Hannes W. Keller, and proudly asserts itself as the market leader in the manufacturing of isolated pressure transducers and pressure transmitters. The piezoresistive pressure sensors offer very high accuracy as well as pressure ranges from 5 mbar to 2,000 bar. In addition to more than 500 standard products, Keller AG also develops and produces customer-specific solutions. In more than 35 highly specialized production islands, they manufacture large series of industrial OEM transducers, as well as special designs in very small quantities using the latest automated manufacturing processes. Applications for the pressure transducers include monitoring groundwater levels, controlling aircraft cabin pressure, switching from natural gas to gasoline in bivalent vehicles and serving as reference sensors in laboratory technology.

PICTURE: © KELLER AG

Most of the motion axes are implemented using compact drive technology.

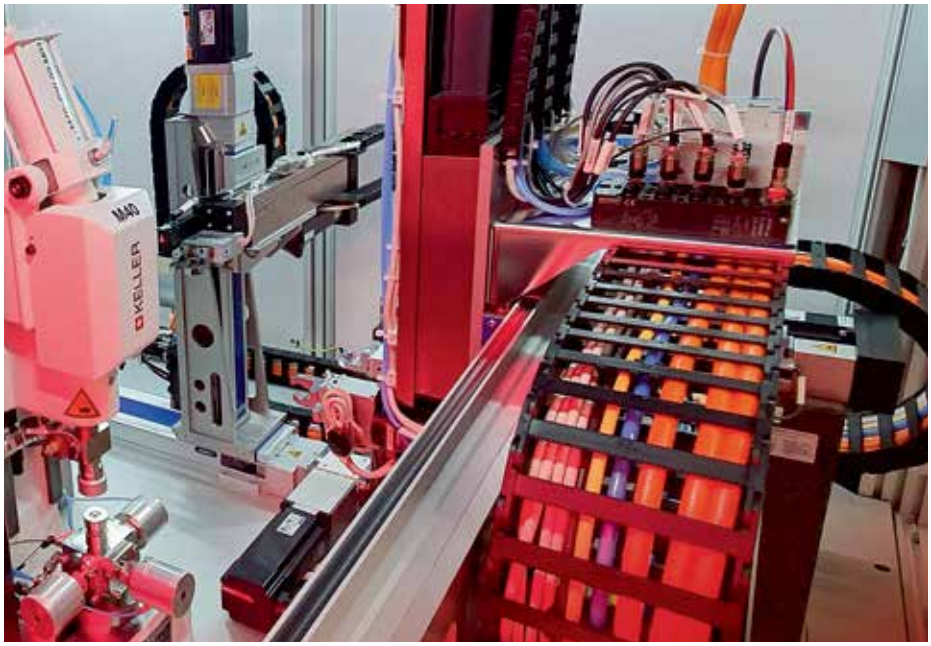
Embossing the sensor diaphragm is an essential process step

Embossing the sensor diaphragm is an essential intermediate process during prefabrication process, as Florian Wernli, Project Manager at Keller AG, explains: "Most of our pressure sensors feature a steel housing filled with oil. The diaphragm is crucial for transmitting the pressure of the surrounding medium to be detected via the oil to the measuring chip inside the sensor."

This requires the diaphragm to have a special shape, which is achieved with a powerful automatic embossing machine. Bruno Thalmann, Development & Production Equipment at Keller AG, adds: "After a leakage pre-test, cleaning with compressed air and a thermal equalization process, we carry out high-pressure embossing and a definitive leakage test in the same process step using a hydrogen sensor.

This is followed by an error check based on image processing and artificial intelligence." The central handling element within the embossing machine is a KUKA robot, which acts as a pick-and-place unit to feed the blanks into the process and separate the finished workpieces into OK and NOK parts.

Thalmann explains the advantage of this fully automatic embossing and inspection system: "Our goal was to automate a process that previously required three manual stations in production. In this way, we were able to increase both manufacturing quality and production quantity." Wernli confirms: "The higher productivity is due on the one hand to the fast, fully automatic process with a throughput time of only 15 s per workpiece, and on the other hand to the fact that production can continue at night despite staff working in a single shift."



PICTURE © KELLER AG

Most of the motion axes are implemented using compact drive technology from Beckhoff with EL72x1 servomotor terminals and AM81xx servomotors – shown here is the embossing core process with the pneumatic high-pressure press (left).

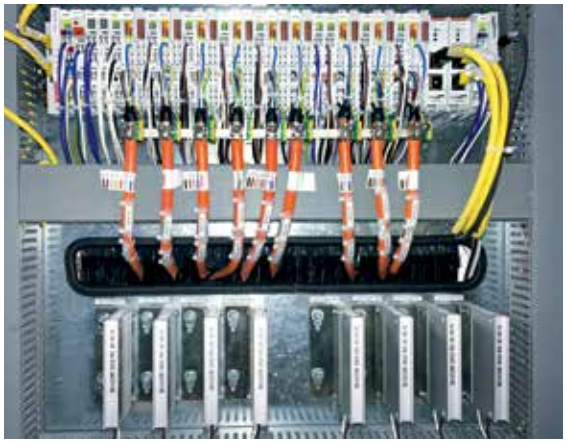
Advantages of open and modular control technology

Keller AG has relied on PC-based control technology from Beckhoff since 2018. Thalmann sees advantages in the level of openness in terms of both programmability and the wide variety of supported interfaces. The optimal scalability of PC-based control also manages easily the system complexity or the desired degree of modularization from centralized to decentralized.

All in all, TwinCAT 3 benefits from a modern, object-oriented software platform that is integrated into Visual Studio® and, together with TwinCAT HMI, offers powerful visualization capabilities that are consistent right through to tablet operation. In addition to the high computing power of the C6920 control cabinet Industrial PC, further important solutions from Beckhoff include compact drive technology with One Cable Technology (OCT), the EtherCAT P and CP-Link 4 one-cable solutions, safety technology integrated into the system with TwinSAFE, and the simple integration of EtherCAT-capable third-party components such as vision systems, flow controllers, valve terminals and electric grippers.

Wernli cites the simple robot integration as a particular example of the advantages of system openness: "By integrating the robot via the EL6695 EtherCAT bridge terminal and TwinCAT Robotics mxAutomation, it was possible to implement the pick-and-place functionality via simple configuration without the need for special robotics expertise. The fact that we have full control of the robot via PC-based control makes this the perfect solution for us."

In addition to the C6920, the hardware core of the automation solution is the CP3921 multi-touch Control Panel connected via CP-Link 4, which has a 21.5-inch display and push-button extensions. According to Wernli, this provides the machine end user with a control unit that is as convenient as it is striking: "For us, design is an extremely important factor within the overall machine concept. Added to this is the high display resolution, which is necessary for convenient access to our inspection system. Featuring a remote control panel mounted on a support arm, the design means that the machine, which offers 360-degree accessibility, really can be operated quite flexibly from all sides."



PICTURE © KELLER AG

The EL72x1 servomotor terminals (top) and the compact ZB8110 brake resistors (bottom) make for a space-saving control cabinet design.

Compact and flexible drive technology and I/O level

Since the automatic embossing machine handles only small workpieces, compact drive technology from Beckhoff is practically made for this application. A total of 11 EL7211 and two EL7221 servomotor terminals, 11 EL9576 brake chopper terminals with ZB8110 external brake resistors, and 15 AM8100-series servomotors are used. Complementary motion axes from the portal system are implemented via three AX5203 Servo Drives and AM803x servomotors.

According to Wernli, EtherCAT also offers great advantages in terms of data communication: "We consistently rely on the EtherCAT standard because, for one, we can count on a very wide range of components from both Beckhoff and third-party suppliers. Another bonus is that we benefit from the extensive diagnostic functions and level of openness when integrating other bus systems, for example." He sees another important aspect in the various options for reduced cabling effort: "Essentially, every cable we don't have to lay is a real bonus for us. PC-based control opens up additional optimization potential here with EtherCAT P – in addition to CP-Link 4 and OCT. In the I/O area, we consistently rely on EtherCAT P – that is, in the case of the automatic embossing machine, on I/O Box modules from the EPP series." Specifically, these are an EPP1004 4-channel digital input, five EPP1018 8-channel digital inputs, nine EPP1809 and two EPP1816 16-channel digital inputs, as well as two EPP3184 4-channel analog inputs.

Thalmann also confirms the practical advantages: "EtherCAT P simplifies not only installation, but also maintenance. If, for example, a sensor fails, all you have to do is simply unplug the cable at the socket rather than having to pull the whole thing through all the drag chains. And, after replacing the device, you simply plug it in and the system is ready to go again."

Stefan Keller, Area Sales Manager, ***Beckhoff Switzerland.***

Visit Website

PROFINET communication in private industrial 5G networks

VXLAN is a protocol that embeds the logical Layer 2 communication in Layer 3 packets. This makes it possible to transmit Layer 2 protocols transparently across network boundaries, such as in routed Layer 3 5G infrastructures. This new approach is enabling use of PROFINET over private 5G industrial networks.

SOURCE: SIEMENS

PROFINET COMMUNICATION HAS BECOME AN indispensable part of today's automation technology. Many industrial applications require real-time transmission that the PROFINET standard offers. However, with the advent of 5G technology and its advance into industrial fields, users from the industrial environment are confronted with one difficulty: The currently available 5G technology cannot yet transmit PROFINET IO packets, which are necessary for the communication between a central controller and distributed I/O devices. This problem, though, can already be solved today using innovative communication technologies.

With 5G, a new mobile communications standard was developed for the first time that took into consideration industrial use cases – and it is already being used today in both public and private mobile communications networks. The 5G standard offers the possibility of adapting networks to different scenarios.

The three main scenarios are: enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine-Type Communication (mMTC). All scenarios serve different application areas: eMBB is bandwidth-oriented and URLLC supports the requirements of industrial IoT applications such as low latency with best possible reliability. MMTC is used for applications that require low power consumption and have a large number of connected devices.

Since a single wireless network cannot fully support all scenarios at the same time, i.e., maximum number of users and bandwidth with lowest latency, different typical 5G networks are emerging. One form of this are public mobile communications networks, in which the main scenarios eMBB and mMTC predominate to provide as much bandwidth as possible to many users for video telephony, video streaming, and other data-intensive applications.

SOURCE: SIEMENS

The SCALANCE MUM856-1 5G router from Siemens enables the transmission of PROFINET communication over 5G.

However, these are less relevant requirements for industrial wireless networks, since industrial real-time protocols such as PROFINET IO rely on low latency and high reliability, as described by the URLLC scenario.

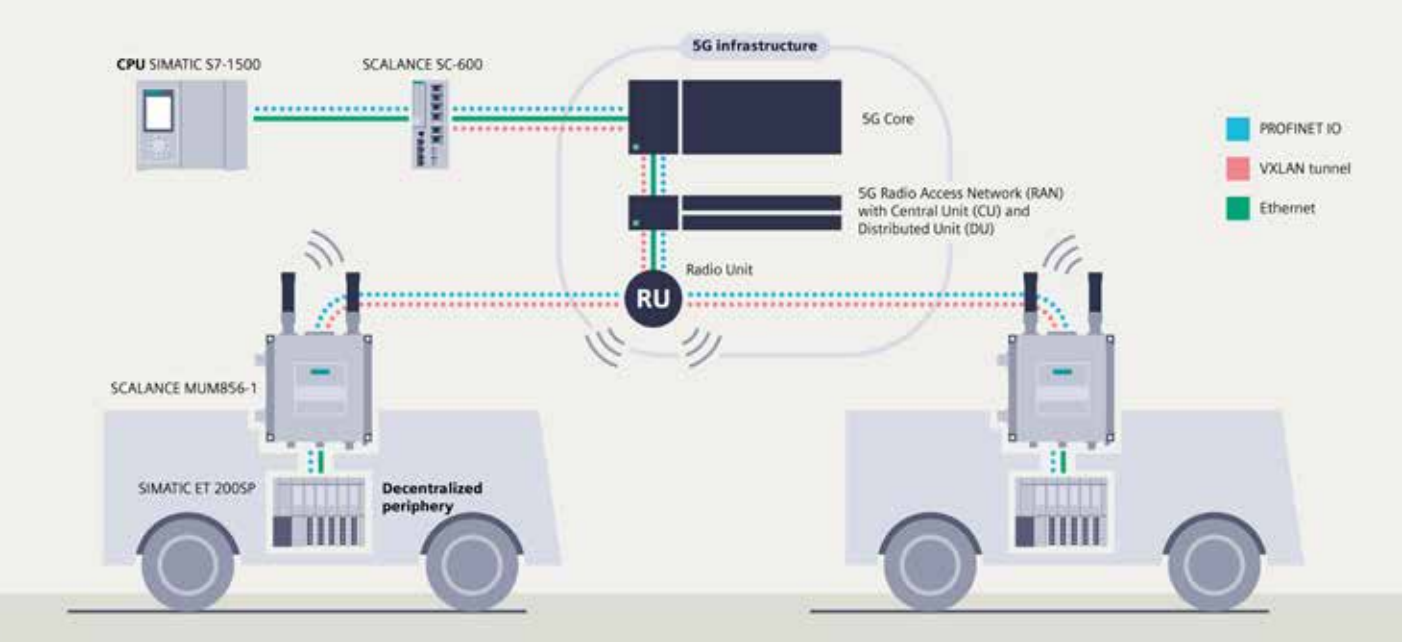
Private 5G networks for industrial real-time transmission

Reliability, latency, and control over a 5G network can be dramatically improved by companies establishing their own, local 5G networks and customizing them to meet the requirements of their mission-critical applications. For this purpose, the Bundesnetzagentur (German Federal Network Agency) has reserved part of the frequency spectrum for use in private, local 5G networks.

This spectrum can be requested for local use for a small fee. With these private 5G infrastructures, the available spectrum can be used exclusively, which has a positive effect on the performance of the network and, for example, enables time-critical applications.

The 5G technology standard currently available on the market corresponds to 5G Release 15. A current challenge here is that important elements such as the URLLC

SOURCE: SIEMENS



PROFINET communication over a private 5G network enables the use of a central controller for multiple mobile participants and significantly reduces energy and maintenance expenses.

standard will only be introduced in the future with Release 16. However, companies are already working with private 5G networks today to take advantage of their benefits – and would also like to use them for their industrial real-time protocols such as PROFINET IO. In doing so, they are faced with a challenge since the current Release 15 infrastructure cannot transmit the Layer 2 communication of the OSI layer model, which is frame-based. Only the layer above, Layer 3 with data packets (TCP and UDP), is supported.

This makes it possible, e.g., to access internal configuration web pages, for instance the web-based management of devices, or to establish OPC UA or MQTT communication. However, one of the currently most widely used fieldbus systems, PROFINET IO, cannot be used natively with this because it requires a Layer 2 connection, which will only be supported in the 5G standard with Release 16.

New approach enables PROFINET communication over 5G

However, PROFINET IO can already be used in private 5G networks today by means of innovative transmission technologies, as utilized, for example, in the SCALANCE products from Siemens. This is achieved by using the VXLAN (Virtual Extensible LAN) protocol. VXLAN is a protocol that, in simplified terms, embeds the logical Layer 2 communication in Layer 3 packets. This makes it possible to transmit Layer 2 protocols transparently across network boundaries, such as in routed Layer 3 5G infrastructures.

This approach opens up completely new possibilities. For example, several automated guided vehicles (AGVs) can be controlled centrally with one SIMATIC S7-1500 controller. PROFINET IO is used as the protocol between the SIMATIC S7-1500 and the SIMATIC ET 200SP distributed I/O devices on the AGV. At the heart of the communication is a private Release 15 5G infrastructure to which the SCALANCE MUM856-1 5G routers are connected. The infrastructure consists of the 5G core, which manages the entire network and the data traffic, the central unit (CU), which manages the wireless network, the distributed unit (DU), which processes the digital wireless signal, and the radio unit (RU), which transmits the wireless signal via antennas.

VXLAN enables the necessary transmission of PROFINET IO packets

The special feature of this network, however, is that there is a VXLAN tunnel between the SCALANCE MUM856-1 5G router and a SCALANCE SC-600 security firewall, which is placed between the controller and the 5G core. The two devices encapsulate and decapsulate the PROFINET packets with the aid of VXLAN – thus enabling the wireless PROFINET communication between the controller and the distributed I/O devices. However, this "tunnel" should not be confused with classic VPN tunnels, since no additional encryption is performed here by the VXLAN protocol – only the transmission of the packets takes place.

By means of the VXLAN tunnel, the two AGV networks with the ET 200SPs and the central S7-1500 controller are in the same virtual Layer 2 network and, for the first time, the PROFINET IO protocol or other Layer 2 protocols can be used for the communication over a 5G network. It should be noted here that, similar to other wireless technologies, the update times and retransmission repetitions of PROFINET IO packets must be adapted to the performance of the wireless network (the 5G infrastructure) to maintain deterministics and real-time capability. As 5G releases progress, the performance will continue to improve with, for example, URLLC extensions.

Significant reduction of energy and maintenance expenses thanks to central controller

By using central PROFINET IO communication, a distributed I/O device can be used on the AGV and there is no need for a local controller. This result in space, cost, energy and, maintenance savings. By means of a controllable digital output of the SCALANCE MUM 5G router, the entire AGV can be switched currentless via a separate relay to save energy during idle times. For longer planned downtimes, the 5G router can also be put into a deep sleep mode, in which power consumption drops to an absolute minimum. This means that power consumption can be reduced even during longer downtimes, such as on weekends, thus increasing the battery charge of the AGV. The advantages of the current implementation using VXLAN are clear and show that powerful industrial protocols such as PROFINET IO can already be operated in today's private 5G networks within the given framework conditions.

Lars Walpurgis, Product Manager - Industrial 5G Products, ***Siemens.***

Visit Website

World's first 15 MW wind turbine built by Vestas

More than 10,000 Vestas wind turbines with scalable distributed control system have been deployed in the field, and Vestas continues to integrate the DCS into thousands of wind turbines each year. Now, TTTech Industrial's distributed control system was integrated into the world's first 15 MW wind turbine built by Vestas.

SOURCE: TTTECH-INDUSTRIAL

Nerve node software runs on devices at the edge, and provides a management system that runs in the cloud or on a local server.

TTTECH INDUSTRIAL AND VESTAS, ONE OF the largest manufacturers of wind turbines worldwide, have been working together successfully for more than 10 years. Wind energy is a clean, renewable source of energy and, according to WindEurope, about 16% of electricity in Europe already comes from wind power.

The market for wind energy is likely to continue to grow and TTTech Industrial is proud to contribute to more sustainability in energy production as a supplier to Vestas. The company's scalable distributed control system (DCS) is being integrated into thousands of Vestas wind turbines every year, most recently into the world's first 15 MW turbine, the V236-15.0 MW™, released in November 2021.

More than a decade ago, Vestas approached TTTech Industrial looking for a solution to simplify the internal control systems in their turbines. Vestas' primary goals were to avoid developing new system architectures for each and every new turbine model and to reduce system complexity to facilitate easier service and maintenance. To meet these requirements, TTTech Industrial developed a scalable distributed control system for Vestas.

With this solution, Vestas optimized their development and is now able to reuse more than 70% of the turbine architecture when developing new turbine models. The DCS enables the connection of multiple control devices inside the wind turbine, with safety-critical and non-safety-critical functions being able to run next to each other on a specially developed controller. Data from multiple controllers is transmitted on a single network cable with Deterministic Ethernet technology, ensuring optimal bandwidth usage. This makes the entire system easier to maintain and reduces the need for expensive cabling inside the turbine.

"We have been working successfully with TTTech Industrial for more than a decade. From the very beginning, high competency in functional safety and experience with safety-critical applications were a must for us. The DCS makes building new turbines easier and more cost-effective and speeds up time to delivery and installation. This ensures higher availability of the turbines and reduces energy costs for our customers. We currently use TTTech Industrial's DCS in our turbines in the onshore sector and have now also included it into our newest offshore turbine, the V236-15.0 MW™," explains Jan Sondergaard, Module Owner/VP at Vestas.

The Vestas' V236-15.0 MW™ wind turbine for offshore environments, which was released in November 2021, also contains TTTech Industrial's DCS. It is the world's first 15 MW wind turbine, capable of producing up to 80 GWh/year, which equals to energy for over 200,000 households, depending on the conditions at the site.

"The partnership with Vestas was a milestone for TTTech Industrial in the energy sector. Our long cooperation started with the integration of our DCS in a 4 MW turbine and continued with the roll-out of the DCS in other turbine variants. We are proud to contribute to renewable energy production together with Vestas and look forward to our continued cooperation," says Thomas Berndorfer, Member of the Executive Board, TTTech Industrial.

Since 2016, TTTech Industrial's DCS has been integrated into around 10,000 Vestas wind turbines all over the world. Based on the output of a 4 MW turbine that produces about 13 GWh electricity per year, these 10,000 turbines can supply around 33 million European households with electricity.

*Application report by **TTTech Industrial.***

Learn more

10BASE-T1L MAC-PHY for Low Power Ethernet Connectivity

A 10 Mb Ethernet physical layer (10BASE-T1L) combined with power delivery (Engineered Power/PoDL/SPoE) on two wires, up to 1 km, will enable new types of Ethernet-connected devices that generate higher value insights that are now more accessible via a converted IT/OT Ethernet network.

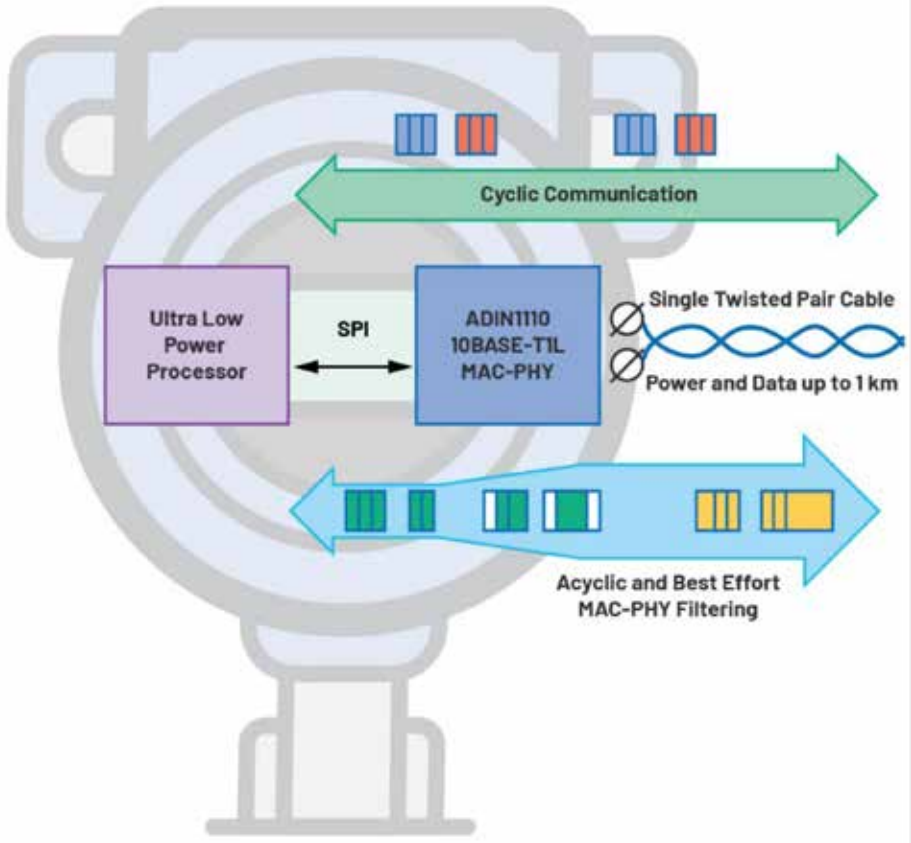
THIS ARTICLE EXPLAINS HOW TO CONNECT TO an increased number of low power field or edge devices with a 10BASE-T1L MAC-PHY. It will also detail when to use the MAC-PHY vs. a 10BASE-T1L PHY and how these systems meet the requirements of tomorrow's Ethernet-connected manufacturing and building installations.

Background

Single-pair Ethernet 10BASE-T1L use cases, including Ethernet-APL, continue to expand across process, factory, and building automation applications driven by the requirement to connect more devices to Ethernet networks. With more devices connected, richer datasets are made available to the higher level management systems, leading to significant increases in productivity while reducing operating costs and energy consumption.

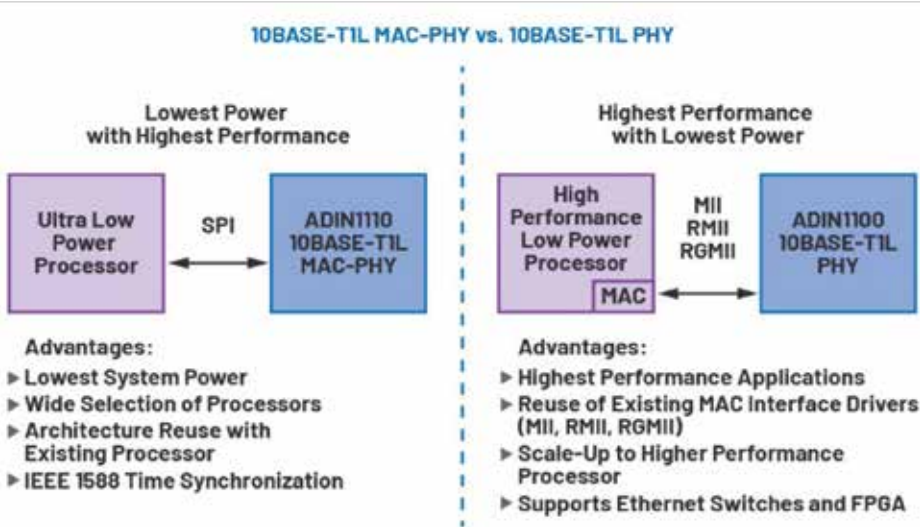
The vision of Ethernet to the field or edge is to connect all sensors and actuators to a converged IT/OT network. To achieve this vision there are system engineering challenges, as some of these sensors are limited in power and space. There is a growing market of low power and ultra low power microcontrollers with significant internal memory capabilities for sensor and actuator applications.

But most of these processors have one thing in common—with no integrated Ethernet MAC, they don't support an MII, RMII, or RGMII media independent (Ethernet) interface. A traditional PHY cannot be connected to these processors.



SOURCE: ANALOG DEVICES

A 10BASE-T1L MAC-PHY significantly reduces the power and complexity of devices with advanced packet filtering.



SOURCE: ANALOG DEVICES

Comparison of the advantages of a MAC-PHY vs. a PHY for 10BASE-T1L connectivity.

Why Use a 10BASE-T1L MAC-PHY

To enable long range Ethernet connectivity to an increased number of lower power devices, a 10BASE-T1L MAC-PHY is required. With a 10BASE-T1L MAC-PHY, Ethernet connectivity is provided to a processor via SPI, reducing the burden on the processor by removing the need for an integrated MAC.

The MAC functionality is now integrated directly with the 10BASE-T1L PHY. A 10BASE-T1L MAC-PHY provides device architects increased flexibility and choice by enabling a variety of ultra low power processors. By optimizing the application partitioning, a 10BASE-T1L MAC-PHY enables lower power field devices for Zone 0 intrinsically

Part	ADIN1100	ADIN1110
	10BASE-T1L PHY	10BASE-T1L MAC-PHY
Interface	MII, RMII, RGMII	SPI
Integrated MAC	No	Yes
Supports Intrinsic Safe	Yes	Yes
Power Consumption	39 mW	42 mW
Auto-Negotiation Capability	Yes	Yes
On-Chip FIFO	No	20 kB receive/ 8 kB transmit
MAC Filter (16 Entries)	No	Yes
Prioritizing of Traffic	No	Yes
IEEE 1588 Timestamp Support	No	Yes
Temperature Range	–40°C to +105°C	–40°C to +105°C
Package	40-lead LFCSP	40-lead LFCSP

SOURCE: ANALOG DEVICES

A 10BASE-T1L MAC-PHY significantly reduces the power and complexity of devices with advanced packet filtering.

safe deployment through what is referred to in the process industry as Ethernet-APL. Within intelligent building applications, a MAC-PHY will enable more lower power devices to be connected to an Ethernet network. Intelligent building applications include HVAC systems, fire safety systems, access control, IP cameras, elevator systems, and condition monitoring.

10BASE-T1L MAC-PHY Advanced Packet Filtering

The integration of the MAC functionality with a 10BASE-T1L PHY provides new features to optimize Ethernet traffic on the network. A 10BASE-T1L MAC-PHY with advanced packet filtering will significantly reduce the overhead of handling broadcast and multicast traffic, while freeing the processor from this task. To filter by the destination MAC address is key.

Instead of just a single MAC address, a MAC-PHY can support filtering using up to 16 unicast or multicast MAC addresses. In addition, address masking is supported for two MAC addresses. This gives a great degree of freedom, filtering for the device address as well as commonly supported multicast addresses such as LLDP (Link Layer Discovery Protocol).

By supporting an additional queue for higher priorities, some messages can be prioritized and therefore get improved latency and robustness. The priority of a frame can be identified by the MAC filtering table. For example, broadcast messages can be fed into a lower priority queue and unicast into the higher priority queue to prevent the receiver from being overloaded by a broadcast storm or traffic surge. These MAC-PHY filtering features enable netload robust devices. Frame statistics are also gathered by the MAC to assist in monitoring the network traffic and the quality of the link (see Figure above).

The MAC in the MAC-PHY also supports IEEE 1588, and therefore 802.1AS time synchronization as required in process automation. The MAC-PHY provides support for a synchronized counter, timestamping of received messages and timestamp capture for transmit messages. This greatly reduces the complexity of the software design, as there is no further hardware support needed to implement time synchronization beyond the MAC-PHY itself.

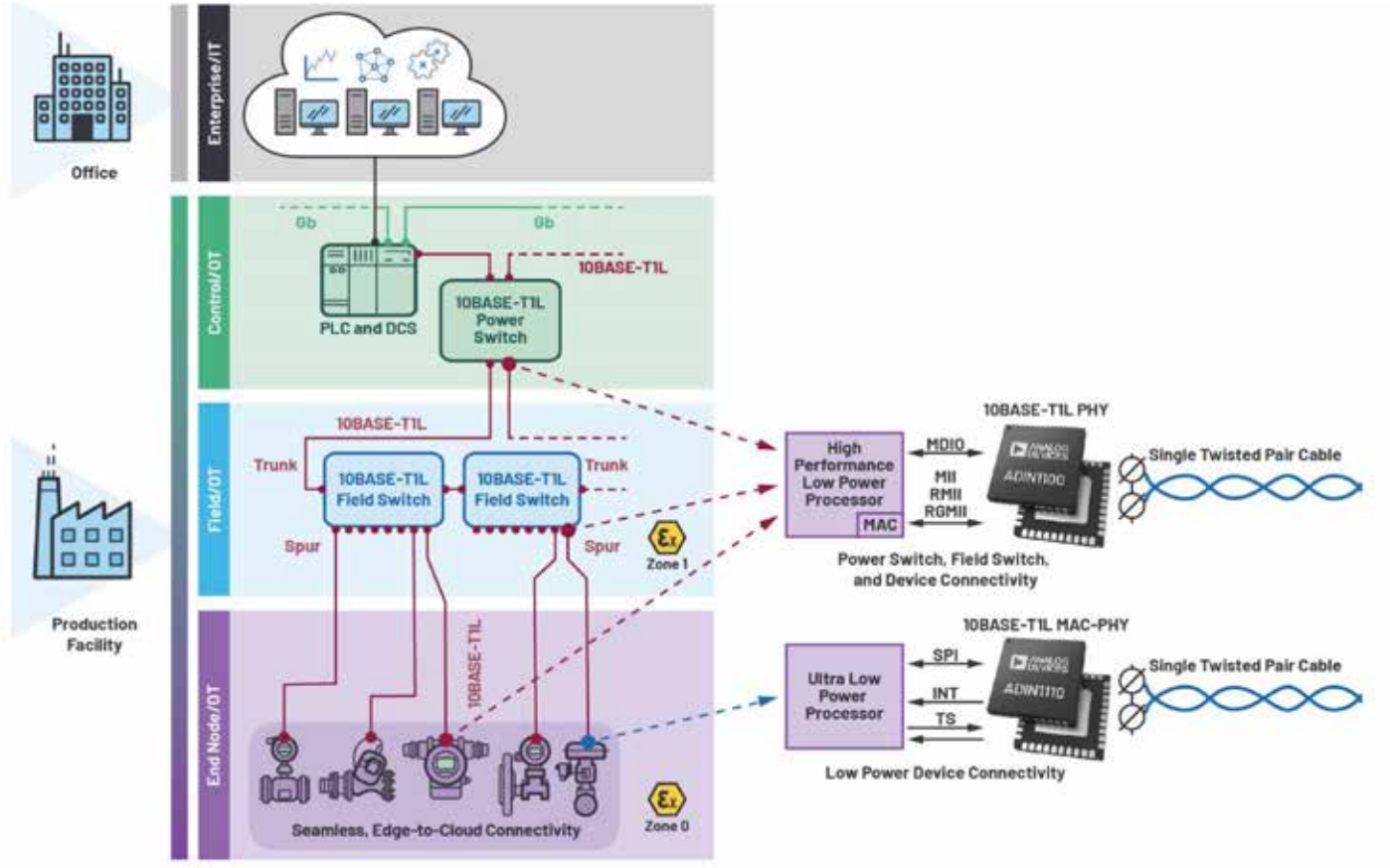
The MAC can generate an output waveform timed to the synchronized counter, which may be used to synchronize external application-level operations. The SPI interface supports the Open Alliance 10BASE-T1x MAC-PHY Serial Interface. The Open Alliance SPI is a new and very effective SPI protocol designed specifically for use with a MAC-PHY.

When to Use a 10BASE-T1L MAC-PHY and a 10BASE-T1L PHY

Both a 10BASE-T1L PHY and a 10BASE-T1L MAC-PHY bring significant advantages in different use cases. For power critical applications, a 10BASE-T1L MAC-PHY enables lower system power by providing more flexibility on the choice of host processor to include ultra low power processors that do not have an integrated MAC.

When upgrading an existing device to add Ethernet connectivity, a 10BASE-T1L MAC-PHY provides a route to reusing the existing processor and adding Ethernet connectivity via

SOURCE: ANALOG DEVICES



Trunk-and-spur network topology for process automation with 10BASE-T1L MAC-PHY and 10BASE-T1L PHY.

an SPI port, removing the requirement to move to a larger processor with an integrated MAC.

For high performance applications where a field or edge device requires a high performance processor that may already have an integrated MAC, a 10BASE-T1L PHY with MII, RMII, and RGMII MAC interfaces allows a 10BASE-T1L PHY to be quickly developed. This is done by reusing existing MAC interface drivers to add Ethernet connectivity.

Tomorrow's Ethernet-Connected Process Installations

With the availability of both 10BASE-T1L PHYs (ADIN1100) and 10BASE-T1L MAC-PHYs (ADIN1110), device architects now have increased flexibility to meet the requirements of tomorrow's Ethernet-connected manufacturing installations.

Ultra low power devices and high performance devices can be deployed on the same Ethernet network and comply with strict maximum power limitations for hazardous area use case requirements.

10BASE-T1L power switches and 10BASE-T1L field switches require robust, low power 10BASE-T1L PHYs to be used with Industrial Ethernet switches to deploy a trunk-and-spur network topology that provides both power and data over a single twisted pair cable, including hazardous area use cases.

Field device connectivity requires both 10BASE-T1L PHYs and 10BASE-T1L MAC-PHYs to enable Ethernet connectivity to a wide range of field devices. Higher power field devices, including flowmeters, will use a high performance processor, with an integrated MAC with a 10BASE-T1L PHY. Lower power field devices, including temperature sensors with an ultra low power processor that does not have an integrated MAC, will use a 10BASE-T1L MAC-PHY for Ethernet connectivity via an SPI interface to the processor.

Comparison of 10BASE-T1L PHY and 10BASE-T1L MAC-PHY Key Features

The ADIN1110, ADI's 10BASE-T1L MAC-PHY, enables lower power Ethernet connectivity via an SPI interface to a host processor with only 42 mW of power consumption. The ADIN1110 supports the Open Alliance 10BASE-T1x MAC-PHY Serial Interface for full-duplex SPI communications at 25 MHz clock speed.

The ADIN1100, ADI's 10BASE-T1L PHY, enables low power Ethernet connectivity via MII, RMII, and RGMII MAC interfaces to a host processor with only 39 mW of power consumption—see Table 1 for a comparison of the ADIN1100 10BASE-T1L PHY and ADIN1110 10BASE-T1L MAC-PHY. Both products are based on 10BASE-T1L core capability of a full-duplex, DC balanced, point-to-point communication scheme with PAM 3 modulation at a 7.5 MBd symbol rate with 4B3T coding.

10BASE-T1L supports two amplitude modes: 2.4 V peak-to-peak up to 1000 m cable and 1.0 V peak-to-peak at a reduced distance. The 1.0 V peak-to-peak amplitude mode means that this new physical layer technology can also be used in the environment of explosion proof (Ex-proof) systems and meets the strict maximum energy restrictions.

Summary

A 10 Mb Ethernet physical layer (10BASE-T1L) combined with power delivery (Engineered Power/PoDL/SPoE) on two wires, up to 1 km, will enable new types of Ethernet-connected devices that generate higher value insights that are now more accessible via a converted IT/OT Ethernet network.

These new insights will drive higher productivity and reduce energy consumption in process and factory automation applications. In building automation applications these new insights will enable higher levels of energy efficiency, safety, and comfort. As a result, a 10BASE-T1L MAC-PHY will accelerate lower power device availability.

Maurice O'Brien, Strategic Marketing Manager, and Volker E. Goller, Systems Application Engineer, ***Analog Devices.***

Visit Website

IoT maturity is not without its challenges

Wi-SUN's latest research report shows that organisations are becoming more ambitious and sophisticated in their thinking. IoT is now a bigger priority than ever, and the scale of what is being planned over the next few years is encouraging.

SOURCE: WI-SUN ALLIANCE

IN 2017, WI-SUN ALLIANCE PUBLISHED ITS first research report on the state of the IoT industry. It made interesting reading as the early adopters of IoT technologies highlighted the challenges and barriers (as well as the opportunities) to adoption. We revisited this 'state of the nation' report this year to see how perspectives and adoption patterns have changed over the last five years.

Half of the survey respondents, IT decision makers who are IoT adopters in UK and US organisations, view IoT enablement as a top three priority for the next 12 months, and it is also most likely to be the single top priority among the respondent base.

As the use cases mature and organisations see repeated successes among their peers, they are looking increasingly to the technology as a way to differentiate themselves. More than nine in 10 respondents believe that they must invest in IoT over the next 12 months to remain competitive. IoT technologies can help drive reliable systems and services. Adopters believe that implemented correctly, IoT could help to make them more agile, which is a key driver for adoption this year.

This equips them to meet volatile operating conditions during a pandemic that has changed everyone's operating rules.

Private businesses and public sector bodies alike need to enhance their user experiences, as they grapple with new ways to engage people in no-touch and remote environments. This is especially true in smart cities, which are looking for ways for increasingly dense populations to co-exist alongside each other.

Adopters might recognise the importance of IoT projects and the need to invest in it regardless of size or sector, but they still have plenty of work to do. Our research this year indicates that fewer than half (47%) of all companies have a fully implemented IoT strategy, while 42% have a partially implemented strategy, and 11% a plan that is either under review or still in development.

The UK is falling behind, with fewer than four in ten (39%) organisations with fully implemented IoT strategies compared to just over half (51%) in the US.

What is encouraging however is that respondents responsible for smart cities, smart utilities, and industrial IoT (IIoT) projects have advanced across the board. Almost 70% of companies have implemented their smart city initiatives, up from 42% in 2017. Full IIoT project implementation has risen from 46% to 65%, while half of companies with smart utility strategies have delivered, up from 38% five years ago. Fewer projects are now in the pilot/testing stage, demonstrating the progress made over recent years.

But it seems that the journey to IoT maturity is not without it challenges.

Focus on security and compliance of IoT projects

Our survey respondents are focused more heavily on the security and compliance of IoT projects than they were five years ago. Since 2017, stricter privacy laws have increased pressure on organisations to protect sensitive data in the UK and in the US. This includes the General Data Protection Regulation (GDPR) in Europe and the California Consumer Protection Act in the US.

The focus is strong in the UK, where more than half (53%) of organisations include secure data collection in their IoT strategies, compared to just a third (34%) in the US. But the UK's concerns over security and data usage doesn't overshadow its focus on the benefits of the technology. With 47% of UK organisations including data usage strategies in their IoT plans, they are still connecting their IoT strategies firmly to business goals.

As IoT strategies mature, security is becoming far less of an issue than it was five years' ago. Those respondents ranking it as one of their 'top three challenges when rolling out IoT' dropped from 58% in 2017 to 24% in 2022. The number of IoT adopters viewing security as a technical challenge also fell, from 65% in 2017 to 42% this year.

But organisations are still eager to ensure their IoT systems are secure. Our latest report shows a slight rise in the proportion of respondents demanding proven security with multi-layer protection and continuous monitoring when considering smart city

solutions. This is either very important or critical for 86% of respondents, compared to 82% in 2017. They might be more relaxed about security challenges thanks to protection like device identity certificates, but they also understand its importance more than ever and demand secure implementations from vendors.

Data privacy concerns grow

While some barriers to adoption have eased, others have increased, as companies comprehend the full implications of designing and deploying IoT solutions. One of these is data privacy, which has become more of a concern as security concerns fall.

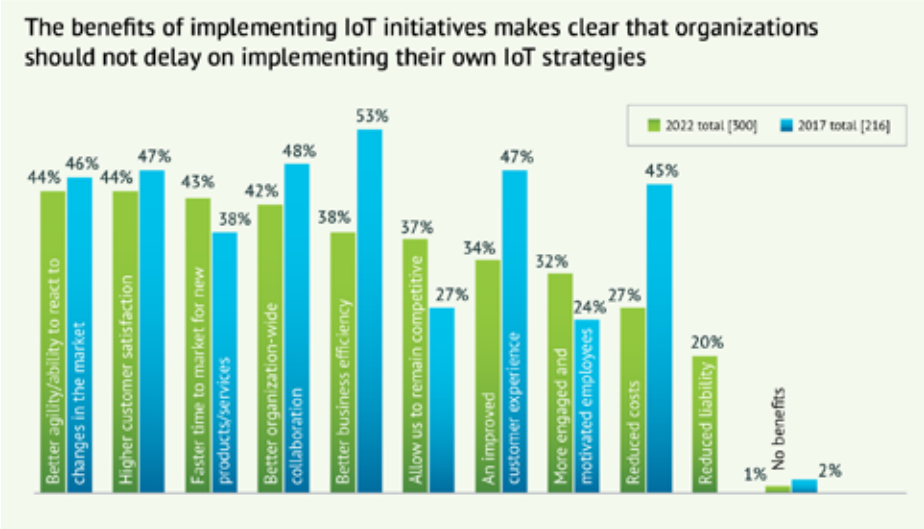
IoT projects by their nature have the potential to generate huge quantities of data. Even if this information is secure, handling it responsibly represents a privacy risk. Managing large volumes of data is technically difficult, especially when regulators interpret it as sensitive personal information. Organisations that mishandle or misuse it risk running into regulatory or compliance issues.

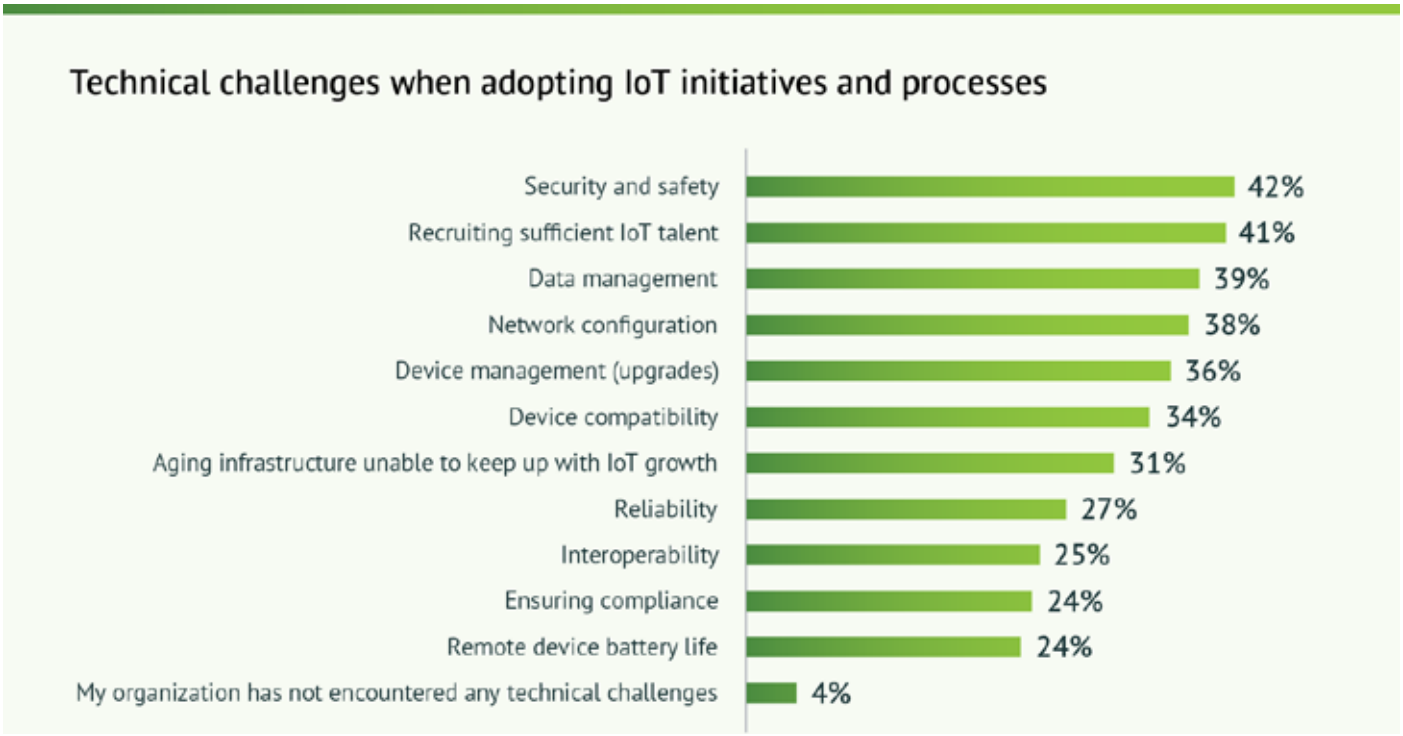
Data privacy regulation is ranked as the second most important political, economic or social challenge for IoT adopters, with 36% placing it in their top three. Fears over big data have jumped to 19% from 11% placing it in their top three IoT rollout challenges in the last five years, and one in four respondents cited regulatory concerns. Five years ago, the IoT market was less mature with many smart city and smart utility projects in their infancy.

Phil Beecher, CEO & President, ***Wi-Sun Alliance.***

Visit Website

SOURCE: WI-SUN ALLIANCE





Analysis of technical challenges organizations encountered when delivering IoT initiatives and processes.

BeerMaker intelligent process control solution

Brewery-specific ABB Ability™ BeerMaker intelligent process control solution will support safety and quality improvements, boost productivity and raise operational efficiency

SOURCE: ABB

Brewing teams will be empowered to take better decisions at the right time using modern interfaces and intuitive insights.

ABB HAS LAUNCHED ITS ABB ABILITY™ BeerMaker intelligent process control solution to further support breweries in their operational efficiency through digital transformation. ABB's brewmaster, who has the notable achievement of qualifications from Technical University of Munich in Weihenstephan, devised the new package alongside a team with deep process knowhow.

It will benefit beermakers seeking to optimize their processes, reduce their impacts on water and energy resources and meet consumer demand for more sustainably crafted drinks. The new solution is based on the ABB Ability™ System 800xA® distributed control system and will help brewers improve process quality, achieve high engineering and operator efficiency, enhance safety and boost plant productivity. It has been made available to ABB's end customers and channel partners.

The process automation solution comprises a technological package including a control system with batch functionality following the worldwide S88 standard and a digital twin to simulate new recipes. Crafted and tested with brewing knowledge from ABB's brewmaster, it can be adapted for each customer using a variety of parameters. Ready-made and tested templates and objects bring a high level of automation and intelligence of plant functions into operators' hands. There is a prepared inventory for queue handling, diagnostics and comprehensive cleaning in place (CIP) support.

Designed to meet the industry's need for intuitive, visual solutions, BeerMaker will help to empower operators to manage their preferred operating procedures and have freedom to use the package on computers, tablet or mobile devices. Teams can gain greater process certainty by testing on a real-time digital twin, a complete and operational representation of the control system and a powerful tool for companies deciding on a new strategy to easily simulate new recipes.

SOURCE: ABB

Connectivity of plant processes will enable sustainable water and energy usage and drive effective digitalization in breweries.

Additional digital solutions based on ABB Ability™ Manufacturing Operations Management (MOM) have the capabilities to identify energy consumption, beer or extract losses and provide reporting functions and dashboard visualization. These include the ABB Ability™ BatchInsight concept, which can use big data analytics to identify process anomalies at the earliest stages. Operators and customer brewmasters will benefit from making decisions in real time to further improves processes, quality and productivity.

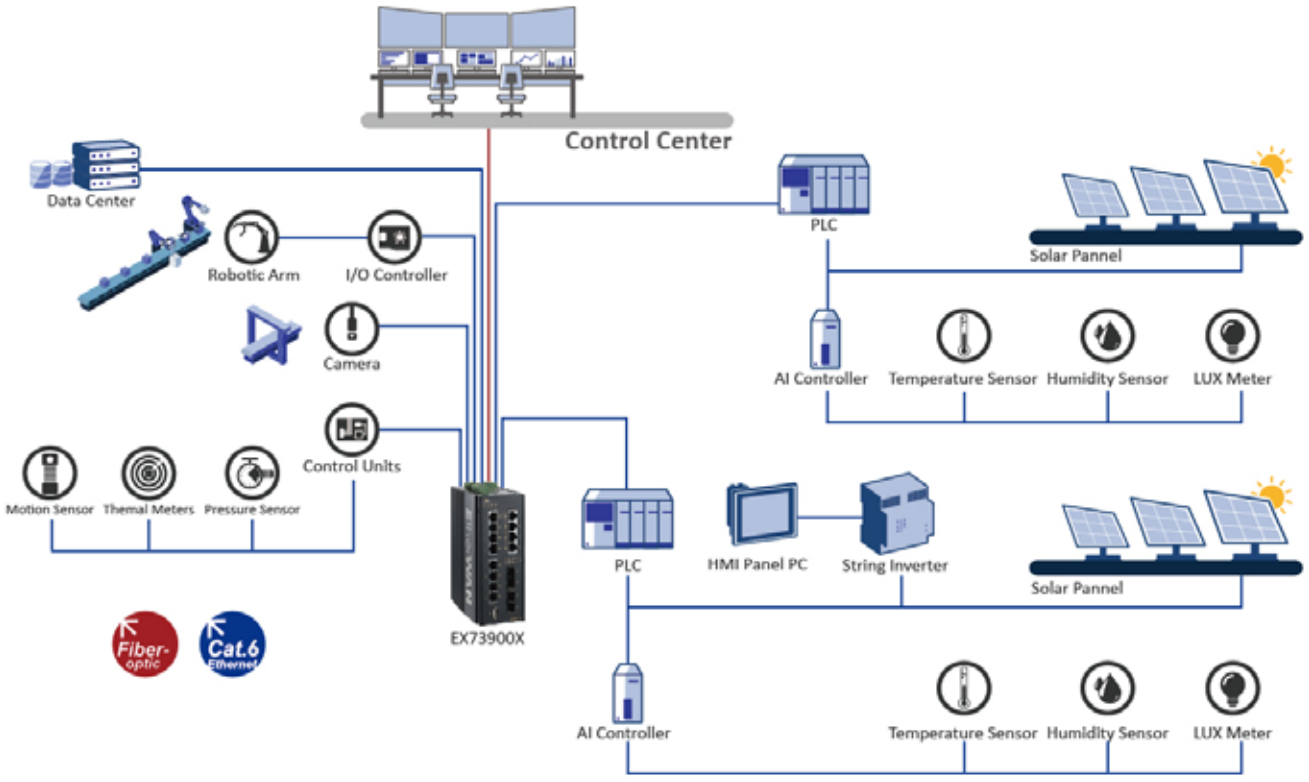
"Our new solution is from our own ABB brewmaster for brewmasters and truly has domain-specific knowledge embedded as well as ABB's expertise from years in this field," said Marcello Gulinelli, Global Head of Food and Beverage, Process Automation, ABB.

*Technology report by **ABB**.*

Visit Website

Layer 3 managed switch with 10G bandwidth

New managed switch from EtherWAN provides high bandwidth and high electromagnetic compatibility for industrial automation, machine vision, enhanced data, machine learning, and artificial intelligence.



SOURCE: ETHERWAN

The EX73900X's high bandwidth meets the requirements of Industry 4.0 architectures, edge-computing, machine vision, enhanced database, machine learning, and artificial intelligence.

EQUIPPED WITH UP TO 12 GIGABIT ETHERNET and 4 dual-rate 10 gigabit SFP+ ports, the EX73900X supports 10G transmission bandwidth, which corresponds to higher resolution image recognition and faster data transmission to meet the requirements of industrial automation, machine vision, enhanced data, machine learning, and artificial intelligence. It delivers a high bandwidth, low latency, and high electromagnetic protection solution.

Hardened design ensures reliable operation over a wide temperature range of -40 to 167°F, with support for an extended voltage range from DC 12V to 48V with redundant inputs, high levels of EMI immunity & up to 6KV surge Protection per port, ideal for harsh production environments with strong magnetic fields or unstable power supply.

With a slim, DIN-rail mountable design, the EX73900X is also IEC 61850-3, IEEE 1613 and NEMA TS2 certified, ideal for industrial Ethernet applications, national-scale public infrastructure, Intelligent Transportation Systems, and power substation automation.

As a Lite Layer 3 switch, the EX73900X offers many security features, as well as the routing functionality often needed in small to medium-sized networks for mission-critical applications in harsh environments. EtherWAN's built-in DnA (Detect and Alert) solution provides local risk prevention and instant response. It minimizes the risk of non-malicious network events and further increases network availability.

EtherWAN EX73900X managed switch.

The EX73900X's high bandwidth meets the requirements of Industry 4.0, edge-computing, machine vision, enhanced database, machine learning, and artificial intelligence.Faced with the exponentially increasing demand for data bandwidth in Industry 4.0 factory architectures, an increase in edge-connected devices, higher resolution cameras, and faster Wi-Fi access points, EtherWAN's EX73900X series with 10 Gb speeds ensure handling of data-intensive applications.

*Technology report by **EtherWAN**.*

Visit Website

IP67 managed Industrial Ethernet switch

Xelity 10 TX IP67 managed switch offers new possibilities for decentralized, cabinet free, data management.

With the new Xelity 10 TX IP67, Murrelektronik offers a line of robust, space-saving switches designed for the heavy traffic that comes with today's installations. The ten port switches are available in three models: 10 x 100 Mbit/s, 10 x 1000 Mbit/s, and 2 x 1000 Mbit/s + 8 x 100 Mbit/s. Each model can also be ordered specifically for a ProfiNet system.

Developed in-house, Xelity 10 TX IP67 is Murrelektronik's response to the desire for machine builders to replace classic control cabinet solutions with IP67 components in the field. The growing trend of decentralized wiring offers advantages that include significant space savings in the control cabinet as well as shorter cable runs.

Its L-coded M12 power connectors (4 or 5-pin) ensure fast connections as well as the ability to daisy chain several devices as long as the combined power usage does not exceed 16A. Each model uses the same drilling pattern and power connector connection. There are no specifications for grounding thanks to the free grounding concept. It can also be combined with other M12 power modules to create a single source power concept.

The IP67 rated metal housing allows the switch to be used in harsh industrial environments. It also offers faster and simpler fault detection, full topology flexibility as well as fast scaling and easy commissioning.

SOURCE: MURRELECTRONIK

With up to ten Gigabit ports in a robust housing, it represents a new standard in switches.

The range of models and simple installation and configuration make the Xelity 10 TX IP67 extremely versatile. The switch is ideal for machine builders, plant engineers and component manufacturers alike.

Thanks to its various expansion levels, users can easily adapt the Xelity 10 TX IP67 to specific applications.

Murrelektronik

Learn More

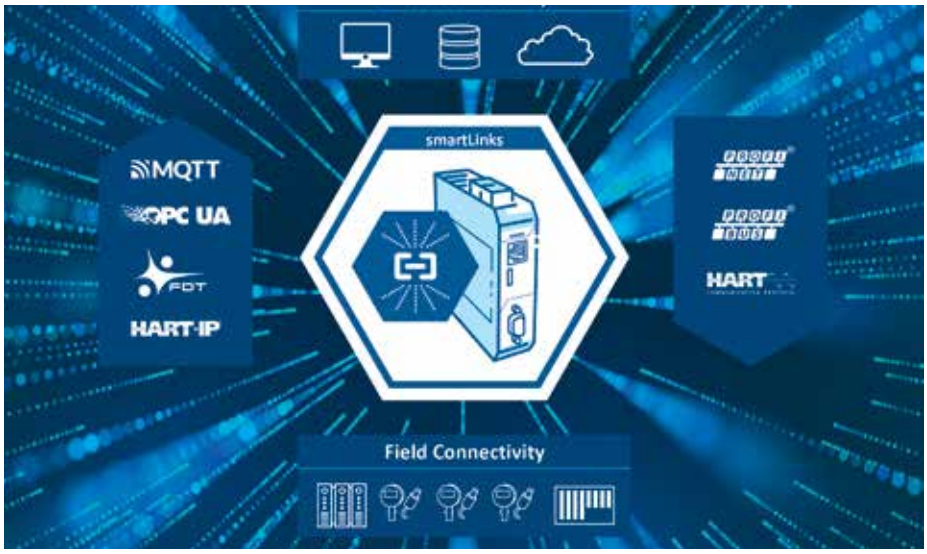
Plant asset management solution

Softing's smartLink product family offers extended functionalities for Plant Asset Management.

Two product releases from Softing's smartLink family offer enhanced functionalities for Plant Asset Management and the implementation of Industry 4.0 connectivity in industrial networks.

The smartLink product family from Softing enables end customers to make efficient use of connectivity at the interface between OT and IT. The products allow simple and scalable integration of device data into plant asset management applications. The new versions of smartLink HW-DP v1.20 and smartLink SW-HT v1.20, which are now available, offer enhanced functionalities for data transfer and connectivity.

smartLink HW-DP enables access to process, asset, and diagnostic data from PROFIBUS devices and HART devices connected to PROFIBUS remote I/Os, as well as secure export to any system inside and outside the user's own network. The new version v1.20 now adds support for providing asset and diagnostic data from field devices via MQTT. This allows easy integration into typical IoT system architectures, such as the Namur Open Architecture (NOA) or the IoT reference architectures of large cloud platforms.



SOURCE: SOFTING

smartLink SW-HT allows access to configuration and diagnostic data via Emerson's AMS Device Manager or other HART IP-enabled Plant Asset Management applications. As the only solution available on the market, smartLink SW-HT has so far supported Schneider Electric M580 controllers and drop I/Os as well as Allen-Bradley controllers and remote I/Os.

Softing

Visit Website

Gateways using AWS IoT Greengrass

Edge gateways extend cloud intelligence to the edge for IT and OT convergence.

SOURCE: ADVANTECH

Advantech's UNO series of IoT edge gateways have qualified for Amazon Web Services (AWS) Internet of Things (IoT) Greengrass, an IoT open source edge runtime and cloud service that facilitates the development, deployment, and management of device software. This means that the UNO series gateways (UNO-137, UNO-148, UNO-2271G V2, UNO-2372G, UNO-410, and UNO-430) are compatible with most mainstream cloud services and pre-built software components, providing platforms for cost-efficient local software development.

Integrated with AWS IoT Greengrass, the UNO series IoT edge gateways seamlessly extend AWS functionality and cloud intelligence to the edge. For example, with AWS IoT Greengrass, AWS Lambda functions and prebuilt software modules can be used to build edge applications for stream analytics, machine learning, image recognition, and other high-value AI applications that are deployed from the cloud to the edge for local execution. Similarly, Amazon SageMaker Neo DLR and TensorFlow Lite frameworks allow machine learning inference to be conducted at the edge on using cloud-trained models. This enables local devices to act on locally generated data, while storing, analyzing, visualizing, and decision-making tasks are conducted through the cloud, streamlining data processing operations and facilitating the convergence of OT and IT.

To support a wide range of IoT and automation applications, UNO edge gateways are equipped with multiple I/O for integrating secondary expansion stacks and Wi-Fi, LTE, and 5G connectivity modules that extend the system functions. UNO gateways also feature edge container technology that supports third-party container-native applications and allows cloud services to be deployed as decentralized computing resources.

Advantech

Visit Website

IP67 M8 Single Pair Ethernet connections

Solution offers uninterrupted connectivity from remote field devices to the cloud for increased uptime.

SOURCE: AMPHENOL

TTI, Inc. is now stocking Amphenol IP67 M8 Single Pair Ethernet (SPE) connections for rugged industrial applications. Engineers can benefit from uninterrupted connectivity from remote field devices to the cloud for increased uptime, but with a small M8-sized interface so they can reduce the size of their equipment.

SPE cables simplify the process of connecting and powering edge devices by extending the range and bandwidth of a single twisted pair. The cable supports Power Over Data Lines (PoDL) to 52W so both data and power can be delivered via a single wire pair, and it provides exceptionally fast data transfer of 1Gbit/s per twisted pair as well as a data rate of 1000BASE-T1.

SPE cable is up to 60% lighter in weight than a standard four-pair CAT 6 cable, meaning engineers can reduce the weight on their machine. The M8 interface is also approximately a third of the size of an M12 connector, so equipment size can be minimised.

The mechanical interfaces are all designed and made according to IEEE802.3bp standard offering and provide excellent reliability in harsh industrial environments so users can improve process efficiency. The IP67 M8 connection has a vibration resistance in the frequency of 10 - 2,000 Hz and delivers high levels of protection against the ingress of dust and liquids, including submersion in water up to 1 m depth.

Amphenol's SPE cables are available shielded or unshielded, and there are 4 connector options; M8 (screw thread), M12 (screw thread and Push-Pull), FLOS+ (Push-Pull) and X-Lok (Push-Lock).

Amphenol/TTI

Visit Website

MX-System offers cabinetless automation

Intelligent automation hardware system that can completely replace conventional control cabinets.

With pluggable IPC, I/O and drive technology modules from Beckhoff, the IP67-rated system delivers maximum space and time savings for machine builders and end users.

MX-System from Beckhoff is a flexible, space-saving and intelligent automation hardware system that can completely replace conventional control cabinets, creating entirely new levels of efficiency in plant automation. Control system installation processes that normally took 24 hours or more can now be completed in just one hour.

As a modular control cabinet replacement that can also be decentralized on the machine if required, the MX-System saves engineering, assembly, installation and maintenance efforts. This promotes highly efficient processes for the manufacturers and operators of machines and systems – from the planning, setup and installation of the MX-System through to the maintenance of MX-System-equipped machines.

The basic concept of the MX-System is to standardize the electrical and mechanical interfaces for all electronic and electromechanical components. This novel approach results in two interfaces:

SOURCE: BECKHOFF

The data interface integrates each functional module into an EtherCAT network and supplies it simultaneously with 24 V DC and, if necessary, also with 48 V DC.

A second interface has been defined as standard for the low-voltage range. These interfaces distribute the mains voltage of up to 480 V AC and a DC voltage of up to 600 V for the drive system.

This standardization means all functionality traditionally found in a control cabinet can be mapped in a backplane system.

Beckhoff

Learn More

Windows 11 22H2 in real time

RealTime Suite is comprehensive system library for hardware-dependent programming and communication.

Kithara Software, specialist for industrial real-time software, has announced the support for the upcoming Windows 11 version 22H2 with the real-time system Kithara RealTime Suite (KRTS). This will allow for the new version of Windows to be used as a real-time operating system already by the time of its release, which is expected for September 20.

As with Windows 11, extensive testing of the Insider Preview version have ensured support by Kithara RealTime Suite even before the release of version 22H2. This way, the latest Windows version can be utilized as an RTOS, meaning with "hard" real-time capabilities. This makes it possible to turn regular Windows PCs into efficient development and testing systems, which allow for the programming of sophisticated industrial functions in automation, machine vision and automotive fields. The simultaneous support for yearly Windows 11 updates with KRTS is expected to continue in the future due to exhaustive test series with the Insider Preview version.

The procedure to enable real-time capability for 22H2 is the same that have been used with previous Windows versions. Both the Kithara real-time system as well as the Windows OS are booted separately on user-defined dedicated CPU cores. From this point onwards, KRTS and Windows run parallel yet separate, without negatively impacting each other, benefitting from both the graphics and user interface of Windows and the performance properties of an RTOS.

SOURCE: KITHARA

Kithara

Learn More

Motor control MPU & Ethernet

Combines high performance motor control and TSN-Compliant Industrial Ethernet network on a single-chip.

The RZ/T2M combines fast and highly precise real-time motor control capabilities and the latest industrial Ethernet on a single chip, while also supporting functional safety operation. By providing all essential peripheral functions for motor control, the RZ/T2M enables customers to reduce the number of external components.

The RZ/T2M is built around two Arm Cortex®-R52 cores with a maximum operating frequency of 800 MHz. Connecting the peripheral functions used for motor control to a dedicated bus linked directly to the CPU enables the CPU to access these functions with low latency. In addition, the large memory capacity (576 KB) is tightly coupled with the CPU, reducing the fluctuation in execution time that can occur when cache memory is used and delivering deterministic, fast-response processing. These advantages enable the RZ/T2M to deliver rapid and highly precise control for applications such as AC servos, inverters, and industrial robots.

In addition to major industrial networking protocols such as EtherCAT, PROFINET RT, and EtherNet/IP, Renesas has added support for the PROFINET IRT protocol in the RZ/T2M. The new MPU also includes an Ethernet switch that supports the next-generation Time-Sensitive Networking (TSN) standard, allowing multiple devices to operate in precise synchronization.

SOURCE: RENESAS

Highest-performance RZ/T2M motor control MPU enables fast, high-precision control of servo motors.

In most cases, building industrial equipment that complies with functional safety requirements involves two external MCUs for safety monitoring, which increases BOM costs. The RZ/T2M has a hardware configuration designed with functional safety operation in mind, so only one external MCU is needed to implement functional safety.

Renesas

Visit Website

Test and validate IoT solutions

u-blox XPLR-IOT-1 enables end-to-end proofs of concepts for IoT products and applications.

The u-blox XPLR-IOT-1 IoT explorer kit is an all-in-one package to test, evaluate and validate IoT applications. Integrating all relevant u-blox technologies and services into a capable prototyping platform with a vast selection of sensors and interfaces as well as cloud connectivity, XPLR-IOT-1 makes it easier than ever to explore the potential of IoT applications.

The increasing complexity of IoT devices, which often require satellite-based positioning, Bluetooth low energy, Wi-Fi, and cellular connectivity via, for example, LTE-M is raising the importance of prototyping and validating ideas before bringing them to production.

The XPLR-IOT-1 gives users everything they need to prototype low-power IoT use cases such as logistics container trackers, industrial automation, sensor-to-cloud applications, and fleet management solutions. The board's u-blox NORA-B106 Bluetooth LE 5.2 radio module doubles as its main MCU, hosting the application software and controlling the other modules. These include a u-blox SARA-R510S for LTE-M and NB-IoT cellular connectivity with built in cloud security, as well as a u-blox NINA-W156 for 2.4 GHz Wi-Fi.

SOURCE: UBLOX

XPLR-IOT-1 makes it easier than ever to explore the potential of IoT applications.

The board also hosts an ultra-low-power MAX-M10S positioning module capable of concurrently tracking four global navigation satellite system (GNSS) constellations, delivering highly reliable location data wherever GNSS coverage is available.

UBLOX

Visit Website