10.2015 Issue 90
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Network Connectivity

www.iebmedia.com/ethernet www.iebmedia.com/wireless

Machine control networking in the Digital Enterprise

At the Hannover Fair several years ago, I distinctly remember an evening press conference that highlighted the future impact of the Internet of Things and Industry 4.0. Of course, there were many bold predictions made that night,but my lasting pondering was how this new wave of technology would impact the world of factory automation and machine control networking that I had covered as a journalist for years.

In many ways, the world of automation and machine control had been way ahead of its time when it came to device networking, remote connectivity, information sharing and IoT type functionality. But it was also clear from the beginning that the investments poured into IoT technology would bring positive change, rejuvenation and opportunity to the world of factory automation.

Anton S. Huber, CEO of the Siemens Digital Factory Division, wrote recently that he sees the industrial enterprise of the future primarily as a *Digital Enterprise*.

"Because many activities in a company are now supported by software, the task is to seamlessly digitalize the companies' core processes and the overall product development process and to support it with software tools. In the future, no part of this value chain will be able to do without its digital copy. This includes the product concept, the engineering of both product and production, commissioning, and use, as well as new services offered in the context of or on the basis of the product. The main aspect of a Digital Enterprise is that it has seamlessly and digitally mapped and linked the value chain processes."

I think Mr. Huber's viewpoint summarizes some of the primary impact that automation and control networking will see in the next decade and beyond. In the past, control networks have specialized in enhancing machine productivity and performance, and offered a level of connectivity within the enterprise.

But now with the emergence of the Digital Enterprise, the level of software, business and supply chain connectivity will be driven to new levels. End-to-end software integration of processes and new types of control algorithms focused on business rather than machine control problems will usher in new waves of innovation.

What I expect to see is an evolutionary move, already underway, driven by more processing power than ever before at the controller and device levels, and an even greater push to networking sophistication and connectness. The good news is that there has never been a better time to be involved in this industry.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **November 2015**
Deadline for editorial: October 2, 2015 **Deadline for artwork:** October 23, 2015

Product & Sources Listing

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

Update your own products

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

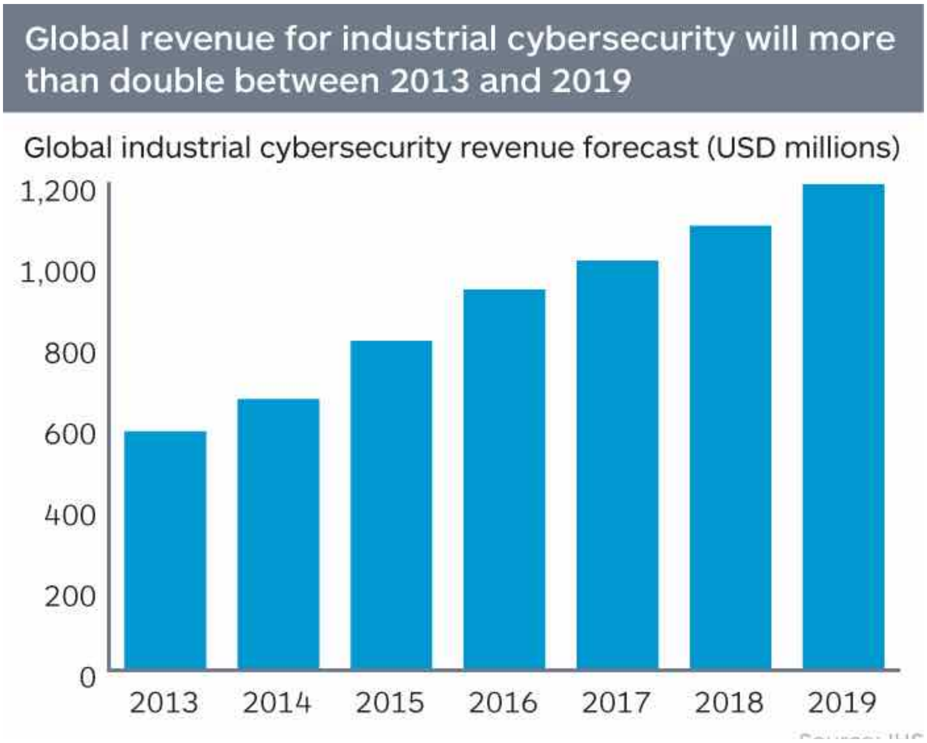
Do you want to receive issues of Industrial Ethernet Book? Call, mail or e-mail your details, or subscribe at **www.iebmedia.com/service/**

Editor: Al Presher, editor@iebmedia.com
Contributing Editor: Leopold Ploner, info@iebmedia.com
Advertising: map Mediaagentur Ploner, info@iebmedia.com
Tel.: +49-(0)8192-933-7820 · Fax: +49-(0)8192-933-7829
Online Editor: Adela Ploner. info@iebmedia.com
Circulation: subscriptions@iebmedia.com

Published by IEB MEDIA
IEB Media, Bahnhofstrasse 12, 86938 Schondorf am Ammersee, Germany
ISSN 1470-5745

New world of cybersecurity

Only $589 million was spent on industrial cybersecurity systems worldwide in 2013. But the potential for growth is huge, as cybersecurity strategies are developed to combat increasingly dangerous cyberattacks.



SOURCE: IHS

CYBERSECURITY'S MANDATE IS TO PROTECT and secure an organization's assets to ensure their continued availability, integrity, and confidentiality.

Yet many corporations still do not have strategic cybersecurity plans in place even as more devices are interconnected and virtually anything of importance is accessible from the Internet. Indeed, cybersecurity is becoming as critical as physical security precisely because of this ubiquitous interconnectivity through which cyberattacks can quickly spread.

The cybersecurity market remains small at present—just $589 million was spent on industrial cybersecurity systems worldwide in 2013. But the potential for growth is huge, especially as the world begins to craft coherent cybersecurity strategies to combat increasingly dangerous cyberattacks.

Cyberthreats & emerging technology

Cyberattacks are increasingly sophisticated as their destructive incursions seek new ways to breach security and inflict maximum damage. And in an age of increasingly porous digital borders, three areas pose grave challenges in the cybersecurity wars:

- The all-things-connected phenomenon known as the Internet of Things
- Cloud computing, or the online storage and repository of data
- The continuous churn of enormous amounts of information being gathered

The Internet of Things

In the coming years, billions of new devices from cars to household appliances will be fitted with computer chips that enable interconnectivity with the Internet. Experts estimate there will be nearly 50 billion connected devices by 2020, with an average of more than six connected devices per person.

There are three categories of cyber threats in the world of connected devices. On the lower end of the scale, denial of service is an immediate threat, potentially paralyzing all services offered by a network of smart devices. Higher up is the threat from botnets and malware-based attacks.

Here, a malicious code could infect computers in order to gain control of a network of smart devices, or to compromise the software running them, with the objective of converting the connected devices for heinous purposes. Lastly, data breaches can exploit the aggregation of valuable information resulting from the daily actions of individuals, in order to access private communications or expose sensitive data on the cumulative behavior of population subsets.

Cloud computing

Cloud computing enables convenient, on-demand access for individuals and businesses to a shared pool of computing resources including networks, servers, data storage, and other applications. But these very advantages represent an attractive target for cyberattacks. This is because an attack on a stand-alone system is ultimately less dangerous than an attack on a networked model like the cloud, which could result in a cascade of failures across the network.

Big Data

Big Data exploits the reams of data cascading over the Internet, driven in part by the growth in social media and mobile devices, in order to identify underlying patterns and trends. From a security perspective, Big Data allows companies to observe the larger threat picture against enterprises, incorporating internal and external threats. By pooling internal data and relevant outside information to correlate high-priority alerts across monitoring systems, companies can cut down on the noise and false alerts endemic to monitoring tools.

For these reasons, Big Data is not so much another vulnerability but a tantalizing new opportunity for corporate players to take proactive measures against cyberthreats. A Big Data paradigm can efficiently log information, events, and activities occurring within a preselected tracking environment; consolidate data in a central location; and use advanced analytics to help identify patterns that no individual monitor can do on its own, in the process creating a holistic picture to analyze and investigate security-related issues.

The way forward

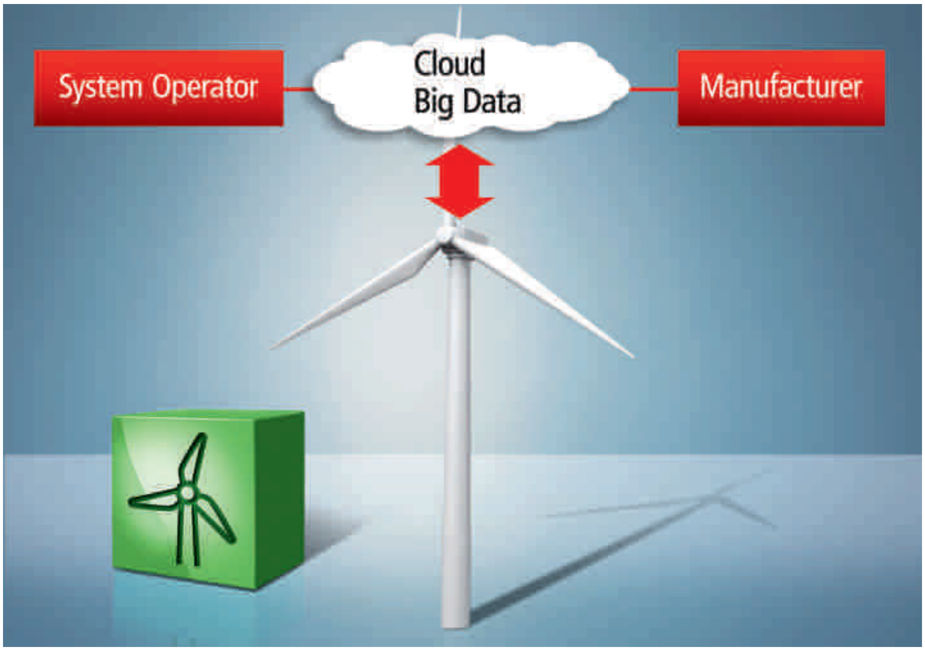
Cyberattacks have become a pervasive peril to businesses, so managing the risks must become a priority. But understanding the challenges and implementing appropriate strategies for the long term requires resources and expertise. The threats are evolving as are the tools and technologies. To manage the emerging risks successfully, it's useful to keep three things in mind:

- Cybersecurity is a corporate imperative.
- Government and industry must enhance their collaboration in identifying, assessing, and responding to cyberthreats.
- Finally, cybersecurity is too important to be left to technology or security specialists alone.

Thomas Lynch, Christoforos Papachristou and Dennis Murphy work for ***IHS.***

Industry 4.0 gaining a foothold in wind farms

Advanced software technology improves operational efficiencies by incorporating all basic functions from management through the state machine, event management and a database connection to simulations.



SOURCE: BECKHOFF

Industry 4.0 technologies are enabling manufacturers of wind turbines to simplify operational management .

MODULAR SOFTWARE that includes all of the necessary functions and tools for the modern and efficient engineering of wind turbines, now allows users to quickly and easily develop their own operational management.

The new framework incorporates the consolidated control expertise from the over 40,000 wind turbines around the world that have been automated using the technology, plus experience gathered during ten years of customer-specific development in the wind industry.

Modular wind turbines

It is already standard practice to modularise the mechanical and electrical elements of wind turbines. Now, TwinCAT 3 Wind Framework technology provides corresponding modular software technology where all basic functions in TwinCAT 3 have been implemented as TcCOM modules which means that the functionality is encapsulated in function blocks that constitute a “programming kit”.

This simplifies developing the application software, and also makes it safer and more flexible. Individual software modules can be added or removed in the same way as hardware modifications are carried out. This makes the engineering process as simple as possible, so that developers can focus on the actual system functions. Customised modules can be developed and tested in parallel, which further reduces time-to-market.

From Industry 4.0 to Wind 4.0.

In its TwinCAT 3 Wind Framework, Beckhoff is making use of both the Industry 4.0 concept and its own experience and expertise in the wind sector. Big Data facilitates the comprehensive real-time collection, analysis and provision of data from Condition Monitoring and power management. All this data is continually recorded, accumulated in the central controller and evaluated. Wear and tear on individual components of the wind turbine installation can be detected at an early stage, increasing system availability.

Support for all common bus systems, such as EtherCAT, Ethernet and PROFIBUS, plus complete connectivity via ADS, OPC UA, live diagnostics, etc., guarantee secure vertical and horizontal communication.

The available programming languages for object-oriented, modular programming are IEC 61131-3, plus C/C++ and MATLAB/Simulink. In line with the Industry 4.0 concept, the engineering process is automated and the engineering tools are able to exchange data. The software technology incorporates all basic functions from management through state machine, event management and database connection to simulations.

Report by Beckhoff Automation.

PLCopen Coding Guidelines: comments published for feedback

In 2013 a working group was started to create guidelines on the software construction process with a focus on IEC 61131-3 and the PLCopen extensions. The goal of this new working group is to provide the definition of Rules, Coding Patterns and Guidance how to use them in industrial automation.

PLC coding guidelines

Although there are coding guidelines for many programming languages, these are nearly non-existent for the important area of industrial control, e.g. IEC 61131-3 and its PLCopen extensions. Nevertheless, as software in the industrial environments becomes more and more important, the software projects become larger and the costs of errors increase. Software nowadays absorbs half of the initial project costs and between 40 to 80% deals with maintenance over the life cycle costs of the software.

Large automation companies have their own rules but many mid-size companies or newcomers are very interested in a helping hand as provided by these PLCopen guidelines. The rules will be very useful to train users and can be a good basis for universities to help them teach IEC 6113-3 programming more efficiently.

As a first result of this PLCopen working group, the Release for Comments of the Coding Guidelines is now published. PLCopen invites all interested parties to give feedback on this document until October 23, 2015.

www.PLCopen.org

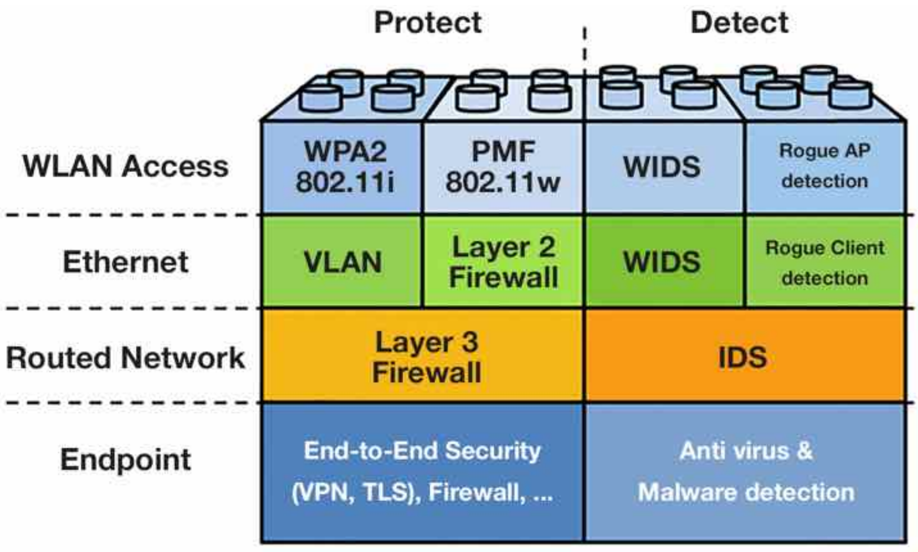
eltromat tradition meets innovation
SEW EURODRIVE
COMAU
CONTROL TECHNIQUES
HEIDELBERG
ADVANCED MOTION CONTROLS
Maxsine
DORNIER
Trusted ePlatform Services ADVANTECH
FLSMIDTH
TEXAS INSTRUMENTS
port
battenfeld-cincinnati
saia-burgess
DENSO DENSO WAVE
MAILLEFER
Bihl + Wiedemann THE AS-INTERFACE MASTERS
Innovasic
B&R
elobau sensor technology
COPALP
makro labelling
DUKANE www.dukane.com/us
XILINX
Lenze
softing
AMADA
general system pack
YASKAWA
PEAK System
KUNBUS industrial communication
FEDEGARI
KEB
ALFA LAVAL
FERROMATIK MILACRON Europe
MESCO Engineering
MABI
ETHERNET POWERLINK
HMS
SYS TEC ELECTRONIC
INDEL
hilscher COMPETENCE IN COMMUNICATION
Schneider Electric
NORD DRIVESYSTEMS
CONTRINEX
kw software
ABB
lika
LAUMAS ELETTRONICA
ASCO numatics
POSITAL FRABA
HARTING
Starlinger
COGNEX
IMA Sharing Passions
bihler
UTECO GROUP
Baumer
SICK
YOUR WORLD OF SENSORS
JOKER
NETSTAL
CREVIS
MTS SENSORS
TR electronic
FESTO
ETHERNET POWERLINK
sepro ROBOTS AUTOMATION SERVICE
kalycito Your R&D Partner
embeX Your embedded experts
IXXAT Member of the HMS group
XMOS
NewTec System-Entwicklung und Beratung
INFRANOR
RENESAS
ALSTOM
EATON Powering Business Worldwide
OSADL
SMC
MILACRON
DATALOGIC
zhaw
WALLNER AUTOMATION
Bottero Glass Technologies
ALTERA
Danfoss
KUKA
www.ethernet-powerlink.org
SIKO
Indu Sol Industrial Solutions
STÄUBLI
LTI MOTION KÖRBER SOLUTIONS
Over 3,200 OEMs

Two pillars of secure wireless network design

Protection and detection of industrial control networks are objectives that require multiple, differentiated and threat-specific layers of defense. For a secure network, the IEEE 802.11i standard specifies procedures for key negotiations, data encryption and verification for transmission of user data within a WLAN.

SECURITY IS ALWAYS TOP OF MIND for industrial applications managers. However, too often, security discussions revolve around the need for encryption mechanisms. Modern security measures offer much more than data encryption alone. Central access control systems, intrusion detection, firewalling, and the protection of management frames are all vital components of an engineer's tool kit for protecting wireless technology against threats to confidential data or intrusion by an attacker.

Industrial control systems (ICS) security requires the deployment of multiple layers of protection to guard critical assets. Through a Defense in Depth (DiD) approach, overt, unintentional, external and internal threats can be detected, isolated and controlled, delivering a far more effective strategy than simply encryption for reliable ICS security. To effectively protect against network threats, there are a handful of critical security mechanisms that system administrators need to know and keep at their disposal.



	Protect		Detect	
WLAN Access	WPA2 802.11i	PMF 802.11w	WIDS	Rogue AP detection
Ethernet	VLAN	Layer 2 Firewall	WIDS	Rogue Client detection
Routed Network	Layer 3 Firewall		IDS	
Endpoint	End-to-End Security (VPN, TLS), Firewall, ...		Anti virus & Malware detection	

SOURCE: BELDEN

Protection and detection schemes use diverse technologies to secure WLAN, Ethernet, routed networks and endpoints.

Identifying security needs

Communication with wireless local area networks (WLANs) opens up a variety of new opportunities for industrial applications, but also introduces new risks to the networks that rely on it. Mission critical applications can't cope with even the shortest amount of downtime or disruption on the network. A small bump in operation can have a deep and negative impact on the bottom line, which unfortunately invites attackers to target control and monitoring mechanisms.

IT administrators typically value data confidentiality over reliability of the network, and will shut down the system in the event of an attack to prevent information from being leaked. If the same method was applied by operational technology (OT) managers, an improper shutdown could paralyze the entire network, defeating the purpose of security measures. Uptime, availability and proper control of the processes in the plant are the main and most important concerns for OT managers.

It's important to consider what actions are required and what type of security is needed to protect an industrial wireless network from both internal and external threats.

Defense in depth principles

It's unwise to rely on a single point of defense for network security, since attackers would only need to break down one defense mechanism in order to enter and make changes to the network.

Defense in Depth, a holistic approach to security that ensures all around infrastructure protection through multiple overlapping layers of security controls, is built on three core concepts:

1. *Multiple layers of defense*: A variety of security solutions are used so if one layer is bypassed, another will provide the needed defense.
2. *Differentiated layers of defense*: Each security layer is slightly different so an attacker can't automatically get through all layers of defense.
3. *Threat-specific layers of defense*: Each defense is designed for the specific context and threat, allowing protection based on the behavior and context of the systems using these protocols.

In addition to considering the strength of the defensive security mechanisms, it is essential to detect if one of these mechanisms is under attack or has been compromised. Hence, prevention and detection have to work in conjunction with one another.

IEEE 802.11i and WPA2

Protecting company data is even more challenging in a wireless networking environment, as a WLAN can exceed the company's property boundaries. As a result, attackers don't need direct, physical access to an industrial network in order to interfere with its operation and capture critical and confidential information.

To establish both the confidentiality and integrity of the network, the IEEE 802.11i standard specifies procedures for key negotiations, data encryption and verification for transmission of user data within a WLAN. Industry regulations require all current products be equipped with this basic -- but strong --protection, regardless of the vendor.

With this standard, pair-wise encryption keys are present between the communication partners, and built-in integrity protection ensures the transmitted data is not only confidential, but also unchanged. This ensures the control system is authentic and attackers can't extract sensitive data.

The manufacturer's association Wi-Fi Alliance has integrated this specified architecture according to IEEE Standard 802.11i into its own procedure known as Wi-Fi Protected Access 2 (WPA2). In this procedure, there are two modes requiring authentication: personal and enterprise.

Reliably Control and Monitor Your Plant
SEL-2730M MANAGED ETHERNET SWITCH
SEL-3530 REAL-TIME AUTOMATION CONTROLLER
SEL-3620 ETHERNET SECURITY GATEWAY
SEL-3610 PORT SERVER

SEL-2730M Ethernet Switch

Fast – Industry-leading network healing times minimize dropped or delayed packets.

Secure – Comprehensive security features allow only authorized access to network.

Intuitive – Easy to install and configure for non-IT personnel.

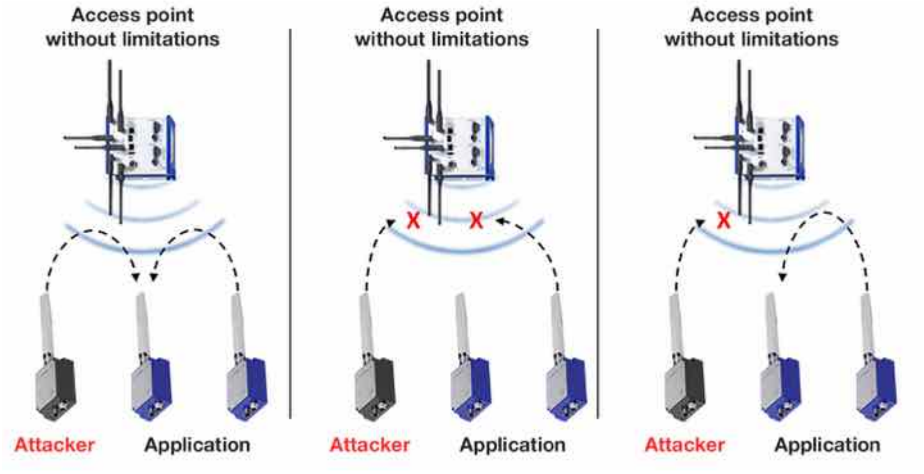
Rugged – Designed to operate in harsh environments.

SEL-2730M Managed 24-Port Ethernet Switch
Made in the U.S.A.

Learn more about SEL's communications solutions at www.selinc.com/2730M-ieb9.

SEL

- Using WPA-Personal mode, there is one common password for all WLAN devices. This password is pre-configured individually for all devices and access points (practical for small networks).
- The WPA-Enterprise mode allows the administrator to assign each device a different key, and manage those keys in a central authentication database. The access point can validate every WLAN device individually, and it's possible to configure a unique key for every device and manage it in the database. Passwords can be managed centrally, and lost or stolen devices can be disconnected from the network by removing their information from the database.


Access point without limitations
Access point without limitations
Access point without limitations
Attacker
Application
Attacker
Application
Attacker
Application

SOURCE: BELDEN

Client isolation or a Layer 2 firewall on an access point offers a level of protection from attackers.

Protected management frames

The management functions of a network are controlled by management frames, which are exceptionally vulnerable to forgery and wiretapping. These network packets are transmitted wirelessly, like data packets, but instead of containing user data, they organize the internal operation of the network.

Devices can use management frames to log on and off the network, initiate new key exchanges and report when they roam from one access point to another. Information can therefore be captured from wiretapped management frames, and forged management frames can be sent out with a wrong sender identity. This helps attackers disrupt the operation of the network by disconnecting a victim device from the network.

To combat such attacks, Protected Management Frames (PMF) encrypt and protect management frames against forgery and make it impossible to misuse the sensible management functions to attack a network by extending the mechanism for authentication and encryption present in WPA2 to management frames.

Limiting communication

Even the most effective WLAN encryption doesn't offer protection when the attacker is an insider. By selectively limiting communication to only what is required to run the industrial application, administrators can establish additional barriers that deter internal attacks from extending their influence. This type of limitation is another Defense in Depth mechanism which considerably increases the all-around security of a network. A few tried-and-true strategies for limiting communication within the network are:

- *Suppress all communication between all connected clients*, isolating all clients from one another. While this can work well in enterprise applications, it's often not applicable for industrial networks because the connected WLAN clients may have to directly relay information in order to operate and monitor plants.
- *Implement a configurable Layer 2 firewall on the Ethernet level*. The firewall will selectively filter traffic between WLAN clients and limit the allowed traffic to specific peers or protocols. This approach enables finer and more flexible control on a per protocol basis.
- *Install an intrusion detection system (IDS) for Ethernet traffic*. The system can identify clients showing erroneous, suspicious or unusual behavior, meaning an attack on the inside of the network can be recognized and recorded.
- *Conduct a stateful deep packet inspection* (DPI). Inspection can restrict communication to certain peers, protocols and even protocol behaviors. Logical relations between the devices belonging to an industrial application can be modeled and enforced.

Detecting anomalies

In wireless applications, operations and communication aren't observable by users, as many processes are performed automatically and are completely invisible. These processes make it difficult to recognize attacks and suspicious user behavior and take the appropriate corrective action. Wireless solutions must therefore be able to quickly detect anomalies in communication before the attacker can affect plant operations.

A wireless intrusion detection system (WIDS) in the access point can detect and report a wide range of suspicious behaviors, such as whether an attacker scans for open networks, forges management frames, or tries to impair network communication by forged authentication messages. The WIDS can record these behaviors and inform the user of them, for example, by email.

A regular IDS can identify suspicious activity within the network. Even simple IDS functions can be very efficient in industrial networks because often, the traffic patterns in the network are predictable. This makes it easy for the IDS to detect suspicious behaviors.

Environment awareness

Two other dangerous situations for wireless networks do not concern the protected company network but relate to other unsanctioned or counterfeit networks. Being aware of the wireless environment is therefore essential for thwarting the following threats.

Rogue access points are access points that provide unsanctioned and insecure access to the production network. For example, an employee who would like to use private wireless devices at his workplace may choose to connect his own – potentially unsecure – access point to the wired network, effectively creating an uncontrolled and potentially insecure entry point for attackers.

Wireless Phishing, or WiPhising, establishes access points near the WLAN network that provide nearly identical wireless services in the proximity of an industrial network in order to lure WLAN clients into a fake network. The fake access points use the same network name or service set identified (SSID) as the industrial network, but often without password protection, leaving the devices vulnerable to disclosing sensitive data.

Both of these attacks stem from the same problem: insufficient awareness of the wireless environment. Without active monitoring, the environment of a wireless network remains largely invisible until actual problems appear. Operators need complete insight into their networks in order to defend against these threats.

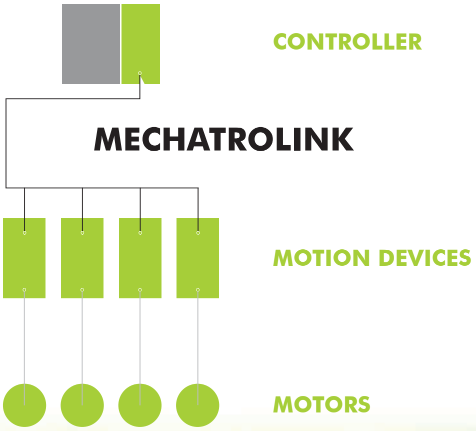
There are many options for securing WLAN networks against both external and internal threats. Each security mechanism described here serves a different purpose and should be used in conjunction with one another to create a holistic construction kit for ICS security. When these features are combined in a single device, they create a flexible and powerful security tool, forming multiple layers of defense against all possible threat sources.

Tobias Heer is manager of embedded software development – functions for ***Belden.***

MECHATROLINK MEMBERS ASSOCIATION

MECHATROLINK

... ANYONE CAN USE IT



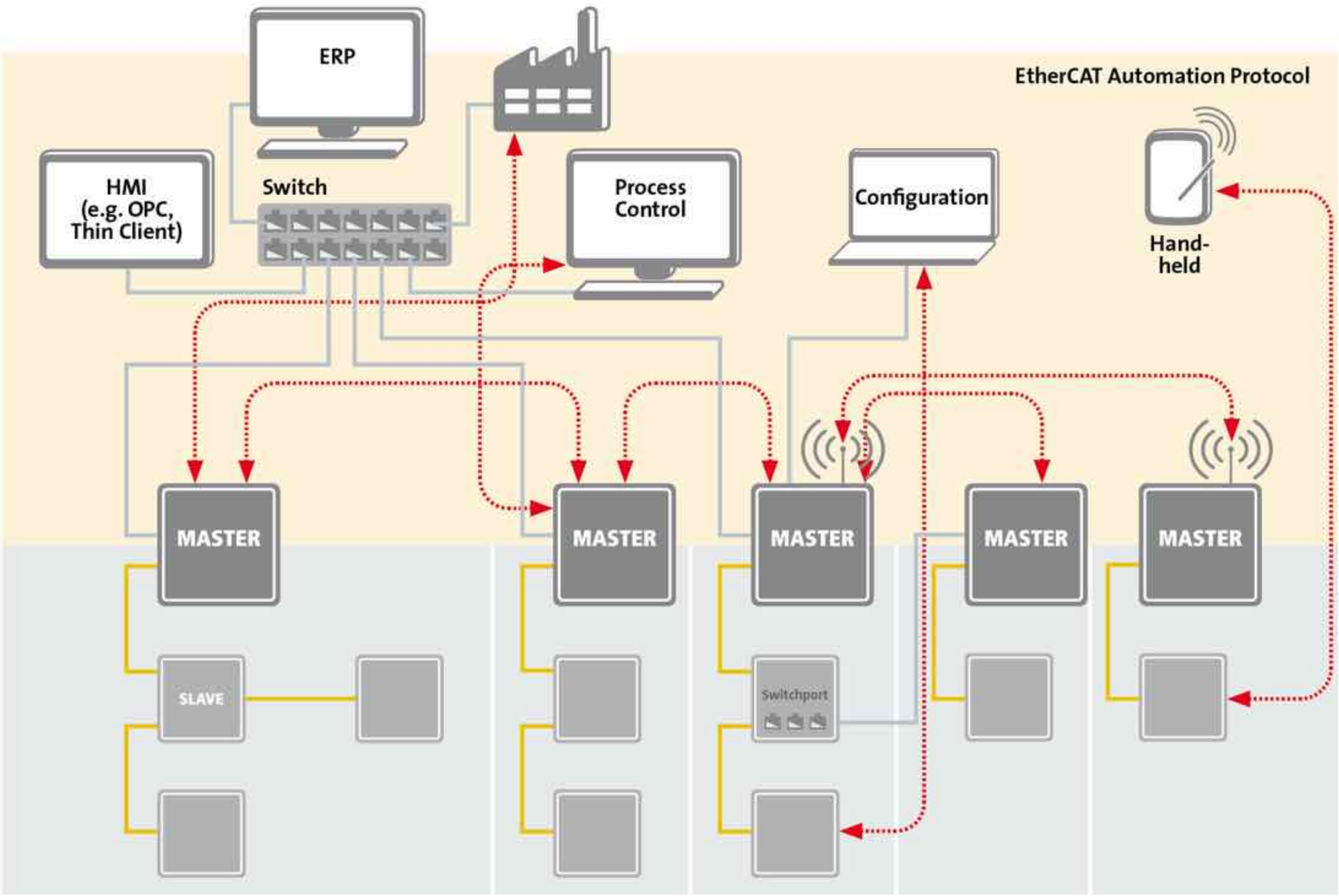
MECHATROLINK is an open field network that connects a controller with a wide variety of motion devices.

JOIN THE MECHATROLINK MEMBERS' ASSOCIATION TODAY AND START BENEFITTING FROM OUR 1500-PLUS MEMBERS NETWORK.

www.mechatrolink.org

EtherCAT Automation Protocol

The EtherCAT Automation Protocol (EAP) enables performant, cyclic communication between controllers via a standard Ethernet network. It supports routing into EtherCAT fieldbus networks down to the single slave device for implementing effective system parameterization, diagnostics and firmware updates.

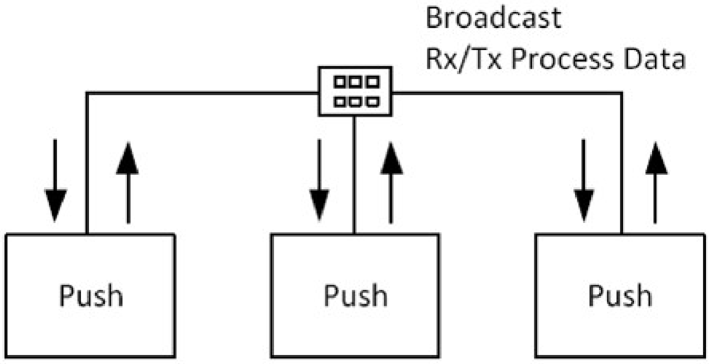


SOURCE: ETG

The EtherCAT Automation Protocol (EAP) is intended for communication between controllers and enables autonomous controller operation, often with different local cycle times. EAP adopts a publisher-subscriber (Pushed Data Exchange) model rather than the master-slave approach implemented using the EtherCAT Device Protocol.

THE ETHERCAT PROTOCOL has become a worldwide, established technology for real-time master-slave communication between controllers and field devices, enabling unique benefits in terms of low cycle times and highly precise synchronization. Many plants and machines currently consist of several machine units with discrete controllers, which perform different control tasks, yet need to work in close cooperation with one another.

The EtherCAT protocol with its unique operating principle, processing datagrams on-the-fly, has become one of the most widespread Ethernet-based communication standards at the fieldbus level in the past 10 years. It is certainly the most used technology in terms of different vendors and device types which feature support for the protocol. The EtherCAT protocol (also named as EtherCAT Device Protocol or EDP) is specifically intended for hard real-time communication between a controller and a variable number of field devices such as I/O, servo drives, servo valves, or gateways. It ensures very low cycle times (down to tens of µs), due to efficient bandwidth usage, as well as a very high degree of synchronization between the devices connected to the network (down to hundreds of ns).



SOURCE: ETG

EAP has adopted a publisher-subscriber (Pushed Data Exchange) model where each EAP device which intends to provide data is configured as Publisher, and transmits the data onto the network.

Many plants consisting of several process operations, with each containing some degree of independence, can be individually managed by a controller to which different field devices are connected. These controllers often need, in turn, to exchange cyclic as well as acyclic data with each other. The EtherCAT Automation Protocol provides an efficient mechanism for cyclic data exchange at the plant level, with communication cycle times in the low single digit millisecond range.

Additionally, acyclic communication for parameter exchange and information routing to single EtherCAT Device Protocol fieldbus networks is supported. These features make EAP a particularly suitable solution for machine builders that need modular plant architectures, where several controllers each take care of specific functionalities, yet need to communicate with each other in order to efficiently and harmonically cooperate to advance the overall work of the plant.

EAP – Communication

Intended for communication between controllers, EAP enables autonomous controller operation, often with different local cycle times. The master-slave approach used by the EtherCAT Device Protocol is no longer optimal, but instead, EAP adopts a publisher-subscriber (Pushed Data Exchange) model.

Each EAP device which intends to provide data is configured as Publisher, and transmits the data onto the network. One or more Subscriber devices can "intercept" the Ethernet packets sent by Publishers and use the corresponding data. Data can be published based on a cyclic event (with a periodicity which can correspond to, or be a multiple integer of, the cycle time of the Publisher device) or on a value change. Publisher devices can configure the transmitted information as unicast (only one specific Subscriber can receive this information), multicast (a subset of Subscribers is defined), or broadcast.

As an alternative to the Pushed Data Exchange, EAP also supports a Polled Data Mode. In this case, the polling device sends output data to one (1:1 connection) or several subscribers (1:N connection) and triggers the polled device(s) to provide data accordingly. The amount and type of data which can be transmitted over EAP is arbitrary. Base data types, as well as structured variables, can be transmitted and received.

Information is provided by the sender together with a 16-bit cycle field (updated with the cycle time of the sender device). This is incremented every time the information is transmitted. Receivers can use this field as a sequence number, in order to check if one or more packets were lost during propagation. In addition, each receiver associates a 16-bit quality field (updated with the cycle time of the receiver device) to the incoming information, reporting the time elapsed after the information is received for the last time. Using diagnostic variables, EAP receiver devices are able to monitor the real-time performance of the communication, and to suitably react in case of communication errors.

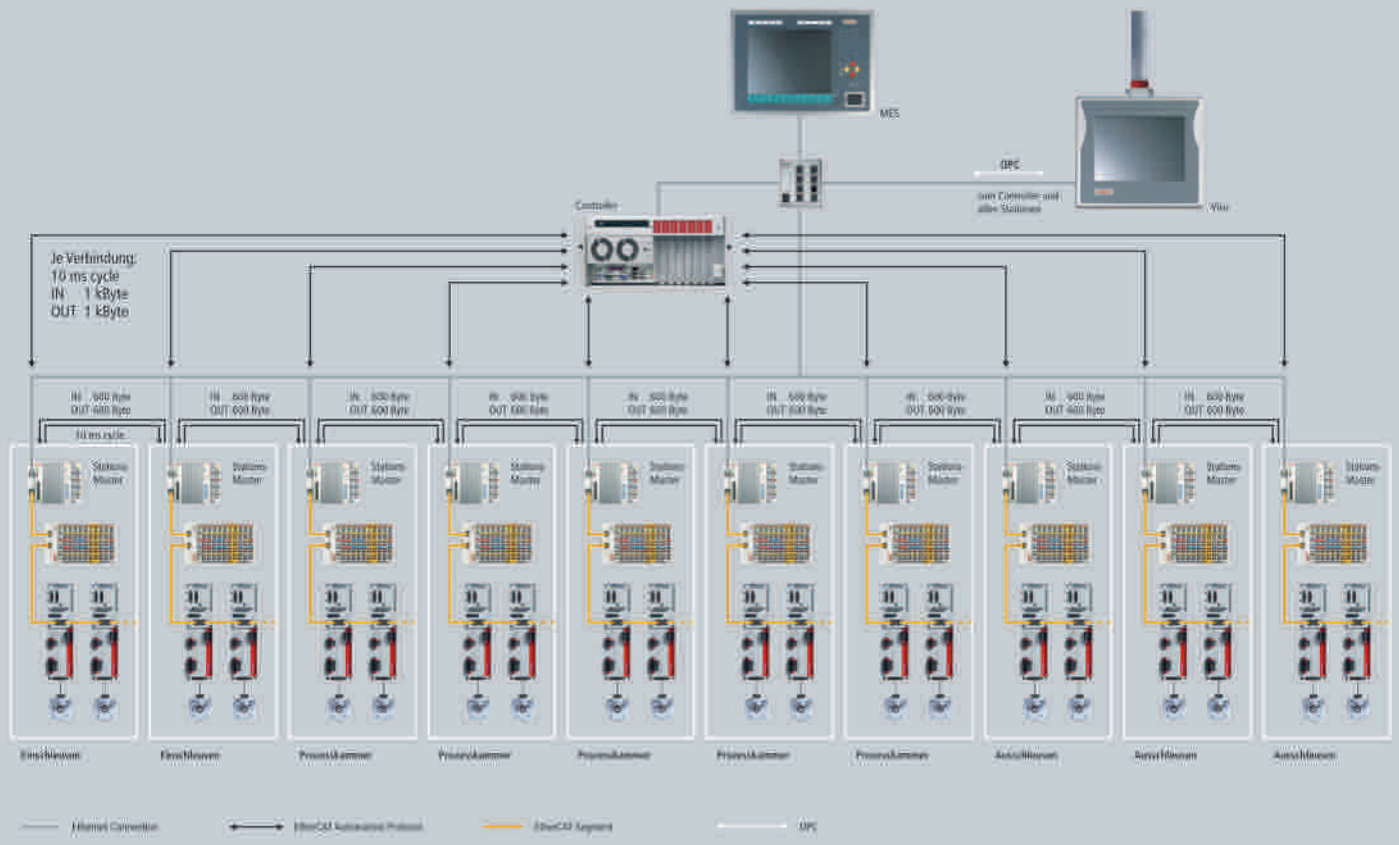
Low hardware requirements

Due to the reduction in real-time constraints required by the communication at the plant level, EAP devices require no dedicated chips (like the EtherCAT Slave Controller for EtherCAT Device Protocol) at all: frames are no longer processed on-the-fly, and the hardware interface is represented by a standard network port. Thus a standard, switched network communication infrastructure can be used with EAP – wireless connections between endpoints are supported as well.

EAP data can be transmitted highly efficient on raw Ethernet frames (if no routing outside the Local Area Network is needed) or mapped into UDP/IP packets (and therefore routable via IP protocol also outside the single subnet). The EtherCAT Automation Protocol can also be transmitted in parallel to other network-based protocols like OPC UA, HTTP or FTP, improving the vertical integration of the communication architecture.

Cyclic and acyclic communication

Besides cyclic communication, EAP supports the possibility to exchange acyclic information, as well, using the AoE (ADS over



SOURCE: ETG

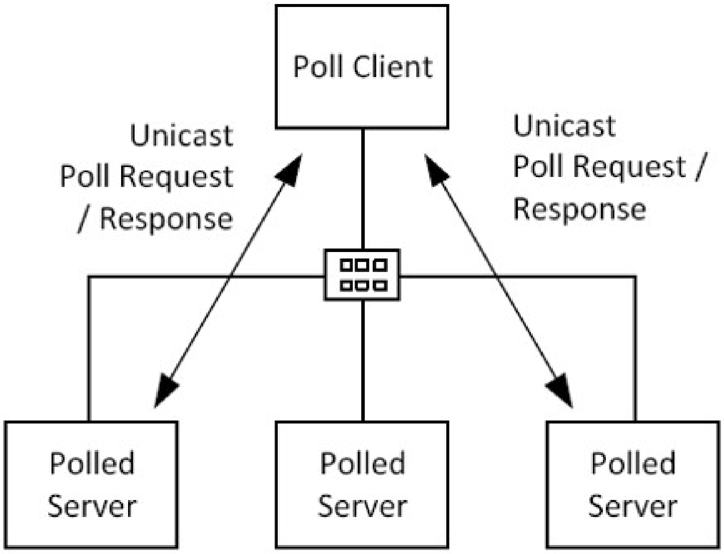
For solar panel production with multiple steps, data exchange among different control units can be implemented over EAP. Every station exchanges status and control information in each direction. Vertical communication to the HMI and MES systems can be achieved using OPC UA in parallel to the cyclic EAP communication.

EtherCAT) protocol. Each EtherCAT EAP or EDP device is identified by a unique AoE address, and information can be routed from one AoE device to another. All the commonly used Mailbox protocols, such as CoE, SoE or FoE (CAN application protocol, Servo drive profile or File transfer over EtherCAT), can be mapped into the AoE telegrams and routed from one EtherCAT controller to another. In this way, configuration and diagnostic tools can send and receive acyclic data, which will be used to configure specific controller properties, or route into the EtherCAT Device Protocol networks, reaching single slave devices for parametrization or diagnostic purposes.

Co-existence with OPC UA

A function of its real-time performance, extended diagnostic capabilities, and the possibility to be transmitted in parallel to other protocols on a traditional network infrastructure without specific hardware requirements, EAP represents a perfect intermediate layer between the fieldbus level and the IT world, distinguished by hard real-time requirements in terms of determinism and synchronization.

In the last few years, protocols such as OPC UA have been established as vendor-independent standards for data exchange at the plant level. From this point of view, EAP should not be seen as alternative to OPC UA, as much as a complementary technology.



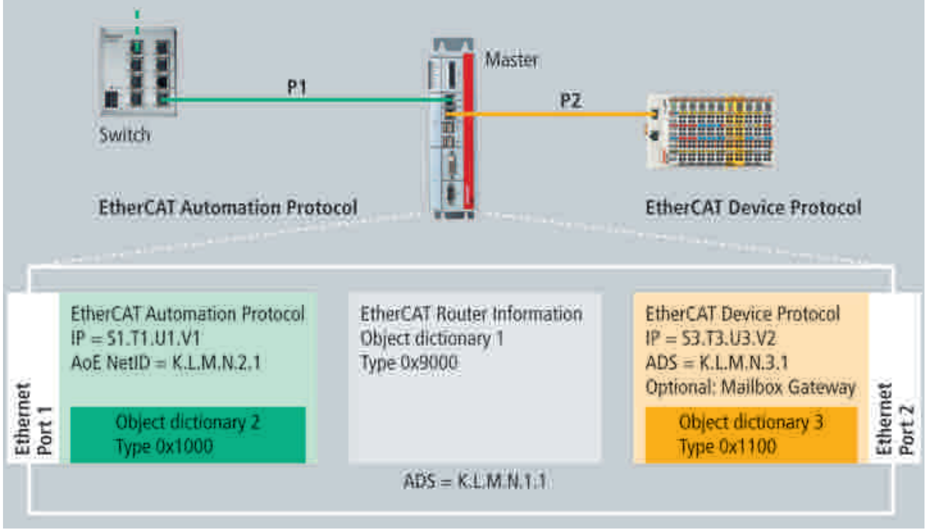
SOURCE: ETG

EAP also supports a Polled Data Mode. Polling devices send output data to one or several subscribers .

While OPC UA is particularly suitable for the vertical integration between the real-time control layer and high-level, geographically distributed client applications like HMIs or databases, benefit from the ability of EAP to set itself at a slightly lower level, primarily intended for the horizontal integration among different controllers. The two protocols can coexist on the same hardware infrastructure, in order to flexibly fulfil the communication needs of the most diverse plant architectures.

Application example

The production of solar panels consists of steps for identification and marking, as well as testing units and special handling modules. The transport system is divided into process isles, up to 14 in this application, and each segment is equipped with a control and an operating unit. Operating panels can also be connected to the system, in a variable number according to process needs and at the necessary point in the production line.



SOURCE: ETG

EAP supports exchange of acyclic information using the AoE (ADS over EtherCAT) protocol. Each device is identified by a unique AoE address, which allows information to be routed from one AoE device to another.

The data exchange among the different control units is implemented over EAP. Every station exchanges status and control information in each direction, both with the preceding and with the following unit: 600 bytes in each direction with a cycle time of 10 ms. Moreover, each local control unit exchanges 1000 bytes of data in each direction with the central unit, at the same cycle time.

Vertical communication to the HMI and MES systems is done via OPC UA in parallel to the cyclic EAP communication. Both technologies complement one another perfectly: EtherCAT as the real-time-capable Ethernet fieldbus for machine and plant controls, leveraging the EtherCAT Automation Protocol for lean data exchange between masters, and OPC UA as a platform for scalable communication with integrated Security by Design, enabling encrypted data transfer up to MES/ERP systems and into the cloud.

Conclusion

Recent technical developments in automation point to a steadily increasing vertical integration of the communication standards at the fieldbus and plant levels with IT technology. The establishment of concepts like Industrie 4.0 or Internet of Things (IoT) confirms this trend. In this scenario, the EtherCAT Automation Protocol, as specified by the EtherCAT Technology Group, represents an important intermediate layer between the fieldbus and web-based technologies.

It enables cyclic communication between controllers, with excellent real-time capabilities and extensive diagnostic capabilities using standard Ethernet networks as the hardware infrastructure. It also allows the transmission of other IP-based protocols in parallel, as well as supporting acyclic communication mechanisms. These can be seamlessly routed into the well-known EtherCAT fieldbus networks for efficient configuration and rich diagnostic functionality.

Alessandro Figini, Technical Support and Test, works with the ***EtherCAT Technology Group.***

Customized production: even down to one-unit lots

Integrated industry is developing as a manufacturing process driven by six fundamental trends: modularization, identification, integration, digitalization, miniaturization and customization. Data integration and network management are the keys to these new end-to-end production systems.

DEVELOPMENT OF THE INTERNET OF THINGS and Services is having a major influence on our society, a very wide range of industrial sectors and our daily life. The change processes are already in full swing and can be experienced in the use of diverse products (such as smartphones and wearables) and services (Web shops and streaming services). This development is a permanent phenomenon and one that will lead to completely new products, services, structures and requirements in terms of education and behavior patterns.

Digitalization and networking

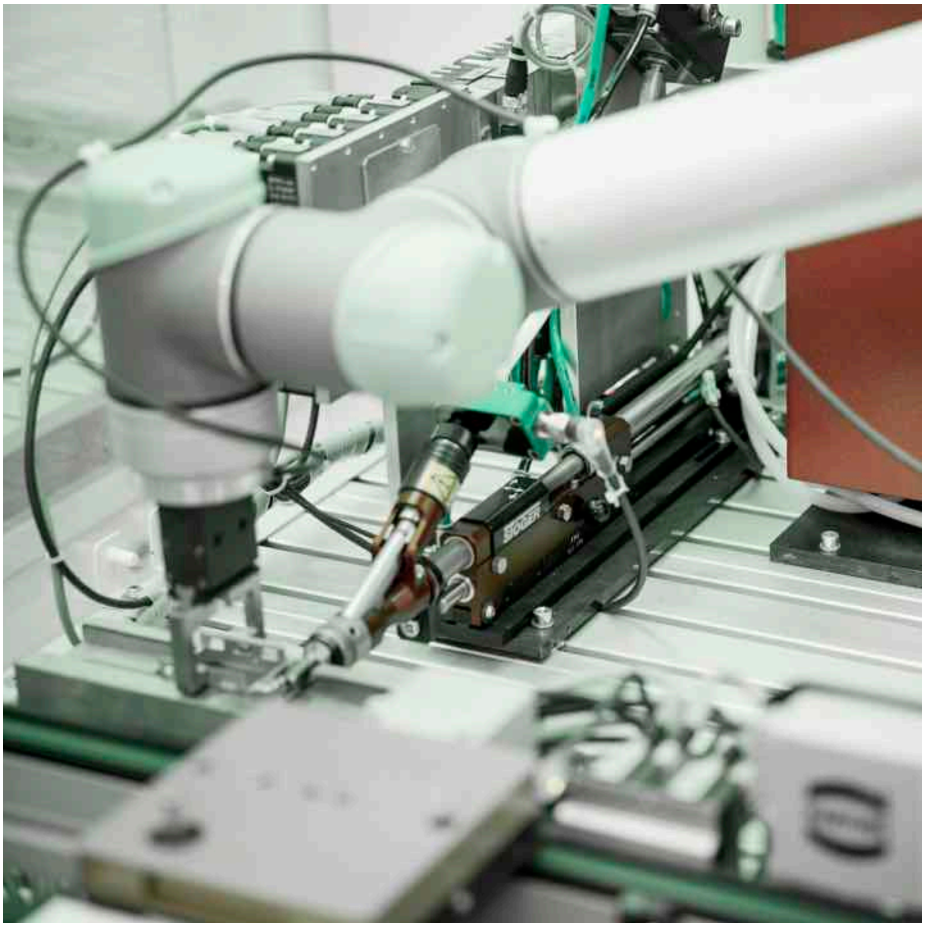
Increasing digitalization and networking are also changing production and delivery processes in the industrial context. Industry is evolving into Integrated Industry on the basis of Internet technology. Unlike the three previous industrial revolutions that paved the way for mass production, this fourth industrial revolution is enabling concrete customized production for customers, even for one-unit lots.

How will Integrated Industry develop in the coming years? We have analyzed the six fundamental trends that are crucial for Integrated Industry: modularization, identification, integration, digitalization, miniaturization and customization.

Modularization means that customers with modular production systems enjoy a new level of manufacturing flexibility. Flexible, resilient interfaces and module-neutral infrastructure solutions are the prerequisites that allow the flexible exchange and supplementation of manufacturing modules.

Manufacturers that want to reproduce their production process comprehensively in IT must first additionally clearly identify system modules and products (identification). RFID solutions give companies real-time transparency with regard to their production systems.

A further important trend that we have seen in many talks with our customers is integration. The end-to-end production process structure requires consistent vertical integration of the field level and corporate management. System integrators combine Smart Objects and ERP with flexible software solutions that result in more granular information on production performance and trends.



SOURCE: HARTING

Integrated industry requires the combined expertise of component, application and system providers.

SOURCE: HARTING

Modular production systems create manufacturing excellence using flexible interfaces and infrastructure.

The digitalization trend is also gaining in importance. The advancing digitalization of industrial manufacturing requires a constant increase in intelligent hardware at the field level. Modular systems support the company in the distributed collection and evaluation of data. Step by step, actual production and IT applications are growing more closely together.

This digitalization of industrial production requires constantly increasing computing power at more points of use and in a more and more compact area. Components and customized solutions deliver maximum performance in a minimum size (miniaturization). And finally, industrial manufacturing is becoming more and more intelligent and flexible. Companies are demanding solutions that match their specific needs. As already mentioned, this means offering customers tailor-made solutions (customization).

Solutions for Integrated Industry

It is important to recognize such trends, and it is crucial to implement these trends in solutions. HARTING Technology Group has positioned itself as a solution provider for Integrated Industry. This allows innovations to already be understood as individual customized production at the connector level. In Integrated Industry we combine our expertise and our solutions as the supplier of components, applications and systems.

The HAII4YOU Factory exemplifies this approach. The Han-Modular connector is becoming more and more important as an Integrated Industry component. This connector is the interface connector of the future. It is advancing modularization, which is a hallmark of Smart Factories. And the active infrastructure box is the key component for a high-performance backbone.

We see connectivity solutions tailored to the customer requirements as the application. For example, this could be cabling systems based on standardized interfaces such as those that are implemented in robotics applications. This also includes the network performance necessary for digitalization, which is ensured by Ethernet switches in the industrial setting and topology.

Data integration at the industrial field level in IT applications is becoming the key to Integrated Industry. With system integration, our concentrated effort is on the data exchange between ERP systems such as SAP and Smart Objects with RFID technology.

Solutions based on these trends are vital to achieving Integrated Industry. Based on these solutions, companies advancing and promoting Integrated Industry are offering their customers genuine productivity gains.

*Philip Harting is President/General Partner for the **HARTING Technology Group**.*

SOURCE: HARTING

Device data integration at the industrial field level in IT applications is becoming a key for Integrated Industry.

Radiating cables deliver RF signals in crowded plants

Radiating cables can be used to communicating to equipment moving on a track, or as a replacement for slip rings in rotating equipment. By providing a clear RF signal, even in crowded plant layouts, it offers both capability and flexibility compared to a traditional antenna.

A CABLE THAT ACTS LIKE AN ANTENNA, who would want that? After all, much research and development has gone into improving cable shields precisely to prevent this. As it turns out, there are several conditions in industrial communication systems where using a radiating cable as an antenna offers major benefits. The most common cases are for communicating to equipment moving along a track, replacing slip rings in rotating equipment, and providing a clear RF signal where obstructions or plant-floor layout prevent a clear "Line-of-Sight" to transmit from a traditional antenna.

SOURCE: PROSOFT

Using a radiating cable solution, new machines can more easily co-exist within the crowded plant RF spaces.

What is a Radiating Cable?

A radiating cable is a long, flexible antenna with slots to radiate RF signals that can be installed around corners, along monorail systems and through tunnels to propagate wireless data signals in situations that are tough or impossible for traditional antennas. Since the radiating cable antenna can be mounted within inches of where the signal needs to be received, it isolates the wireless signal from going to other machines that may be on the plant floor. And, the cable comes in multiple lengths to meet the needs of most applications.

In a typical coaxial cable, a metallic shield wrapped around the cable isolates the signals transmitted on the cable from the electromagnetic waves in the air around the cable. This helps to maintain a strong signal on the cable, and prevents that signal from creating interference with radio frequency (RF) equipment nearby. Without the shield, the cable would act like an antenna, transmitting the signal it carries into the air, and receiving radio waves from other RF devices. For those who remember analog cable TV, we experienced this phenomenon when we saw "ghost" images on certain channels. Instead of just receiving the video signal sent from the cable company along the coaxial cable, we were also receiving that channel's over-the-air broadcast of the same video signal as picked up by the coaxial cable working like an antenna. This was an unintentional use of radiating cable, and produced undesirable results.

The same principle that gave us blurry television pictures back then is used to make a cable that intentionally radiates signals. This is called a radiating cable, or leaky feeder cable. The difference between radiating cable and poorly shielded TV cables is that the shield on a radiating cable is designed with exacting slots that allow for the transmission of signals at a specific frequency. In this way, these cables are tuned to the RF equipment to which they are connected. The cable's shield still works to block unwanted RF, but will allow signals of the correct frequency to emit from, and be received by the cable inside. That makes a radiating cable act just like an antenna.

Placing RF signals in crowded plants

Another benefit of using radiating cables comes from the ability to place RF power very precisely. The use of wireless communication equipment in factories is growing rapidly, which means that factory floors are becoming crowded with radio waves on all the common frequencies. For machine builders who need

SOURCE: PROSOFT

A radiating cable offers a long, flexible antenna with slots to radiate RF signals. It can propagate wireless signals in situations that are tough or impossible for traditional antennas.

SOURCE: PROSOFT

A radiating cable can follow any path and provide wireless signals to areas where antennas can't reach.

to use wireless, this creates a real problem. With a radiating cable solution, new machines can co-exist within the crowded plant RF space without adding to high noise levels. This is because radiating cable emits RF in one direction, and only needs as much power as it takes to link with another antenna at a relatively fixed distance. The equipment on the new machine can operate at a whisper.

This benefit is especially important in rotating machinery which traditionally used slip rings to conduct communication signals from I/O on the moving part of the machine to a controller on the fixed part. Slip rings are expensive to install, require regular maintenance, and even still suffer from poor communication speeds due to noise on the rings and in the pick-ups that ride on the rings. Traditional wireless solutions can work, but often the motion of the machine will obstruct the wireless link, requiring higher gain antennas that result in greater RF "noise pollution." Radiating cable is used in these applications to provide a clear, consistent path to the rotating antenna, without interfering with other nearby wireless systems.

Flexibility with radiating cables

Radiating cable also benefits from its inherent flexibility. Since it is a cable, it can follow almost any path to provide wireless signal in places where antennas just can't reach. One of the early applications for radiating cable was to enable two-way radio connectivity for emergency workers inside highway and rail tunnels. In the industrial setting, there are many hard-to-reach places, whether those are actual tunnels or "RF tunnels" created by obstructions. An example of that would be a warehouse, where the metal racks and merchandise on those racks can cause obstruction and reflection issues for a traditional antenna. Radiating cable can be installed along the aisle ways to provide a strong signal just where it's needed.

For certain industrial communication challenges, radiating cable offers unique advantages. Radiating cable provides consistent data rates over a long distance, can be shaped to provide signal in difficult-to-reach environments, and reduces plant RF congestion by constraining its RF signal to the exact area where it's needed. These benefits are especially valuable in applications where machines move along a pre-defined path, where the terrain of a facility is particularly difficult to reach with broad coverage, and where signals on rotating equipment are otherwise transmitted through slip rings. Care must be taken in selecting and installing the components of a radiating cable solution. However, with a bit of preparation and advice from an experienced industrial RF vendor, a radiating cable system can provide trouble-free communications for your toughest applications.

Application report by ***Prosoft Technology****.*

Automatic identification keeps product variations in control

Automatic identification can help control production and assist in the optimization of production processes. Technology including two-dimensional barcodes and radio frequency identification (RFID), can be key to helping achieve continuous improvement within manufacturing plants.

AUTOMATIC PRODUCT IDENTIFICATION which optimizes operational processes by employing the latest radio or optical code technology can be a key element in helping companies in the 21st century to remain competitive.

As a leading provider of automation products, Siemens faces the challenge of meeting increasingly specific customer requirements with regard to its own products. It goes without saying that, at the same time, the costs have to stay competitive. In many areas of its plants, Siemens relies on the automatic capture of parts and components by means of two-dimensional barcodes (2D codes) or radio frequency identification (RFID), paired with a continuous optimization of the processes in the manufacturing areas.

SOURCE: SIEMENS

Employees receive detailed work instructions on a screen, delivered by a 2D code on each product.

RFID high reading speeds

A practical example is the production of automation components by the plant in Amberg, Germany. The large number of variations, such as Sirius switching devices, in combination with greatly varying demand for each type, if approached conventionally,would require a relatively large number of each device to be kept in stock to cover demand peaks within the standard delivery time.

The approach chosen, however, adopts a demand-driven production that can process incoming orders, down to a lot size of 1, within a short period of time. To this end, flexible machines are employed that can perform a specific production step for each variation – such as inserting the coil core or attaching the cover plate. By means of an RFID transponder in the workpiece carrier, the machine detects the type of the product. Without any changeover time, the production program can be set to another product type. The RFID system Simatic RF300 employed is capable of especially large memory sizes with high reading speeds, so that the cycle times could be reduced as well.

Radio chips transmit work steps

At the latest production line, the employees were involved in the concept to an even greater degree. It became evident that in a rigid production chain, many machines were underutilized whenever a specific production step is only needed for some of the products. Increasing the flexibility of the machines, however, was too complicated.

For this reason, the degree of automation was actually slightly reduced and a total of three manual assembly stations inserted into the production line. At these stations, employees can perform the individual work steps much more flexibly and better control of the resources is achieved. Depending on the circumstances, not all manual assembly stations are manned but RFID still plays an important role since, through use of radio chips, the employees get all work instructions for the specific product displayed on a screen.

Optical codes enable track & trace

The optical codes play an important role, too. For instance, in the plant in Karlsruhe, Germany, all components are equipped with 2D codes which are individually captured during installation which makes a complete tracking and tracing of the products and all components possible. For example, if a component delivery turns out to be faulty, it can easily be determined into which end products these components were installed.

Similar to the Amberg plant, the Karlsruhe plant also utilizes the 2D codes to support the employees during the assembly of the products. Since every Siemens product comes with a 2D code on the type label, work instructions can be displayed on a screen even during packing, e.g., so that the correct accessories for the respective type can be enclosed. These parts are also individually scanned, and the system only closes the work step once all required parts have been captured. The capture occurs either with handheld scanners or stationary devices from the Simatic MV line.

RFID supports quality assurance

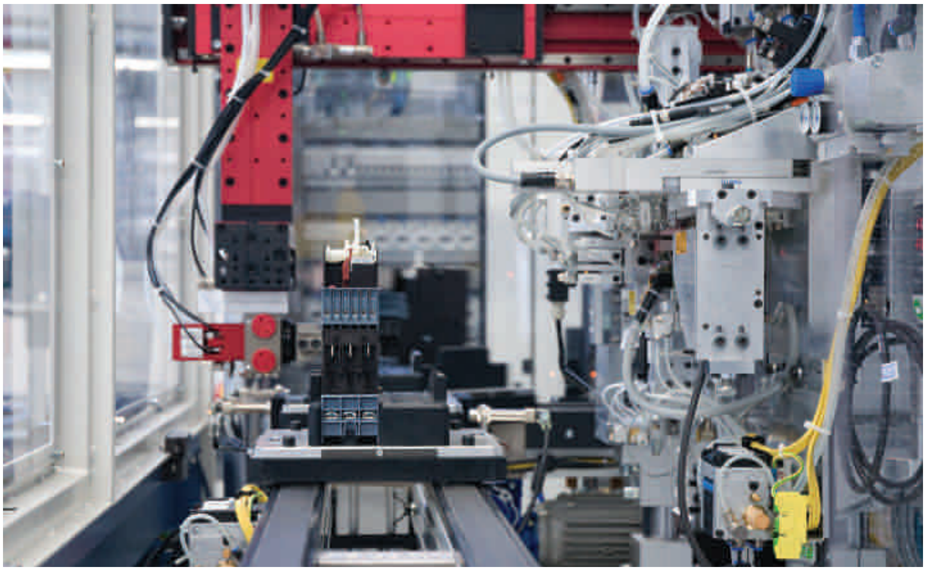
Besides the production control and the tracking and tracing, the focus is also on quality improvement. The plant in Berlin, Germany, utilizes RFID for the tool inspection. At this location, Siemens produces components for its gas turbines. Particular attention has to be paid to the accuracy, since rework would be very complicated and thus expensive. For this reason, tight maintenance intervals are defined for the fixtures and tools, which must be adhered to. But how does an employee know whether a tool can still be used, if the recording of the tool life is possibly incomplete due to manual notes?

The production schedulers in Berlin therefore equipped each tool and each fixture with an RFID transponder, on which the usage data is stored. By means of RFID antennas at

SOURCE: SIEMENS

To optimize goods traffic in the outgoing goods department, transponders inside the telephones capture in bulk to save time and streamline operations.

SOURCE: SIEMENS



RFID chips are employed during the production of Sirius switching devices at the Siemens plant in Amberg to control the flow of materials and the production.

the entrances to the production area and the warehouse, each part is automatically captured and an alarm triggered, if the maintenance interval has been exceeded. Thanks to the complete capture of the usage frequency, a precise overview of the utilization of the individual fixtures can be generated at the push of a button as an important prerequisite to optimize the inventory of the tools.

Optimized goods traffic

Logistics is also increasingly controlled using 2D codes and RFID technology. The use of optical codes in shipping centers during picking and packing is presently considered as state-of-the-art. At the former Siemens telephone plant in Leipzig, Germany, however, this was controlled for the first time by RFID transponders which are installed into each telephone. On the one hand, this RFID transponder serves for the control of individual production steps; on the other hand, the logistics is controlled with it.

When passing through so-called RFID gates, all telephones inside the larger outer packaging are scanned automatically and simultaneously using the bulk capture. Simatic RF600 readers offer a range of several meters, so that normal processes in the warehouse do not have to be changed.

The goods traffic between plant and distribution center can now be monitored and each individual phone be precisely located. Upon delivery to the end customer, the serial numbers of the individual telephones are assigned to the delivery note – which greatly simplifies the management of lease returns or the warranty processing.

Markus Weinländer *is Head of Product Management SIMATIC Ident for Siemens AG, Process Industries and Drives.*

Factory automation and integrated networking solutions

Honda Motor's cutting-edge Yorii Plant has adopted a CC-Link IE Field Network to create higher production line efficiency and to increase its competitive ability in the global market. An integrated approach put the focus on integrated solutions that address visualization, control and safety applications.

HONDA MOTOR CO. LTD. has increased the efficiency of production and operation management at its Yorii Plant by introducing the Ethernet-based CC-Link IE Field Network, which allows communication within a unified network for control signals from factory automation devices such as PLCs, production management information and safety signals. Having established Yorii as the "mother factory", lateral expansion to overseas factories such as a new plant in Mexico and elsewhere is beginning, aiming for enhanced competitiveness on a global scale.

Key technology objectives

The goals of the plant modernization program focused on building a factory automation infrastructure and network:

- Build a simple and robust network worthy of the "mother factory"
- Enhanced visualization of factory automation control devices, and streamlined operation and maintenance management
- Flexible expansion and change as the network also supports communication of safety information

The Yorii Plant opened in July 2013. Since then, it has continued to be at the cutting edge of the vehicle production industry, introducing everything Honda has developed in the way of high-level production technology and high-efficiency production systems.

The rate of new cars sold within Japan has plateaued at around 5 million per year for the last several years, and the industry can no longer count on the consistently rising sales figures of the past. The Yorii Plant was built with a view to increasing cost-competitiveness through highly efficient production and energy management. The site covering 0.95 km^2 including greenbelts, is scheduled for a full production capacity of 250,000 vehicles per year. The Yorii Plant also fulfills the role of "mother factory." Realizing this function entails sharing its production technology and know-how gradually to domestic and international production hubs, increasing overall global competitive ability.

As the construction of the Yorii Plant proceeded with this mission in mind, it was late 2011 when the design and selection of production line control devices began seriously. Taku Yokomukai, the maintenance supervisor for vehicle body assembly production line facilities and involved with the selection of control devices recalled, "We talked a lot about what kind of control devices and networks would be appropriate for a state-of-the-art factory."

SOURCE: MITSUBISHI ELECTRIC

The goal for Honda focused on a unified network for control signals from factory automation devices such as PLCs, production management information and safety signals.

Visualization and safety functions

The first issue which arose when constructing a control network for the vehicle body assembly line was how to handle the overall network architecture. "We did consider a flat construction linking the whole Yorii plant in a single network, but given the possibility that a single failure could stop the entire plant's network, we decided we were better off with multiple networks," Yokomukai said.

However, constructing individual networks by application would not only mean a more complex system but increased introduction and operation costs. Additionally, from the perspective of spreading know-how from the Yorii "mother factory" to other factories, something not only sturdy but simple in construction was called for.

While considering the system architecture, the team also identified two functions essential for the network. One was the centralized "visualization" of FA control devices; the vehicle body assembly line alone uses dozens of PLCs, making individual management inefficient. The target was an environment in which FA control device setup, monitoring, failure detection and so on could be centralized through the network.

The other essential function was the communication of "safety signals." When a worker enters a prohibited area or approaches a robot, safety considerations mandate a sensor for detection and a production facility stop (interlock). However, the traditional practice of using relays to configure a hardware based safety circuit presented the issue of serious time loss during line expansions and changes. Given this situation, they decided to incorporate safety signals into the network as well, aiming for a structure that would allow flexible line changes.

CC-Link IE Field network

Based on these needs, Yokomukai focused on a CC-Link IE Field network solution using a single Ethernet cable that not only allows communication of control information for PLCs and controllers, but also maintenance and safety information from the connected FA devices.

Yokomukai said that he discovered that the network could handle maintenance and safety

SOURCE: MITSUBISHI ELECTRIC

By introducing cutting-edge production technology, the Honda Yorii Plant has achieved a tact time of less than 50 seconds for the production of the FIT.

information as well, reflecting various on-site needs and allowing Honda to build a simple and high-reliability network suitable for the cutting-edge Yorii Plant.

Furthermore, compatibility with FA control devices was also an important point. "In order to fulfill the projected production numbers, the vehicle body assembly line was going to have to be maintained at a near constant 100% operating rate, requiring reliability and guaranteed performance from the FA control devices. So when we were selecting FA control devices for the Yorii Plant's vehicle body assembly line, our in-house proposal was for Mitsubishi Electric's products, which had proven themselves over many years at our Sayama plant (Japan), and which I myself have always held in high regard. Because the 'CC-Link IE Field Network' is highly compatible with Mitsubishi Electric's control devices, we felt that we could construct an optimal system by combining the two," explained Yokomukai.

The CC-Link IE Field Network provides the physical and data layers as defined by IEEE 802.3 (1000BASE-T). As well as covering high-speed I/O and control of distributed controllers, it offers flexible network topology options such as star and ring types, allowing great freedom in the arrangement and configuration of connected devices. In addition, not only does it support management (setup and monitor) and maintenance (monitoring and failure detection) of controller devices, but it also features a "safety communication function" allowing sharing of safety information among multiple safety PLCs.

After in-house deliberation, the final selection included Mitsubishi factory automation control devices and the CC-Link IE Field solution for the vehicle body assembly line. Solutions have also been introduced to the press shop, resin molding process, vehicle body painting line, and other production areas.

Batch management of PLCs

The Honda Yorii Plant began operation in July 2013, and moved to full operation and a second shift in September 2013.

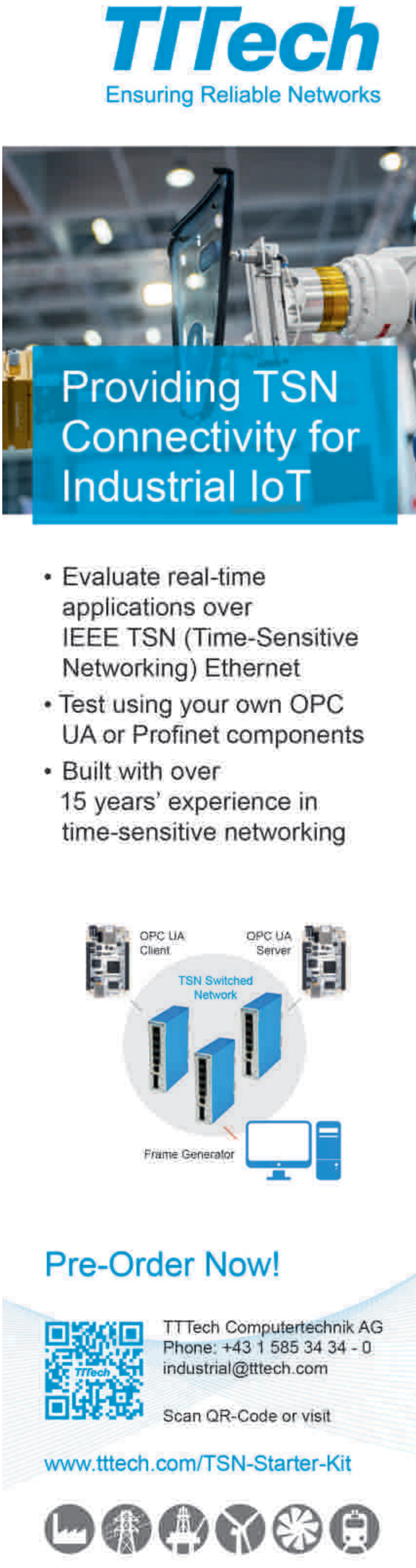
"We really get a sense of the effect of the visualization that we were aiming for originally, even the way that when there's trouble with the equipment or FA control devices, the diagnostic functions of CC-Link IE Field help us locate the problem faster. Also, we're extremely satisfied with Mitsubishi Electric's responsiveness, regarding system construction and support," Yokomukai said.

Using CC-Link IE Field, centralized visualization of FA control devices has been achieved, just as required in the original plan. "The vehicle body assembly line uses as many as 50 Mitsubishi Electric PLCs. We're able to get a centralized overview of the line status or any trouble that may be happening when a necessary signal isn't being received, making operation management efficiency much, much higher. The recovery time has also been shortened," Yokomukai added.

With regard to line expansion and safety information, it is as simple as connecting a LAN cable to a vacant port on the network, and the interlock can be added immediately in a safety PLC, reducing the workload considerably.

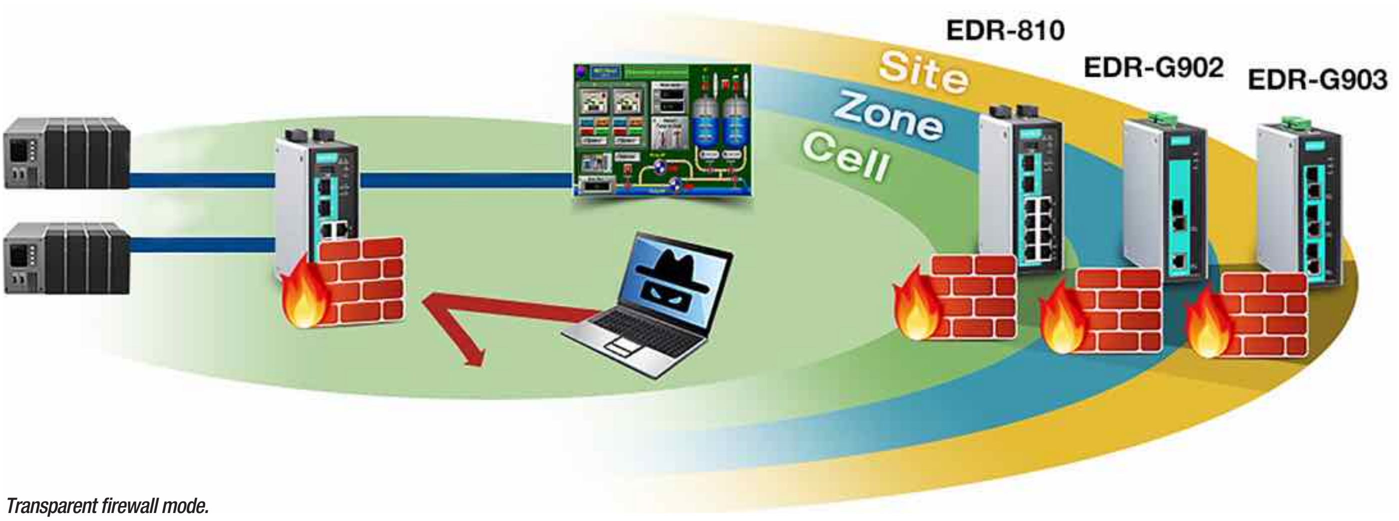
Honda has assessed these merits highly in-house, and introduced a similar system to its new plant in Mexico. Increased competitive capability through increased efficiency is a constant concern for manufacturers, and Honda plans to work towards further increased efficiency while utilizing the Yorii Plant as its "mother factory". The expectation is that there will continue to be higher demands placed on integrated factory automation solutions as users construct future leading-edge production systems.

Application story by ***Mitsubishi Electric.***



Choosing an industrial firewall: top design considerations

Network security for industrial control networks requires a clear understanding of the security challenges and defensive countermeasures. The keys are how to develop mitigation strategies for specific problems, and plans to deploy a full defense-in-depth security program.



SOURCE: MOXA

Transparent firewall mode.

CENTRAL TO INDUSTRIAL CONTROL SYSTEMS, networks help facilitate efficient and safe operations in vital sectors such as utilities, oil and gas, water, transportation, and manufacturing. A resilient control network relies on a network that can effectively detect and filter unwanted traffic. Traditionally, some industrial control networks are physically isolated or air gapped to ensure network security. However, that may not be the best practice as control systems are increasingly more interconnected to exchange data and to enable smarter automation.

One major concern of converged networks is the emergence of a new class of threats that targets industrial automation systems. Often lacking security measures, legacy networks are particularly vulnerable to malicious network attacks or unintended operations. Once compromised, legacy networks can become back doors that allow attackers and unauthorized personnel to gain access to networks.

To address network security issues for industrial control systems, a clear understanding of the security challenges and effective defensive countermeasures are required. A "defense- in-depth" approach can be applied to industrial control systems and can provide a more flexible and usable framework for improving defenses against network breaches.

This article presents a series challenges of implementing network security and network security risk management, along with information on how to develop mitigation strategies for specific problems and directions on how to define a defense-in-depth security program for industrial control networks. Here are the top design considerations:

Changes in network topology

Deploying a new firewall into control networks can be a complicated process due to various issues, such as IP address reconfiguration, network topology changes, and compatibility with existing firewalls. The first challenge is to determine the right firewall type for your network. Generally, a firewall provides two filtering options, routed and transparent (or bridged), to cater to different topologies.

A routed firewall acts as an L3 node and protects networks connected to its two logical interfaces. In the following network topology example, a routed firewall is deployed between the plant network and the enterprise network and at the perimeter of the different network zones. A routed firewall participates in the IP process and can perform tasks such as network address translation (NAT) and port forwarding. Although a routed firewall provides the most capability and flexibility, substantial network configuration may be required.

A transparent firewall is suitable for protecting critical devices or equipment inside a control network where network traffic is exchanged within a single subnet. A transparent firewall does not participate in the IP process and can be installed in the network without having to reconfigure IP subnets.

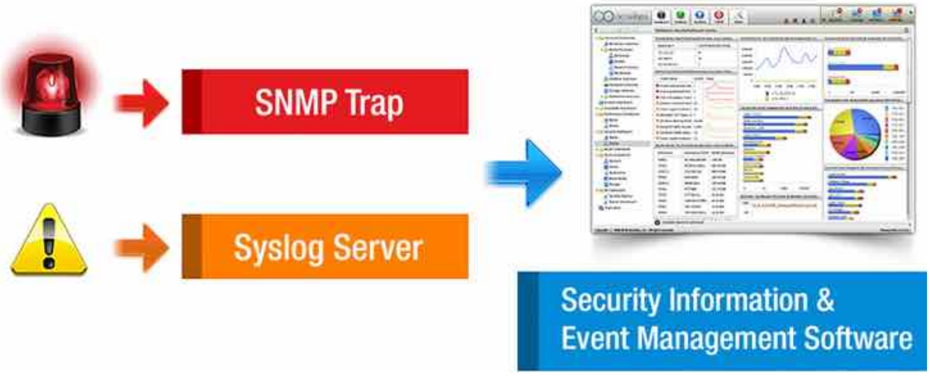
Filtering performance and latency

In most industrial control applications, response time is a critical factor. When firewalls are deployed in a control network, the data filtering processes that are performed create latency. Although many vendors claim maximum performance for their firewalls based on the benchmark of filtering data using one firewall rule, in the real world, hundreds of firewall rules may be activated to filter traffic in a control network, placing doubts on the actual firewall performance.

An industrial firewall should minimize control data interruption and allow as much throughput as possible between controllers and I/O devices. Data filtering performance must be consistent for various types and sizes of control traffic packets. In general automation applications, a response time in milliseconds is required to enable real-time applications such as process control, DCS, and data acquisition.

Event logging and notifications

Regardless of the type of industrial firewalls being implemented, event logging is critical to ensure that the firewall rules are implemented and functioning properly. In addition, logs allow administrators to monitor what is happening in the control network. Equally important, a good log file maintenance plan allows the review of any security events or issues, days, weeks, and even months after they occur. Administrators can also review these logs to evaluate the strength of current



Real-time event alarm.

firewall policies, leading to continuous security enhancements.

According to an IT expert from a major oil company in the US, a firewall must be capable of sending SNMP events with an emergency severity level that require immediate attention. What this means is that an industrial firewall must provide the configuration flexibility that allows administrators to define a severity level for each firewall rule and create a log for each triggered event. On the other hand, to prevent an email inbox from being flooded with notifications for all events, a firewall must offer the option to allow the network administrator to disable automatic notifications for non-critical events.

Mass deployment of firewall rules

In industrial applications, there could be up to hundreds or thousands of firewalls installed to control data traffic and protect field equipment from malicious attacks. As the most widely used method, a firewall whitelist allows only specific traffic on a network. This raises the question of how easy it is to change the firewall rules for the many firewalls in the field once a new service is introduced into a control network. There are two ways to mass deploy firewall rules: batch command (through the command line interface) and centralized firewall management software. Both are easy to use and are effective mass deployment methods. The use of one or the other depends on the preference of the network administrator. An industrial firewall solution should include both options.

Industrial protocol filtering

Most industrial protocols use TCP/IP or UDP as the communication base for data transmission. General firewalls can filter data at the IP or MAC layer to prevent any unauthorized access to critical equipment. Traditionally, firewalls deny all inbound traffic and allow only one-way or round-trip traffic with firewall whitelists. However, whitelisting only blocks any un-authorized hosts but grants access to all authorized hosts at the IP or MAC layer. As network complexity increases, whitelisting is inadequate to provide effective network security for industrial applications. While whitelisting protects unauthorized access to industrial devices, it is not effective in filtering control data. What is needed are well-designed firewalls that can allow or deny traffic based on protocols to enable checks on control data in the network. One such solution is Modbus TCP deep packet inspection.

Intuitive configuration interface

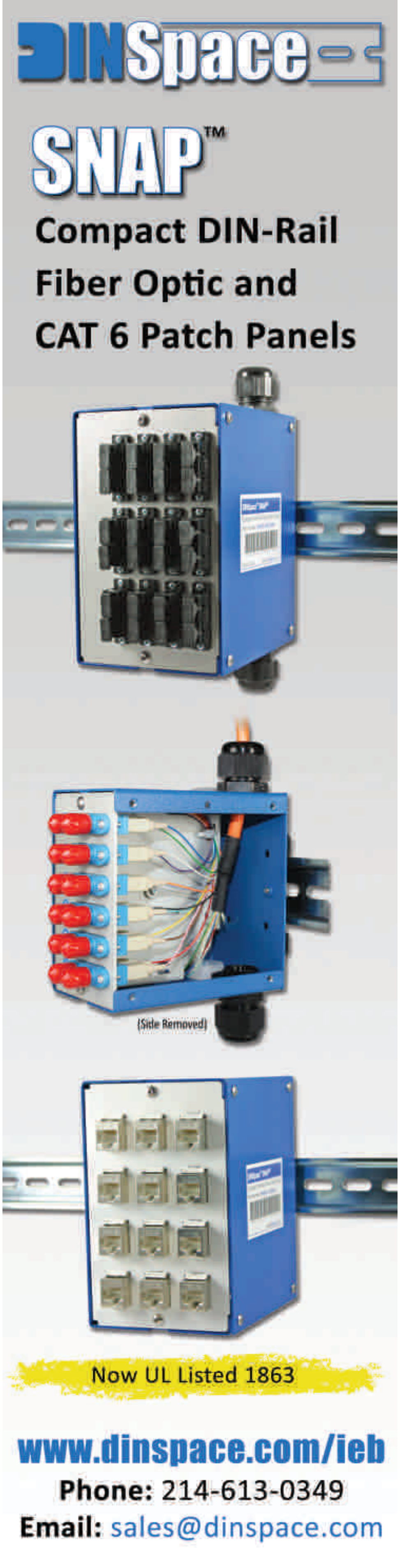
Configuring and deploying firewalls in an industrial control network requires trained administrators capable of designing firewall rules. It is important for vendors to provide intuitive and easy-to-use configuration interfaces to automate the configuration process. An industrial firewall should include a command line interface, a graphical user interface, and, preferably, a firewall setup wizard to allow administrators to get firewalls up and running in the field within minutes.

Design for harsh environments

In industrial applications, firewalls are often located in cabinets under harsh conditions such as high temperatures and vibration. A firewall for industrial applications should comply with industry standards, which could include C1D2 (oil and gas), NEMA TS2 (transportation), EN 50121-4 (trackside), and UL (factory automations).

Today, there are many standards and regulations that define network security guidelines for industrial control systems, ISA/IEC 62443 for industrial automation and NERC-CIP for power substations. NIST also published the SP800-82 standard to guide network professionals who oversee industrial control systems and are tasked with firewall deployment to protect critical industrial devices and equipment. With effective and reliable industrial firewalls, deploying industrial firewalls in the field to secure control networks and ensure maximum system uptime has never been easier.

Technology article by Li Peng, Product Manager for ***MOXA Inc.***



Defending the edge using an industrial demilitarized zone

An effective industrial network security framework needs to be pervasive and core to deployment of automation systems. A defense-in-depth approach using the concept of an industrial demilitarized zone, along with a secure configuration and architecture, is vital to defending-the-edge for industrial networks.

INDUSTRIAL AUTOMATION AND CONTROL SYSTEM (IACS) networks are generally open by default, so the need for openness facilitates both technology coexistence and IACS device interoperability. But openness also requires that IACS networks be secured by configuration, architecture and most importantly, defend the edge.

Many organizations and standards bodies recommend segmenting business system networks from plantwide networks by using an Industrial Demilitarized Zone (IDMZ). The IDMZ exists as a separate network located at a level between the Industrial and Enterprise Zones, commonly referred to as Level 3.5. An IDMZ environment consists of numerous infrastructure devices, including firewalls, VPN servers, IACS application mirrors and reverse proxy servers, in addition to network infrastructure devices such as switches, routers and virtualized services.

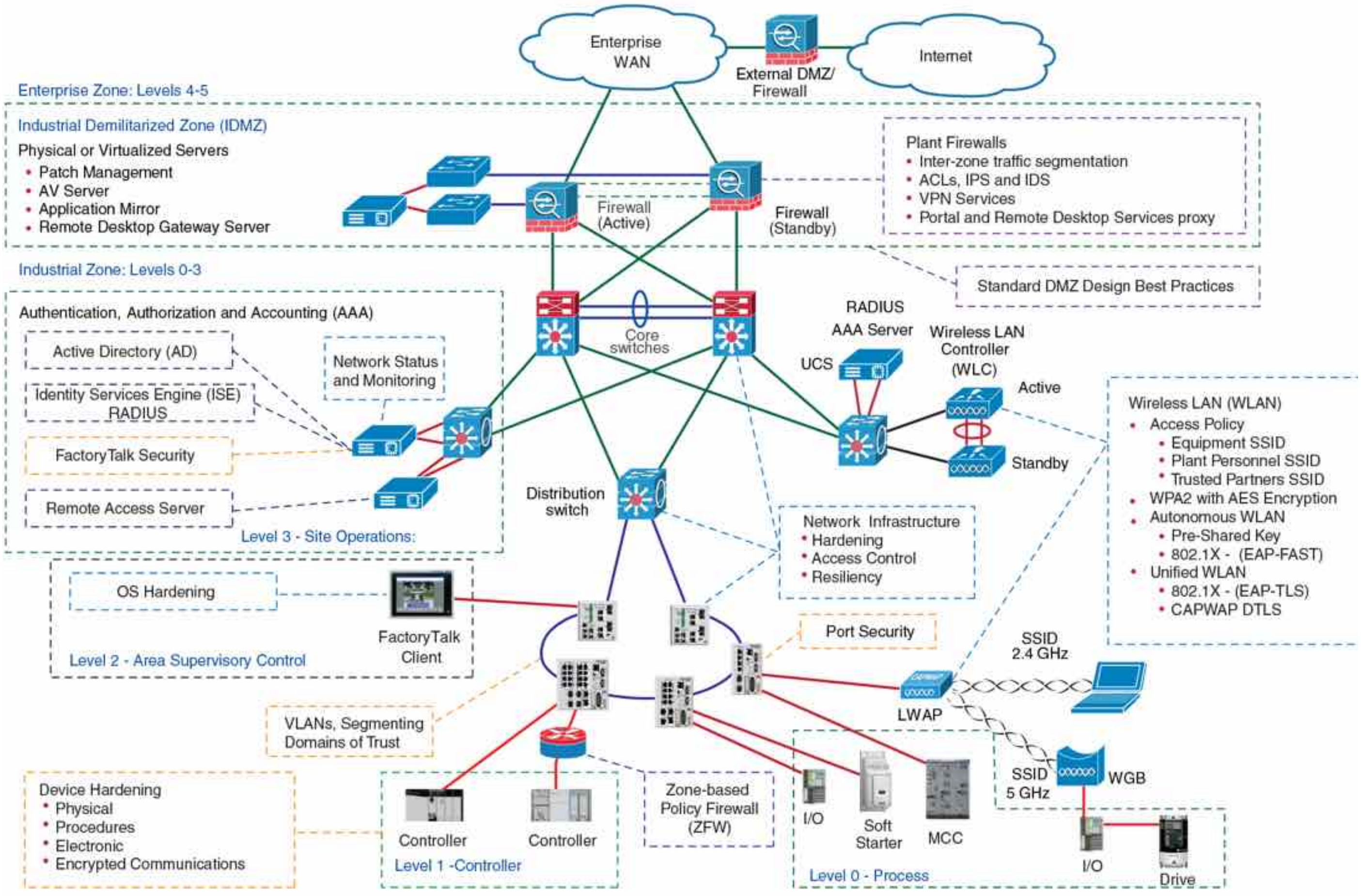
Converged Plantwide Ethernet (CPwE) is the underlying architecture that provides standard network services for control and information disciplines, devices and equipment found in modern IACS applications. The CPwE architecture provides design and implementation guidance to achieve the real-time communication, reliability, scalability, security and resiliency requirements of the IACS.

The CPwE Industrial Network Security Framework, which uses a defense-in-depth approach, is aligned to industrial security standards such as ISA/IEC-62443 (formerly ISA-99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Designing and implementing a comprehensive IACS network security framework should serve as a natural extension to the IACS. Network security should not be implemented as an afterthought. The industrial network security framework should be pervasive and core to the IACS. However, for existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the security stance of the IACS.

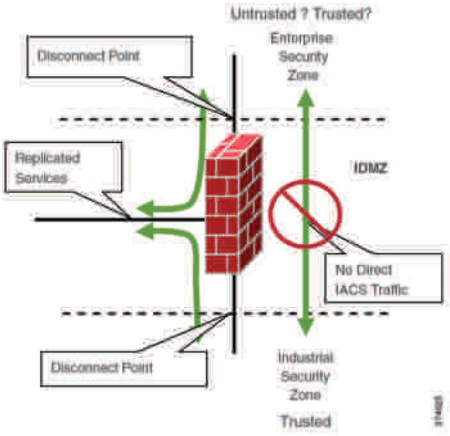
CPwE defense-in-depth layers include technology solutions and collaboration of key groups:

- *Control System Engineers*: IACS device hardening (for example, physical and electronic), infrastructure device



SOURCE: ROCKWELL & CISCO

CPwE industrial network security framework.



SOURCE: ROCKWELL & CISCO

Industrial demilitarized zone high-level concepts.

hardening (for example, port security), network segmentation, IACS application authentication, authorization and accounting (AAA)

- *Control System Engineers in collaboration with IT Network Engineers:* zone-based policy firewall at the IACS application, operating system hardening, network device hardening (for example, access control, resiliency), wireless LAN access policies
- *IT Security Architects in collaboration with Control Systems Engineers:* Identity Services (wired and wireless), Active Directory (AD), Remote Access Servers, plant firewalls, Industrial Demilitarized Zone (IDMZ) design best practices

Industrial demilitarized zone

Sometimes referred to as a perimeter network, the IDMZ is a buffer that enforces data security policies between a trusted network (Industrial Zone) to an untrusted network (Enterprise Zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the Industrial and Enterprise Zones. The demilitarized zone concept is commonplace in traditional IT networks, but is still in early adoption for IACS applications.

For secure IACS data sharing, the IDMZ contains assets that act as brokers between the zones. Multiple methods to broker IACS data across the IDMZ exist:

- Use an application mirror, such as a PI-to-PI interface for FactoryTalk Historian
- Use Microsoft Remote Desktop Gateway (RD Gateway) services
- Use a reverse proxy server

These broker methods, which help to hide and protect the existence and characteristics of the Industrial Zone servers from clients and servers in the Enterprise Zone, are covered in CPwE IDMZ.

High-level IDMZ design principles include:

- All IACS network traffic from either side of the IDMZ terminates in the IDMZ. No IACS traffic directly traverses the IDMZ. There is no direct path between the Industrial and Enterprise Zones, and no common protocols in each logical firewall.
- EtherNet/IP IACS traffic does not enter the IDMZ; it remains within the Industrial Zone.
- Primary services are not permanently stored in the IDMZ.
- All data is transient; the IDMZ will not permanently store data.
- Set-up functional sub-zones within the IDMZ to segment access to IACS data and network services (for example, IT, Operations and Trusted Partner zone).
- A properly designed IDMZ will support the capability of being unplugged if compromised, while still allowing the Industrial Zone to operate without disruption.

Converged Plantwide Ethernet IDMZ

The CPwE IDMZ Cisco Validated Design (CVD) outlines key requirements and design considerations to help with successfully designing and deploying an IDMZ. IACS data and network services between the Industrial and Enterprise Zones include:

- An IDMZ overview and key design considerations
- A resilient CPwE Architectural Framework: including redundant IDMZ firewalls and redundant distribution/aggregation of Ethernet switches.
- Methodologies to securely traverse IACS data across the IDMZ: including application mirror, reverse proxy and remote desktop gateway services.
- Methodologies to securely traverse network services across the IDMZ.
- *IACS applications*: for example, Secure File Transfer, FactoryTalk applications (FactoryTalk Historian, FactoryTalk VantagePoint, FactoryTalk View Site Edition (SE), FactoryTalk ViewPoint, FactoryTalk AssetCentre, Studio 5000)
- *Network services*: for example, Active Directory (AD), Identity Services Engine (ISE), wireless LAN controller (WLC) control and provisioning of wireless access points (CAPWAP), Network Time Protocol and Secure Remote Access
- Important steps and design considerations for IDMZ implementation and configuration

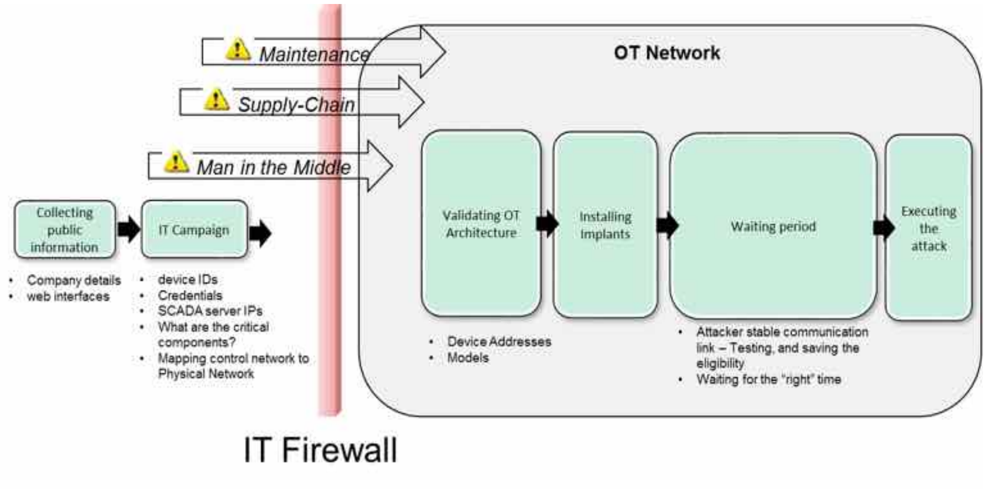
Note: This release of the CPwE architecture focuses on EtherNet/IP, which is driven by the ODVA Common Industrial Protocol (CIP). Refer to the IACS Communication Protocols section of the CPwE Design and Implementation Guide.

Technology report by ***Rockwell Automation & Cisco Systems****.*

Combatting cyber-attacks

Concerns about cyber-attacks targeting automation control are leading to new technology solutions. But the complexity of managing security requires training and development of new business processes.

ADVANCES IN NETWORKING TECHNOLOGY have made remote command and control feasible for industrial companies, allowing operators to optimize manufacturing and distribution. There is a downside, however, as reliance on remotely control and operating SCADA devices may expose critical industrial networks to cyber-threats. Modern infrastructures such as substations, oil and gas pipes, and water treatments are large, distributed complexes. Operators must continuously monitor and control many different units of the facility to ensure its proper operation.


Maintenance
Supply-Chain
Man in the Middle
OT Network
Collecting public information
IT Campaign
• Company details
• web interfaces
• device IDs
• Credentials
• SCADA server IPs
• What are the critical components?
• Mapping control network to Physical Network
Validating OT Architecture
Installing implants
Waiting period
Executing the attack
• Device Addresses
• Models
• Attacker stable communication link – Testing, and saving the eligibility
• Waiting for the "right" time
IT Firewall

SOURCE: RADIFLOW

To optimise a security budget, it is important to understand the potential phases of an attack on an ICS network. This understanding enables a focused defense strategy and development of appropriate control mechanisms.

Emerging cyber-risk

The use of monitoring and controlling industrial processes that use SCADA networked devices can expose a power substation, for example, to significant damage caused by a malicious attack on the SCADA network. Apart from imposing physical and financial losses to the company, an attack against a SCADA network might also adversely affect the environment and endanger public safety. Therefore, the security of SCADA networks has in recent years become a prime concern.

The increased concern for industrial control system (ICS) cyber security has bred many products and regulations designed to confront the risks: industrial firewalls, industrial IDSs, one-way-links, SIEMs and so on, the cost of which are eventually borne by the operator. The complexity of security also requires trained personnel and development of new processes.

Anatomy of ICS cyber campaigns

To help with understanding the attacker's mind, we've summarized our experience from research of industrial control system cyber campaigns. In general, an ICS attack campaign can be divided into several stages. In the first reconnaissance stage, the attacker will gather information about the target. Web tools such as Shodan (ics-radar.shodan.io) provide insight into ICS networks connected to the internet. In addition, information related to SCADA systems, including credentials, IP addresses and operator details, is available on the cyber black-market.

Following the reconnaissance stage, the attacker will find a way into the organizational network, whether through the corporate website, malicious emails or even an infected USB drive. The attacker will look for information about the ICS network on the organizational network: controllers IDs, correlation between controllers and certain physical process, company procedures, credentials and so on.

The attacker will also search for information about potential vulnerabilities in the operational network (contrary to the "isolated ICS network" notion, the air-gap that insulates the ICS network from the outside world is not air-tight). For example, a historian server connected to both the organizational and the operational network, or malware infecting the network during scheduled maintenance, originating from a local technician's PC or from a remote service vendor. Another point of vulnerability is the supply chain: components sent out for maintenance, which are received back with malware installed.

Attacker inside the network

Once the attacker enters the operational network, he needs to validate its architecture as well as the information previously gathered. From the attacker's perspective, this is critical in order to execute an effective attack.

How can the attacker validate the gathered information? He can read the tags from the OPC server, which hopefully would have meaningful names. He can try to take snapshots of the HMI. He will try to sniff the network, to validate the communication to the controllers.

In addition, the attacker will try to send innocent commands to the target controllers. He may also attempt to change parameter values on controllers (while making sure that they continue to report normal values, to prevent detection).

All of these actions guarantee that on attack day the attacker would be able to take control over the platform and cause the desired damage. The validation stage is usually followed by a waiting period, during which the attacker will lay low.

Analyzing the threat

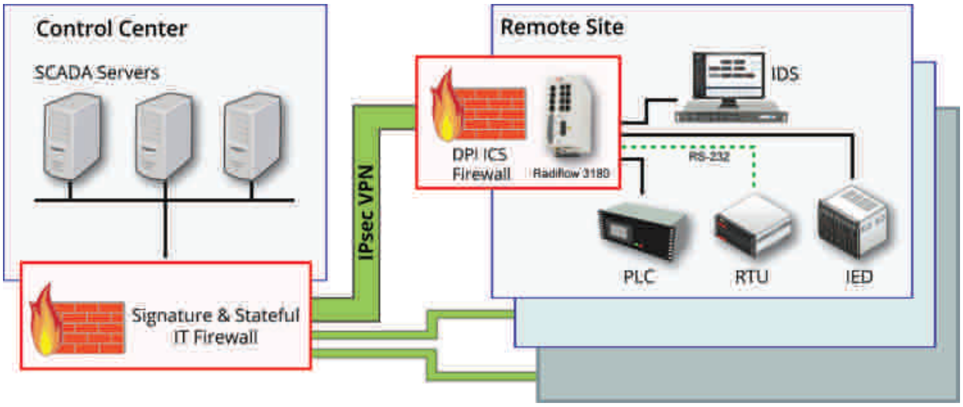
Consider a network with a main control center that communicates with multiple remote sites. Each remote site contains several field devices, such as PLCs and IEDs. For the sake of simplicity, let's say that the remote sites communicate only with the control center, using a trusted VPN between the gateways. The attacker's actions inside the operational network can be broken down into categories:

- *Field-to-Field attacks:* Attacks from one compromised remote site or field device to another remote site.
- *Center-to-Field attacks*: Attacks that initiate traffic from the control center, aimed to harm/manipulate field devices.
- *Field-to-Center attacks*: Attacks that initiate traffic from a remote site to the control center.
- *In Field Attacks*: Attacks from one field device to another device, within the same site. This includes also attacks that occur within the same segregated area.

Network segregation

The mitigation of Field-to-Field attacks starts by routing all remote site traffic to the control center, using an IPsec VPN. In addition, each site requires an industrial distributed Deep-Packet-Inspection (DPI) firewall that enables the operator to set permission policies for blocking traffic from other sites, and allows users to access specific devices.

Deep-Packet-Inspection (DPI) is a method for filtering network traffic based on analyzing the application layer of the packet. In that layer there is informational data about the application that receives / sends this packet. In the industrial protocols, the application layer will often be the receiver unit ID, values set, commands and more. Using the DPI firewall the operator can enforce a specific behavior. The use of the industrial distributed DPI firewall and the VPN ensures that all traffic arrives only from trusted IP addresses, and that each IP address receives the appropriate permissions for specific commands. Mitigating Field-to-Center and Center-to-Field attacks is a bit more complicated. Preventing these attacks will ensure that the remote links are secure, e.g. they do not contain malware or unauthorized traffic.



Mitigation of field-to-field attacks starts by routing all remote site traffic to the control center using an IPsec VPN.

SOURCE: RADIFLOW

The detection of malware traffic is usually done using a firewall loaded with malware signatures. Since the signature database must be updated frequently, it would be most convenient to install a single instance of the firewall at the control center. Another threat is spoofed traffic such as a command initiated at the control center with the SCADA server's IP address, but not actually sent from the server.

The detection of spoofed messages commonly involves the use of stateful firewalls, which check the state of each connection and each protocol, detect attempts to open another connection to the field device, and allow only packets from an open connection to pass. Assuming that authorized devices are already inter-connected, the stateful firewall would be able to block the new, spoofed connections. In addition, it can enforce the direction of opening connections only from one side of it to another.

By employing a distributed DPI firewall alongside a central stateful firewall, it's possible to achieve a well-segregated, yet simple, ICS network. Firewalls with signature-based engines that demand periodical updates should be installed at the center.

Intrusion detection

In-Field attacks are attacks whose source and destination reside within the same substation. While Stuxnet became the "poster child" for this type of attack, there's a long list of less familiar malwares that are loaded onto the network during scheduled maintenance from the maintenance engineer's PC, undetectable by the control center or any other central security monitoring system. To mitigate these attacks it is essential to have an Intrusion Detection System (IDS) sensor inside each of the segregated areas, to monitor the network traffic and detect any suspicious activities.

The IDS sensor needs to monitor several activities. First, it needs to monitor malware traffic, which requires the IDS to have a signature-based engine loaded with known malware traffic signatures. The IDS compares the segregated area traffic to these signatures; in case of a match, an alert is created.

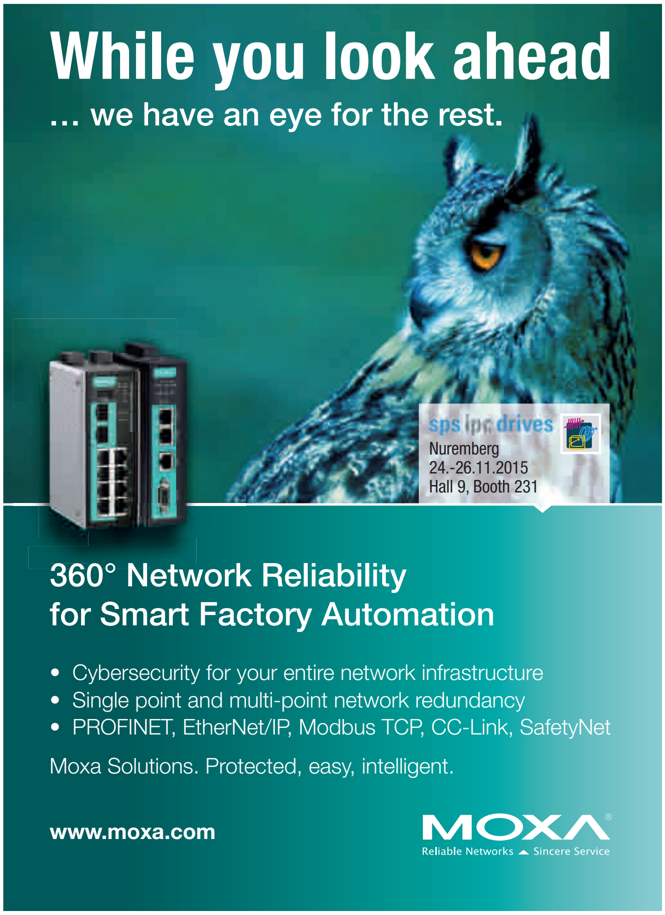
However, detecting malware is not enough. ICS malwares aim to disrupt the ICS process by sending industrial commands through the network. These commands use the industrial protocols, and sometimes even sample "legal" device values. So, the IDS must also have an Industrial Anomaly Detection engine. This engine learns the ICS network behavior, and creates a unique network-fingerprint for each device on the network. Each sampled device has unique values, which may differ based on time and sampling device.

Deployment considerations

So how do you manage all these security products? You'll need a central management hub to deal with all unavoidable system vulnerabilities. Such a system will allow you to view, manage and react to security events, as well as configure the firewalls and the IDS. As a rule, self-learning products are preferable. For example, your firewall should automatically learn the network behavior and firewall rules. IDSs with advanced machine learning are especially important in complex network environments that require extensive configuration.

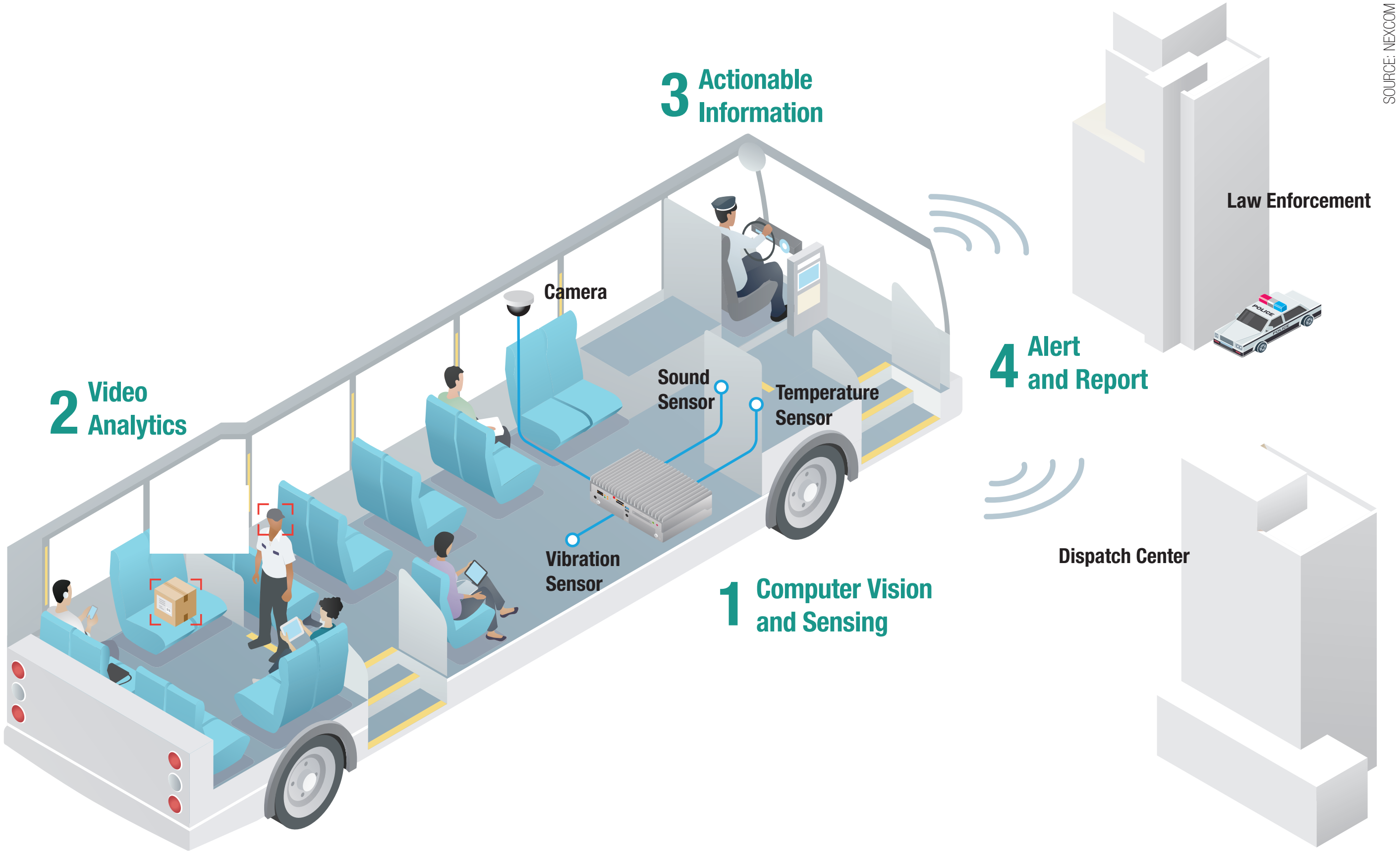
Lastly, the security system must be integrated into the operator's current monitoring tools. To successfully deploy a security system within an ICS network, it's essential that the operator and the security company have a collaborative process of custom-fitting the security management software to the operator's infrastructure.

Yehonatan Kfir is chief technology officer for ***Radiflow****.*



Transportation security using video-based Intelligence

A new paradigm is emerging where mobile computing systems can automatically convert video images into actionable information. This creates an opportunity to communicate GPS location, video footage, and other details over cellular or wireless broadband networks.



SOURCE: NEXCOM

VTCs based on 5th generation Intel Core processors provide server-like capabilities.

COMPUTER VISION, commonly used in the transport sector, has been used to produce video evidence or render visual assistance on buses, commercial fleets, and patrol vehicles. For concerns over transportation security, computer vision can have more active uses to allow precautionary measures to be imposed or immediate response taken on the spot. To this end, computer vision is increasingly inseparable from video analysis.

In-vehicle Computers are leveraging 5th generation Intel Core processors to generate video-based security intelligence, and provide a flexible approach to not only delivering video analysis but also providing consistent performance regardless of evolving analysis techniques. The size and power design of the units, along with design enhancements, give users mobility to adapt to highly dynamic mobile environments. Potential security risks can be addressed by using security tools to create a safe operating environment for video analysis to run.

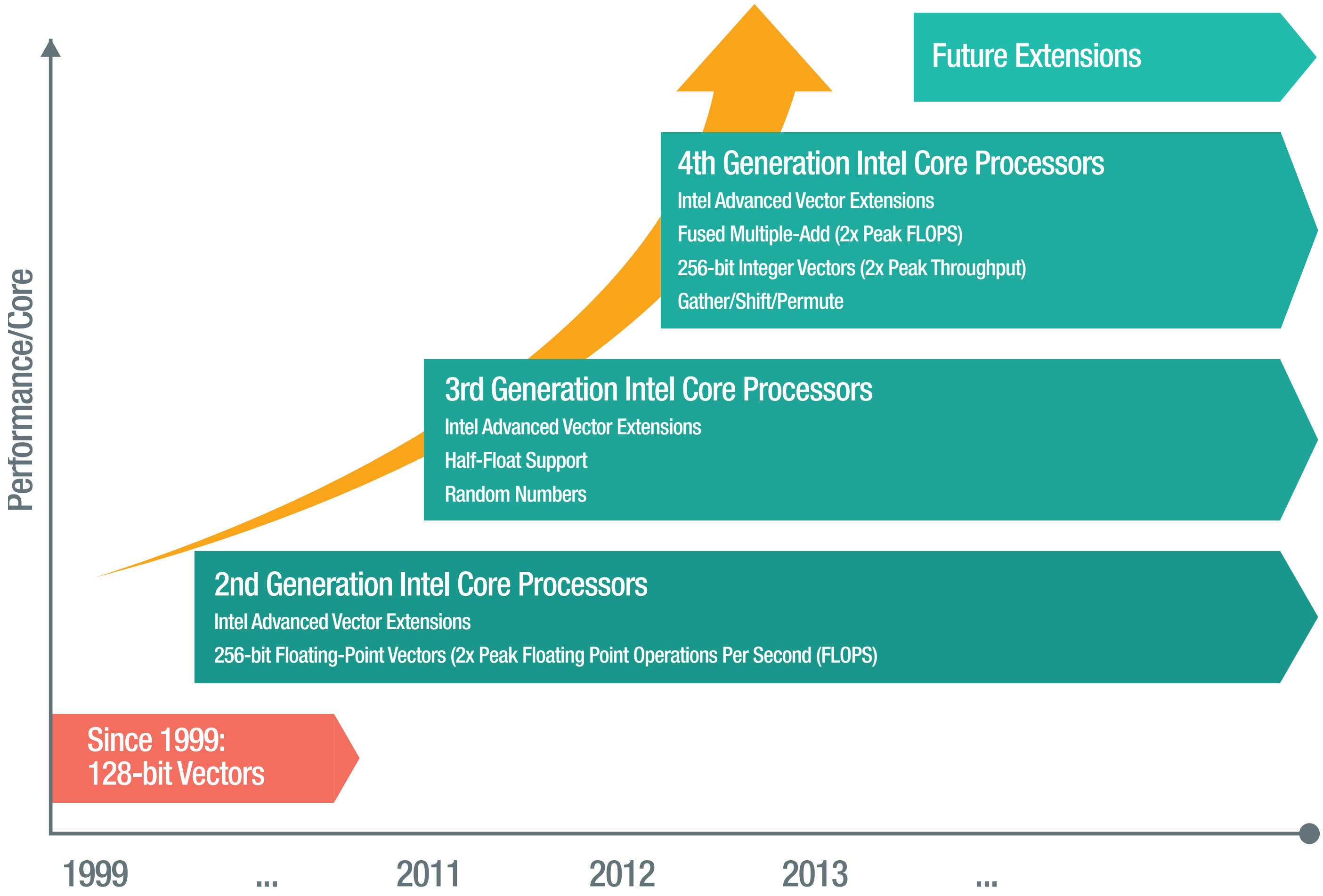
The need for intelligence

Security is a common concern shared among the overall transport sector and law enforcement agencies such as border patrols. Buses and metro transit systems are equipped with mobile surveillance systems to clarify liabilities after a criminal offense or incident takes place. Truck drivers count on cameras providing a view of blind spots for the purpose of gaining situation awareness. Border patrols also deploy camera-equipped trucks to help monitor borders.

Systems can compel drivers to divert their eyes from roads to view video, posing distracted driving risks. A new paradigm is needed where mobile computers can automatically convert video images into actionable information and alert drivers only when necessary.

The new systems must aggregate multiple video streams and data feeds from video cameras and in-vehicle sensors, and perform video analysis based on existing, newly emerged, and yet to be discovered behavioral patterns. Bringing these server-like capabilities onto a mobile system is taxing. NEXCOM in-vehicle computers (VTC Series) based on Intel Core i3-5010U and i7-5650U processors respectively can fulfill the requirements by providing outstanding video analytics performance for detecting, identifying, and tracking suspicious activities and objects shown in video images.

These processors include the Intel Advanced Vector Extensions 2 instruction set, an upgraded vector-processing technology from Advanced Vector Extensions. AVX 2.0 extends most of integer instructions to 256 bits, doubles the number of floating-point operations per second (FLOPS) per clock cycle,


Future Extensions
4th Generation Intel Core Processors
Intel Advanced Vector Extensions
Fused Multiple-Add (2x Peak FLOPS)
256-bit Integer Vectors (2x Peak Throughput)
Gather/Shift/Permute
3rd Generation Intel Core Processors
Intel Advanced Vector Extensions
Half-Float Support
Random Numbers
2nd Generation Intel Core Processors
Intel Advanced Vector Extensions
256-bit Floating-Point Vectors (2x Peak Floating Point Operations Per Second (FLOPS)
Since 1999:
128-bit Vectors
Performance/Core
1999
...
2011
2012
2013
...

SOURCE: NEXCOM

Intel Core processors deliver an upgraded vector-processing technology for signal and image processing.

and adds instructions for floating-point fused multiply-add (FMA), vector gather, shift, and permute operations. These improvements enable higher integer, fixed- and floating-point arithmetic throughput to allow for more vector processing operations. The processors also support graphics programmability features like OpenCL 2.0 so developers can utilize the integrated graphics processing units (GPUs) to further boost video analysis performance.

In-vehicle computers benefit from using these processors, achieving higher precision and speed in signal and image processing. Take for example unattended package detection. On transit systems, an unattended package is typically regarded as suspicious and a potential security threat. To enhance transport safety, these systems can apply image sharpening, image segmentation, and object extraction algorithms—compute-intensive workloads usually handled by servers—to identify a static object on real-time surveillance footage.

On discovering a possibly abandoned object, the technology can be used to send alarm signals to metro conductors and drivers. If necessary, in-vehicle computers can report the incident to metro control centers and metro police, transferring the metro train's GPS location, video footage, and other details over cellular or wireless broadband networks.

Reinforce mobile task forces

The signal and image processing capabilities offered by Intel Core processors also enable in-vehicle computers to ease workloads for commercial drivers. The units integrate a wide variety of interfaces including controller area network (CAN) and on-board diagnostics-II (OBD-II) protocols to connect to in-vehicle electronic systems. By consolidating information from multiple sources such as dashboard cameras, proximity radars, and tank level gauges, in-vehicle computers can evaluate a traffic situation ahead, calculate minimum stopping distance, and suggest drivers slow down to a safe speed to obviate the need to slam on the brake.

Taking such preventive precautions can avoid a potential rollover crash and spill, increasing road safety, and even protecting the environment when goods in transit are flammable materials or hazardous chemicals.

In addition to providing a second set of eyes, in-vehicle computers can assist in fighting illegal border crossing. Temporary placement of in-vehicle computers on scope trucks enables law enforcement agencies to strategically complement surveillance cameras installed along borders. Tracking multiple suspect objects in motion and identifying a wanted suspect are some of practical uses. They can also be used to apply analytics to thermal images, bringing potential incidents to the eyes of border patrol agents. The Intel HD Graphics 5500 and 6000 built into these Intel Core processors enable these systems to show a variety of information simultaneously on as many as three displays with a maximum resolution of 4K.

As opposed to platforms using proprietary video analytics integrated circuits, Intel processor-based VTCs deliver excellent compute and visual performance, and most important of all the flexibility to run diverse algorithms for imaging analysis needed for specific circumstances and needs. Moreover, Intel Core processors manufactured by the 14nm production technology have a thermal envelope of as low as ten watts and support configurable thermal design power. As a result, systems can carry out compute-intensive video analysis using Intel AVX2 and sidestep processor TDP limits to assure performance. The DI and DO channels can even operate when in-vehicle computers are in a power-off state and wake VTCs to tasks when devices sense vibrations, smoke, or other signals.

Keep intelligence in safe hands

Due to the role played by the VTC 7230 and 7240, securing in-vehicle computers holds

SOURCE: NEXCOM

Temporary placement of in-vehicle computers on scope trucks enables law enforcement agencies to strategically complement surveillance cameras installed along borders.

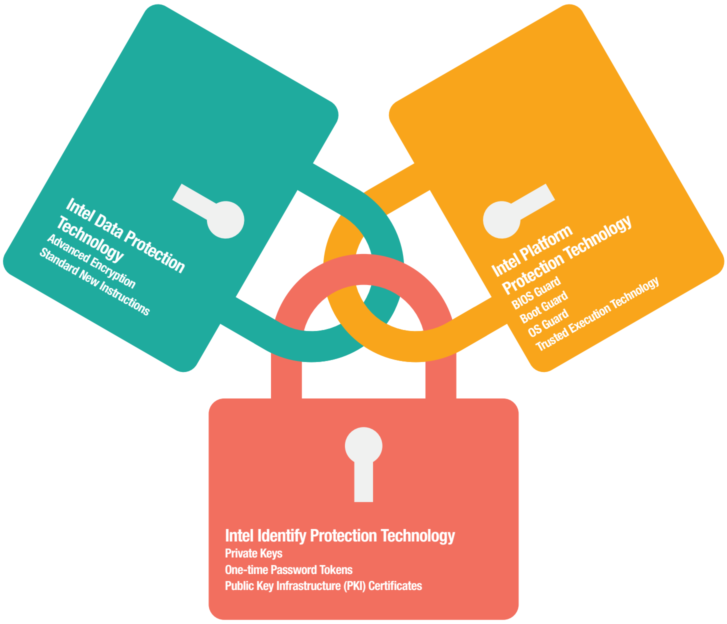
great significance. The computers are armed with Intel Platform Protection Technology, Data Protection Technology, Identify Protection Technology to address security challenges from system boot to application execution.

New Advanced Encryption Standard New Instructions allow faster data encryption and decryption for securing data and helping protect confidential intelligence and surveillance footage stored in the unit from loss. Moreover, the technology uses hardware-based acceleration to achieve security enhancement without performance penalties.

In respect of information sensitivity, Intel IPT can add an additional security layer to restrict information access to authorized in-vehicle computers only. Using a combination of private keys, one-time password (OTP) tokens, and public key infrastructure (PKI) certificates, it is possible to examine the authentication of an in-vehicle computer before connecting it to a virtual private network (VPN) to retrieve intelligence stored in remote databases or servers.

Turning captured images into intelligence is an important prerequisite for a response to an incident. VTCs can relieve the need for security staff to constantly view surveillance video by enabling excellent performance of video analytics. Using these analytics to identify potential dangers in surroundings, can produce alerts to mobile task forces and provide information they can act on. Instead of documenting activities, in-vehicle computers can be an active part of a joint mobile task force, searching for potential threats to public transport systems, catching ticket evaders and bus hooligans, and thwarting border trespassers. As more and more video analysis techniques and applications become available, solutions provide high flexibility, allowing immediate implementation of the latest technology, making it an effective tool for managing and reducing security risks today and in the future.

Technology report by ***Nexcom****.*


Intel Data Protection Technology
Advanced Encryption Standard New Instructions
Intel Platform Protection Technology
BIOS Guard
Boot Guard
OS Guard
Trusted Execution Technology
Intel Identify Protection Technology
Private Keys
One-time Password Tokens
Public Key Infrastructure (PKI) Certificates

SOURCE: NEXCOM

Due to information sensitivity, layers of security protection are provided from system boot to application execution.

中國國際工業博覽會
China International Industry Fair

2015 THE 17TH SESSION 第17届

ufi Approved Event

IAS
INDUSTRIAL
AUTOMATION
SHOW

Industrial Automation Show

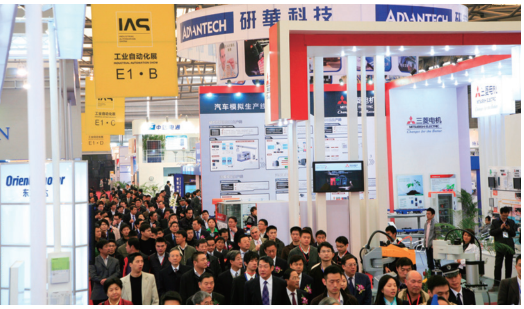
www.industrial-automation-show. com
http://ias.ciif-expo.com

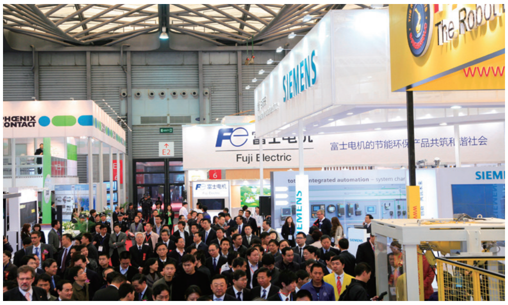
International Exhibition for Factory and Process Automation, Electrical Systems, Robotics and Industrial Automation IT & Software

Time:	3-7 November 2015
Venue:	National Exhibition and Convention Center(Hongqiao, Shanghai)
Organizers:	Hannover Milano Fairs Shanghai Ltd. Deutsche Messe AG Shanghai East Best International (Group) Co., Ltd.
Co-organizers:	China Mechanical Engineering Society China Power Supply Society

Staged parallel with

- MWCS METALWORKING AND CNC MACHINE TOOL SHOW — Metalworking and CNC Machine Tool Show
- ES ENERGY SHOW — Energy Show
- EPTES ENVIRONMENTAL PROTECTION TECHNOLOGY & EQUIPMENT SHOW — Environmental Protection Technology & Equipment Show
- STIS SCIENTIFIC & TECHNOLOGICAL INNOVATION SHOW — Scientific & Technological Innovation show
- ICTS INFORMATION & COMMUNICATION TECHNOLOGY SHOW — Information & Communication Technology Show
- NEAS NEW ENERGY AUTO SHOW — New Energy Auto Show





Deutsche Messe

FIERA MILANO

Rm. 301, B&Q Pudong Office
Tower, 393 Yinxiao Rd. PudongShanghai 201204, P.R. China
Mr. David Zhang / Mr. Klaus Qian / Ms. Flora Fang
Tel. +86 21 5045 6700 ext. 259 / 280 / 282
Fax +86 21 5045 9355 / 6886 2355

daivd.zhang@hmf-china.com
klaus.qian@hmf-china.com
flora.fang@hmf-china.com
www.industrial-automation-show.com

Remote monitoring and control for wind turbines

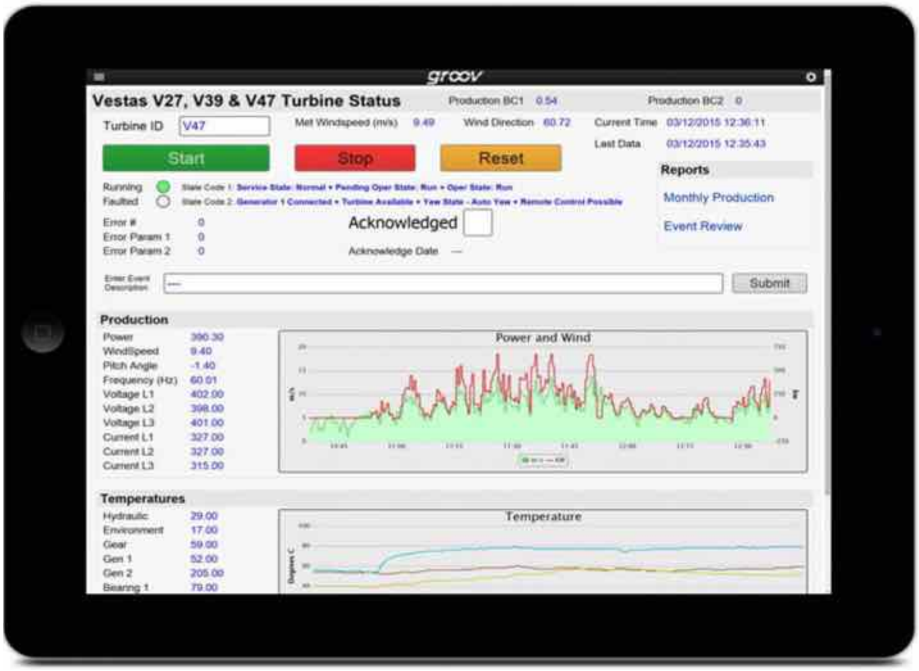
A unique SCADA system makes it easy to monitor and control wind turbines from anywhere using a smartphone or other mobile device. The WindCapture system can also quickly scale back power generation during periods of low demand.

STRONG GROWTH IN THE USE OF WIND ENERGY during the past 30 years has resulted in many aging wind farms. For the utility owners, however, older wind turbines do not have remote monitoring and control systems that simplify curtailment when utilities must scale back power generation during periods of low demand.

"Ironically, too much electricity flowing into a state's electrical grid can be just as disruptive as too little, hence the need for occasional curtailment," said Craig VanWagner, engineer for SCADA Solutions, a provider of SCADA communications, automation, and integration services for wind farms through its WindCapture online monitoring and control system."

"New California guidelines require these older wind farms to be able to curtail whenever energy regulatory companies say so," VanWagner added.

When the California Independent System Operator (CAISO) tells a wind farm operator it needs to curtail power production, the company has as little as five minutes to respond. Before WindCapture, the utility would have to staff the wind farm around the clock with technicians to physically turn on or off individual turbines within the required time frame or face considerable financial penalties. When the wind picked up and the grid was ready, the technicians would bring the turbines back online.



Vestas V27, V39 & V47 Turbine Status

Production BC1 0.54
Production BC2 0
Turbine ID V47
Met Windspeed (m/s) 9.49
Wind Direction 60.72
Current Time 03/12/2015 12:36:11
Last Data 03/12/2015 12:35:43

Reports
Monthly Production
Event Review

Running ●
Faulted ○
State Code 1: Service State: Normal • Pending Oper State: Run • Oper State: Run
State Code 2: Generator 1 Connected • Turbine Available • Yaw State - Auto Yaw • Remote Control Possible

Error # 0
Error Param 1 0
Error Param 2 0
Acknowledged □
Acknowledge Date —
Enter Event Description —

Production
Power 390.30
WindSpeed 9.40
Pitch Angle -1.40
Frequency (Hz) 60.01
Voltage L1 402.00
Voltage L2 398.00
Voltage L3 401.00
Current L1 327.00
Current L2 327.00
Current L3 315.00

Temperatures
Hydraulic 29.00
Environment 17.00
Gear 59.00
Gen 1 52.00
Gen 2 205.00
Bearing 1 79.00

SOURCE: OPTO 22

The iPad interface makes it easy to monitor and control wind turbines from anywhere using a smartphone or other mobile device.

SOURCE: OPTO 22

The WindCapture system allows SCADA Solutions to quickly scale back power generation during periods of low demand.

Flexible SCADA solution

Using SNAP PAC industrial controllers from Opto 22 that supervise individual I/O controllers on each turbine, a wireless mesh radio network for communications and a groov operator interface for mobile devices, SCADA Solutions was able to quickly develop an affordable solution to remotely monitor and automatically manage wind farm electrical power generation output down to the individual turbine.

"We can take the analog and digital data from the field and bring it into control software that monitors and manages the whole wind farm. Opto 22's software application suite gives us a variety of interfaces and protocols and the ability to push OPC data to the cloud, while groov allows our customers to access live turbine data and control those turbines from a smartphone or other mobile device," VanWagner explained. "It also makes it really easy to get in front of new customers when you show them, on their own personal phone, how they can monitor and control their wind turbines from anywhere."

SCADA Solutions has installed the WindCapture system at two wind farms and is working on a third. VanWagner expects utility owners to see significant additional revenue from enabling wind farm control systems that automatically optimize generation for maximum revenue.

He also expects substantial savings from reducing technician travel and labor costs—not to mention the benefits of the system's preventive maintenance capability. "If at any time a turbine starts to degrade from a pre-established baseline, WindCapture can send an alert to the customer before there's a failure," VanWagner said.

Application report by ***Opto 22.***

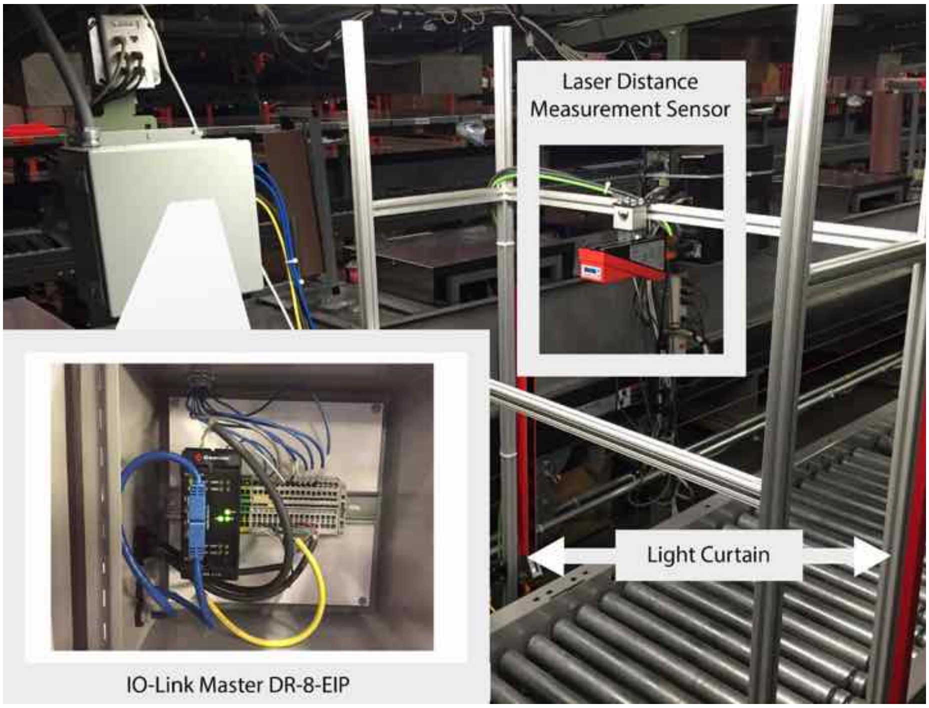
Material handling using IO-Link communications

Using IO-Link communications to control light curtains and laser distance measuring sensors created an effective solution for a material handling system integrator, improving efficiency and product quality.

A LARGE MATERIAL HANDLING systems integrator in the Midwestern U.S. had a customer that was experiencing difficulty along their 24V powered roller conveyor system. Needing a solution that could eliminate this from continuing in the future, the industrial supplier turned to a systems integrator and an IO-Link master controller.

The customer is a large industrial supplier and uses small and large plastic totes to transport material throughout their factory. At specified locations along the line, the totes are empty and need to be moved to a stacker machine. Occasionally these totes entered the stacker machine with material left inside, causing it to jam and interrupt production.

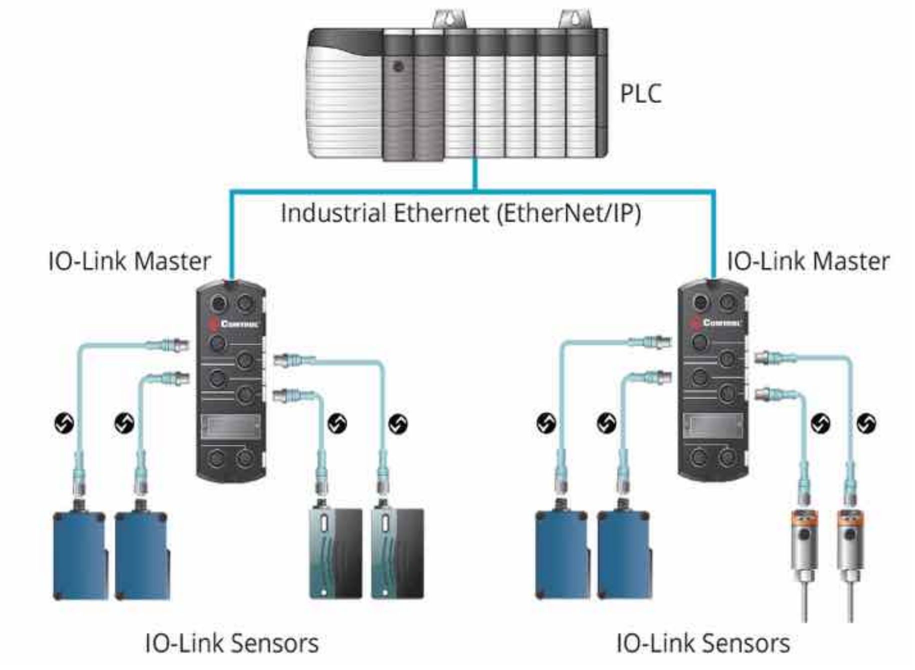
The system integrator opted to implement a solution using Comtrol's IO-Link Master DR-8-EIP to control Leuze Electronic IO-Link enabled light curtains and laser distance measuring sensors. Now as the totes pass along the conveyor line the light curtains, located along the side, determine how the totes are stacked. This information is then relayed through the IO-Link master to the Rockwell ControlLogix Programmable Logic Controller (PLC).



SOURCE: COMTROL

The IO-Link master is used to control both light curtains and laser distance measuring sensors.

The laser distance measuring sensor, found above the conveyor line, scans the inside of the totes for material left inside. When the tote is emptied, it proceeds along the line and is stacked by the stacker machine; if the scanners determine there is any material left inside the tote, it is not stacked and is sent to a rejection area. As a result of this implementation, the industrial supplier has increased efficiency and prevented potential damage to their stacker machines.



SOURCE: COMTROL

IO-Link Master common configuration networking diagram.

The IO-Link Master (DR-8-EIP) offers:

- Multi-link technology allows the user to simultaneously communicate with EtherNet/ IP and Modbus TCP protocols.
- Access to IO-Link process, service, and event data through EtherNet/IP, Modbus TCP, and Profinet IO.
- Configuration flexibility to support up to 20 device connections.
- IO-Link ports, dedicated digital I/O Output ports, and digital inputs.

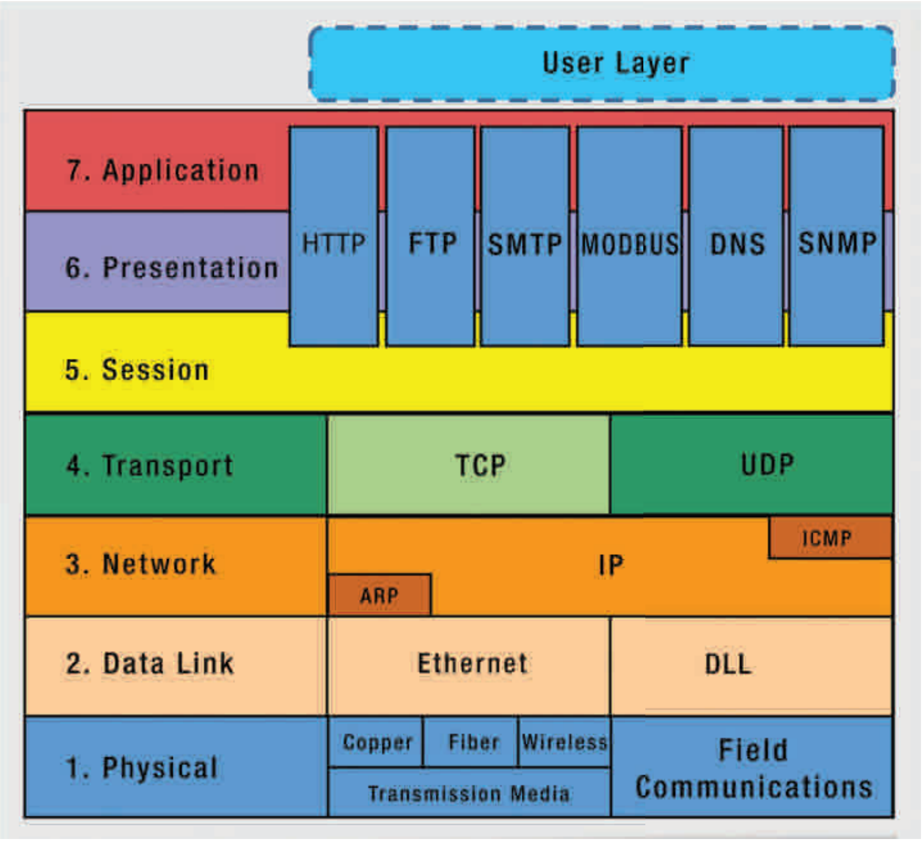
The technology combines the benefits of the IO-Link standard with the EtherNet/ IP protocol by providing a gateway that's a streamlined bridge between the field level sensor network and the industrial EtherNet/ IP backbone, making retrofitting or expansion simple. The IO-Link Master is easily integrated into a system network, and is compatible with existing and new industrial Ethernet environments.

*Application report by **Comtrol.***

Industrial Automation NORTH AMERICA
Industrial Automation
HANNOVER MESSE
Otomasyon EURASIA
Industrial Automation INDIA
Industrial Automation SHENZHEN
IAS INDUSTRIAL AUTOMATION SHOW
Industrial Automation BEIJING

Newer real-time protocols make connecting easier

While older proprietary protocols still have their place, newer and more open protocols such as EtherNet/IP are improving both automation and operations. Implicit and explicit messaging, for example, are expanding the usability of network and transport layers to enhance communications.



Developed to assist creation of detailed interface standards, the Open Systems Interconnection (OSI) standard is a common reference model showing how applications can communicate over a network.

SOURCE: AUTOMATION DIRECT

PLC COMMUNICATIONS HAS EVOLVED as automation has advanced over the years, with hardware requirements and PLC vendors pushing these communication standards to new levels of performance. The present and future is looking bright for PLC communication standards as we look at what the future holds.

One example is EtherNet/IP, as it moves past its 15th birthday, which through the years has expanded into a reliable and popular industrial Ethernet communication network connecting machines, processes and factories. Some keys to its success are the network and transport protocol layers where explicit and implicit messaging is used. EtherNet/IP's features and terminology will be discussed to help with application of its networks in industrial automation.

PLCs Make the Connection

PLCs must communicate in real-time to a wide variety of devices such as local and remote I/O, motors, drives, servo controllers or other PLCs. An interface to a PC-based HMI or an operator interface terminal (OIT), and possibly the Internet may also be required. There may also be communication to upper level server PCs running various quality, manufacturing and enterprise applications.

All of these communications require two things: a physical connection or layer, and a shared protocol. The physical layer defines the electrical, wiring and connection requirements. The shared protocol is the common language allowing each device to understand what the bits and bytes in the communication messages mean.

Through much of the PLC's early years, it was common for PLC vendors to use proprietary communications. This provided a robust and well defined communication to the supplier's family of products, but made connections to other suppliers' software and hardware difficult.

Proprietary communications

Many of the older, proprietary communication protocols are still in use due to easy connection among a single supplier's products. And even on newer smaller systems with no plans for expansion or connection to other systems, the proprietary communication option is still a viable approach. These older connections using RS-232C, RS-422 and RS-485 and related protocols are still supported by many suppliers.

For example, some PLCs use a serial RS-232C or RS-422 physical layer network such as the DirectNET protocol for communications. This protocol can be used for PLC-to-PLC communication over a point-to-point or multipoint network using standard PLC instructions, or to talk to HMIs. If the control system will include multiple suppliers or communications to other computing systems, standard communication protocols become more important. These standards start at a physical layer.

The physical layer is often confused with the physical medium such as the cable, connectors, network interface cards and wireless transmission hardware. But, the physical layer instead defines the interface requirements necessary for proper connection to the physical medium.

The physical layer defines how to connect the upper data link layer in the Open Systems Interconnection (OSI) communications model within a computer to physical devices. It defines the hardware requirements, schematics and specifications for successful bit-level communication to different devices. The physical layer defines items such as bit rates; transmission electrical, light or radio signals; flow control in asynchronous serial communication; cable types; and the mechanical design of connectors.

With the physical layer mechanical and electrical requirements defined, a variety of different protocols can reside in the physical layer. Ethernet, USB and Bluetooth are the most common physical layer protocols specified in new products and applications, and represent the future direction of PLC communications.

But common physical layer protocols also include:

- Proprietary protocol for a RFID reader using an RS-232 point-to-point connection

- VFD protocol connecting multiple devices on an RS-422/485 multi-drop connection
- Printer protocol over a parallel interface
- Ethernet for connection to a plant or control network
- USB for connection to keyboard
- Bluetooth for connection to a wireless microphone

Protocols travel the physical layer

A protocol defines a set of rules for communication among networked devices on a physical layer. Some common protocols used in the industrial arena include Modbus RTU, EtherNet/IP, Ethernet TCP/IP, Modbus TCP/IP, Profibus DP and Profinet.

One of the more common industrial serial communication protocols is Modbus RTU, developed by Modicon and usually running on an RS-485 network. This is just one of many popular serial protocols, supported by suppliers and used by a wide range of automation professionals. However, performance limitations make serial protocols a poor choice for high-speed and high-performance applications.

Ethernet has become the dominant standard for the physical layer of many industrial protocols such as EtherNet/IP, Ethernet TCP/IP, Modbus TCP/IP and Profinet due to its performance and other advantages. And unlike serial protocols, multiple Ethernet protocols can run on the same Ethernet physical layer.

It has become common to use Ethernet to interconnect several devices such as PLCs, HMIs, field I/O and valve banks. Plus, the communication remains fast while talking to several dissimilar devices on the same cable, due to the very high speed of Ethernet as compared to older serial networks.

Today's physical, wired layer is moving to Ethernet for most control system communications with EtherNet/IP becoming a very popular industrial protocol. But with this protocol, explicit and implicit messaging should be understood to optimize network operation.

EtherNet/IP messaging modes

To help optimize a real-time EtherNet/IP network, it's important to select a controller supporting explicit messaging as a client or server, and implicit (real I/O) messaging as a scanner or adapter. With explicit messaging, the controller is called the client and the field devices are called servers. With implicit messaging, the controller is called the I/O Scanner and the field devices are called I/O Adapters.

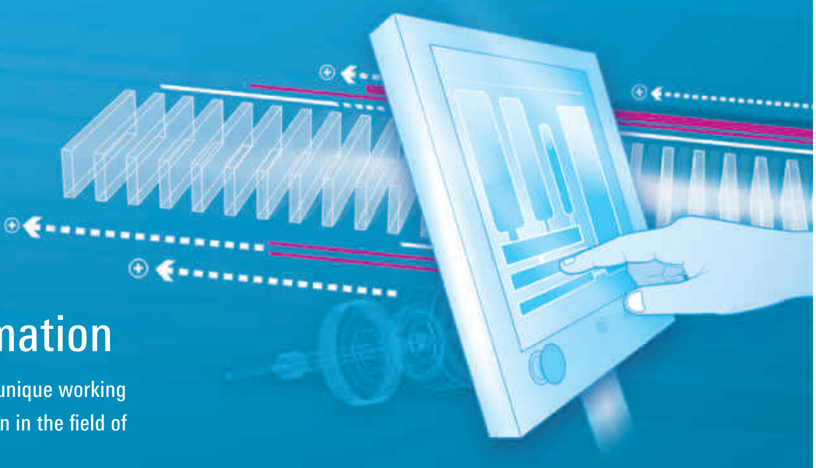
While a controller generally supports both explicit and implicit modes as a client, server, scanner or adapter, the choice often depends on the field device itself. Many times, field devices only support one messaging mode.

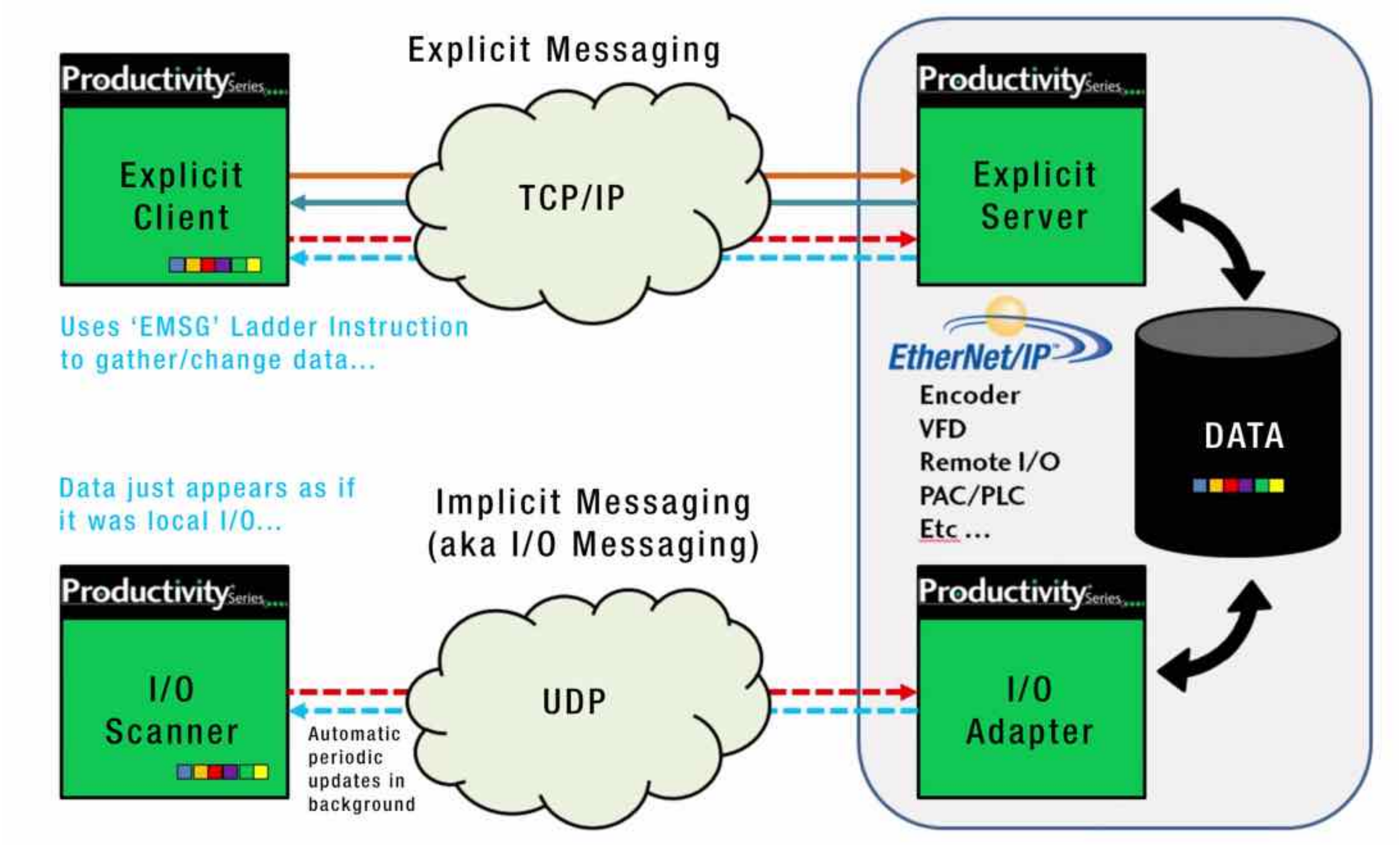
Explicit messaging is often the better choice if the application requires large amounts of data. In this case, explicit messaging can save bandwidth as data is only transmitted when needed or requested.

Implicit messing is typically the best choice for real-time, high speed applications. Think of the "i" in implicit as the "I" in I/O messaging, which of course requires high speed as I/O is generally used for real-time control.

Explicit messaging requires programming in the controller for setup as the data must be explicitly requested. Programming is required to request the data, provide handshaking, acknowledge the data, and move the data where it's needed in the controller.

Real-time implicit messaging, by comparison, is quickly configured with little or no programming. The controller is configured as a scanner to send and receive data, and to connect to a remote EtherNet/IP device, all by filling in the blanks in the controller programming software. The configuration defines what the data is and where it will be





SOURCE: AUTOMATION DIRECT

This diagram highlights some of EtherNet/IP's explicit and implicit message modes, terminology and usage. Explicit messaging handles requests and definition of information, while implicit messaging is data only, and no protocol information is included (also known as I/O Messaging).

in the controller data table. Once configured and with the controller up and running, the data appears in controller memory without handshaking or data handling.

Controller outputs are sent to field devices, local bits are set, and integers and floating point words are written as the data is automatically sent to the device based on program scan. Data is transferred at the specified rate, typically in the 5 to 20ms range.

Explicit messaging applications

With the EtherNet/IP protocol, the explicit message connection is a client/server relationship. A client such as a PLC requests data from a server and the VFD, for example, sends the information back to the controller.

Since the request for data issued by the client uses TCP/IP services, the server has the information necessary to explicitly respond to the message. The client/controller requests the data and specifies how it is formatted, and the server/VFD provides the data, formatted as specified.

Typically, explicit messaging is used in applications that are not time critical. The monitoring and configuring ability common to explicit messaging works well in applications where the client can send data requests or configuration parameters anytime, and the server can respond when available.

Implicit messaging applications

With the EtherNet/IP protocol, implicit messaging is commonly used for time-critical control applications. Implicit messaging is sometimes called I/O messaging since a common application is communication between a controller and remote I/O. Because the I/O scanner and I/O adapter are pre-configured to implicitly know the data format and communication requirements, implicit messaging is significantly more efficient when compared to explicit messaging.

EtherNet/IP terminology	Explicit Messaging	Implicit Messaging
Originator (master)	Client (controller)	I/O Scanner (controller)
Target (slave)	Server (field device)	I/O Adapter (field device)
Form of messaging	Unconnected but can be connected	Connected
Typical use	Diagnostic/event/configuration data	Real-time control data

SOURCE: AUTOMATION DIRECT

Explicit versus Implicit Messaging

Since the data has been pre-defined, real-time implicit messaging basically just copies the data with little overhead information required in the message. Neither end of the message communication link needs to be told what the data is as the meaning of the data is implicit or implied. Both the controller and field device know what each bit and byte mean.

Connected messaging

Other terms often used with respect to Ethernet/IP messaging are unconnected and connected. Explicit messages usually are unconnected messages. Implicit messages are typically connected messages configured in advance for real-time I/O messaging. These connected messages also use features built into each device to enable this high speed connection.

With the popularity of Ethernet communication in industrial applications, continued improvements and additional standardization should be expected in the future. For today, in simple applications, a proprietary protocol may be the best solution. However, when the application requires high speed, extensive connectivity and scalability, an Ethernet protocol is likely the best solution.

Rick Folea is Senior Technical Marketing Specialist at ***Automation Direct****.*

industrial ethernet book

Reader Service Card

IEB issue 90 - October 2015

Service

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

Return by mail to:

IEB Media
Bahnhofstr. 12
86938 Schondorf
Germany

Or fax back to:

+49 8192 933 7829

Or use our online reader service at:

www.iebmedia.com/service

Please enter your contact details below:

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

I want to:

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

Signature: ______________________________

Date: ______________________________

Company Activity (select one)

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

Job Activity (select one)

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

IEB Media reserves the right to refuse an application for a free copy of Industrial Ethernet Book or the provision of information on any of the advertisers or articles

PROFINET solution platform for process automation: part 1

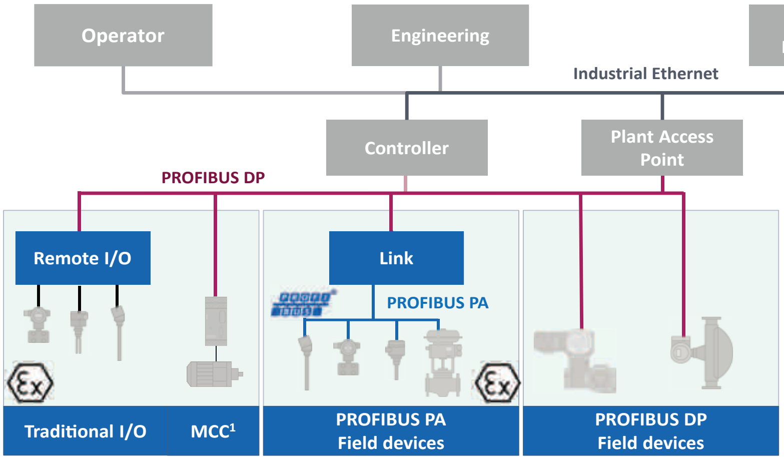
Process automation places additional demands, compared to factory automation, on the use of communications technology. This article is the first installment of a technical discussion of how PROFINET technology can address the complexities of process control applications.

PROFINET AS A SOLUTION PLATFORM for process automation provides all the technology and tools required by process industries to fulfill the need for integrated automation of plants and effective networking based on the use of Industrial Ethernet technology. The major first step is the application PROFINET in new process automation plants and new plant sections with tools for integration of the installed base of 4...20 mA, PROFIBUS PA, and other bus systems.

Technologies for a horizontally and vertically integrated PROFINET automation solution for process technology will be developed in the near future. Both steps will contribute to improving the efficiency of companies and their competitive position in the application environments created by Industry 4.0 and the Industrial Internet of Things.

Process automation, compared to factory automation, places additional demands on the use of communication technology. Plants usually extend over wide areas and have a lifespan of 15-40 years. These plants also often consist of continuous production processes where interruption or disturbance can pose a serious hazard for people and the environment.

An unplanned stoppage can also mean a large financial loss. Plant owners want to achieve an integrated data and information flow both horizontally and vertically. This yields clear specifications and requirements for the communication technology.



SOURCE: PI NORTH AMERICA

Communication structure of a plant with PROFIBUS DP and PROFIBUS PA.

Process industry requirements

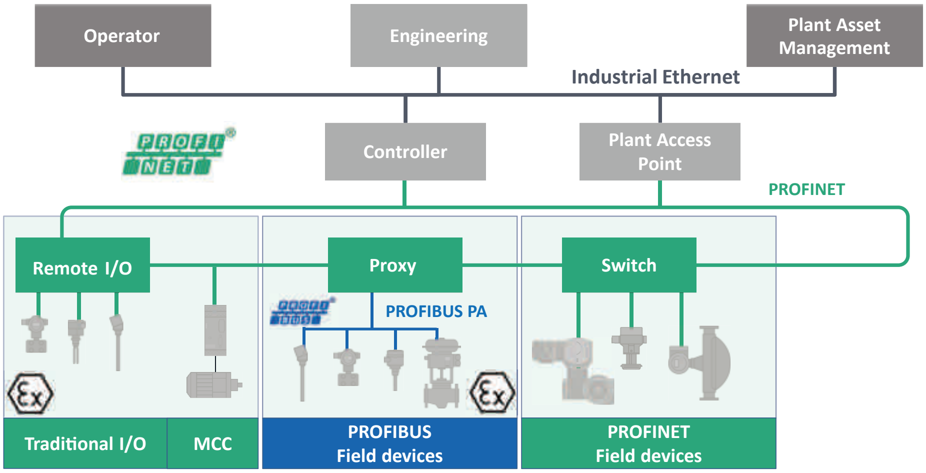
- Installation technology and field devices can be handled easily and by skilled staff
- Application in hazardous areas, including intrinsically safe ignition protection
- Long cable distances (up to 1,000 m)
- Flexible topology design
- Robust connection technology
- Redundancy concepts for critical components

The communication interface is to be standardized in order to ensure the smooth interaction of components of different manufacturers. The communication interface and the systems for engineering, asset management, and plant control should have the following properties:

- Maximum reliability and availability
- Disturbance-free configuration during plant operation
- Easy handling, for device replacement
- Investment protection for existing plants, including changes of the process control technology
- Suitable for large quantity structures of 10,000 or more devices

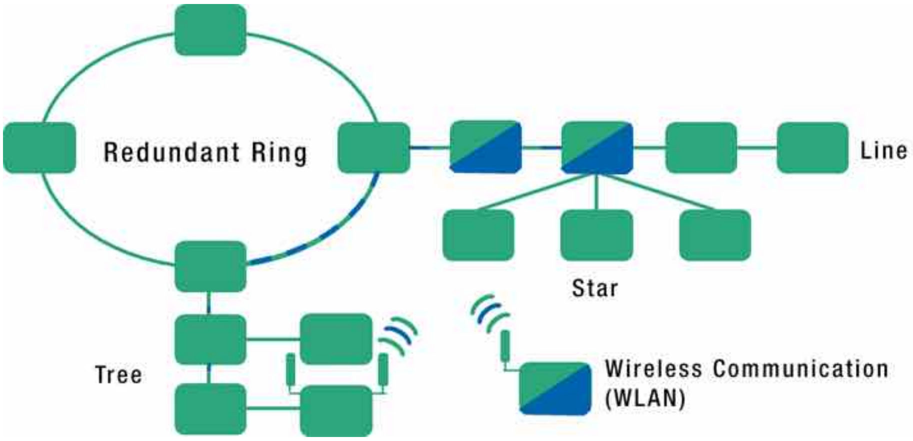
A particular expectation of the chemical industry was addressed in a keynote speech at the 2014 NAMUR General Meeting: the merging of automation technology with the IT world, with the goal of protecting the competitive capability of chemical companies into the future. Together with the large plants in the chemical, petrochemical, and oil & gas industries, there are industry sectors with clearly lower requirements for, e.g., cable distances and explosion protection.

PI defines the underlying technology for all listed requirements. The following sections provide an overview, starting from the current status of today's available technology and products, continuing with specifications already being implemented or about to be implemented and ending with planned further improvements. The further development of existing specifications and new definitions of technologies take aim at requirements that must be fulfilled in the future. The open and fact-based discussion in the PI committees



SOURCE: PI NORTH AMERICA

PROFINET & PROFIBUS PA.



SOURCE: PI NORTH AMERICA

Flexible network configuration of PROFINET.

leads to vendor-neutral, well-defined solutions for a heterogeneous process landscape.

PROFIBUS PA fieldbus

PROFIBUS PA is the fieldbus that enables long cable distances and explosion protection for the harsh environments of process automation and offers complete digital integration of field instrumentation in control and asset management systems. The connection is made using a link/coupler typically via PROFIBUS DP.

The user benefits of PROFIBUS PA result from use of digital instead of analog communication with many positive consequences, a simple validation of intrinsically safe ignition protection (FISCO Model), and the properties of the PA 3.02 device profile tailored specifically to process industry needs.

The fieldbus combination "PROFIBUS DP with connected PA segment" is found in many installations worldwide, where it proves itself as both a high-performance and stable solution. Specifications and guidelines such as the proven PA 3.02 device profile provide the needed standardization, while the many field devices from various manufacturers provide users with a great deal of choice when selecting instrumentation for their plants.

To date, some requirements have not been tackled, especially in connection with device replacement and device integration. There used to be a need regarding excessive time expenditure and reliability of handling and an uneasiness about the existence of two very different integration technologies, which caused significant effort for users and manufacturers alike. Version 3.02 of the PA profile standardizes the compatibility of devices so that device replacement is possible independent of manufacturer and software version. The duplication of integration tools will soon end with the newly completed joint industry standard FDI (Field Device Integration) that also supports PROFIBUS PA.

PROFIBUS PA provides benefits in all stages of the life cycle of a process plant; from plant planning and construction as well as for installation, operation, and maintenance of the plant. PROFIBUS PA generates these benefits through automatic documentation and a shortened and effective loop check, reduced installation effort, easy proof of intrinsic safety for operation in hazardous areas, requirement-oriented maintenance, easy device replacement, etc.

PI sees PROFIBUS PA as an up-to-date key technology for the digitalization of field communication. Proxy specifications are well defined to implement the integration of current and future installations on PROFINET-based environments. This technology, optimally and transparently designed for engineering and operation, enables the migration strategies needed for the longevity of a process plant.

PROFINET in process automation

Applications with PROFINET already exist today, especially in areas in which PROFIBUS DP was previously used, and remote I/O or motor management systems were connected. However, this use case is subject to limitations because PROFINET functions such as "System Redundancy" and "Configuration in Run" are not yet implemented in all products.

PROFINET devices such as Remote I/O and Motor Control Center (MCC), PROFIBUS PA field devices for explosion-proof applications can be integrated in PROFINET using a proxy. A switch connects PROFINET field devices for applications without requirements for explosion protection, optionally supplied via Power over Ethernet (PoE).

PROFINET technologies important to process automation and field devices are: network configuration, connection technology, network diagnostics, topology display, detection of neighboring devices, device replacement and diagnostics. These functions enable automatic address configuration during device replacement, and display of a plant which can be used to ensure that a replacement device was connected at the correct port. The replacement receives the same name and parameters as the replaced device.

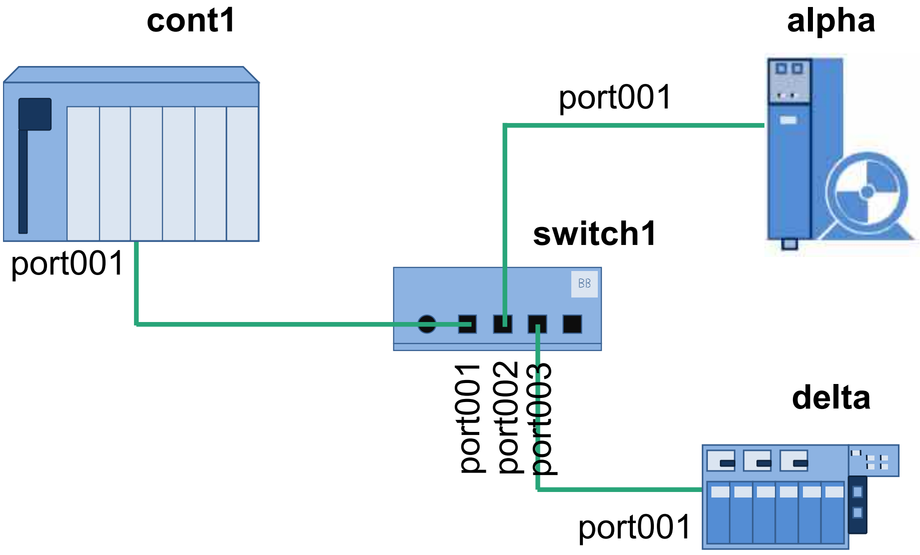
Network installation and diagnostics

Maximum reliability and system availability is a basic requirement for use of communication technologies in process automation plants. This also applies to PROFINET and its connection technology. The network configuration of PROFINET can be designed flexibly, and optimally reflects the plant conditions. The following topologies are supported:

- Line topology connects field devices with integrated switches in the field
- Star topology with a central switch located in the control cabinet
- Ring topology, primarily for implementation of media redundancy
- Tree topology, in which the topologies listed above are combined

Today's defined and utilized connection technology meets the requirements for wiring these switching techniques.

The connection of PROFINET devices is carried out exclusively using switches as



SOURCE: PI NORTH AMERICA

PROFINET field devices know their neighbors.

network components, which are often already integrated in the device. PROFINET-suitable switches must support bot "Auto-Negotiation" and "Auto crossover" functions. As a result, communication can be established autonomously, and the physical cable designs are uniform. The nodes (devices and switches) are connected by copper cable up to a distance of 100 m. For longer transmission distances, fiber-optic cables are used.

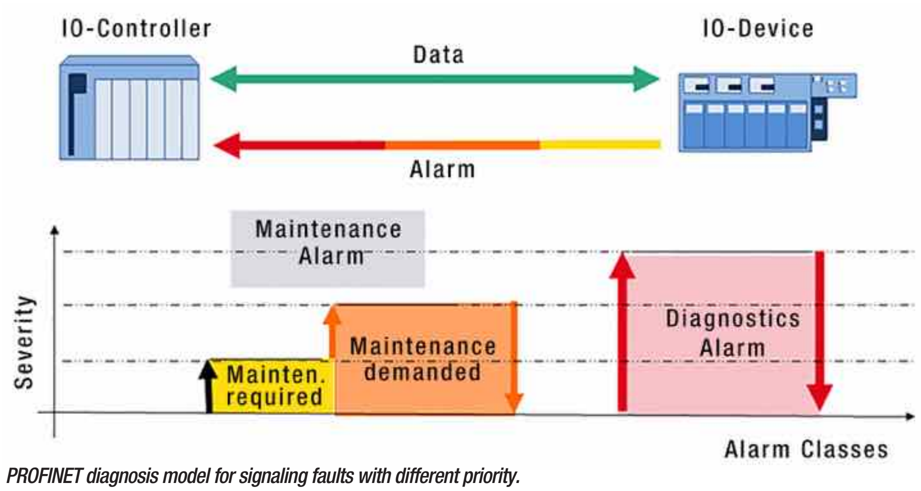
Network management

In IT networks, the SNMP (Simple Network Management Protocol) has established itself as the de facto standard for maintenance and monitoring of network components and their functions. For diagnostic purposes, this protocol can read-access network components, in order to read out statistical data pertaining to the network as well as port-specific data and information for neighborhood detection. SNMP must be implemented for devices of Conformance Classes B and C.

Network diagnostics

PROFINET field devices use the LLDP (Link Layer Discovery Protocol) according to IEEE 802.1AB to exchange the available addressing information via each port. This allows the respective port neighbor to be explicitly identified and the physical structure of the network to be determined.

With this neighbor detection, a preset/actual comparison of the topology is possible and changes of the topology during operation can be recognized immediately. This is also the basis for the automatic naming during device replacement. The collection of the information obtained via neighborhood detection using the SNMP protocol enables a graphical representation of the plant topology and port-specific diagnostics.



SOURCE: PI NORTH AMERICA

PROFINET diagnosis model for signaling faults with different priority.

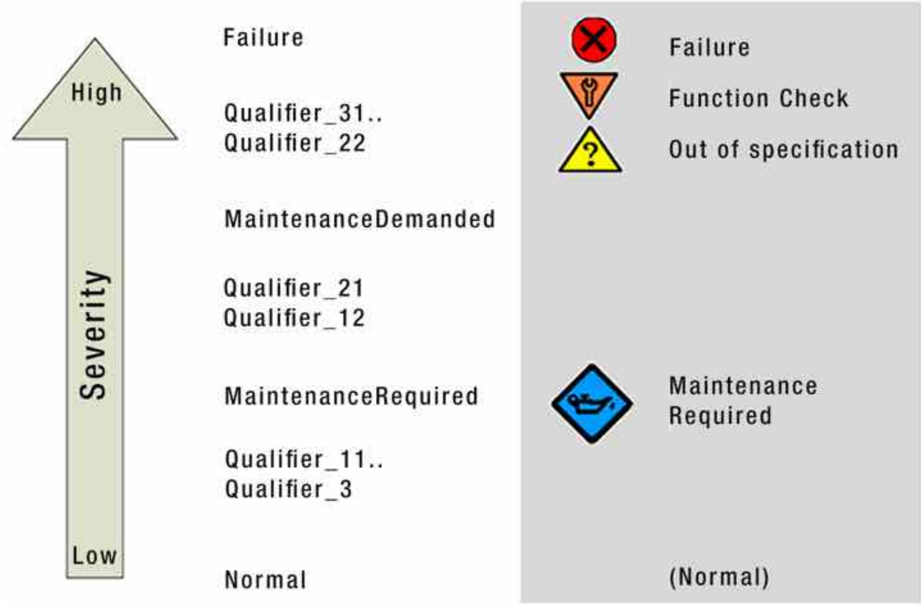
Device diagnostics

Status-oriented maintenance is important for operation and maintenance of plants. It is based on the capability of devices and components to determine their status and to communicate using standardized mechanisms.

PROFINET provides a system for reliable signaling of alarms and status messages from the devices to the controller. This diagnosis model covers system-defined events such as removal/insertion of modules and the signaling of malfunctions such as a wire break that are detected by the control mechanisms.

Besides the "good" and "faulty" status, the underlying status model also knows the optional levels "maintenance required" (e.g. when media redundancy is lost) and "maintenance demanded". The module also distinguishes between diagnostic alarms (events within a device or component) and process alarms (events in the process, e.g. limit temperature exceeded).

To ensure a uniform display of the different diagnostic messages, the results of the PROFINET diagnosis model have been assigned to the diagnostic display according to the NAMUR NE 107.



SOURCE: PI NORTH AMERICA

Assignment of the PROFINET device diagnostics to NAMUR NE 107 requirements.

Device replacement

Replacement of PROFINET field devices can be performed easily due to the cyclic exchange of neighborhood information of devices. If a device fails, its neighborhood is known. A replacement device that is "nameless" to start is inserted, and the controller searches for the explicitly identifiable neighbor device of the defective device. As a result, the replacement device can be assigned the same position in the network, the same address, and the same parameter set as the failed device. In addition, the address and positioning of the device is also shown in the diagram of the plant topology and can be verified once installed. This enables fast and reliable device replacement even without an engineering tool.

This continuous visualization of the network and the related ability to immediately detect, for example, address conflicts lend support to plant commissioning, modification and expansion. The result is significant time savings compared to past procedures.

Summary of user benefits

- Automatic creation and checking of the topology (visualization)
- Accelerated commissioning and easy device replacement
- Easy configuring, even without an engineering tool
- Prevention of address conflicts
- Easier handling than 4...20 mA technology
- Continuity of diagnostic displays based on NAMUR NE 107

In the next issue of the Industrial Ethernet Book, this coverage of Profinet in Process Applications will continue with information on how PROFINET addresses security, availability and advanced system architectures.

*Technology report by **PI North America**.*

Managed gigabit PoE++ switches

EtherWAN Systems: The EX78900 series, a hardened managed DIN-Rail 16-port Gigabit PoE switch, supports PoE++ (also known as Ultra PoE) of 60W per port.

The EX78900's PoE/PSE ports are not only IEEE802.3af/at compliant, but they are also enhanced with ultra-powerful PoE chips to boost the PoE output power up to 60 watts per port, utilizing all 4 pairs of a single CAT5e cable. It enables a wide range of applicable cases with broader end devices support, such as VoIP telephony, Wireless Access Points, high-definition PTZ dome cameras, infrared network illuminators, physical access control with door locks, information kiosks, digital signage, and so on.

In additional to high-power PoE support, the EX78900 switch is equipped with a total of 16 Gigabit ports. The versatile design of the EX78900 series allows port configurations as many as 12 full Gigabit copper ports including 8 PoE ports (60W of each at maximum PoE power budget of 240W) and 4 SFP slots for uplink communication or redundant topology. The overall 32Gbps switching capability is enabled, which is ideal for large video packets transmission.

Fast Industrial Ethernet switches

Belden: Hirschmann RED25 switches provide cost-effective and customizable networking solutions for industries in need of redundancy and security.

RED25's focus on redundancy makes these switches a solid fit for the automotive, manufacturing and machine building industries which tend to have automation systems that are part of the network infrastructure. When a system failure occurs, it happens most often within the network and causes service interruptions. RED25's redundancy technology can reduce the effects of these failures, minimizing the risk of outages while maximizing productivity, ensuring consistent communication and keeping plants operating.

In addition to supporting various redundancy technologies, the RED25 switches have comprehensive built-in security features to provide reliable protection against network attacks or operating errors. They are also customizable based on specific port needs or environmental factors, such as temperature range.

RED25 provides maximum productivity and network uptime, thanks to interruption-free data communications based on parallel redundancy protocol (PRP) and high availability seamless redundancy (HSR).

10-Port Industrial PoE+

Antaira Technologies: The LMP-1002G-SFP and LMP-1002G-SFP-24 series are cost effective 10-port industrial gigabit PoE+ managed Ethernet switches, with a 48~55VDC high power input (LMP-1002C-SFP) support, and a 12~36VDC low voltage power input with a built-in voltage booster (LMP-1002C-SFP-24), of which, the unit provides a full 48VDC PoE power for any low voltage power source or mobile PoE application environment.

Each unit is designed with eight 10/100/1000Tx Fast Ethernet ports that are IEEE 802.3at/af compliant (PoE+/PoE) with a PoE power output up to 30W per port and two dual rate 100/1000Tx SFP slots for fiber connections. This product series supports Jumbo Frames up to 9.6Kbytes, and it provides high EFT, surge (2,000VDC) and ESD (6,000VDC) protection. In addition, all units have a dual power input design with a reverse polarity protection and a relay warning function to alert maintainers when any ports break or power failures occur. This makes it ideal for applications in a harsh environment requiring high reliability and distance extension capability.

The switches have been designed to fulfill outdoor industrial automation application environments. Some of these environments include high density traffic control equipment within ITS applications, remote PoE wireless radios, security surveillance systems, GigE vision systems, and quality inspection systems within factory automation.

40G BiDi MMF QSFP+ transceiver

Avago Technologies: A 40G bidirectional (BiDi) multimode fiber (MMF) QSFP+ transceiver module, the AFBR-79EBPZ is designed for highspeed data center interconnect and networking applications. Based on innovative 2x20G BiDi optics, the module enables 40GbE links on existing installed LC duplex multimode fiber of 10G network, providing a cost-effective upgrade path to 40G Ethernet in the data center. The AFBR-79EBPZ supports 40GbE data transfer over 100 meters of OM3 fiber or 150 meters of OM4 fiber.

40G Ethernet is an important technology in the data center as enterprises transition the aggregation/spine layers of their network towards higher speeds. As this transition occurs, Avago expects 40G Ethernet switches to surpass 10 million ports in 2017, almost a four-fold increase from 2014 levels, especially with the increased availability of high ROI, low TCO solutions that leverage the existing 10G cabling infrastructure.

The 40G BiDi transceiver technology is an important product because it will facilitate many end companies in their transition from 10G to 40G network to meet the ever-increasing demand for bandwidth.

New flexible RFID system

Balluff: The BIS V industrial RFID system is capable of reading three different frequencies of RFID tags, and is designed to address the challenges of a flexible manufacturing environment.

With four dedicated RFID ports and one IO-Link master port, RFID can now be mixed with sensors, hubs, actuators, and even SmartLight tower lights all in one processor. Since it has an IP65 rating, this Balluff BIS V processor can be mounted directly on the production line instead of making long runs back to a control cabinet. Being released along with the processor are several new read/write heads. These heads were designed to address applications where the part or pallet must be read on-the-fly, since they can transfer a relatively large amount of data very quickly. In addition, there are multiple form factors available that allow mounting in the tightest of spaces.

As with most other Balluff RFID systems, the BIS V can connect to all major control systems. Since each device houses a network In and Out port, the network can be configured in multiple topologies and make a single connection back to the PLC via Ethernet/IP, Profinet, Profibus, CC-Link, or Ethercat.

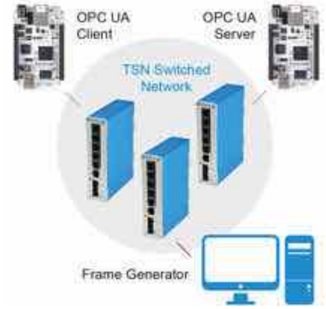
VeriSens PROFINET gateway

Baumer: A new VeriSens PROFINET gateway provides additional benefits through efficient VeriSens interfacing on PROFINET with visualization and FTP communication in parallel with real-time Ethernet. The features of the VeriSens remain available while removing load from PROFINET communication in the form of the high data packets of image processing.

PROFINET as a common real-time Ethernet standard is ideally suited for the integration of intelligent automation components like vision sensors. The VeriSens PROFINET gateway allows for efficient interfacing of up to four VeriSens on PROFINET. The integrated switch simplifies architecture of the typical linear network topology.

In image processing tasks visualization is normally a must and can now be easily established in parallel with PROFINET communication. The VeriSens Ethernet port remains available for visualization via configurable web interface and image saving on an FTP server. The VeriSens PROFINET gateway is supported by the VeriSens Application Suite software, also available is the product-specific PROFINET GSD file for integration.

Deterministic Ethernet starter kit



TTTech: The DEStarter Kit supports IEEE TSN (Time-Sensitive Networking) and is a tool for the evaluation of industrial applications over standard real-time Ethernet. The starter kit offers an out-of-the-box set up which for the first time allows users to test the performance of OPC UA and Profinet components over a TSN network. Included in the kit are TSN-enabled switches from TTTech, nodes with OPC UA and pre-loaded configurations.

TSN (Time-Sensitive Networking) is a set of IEEE 802 Ethernet substandards that are defined by the IEEE TSN task group. The emerging standards enable time-scheduling of Ethernet traffic, and therefore fully deterministic real-time communication within the 802 suite of standards.

TSN users benefit from Guarantee of Service, which allows for the convergence of controls, streaming and data traffic over one standard Ethernet network without affecting real-time performance or wasting bandwidth. This convergence means that real-time industrial systems can be connected to cloud services and synchronized with one-another over standard Ethernet.

With this starter kit, which will be available in Q4 2015, customers can learn more about TSN and evaluate their own applications over a Deterministic Ethernet network.

PoE added to wireless gateway

Emerson Process Management: Adding Power over Ethernet (PoE) allows the smart wireless gateway to easily integrate with compatible infrastructure without the need for extra wiring

Added PoE to the Smart Wireless Gateway 1420, makes it possible to power the gateway and compatible devices using a standard Ethernet cable. PoE allows easy, economical installation of wireless Gateways without requiring extra power wiring infrastructure.

The PoE Gateway provides infrastructure flexibility in places where there is limited access to power. By using an Ethernet cable connection, a new PoE Gateway can be easily installed and powered by an existing wireless access point. Alternately, PoE allows the Gateway to power any Ethernet-enabled instrument. Taking advantage of existing power infrastructure results in a significant cost savings compared to running new wiring.

New Wireless AP/Bridge/Client

Moxa: AeroLink Protection on the new AWK-3131A automatically restores communications within 300ms of connection failure to help industrial wireless networks avoid interruptions.

In industrial networking applications, such as communications between offshore oil platforms or train-to-ground communications, a reliable wireless bridge is essential to minimize system downtime and maximize availability. Moxa's new AWK-3131A wireless AP/bridge/client delivers fast, ultra reliable wireless performance in industrial settings by supporting IEEE 802.11n technology with a maximum net data rate of 300 Mbps, plus AeroLink Protection redundancy to prevent a single point of failure from bringing down an entire network.

With AeroLink Protection, a network has two or more protected wireless client nodes connected to a single access point. One serves as the active node, while the others are passive backup nodes. If the active node stops sending or receiving data for any reason, AeroLink Protection completely restores the communication link within 300ms (milliseconds) by bringing backup nodes online.

Gigabit Managed Industrial Ethernet

ORing: A new series of industrial Ethernet switches compliant with IEC 61850-3 and IEEE 1613 standards are targeting the power substation and railway markets. The IGS-P9000 series, which consists of four models featuring unique characteristics, are able to cater to customers' various needs in different environments.

Four models provide a high port density for large-scale deployments. The provisioning of 8 to 16 Gigabit copper ports, depending on the switches installed, makes fast transmission of large volumes of traffic across a network possible.

With fiber-optic connections via SC connectors or SFP transceivers, the switches provide high-performance aggregative connectivity for bandwidth-hungry applications such as multimedia content and videos. The versatile copper/fiber combinations guarantee long distance data communications in a cost-effective way between the core layer and the edge layer of your network.

The series supports the company's device backup unit DBU-01 to back up or restore device settings easily via the console port. All switch settings can be stored or restored to previous conditions within seconds, significantly simplifying configuration of network layouts.

.NET Software Development Kit

Opto 22: A new .NET Controller Software Development Kit (SDK) for writing custom Microsoft Windows software applications that communicate directly with Opto 22 SNAP PAC controllers. This new SDK is well suited for machine builders, original equipment manufacturers (OEMs), and others who integrate custom applications with Opto 22 control systems. The .NET Controller SDK for SNAP PAC supports modern .NET frameworks and Visual Studio environments, which reduces the time and cost of software development and testing.

Developers use the .NET Controller SDK for SNAP PAC to build software applications that directly access the control program, or "strategy," running on a SNAP PAC controller. Applications can read from and write to integer, float, and string variables and tables, as well as analog and discrete input and output points.

The SDK supports Microsoft's .NET frameworks 4.0 through 4.5 and Visual Studio 2010-2013, includes sample .NET code and comprehensive documentation for packages and classes, and is available as a 100% managed DLL. The .NET Controller SDK for SNAP PAC is available now and can be downloaded free of charge.

Process data acquisition system

iba AG: The process data acquisition system, ibaPDA, is now also available with IEC 61850 interface to facilitate fault recording in the field of energy technology .

The new IEC 61850 interface allows for acquiring and recording information according to the MMS standard or GOOSE events from IEC 61850 capable protection devices. The iba system supports two functionalities: the client version for pure measurement data acquisition as well as a server version for generating alarm and status messages and transferring them to superimposed control systems. In both cases communication and data exchange will be easier to handle for the user in ibaPDA via the IEC 61850 communication than before with common hard-coded protocols.

The IEC 61850 standard of the International Electrotechnical Commission (IEC) has been established as a trend-setting solution in the field of switchgear automation. The standard defines communication structures and the object oriented data model for protection and control technology in medium and high voltage switchboards on basis of TCP/IP. The Manufacturing-Messaging Specification (MMS) is the standard for the common client communication; the GOOSE standard is used for transferring events or error messages of a protection device to the control system.

Multi-Carrier capabilities added

Red Lion: New 4G LTE multi-carrier cellular support for major North American carriers is now built into rugged Sixnet series RAM and IndustrialPro cellular automation products.

New multi-carrier capabilities enable customers to simplify deployment and reduce inventory requirements by selecting from a list of preconfigured wireless carriers that include AT&T, BELL Mobility, Rogers, TELUS and Verizon Wireless.

With 4G LTE support for multiple North American carriers in each unit, customers using Red Lion's RAM cellular RTUs and IndustrialPro routers can easily select and switch between wireless carriers to alleviate varying cellular coverage or bandwidth issues without having to replace equipment. In addition, a powerful built-in event engine can trigger I/O or send SMS text messages based on real-time data to provide automation engineers, technicians, production managers and network operators local control and real-time remote monitoring of field-deployed assets.

Red Lion cellular automation devices combine optional I/O and Wi-Fi with active GPS and multiple serial and Ethernet ports to securely monitor remote devices over a 4G LTE cellular network with fallback to 3G. Ideal for deployment in industrial M2M networks such as oil and gas, water/wastewater, utility, transportation and mining applications,

dataFEED OPC supports Windows 10

Softing: The 4.04 release of the company's dataFEED OPC Suite includes support for Microsoft's Windows 10 operating system. For license holders of the suite who are planning to migrate to Windows 10, the update is free of charge. With the support of Windows 10 in the current update 4.04 of its dataFEED OPC Suite, Softing responds to the release of the long anticipated Windows 10 operating system from Microsoft and allows its licence holders a smooth transition without additional costs.

Using the FG-260, machine builders can offer customers an easy solution for direct data exchange in EtherNet/IP systems. For system integrators looking to implement their devices with PROFINET communication functions in EtherNet/IP systems, the FG-260 provides direct connectivity without the need for an additional PROFINET controller.

The dataFEED OPC Suite combines OPC Server and OPC Middleware functionality into one compact software solution. The integrated OPC UA Server allows the simple integration of legacy and new controllers into "Industrie 4.0" solutions.

2-factor authentication security

eWON: More than 5,000 of the company's users are benefiting from the 2-factor authentication (2FA) security feature, which was launched at the beginning of 2015.open source software.

The 2FA security feature is aimed at protecting eWON customers from unauthorised access to their account and machine information. 2FA prevents hackers from using stolen passwords in order to gain access to remote PLCs and machine networks.

2FA is a secure identification mechanism that combines two different components for unambiguous authentication. It adds an extra step to the user login procedure based on the principle that an unauthorised actor is unlikely to be able to supply both factors required for access.

Extremely compact wireless switches

Steute: New wireless switches can be integrated just as easily and flexibly into steute Wireless systems as the company's larger series. Like them, the RF 13 is also equipped with an electrodynamic energy generator.

This miniaturised generator converts the kinetic energy produced by actuating the switch into electrical energy, which is then used to transmit the signal. This means that the switch is able to work self-sufficiently. It needs neither batteries nor an external power supply, i.e. no cables.

Another factor which makes it flexible to incorporate is the fact that it is compatible with all actuators in the Steute range. Its miniaturised design makes the RF 13 perfectly suited to applications for wireless switches in places where they really make sense because space is tight such as for position monitoring in or on moving systems such as tools, feeders and handling systems.

One step measuring and testing

Bosch Rexroth: National Instruments and Bosch Rexroth introduced a matched control and drive solution at this year's NIWeek conference. The advantages of the CompactRIO control hardware and the LabVIEW programming environment are combined with servo technology.

Rexroth's pre-configured drive systems for measuring and testing machines cover a wide range of services and shorten the initial commissioning to just three minutes by means of a software wizard. Using a jointly tested and already proven interface, machinery manufacturers are programming motion sequences in the graphic environment LabVIEW without a single line of PLC code.

Using the interface CAN over EtherCat, the CompactRIO control directly accesses the servo drives as master. Manufacturers can program process and motion control via the graphical programming environment LabVIEW exclusively, thereby making any additional PLC programming redundant. The plugin SoftMotion Drive Interface (SDI) required for IndraDrive Cs can be downloaded and installed directly from the LabVIEW development environment. MotionWorks IEC version 3 software makes automation programming faster, easier and more effective with features including support for PLCopen Part 4, a built-in cam editor, an HMI tagging tool, an enhanced logic analyzer and other improvements.

Machine-mountable EtherCAT I/O

Beckhoff: Machine-mountable EtherCAT Box I/O offers benefits for PROFINET applications.

Through the openness of PC-based control technology, major technological benefits can be leveraged in conjunction with numerous communication networks. The new EP9300 EtherCAT Box provides a gateway to PROFINET RT networks. This enables the use of the high-performance EtherCAT Box I/O system as an integrated IP 67 solution in PROFINET environments.

The IP 67-protected EP9300-0022 EtherCAT Box connects PROFINET RT networks with EtherCAT I/O modules, enabling local installation in the field. This extends the higher-level network entirely without the use of a control cabinet with a subordinate, high-performance, and ultra-fast I/O solution. The telegrams are transferred from PROFINET RT to EtherCAT and vice versa, so that the EtherCAT Box modules can be integrated seamlessly.

Connecting industrial outstations

Siemens: The new CP 1243-8 IRC communication processor enables telecontrol applications based on the Sinaut ST7 telecontrol protocol. The new communication processor makes it possible to connect Simatic S7-1200 controllers as outstations (remote terminal units/RTUs) to higher-level ST7 stations with minimum effort and low costs. The solution is suitable for use in new and existing systems.

Redundancy and comprehensive security functions ensure high availability and security. Key applications for the CP 1243-8 IRC are distributed plants in the fields of drinking water supply and distribution, sewer networks, and rain overflow tanks. In addition, the communication processors can be used for environmental monitoring and as local transport and distribution grids for district heating and electrical energy networks.

Connected RTUs are contacted via public or private communications networks. An industrial router can be connected to the Ethernet port of the device to establish an internet or cell phone connection. Additional connections for analog dial-up or private wireless network can be established via separate modules.

EyeVBox i3-machine vision

EVT: The compact EyeVBox IV and EyeVision image processing software is designed for application areas such as measurement technology, pattern of comparative, object detection, code reading, clear writing reading etc. Wherever place needs to be saved, the EyeVBox IV. is a compact solution. Especially with the VESA-compatible holding device, a mounting at the attachment, the monitor or the wall is possible.The EyeVBox IV is equipped with an Intel Core i3 processor and 4 GB DDR3 main memory. The CPU with an overclocking of 2 x 1700 MHz provides the great DualCore computing power. An Intel WIFI and a Gigabit Ethernet connection are available as interfaces for the network connectivity and with each two USB 3.0 and USB 2.0 Ports, corresponding cameras can be connected comfortably.

In the robust Newton housing there is also the EyeMIO (Multifunction-IO-module), which is created by EVT. This equips the VBox with various Status-LEDs and also a temperature sensor. The EyeVBox IV will be shipped with the standard command set of the EyeVision software but is also available, to customer specification, with the basic or professional command set.

Ethernet & PoE I/O modules

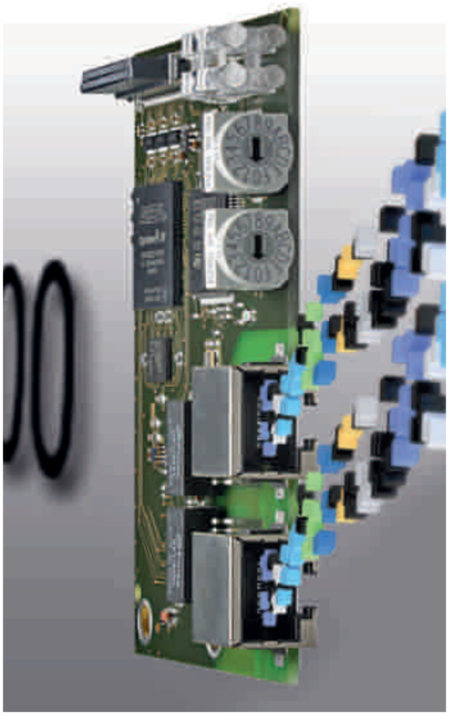
Sealevel Systems: The eI/O family of Ethernet digital I/O solutions for embedded OEM applications is designed for commercial and industrial computing applications requiring an embedded Ethernet I/O solution. eI/O OEM modules provide system designers with a compact, low-cost monitor and control alternative for a variety of applications including process control, facility management, security, and broadcast automation.

Available in six I/O configurations, eI/O OEM modules include Reed, Form C or solid-state relays; optically isolated or dry-contact inputs; as well as A/D functionality. I/O connections are simplified via removable 3.5mm terminal blocks that are compatible with 16-30 AWG field wiring. Optional spring-clamp terminal blocks are available as accessories.

OEM modules are available as Class 0 (IEEE 802.3af-2003) Power over Ethernet devices that allows power and data to be transferred over a single CAT5 cable, eliminating the need for an external power supply. Alternately, users can choose modules powered by a 9-30VDC source. Input power on DC modules is via a removable spring-clamp terminal block, requiring no tools and simplifying field installation. A variety of optional Sealevel power supplies are available.

The SeaMAX software suite supports the eI/O family and is designed to work with third party applications via the SeaMAX API. Sealevel's SeaMAX software drivers and utilities make installation and operation easy using Windows.

POWERLINK module



EPSG: KUNBUS simplifies the integration of sensors and actuators into a POWERLINK network. The KUNBUS-COM module for POWERLINK enables Ethernet-based interface connections without affecting the design of the circuit board. This makes it easy to retrofit a POWERLINK interface with minimal added development.

With compact dimensions of 85 x 65 millimeters, the module can easily be plugged into the control card of existing sensors and actuators or connected by a cable. In terms of software, the module features a Modbus RTU, a shift register interface, a dual port RAM interface and an easy-to-program script interpreter. The interface for the electrically isolated POWERLINK network is formed by two RJ45 connectors. The module has rotary switches for setting the node address and LED indicators for diagnostics.

The POWERLINK module is able to process 512 bytes of input and output data and is designed for cycle times of 250 microseconds. The KUNBUS-COM platform has a standardized pinout, so the module can also assume the function of a cost-effective option card for a range of fieldbus or network protocols.

Good old vinyl makes a comeback in the digital age

At one point, the days of vinyl records seemed to be over. In 1988, the Compact Disc surpassed the gramophone record in popularity and vinyl records experienced a sudden decline. It looked like only a matter of years till the format would become extinct. But just as CDs come under pressure from downloads and streaming music, the good old vinyl makes a little comeback.

RECORDING INDUSTRY ASSOCIATION IFPI reports that vinyl sales increased by 54.7 per cent in 2014 to US$346.8 million, while CD sales value declined by 8.1 per cent.

There must be something about gramophone records that keeps people coming back. If you want to give it a try, here are some affordable turntables to get you started.

Minimalist Gramophone

PHOTO: LIVIA RITTHALER

The Minimalist Gramophone, a concept by Berlin-based designer Livia Ritthaler, is certainly the most basic form of a turntable.

It is made out of just a needle, a cone of paper and a rotating plate with a central stick on a wooden base. There is no power mechanism, so to play a record you have to twirl it with your fingers.

There are no amplifier circuits, either. The paper cone amplifies the vibration of the needle as it travels over the record.

www.minimal-gramophone.com

Crosley Cruiser

The Crosley Cruiser is a portable turntable, constructed of wood and bound in a leatherette material, that plays 7” and 12” records at 33 1/3, 45 & 78 rpm.

It features built-in stereo speakers so you can listen to your music without having to connect it to a speaker system. Do not expect high-fidelity sound quality and be prepared that the needle might skip every now and then. The briefcase-styled record player is lightweight and easily transported, so you can take it over to a friend’s house and experience vinyl sounds together.

www.crosleyradio.com

Entry-level system

Pretty much any top list of serious budget turntables includes the Pro-Ject Debut Carbon, priced at around US$300. It’s not the newest turntable around but even after several years it’s still among the class leaders.

The unique feature is its super-light tonearm, made of carbon fibre, a material usually reserved for far more expensive models. The proven belt drive design offers low noise AC motor with effective motor decoupling and ultra precision AC generator for speed stability without unwanted vibration.

One great thing about this turntable is, that you start with a very decent system and can upgrade it later on. Pro-Ject offers a number of add-ons like an acrylic platter, a record clamp to eliminate unwanted resonances, or hi-end signal cables.

www.project-audio.com

PHOTO: PRO-JECT

Win a stylish turntable

PHOTO: CROSLEY

The Crosley Cruiser three-speed portable turntable features built-in stereo speakers, is lightweight and easily transported.
For a chance to win one, enter our quiz at:
www.iebmedia.com/quiz
The winner will be announced November 5.

Contest sponsored by:

CC-Link CLPA PARTNER ASSOCIATION

CC-Link Partner Association
G2A.CCLinkAmerica.org
CC-Link-G2A.com

Already have a turntable?

It could well be that you still have a turntable sitting somewhere in your basement, or you may find an affordable one at a yard sale.

Problem is, that in most cases you cannot hook it up directly to your sound system. The signal from the magnetic cartridge is too weak for a standard line input. It needs a special pre-amplifier, also to compensate the non-linear output of the cartridge.

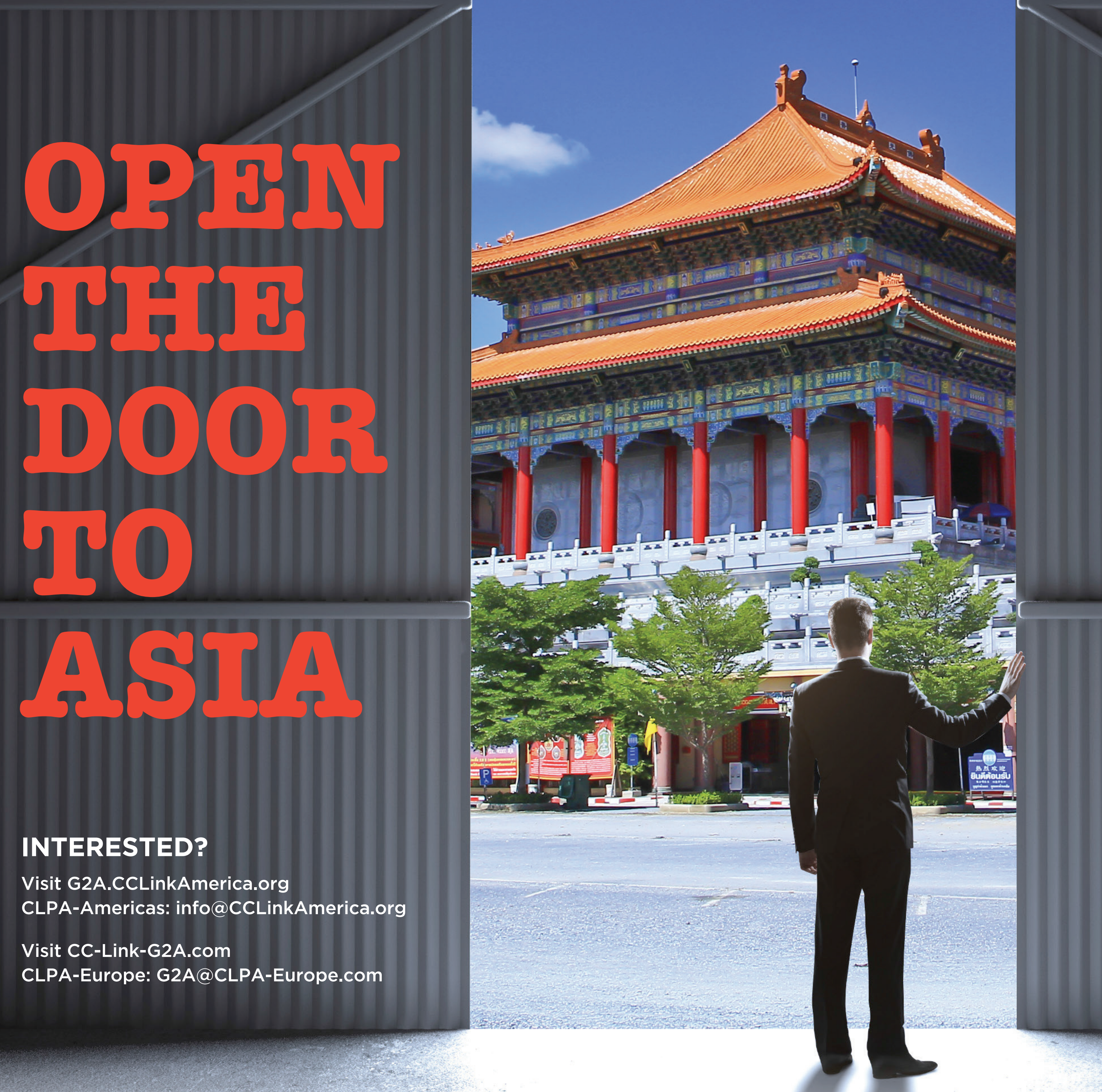
PHOTO: NAD

Offering superb sonic performance, the NAD PP 4 digital phono/USB preamp makes it easy to add phono to many of today’s stereo and AV receivers. It features inputs for both moving magnet and low noise moving coil types for a wide variety of phono cartridges.

The PP 4 goes one step further with a USB interface, which enables you to digitize your vinyl collections to a PC or Mac. A shielded USB cable and recording level control combine to reduce noise and improve the analogue-to-digital conversion process.

nadelectronics.com

Leopold Ploner



INTERESTED?

Visit G2A.CCLinkAmerica.org
CLPA-Americas: info@CCLinkAmerica.org

Visit CC-Link-G2A.com
CLPA-Europe: G2A@CLPA-Europe.com

You've implemented the local open network technologies in your products. But now it's time to look further afield. Chances are these technologies leave a large part of the Asian market inaccessible. So how can you also capture that? CC-Link is a market leading technology for open automation networking in Asia. Adding this connectivity can lead to a significant business increase in critical markets such as China. Our Gateway to Asia (G2A) program offers a comprehensive package of development and marketing benefits to capture this additional market share.

CC-Link IE™

CLPA
CC-Link
PARTNER ASSOCIATION

OPTO 22
SNAP-PAC-RCK4
OPTO 22
SNAP PAC Brain
SNAP-PAC-EB1
OPTO 22
SNAP PAC Brain
SNAP-PAC-EB2
Dual Channel Analog Input 100 ohm Pt.
A-D
Dual Channel Analog Output 0 to 10VDC
D-A
Dual Channel Analog Input PH/ORP
A-D
A-D