4.2015 Issue 87
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Network Connectivity

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

THE PFC200 CONTROLLER

Compelling, Fast and Intelligent

PFC200

V2 V3

CODESYS

High processing speed

Programmable with CODESYS 2 and **e!***COCKPIT* (based on CODESYS 3)

Configuration and visualization via Web server

Integrated security functions

Robust and maintenance-free

www.wago.com/pfc200

WE INNOVATE!

WAGO®

GET CONNECTED…

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

Contents

Connecting the OT/IT worlds...

Industrial networking technology has become a primary focus in the automation and control world, driven forward by an unprecedented need for collaboration to produce a new set of open standards to connect the industrial world. But the real challenge may be an ability to combine operational (OT) and information (IT) technologies that haven't always worked together well in the past.

One example of how collaborative efforts are achieving new cooperation is a testbed between Bosch and other members of the Industrial Internet Consortium. The project is a "Track and Trace" system to determine the position of a cordless nutrunner on the shop floor with extreme precision.

The system uses positioning information to automatically select the correct torque for the respective task, making it possible to tighten safety-relevant bolts with exactly the required torque. It also can automatically document settings to ensure and test product quality. Plus, use of open standards are set to enable the seamless integration of industrial power tools used to drill, tighten, measure, and solder into an overall system of networked tools in the future.

The new solution is made possible by connecting tools with each other, and with the production data for the products to be manufactured. Thanks to the tool's positioning information and the precisely determined location of a component, such as an aircraft on the shop floor, the user knows the tool is currently located at the vertical stabilizer, for example. Backend software automatically sends instructions that specify the torque needed to tighten bolts there.

This application is an example of what we can expect from developments with the IoT moving forward. It demonstrates how open standards, in this case a system of connected tools, can create universal solutions. But more importantly, the testbed highlights the power of digitally connected manufacturing.

But perhaps the most important thing to highlight is cross-industry cooperation on equal footing among companies working to create open standards for the purpose of data exchange. Hardware, software, localization technology, backend integration and safety features are all integrated in the solution architecture. This result is new options, and a higher level of data analysis.

Industrial networking has been thrust into the spotlight, but a key moving ahead is finding true collaboration and much more powerful solutions that combine OT (operational) and IT (information) technologies. Our goal as a magazine is to continue to highlight how this change is unfolding beginning in 2015.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **May 2015**
Deadline for editorial: April 3, 2015 Deadline for artwork: April 17, 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, both the printed and online version. 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. All updates received by April **3, 2015** will be incorporated into **www.iebmedia.com** for the next issue.

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

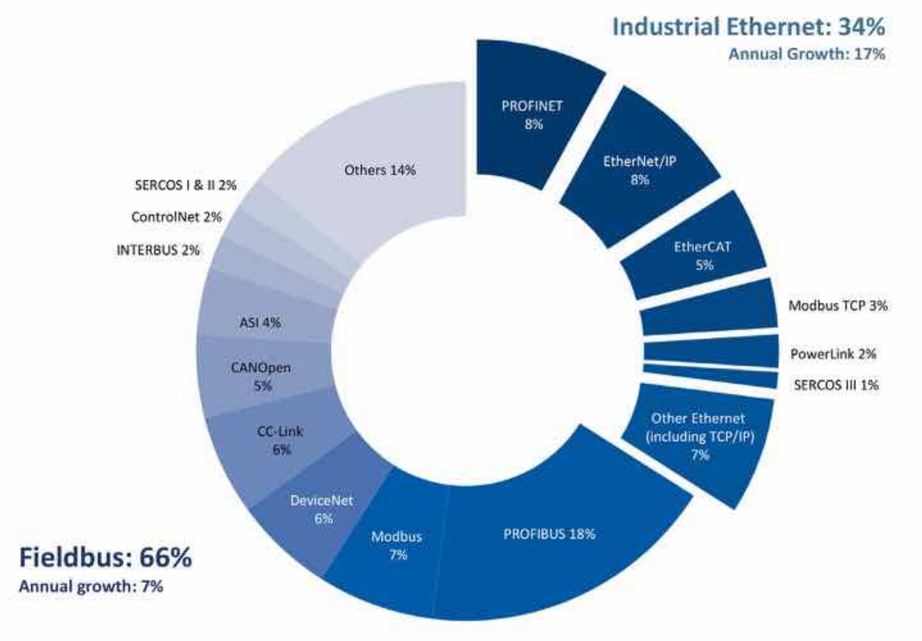
Published by IEB MEDIA
IEB Media, Bahnhofstrasse 12, 86938 Schondorf am Ammersee, Germany
ISSN 1470-5745

Industrial networking trends point to global expansion

HMS Industrial Networks offers its view of the industrial network marketplace in 2015. Fieldbuses are still the most widely used type of network with 66% of the market, followed by Industrial Ethernet at 34%.

HMS Industrial Networks has presented its view of the industrial network market in 2015. According to HMS, PROFIBUS remains the most widely used industrial network globally but several networks are closing up. PROFINET and EtherNet/IP compete for first place within industrial Ethernet and no network consolidation is in sight.

Here are some of the trends HMS sees within industrial communication right now.



SOURCE: HMS INDUSTRIAL NETWORKS

Expansion of Industrial Ethernet networks (17% per year) is increasing faster than fieldbuses (7% per year).

Ethernet segment growing fastest

Both fieldbus and industrial Ethernet networks are growing, but Ethernet is growing faster than the other networks.

Looking at new installed nodes within factory automation globally, fieldbuses are still the most widely used type of network with 66% of the market. An interesting fact is that HMS sees fieldbuses still growing by approximately 7% per year. The main drivers for fieldbus growth is simplicity, tradition and reliability. The dominant fieldbus is PROFIBUS (18% of the total world market including industrial Ethernet) followed by Modbus (7%), DeviceNet (6%) and CC-Link (6%).

Industrial Ethernet networks make up for 34% of the market and are increasing faster than fieldbuses (17% per year), but HMS concludes that it will take some time before Industrial Ethernet outgrows fieldbuses. The main drivers for Ethernet growth are higher performance and office network integration. PROFINET and EtherNet/IP are the two biggest Ethernet networks with 8% of the total network market each. Runners-up are EtherCAT, Modbus-TCP and POWERLINK.

Regional variations

In Europe and the Middle East (EMEA), PROFIBUS is the dominant network while PROFINET has the fastest growth rate. Runners up are Modbus and EtherCAT.

The US market is dominated by the CIP networks where EtherNet/IP is overtaking DeviceNet in terms of market shares. Runners-up are PROFIBUS and EtherCAT. Furthermore, PROFINET gains market shares and Modbus is still popular.

In Asia, no network stands out as truly market-leading, but PROFIBUS, DeviceNet and Modbus are widely used. CC-Link is dominating in Japan, and EtherCAT is also gaining traction.

More connected devices

"With more than 25 years of experience in industrial communication, we have a very good insight in the industrial network market," said Anders Hansson, Marketing Director at HMS Industrial Networks.

"The figures we present are based on insights from colleagues in the industry, our own sales statistics and overall perception of the market. On a general note, we see a shift towards industrial Ethernet but the migration to Industrial Ethernet is taking longer time than first expected. We still get a lot of requests for connectivity to both fieldbus and industrial Ethernet."

"What is completely evident, however, is that the network market remains fragmented and that industrial devices are getting more and more connected. This is accentuated by trends such as Industrial Internet of Things and Industry 4.0," Hansson said.

B&R receives PLCopen compliance certification for coordinated motion

PLCopen Motion Control Part 4 – Coordinated Motion specifications encompass predefined function blocks and machine state descriptions to control any multi-axis system with a standardized interface. "What these PLCopen blocks have done is to make it just as easy to configure any type of robot – regardless of its kinematic structure – as it is to set up single axes," explained Gernot Bachler, technical manager of Motion at B&R. Identical command execution is guaranteed by the use of standardized interfaces.

| EK11-08E |

The servo terminal for motors with One Cable Technology.

Directly connect AM8100 servomotors to a 12 mm Bus Terminal.

www.beckhoff.com/EL7201-0010

The space-saving servo terminals in the EL7201 series of the Beckhoff EtherCAT Terminal system integrate a complete servo drive for motors up to 200 W in a standard terminal housing. The new EL7201-0010 variant supports “One Cable Technology” (OCT), a key innovation of the AM8100 servomotor series:

- Direct connection of power and feedback signal in a single cable to 12 mm Bus Terminal
- Material and commissioning costs are drastically reduced (up to 50 %).
- The EL7201-0010 supports the direct connection of the servomotors AM8121 (0.5 Nm), AM8122 (0.8 Nm) and AM8131 (1.13 Nm).
- All AM8100 motors have absolute feedback and an electronic identification plate that can be read automatically by the EL7201-0010.

IPC
I/O
Motion
Automation

HANNOVER MESSE

Hall 9, Booth F06

New Automation Technology **BECKHOFF**

Microchip licenses EtherCAT for standalone slave controller

Leading provider of microcontroller, mixed-signal, analog and Flash-IP solutions licensed EtherCAT technology for its next-generation Ethernet controllers with focus on standalone slave controller.

ADDING ETHERCAT TECHNOLOGY to Microchip's next-generation Ethernet controllers provides system developers with the high level of integration, flexibility and stability required to design products for today's evolving industrial standards.

SOURCE: IIEB

Martin Rostan, Executive Director of the EtherCAT Technology Group (left) and Frederick K. Weber, Sr. Manager Product Marketing UNG Products, Microchip at the Embedded World trade show in Nuremberg.

Standalone slave controller

"The industrial Market segment has always been a target for our Ethernet products. It meets our long-term supply objectives and is a great fit for us," Fred Weber, Senior Manager - Product Marketing for Ethernet products at Microchip told IEB during a recent interview.

"The EtherCAT announcement allows us to develop unique next generation products that build on our existing IP. Designers who want to develop motor and motion control systems, or any application that is synchronizing nodes in a network using the EtherCAT Industrial Standard, will be able to seamlessly implement our next generation devices. EtherCAT provides excellent performance at the node or machine control level, which is attractive to us because those applications represent volume opportunities," he added.

Weber said that recent market data produced by IHS reports that the Ethernet segment of industrial automation is estimated to grow at an annual rate of 17% making this a very attractive target.

"EtherCAT is one of the fastest-growing standards in industrial automation," Weber said. "Ease-of-use, its synchronization method and the speed of data transfer create a lot of benefits for end user applications."

Technology benefits

With EtherCAT technology's "on the fly" processing capabilities and use of standard Ethernet cabling which eliminates expensive switch fabrics, Microchip's next-generation slave controllers potentially offer a high level of integration and cost optimization.

"The EtherCAT standard is a proven and robust industrial communication protocol that is expanding its market presence in drive and I/O applications," said Mitch Obolsky, VP of Microchip's USB and Networking Group. "By adding this technology to our industry-leading Ethernet controllers, we plan to provide engineers with compelling new connectivity options for their designs. This includes the Internet of Things (IoT), since EtherCAT technology is a perfect fit for adding connectivity to industrial IoT designs."

"Microchip's decision to implement EtherCAT technology into their next-generation industrial-Ethernet products will further accelerate the adoption of our communication standard within the industrial-control segment and beyond," said Martin Rostan, Executive Director of the EtherCAT Technology Group. "We welcome this move, which expands the choice of EtherCAT Slave Controller chips for our members. Microchip is making a clear statement by adding EtherCAT technology to its silicon, as a real-time Ethernet option for its customers."

For more information, visit the website: www.microchip.com/ethercat.

25 years of Sercos

The Sercos automation bus is celebrating its 25th anniversary. The first generation, presented to the public for the first time at the EMO show at Hanover in 1989, supported 2 and 4 Mbit/s transmission rates and initially was used mainly in tool machine applications. In the following years, Sercos was successfully deployed in a wide variety of applications around the globe and in a wide variety of applications and industries. In 1995, Sercos was recognized as IEC standard 61491.

Leading **MANUFACTURERS.**
High-quality **PRODUCTS.**
Countless **APPLICATIONS.**
Global **STANDARD.**

ETHERNET
POWERLINK
Standardization Group

Engineering best practices for substation networking design

Achieving the transformational objectives required to implement Big Data, Industry 4.0 and the promise of the Industrial Internet will require an unprecedented level of engineering collaboration and cooperation. In 2014, more than 125 of the biggest technology companies in the world joined to work together. This report looks into how the group is operating, the technical focus of its work and how you might become involved.

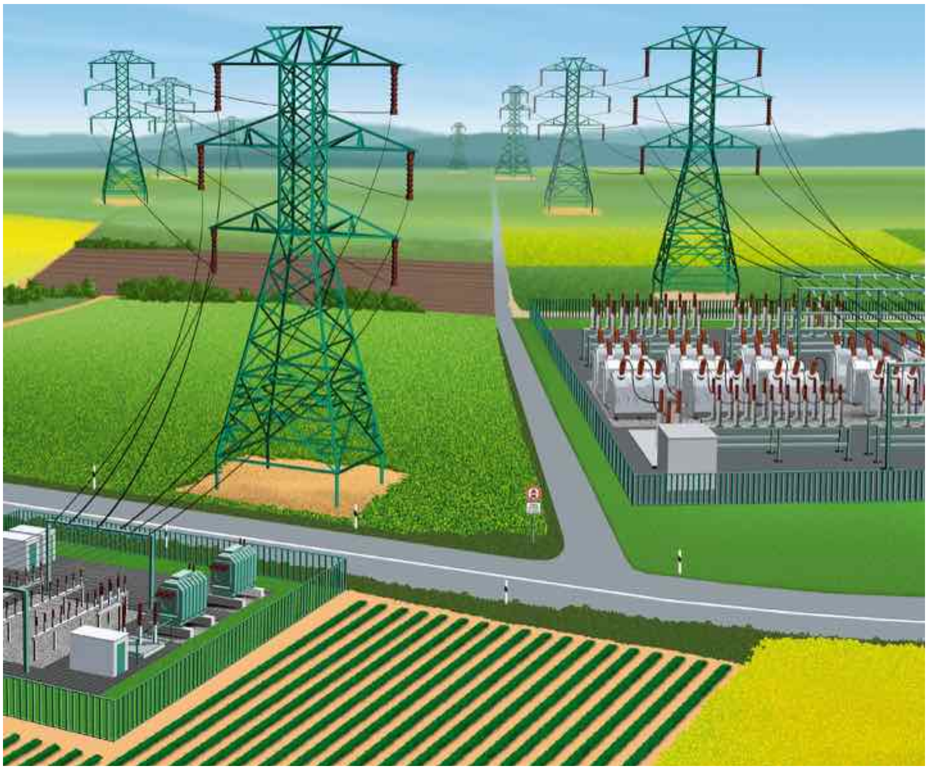
TWO TRENDS HAVE CONVERGED over the past decade, and caused many utilities to re-evaluate their substation communications infrastructure. One trend is the migration of the electrical grid from a reliable, but inflexible system to the "Smart Grid" which promises adaptability and efficiency. It also requires the two-way communication of data, something that is not possible with traditional electrical grids.

Emergence of Ethernet networking

The other trend is the increasing adoption by industry of Ethernet networking technologies for their communications. The ARC Advisory Group estimates that the adoption of industrial Ethernet networks is growing at a >12 percent plus CAGR (Compound Annual Growth Rate).

As a result of these trends, many utilities are faced with having to design and implement communications infrastructures that are unlike anything they have been involved with before.

To help, we have consolidated our experience in helping customers design robust substation communications networks. The result is a process that can assist in designing new or upgraded communications systems.



SOURCE: BELDEN

Migrating to the Smart Grid will require designing upgraded and robust substation communication networks.

Foundation of the Smart Grid

Electric utilities are constantly searching for the efficient, reliable and cost-effective ways to deliver electricity. A vision for doing just that and more is provided with the smart grid model. One definition of the smart grid, based on work from the U.S. Department of Energy, is: "A modernized electrical grid that uses information and communications technology to gather and act on information in an automated fashion...to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity."

The promises of the smart grid are exciting on many fronts. It pledges to:

- Integrate renewable energy sources into the grid, thus reducing dependency on traditional sources that may be harmful to the environment.
- Save electricity in its own operations, improving the efficiency of the system.
- Improve reliability by monitoring equipment and fixing problems before they cause an outage.
- Improve recovery time by being able to smartly switch power around downed areas.
- Meet peak demand without requiring the build-out of additional traditional generating facilities.

To accomplish all of this, the elements of the electrical grid have to be able to communicate and share data quickly. Utilities, consumers and the system must be communicating with each other all the time, a capability that requires a colossal modernization. A new two-way communications infrastructure is being built to do this, and at its heart is the substation.

Reliable substation communications

Today, the majority of utilities are still using technologies ranging from modem connectivity to serial bus technology to 'talk' to their substations to gather important, needed information. In order to integrate with the smart grid, substations need to be upgraded to modern Ethernet and IP-based systems.

But the large investments in substations being undertaken today will only pay off if the resulting communications infrastructure is high performing, reliable and secure. Through years of experience in automating substations around the world, we have developed 10 best practices for reliable substation communications. These practices are part of our Substation Communications Legacy to IEC 61850 Design Checkup, a process we use with utilities to ensure that network upgrades benefit from proven techniques. Here are the best practices.

Segment operational networks

The first best practice we recommend is to segment all networks into operational zones or areas. Networks tend to grow incrementally, resulting in large, flat networks. Too often we find networks that have become vast, sprawling systems that are difficult to manage or secure.

By dividing up large networks into smaller

SEL-2730M MANAGED ETHERNET SWITCH
SEL-3530 REAL-TIME AUTOMATION CONTROLLER
SEL-3620 ETHERNET SECURITY GATEWAY
SEL-3610 PORT SERVER

SEL®

Reliably Control and Monitor Your Plant

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-ieb3.

ones, you can improve the manageability, reliability and security of your system. This is a key requirement in many standards, including the ISA IEC 62443 standard for industrial security. It also makes isolating network issues much easier and improves overall system reliability.

There are a number of options for technologies to divide your networks into zones. These include:

Subnets: This technique divides up devices into physical groupings based on function or location for ease of maintenance and security. Each subnet has a specified range of IP addresses and is connected to other subnets using a Layer 3 switch or router.

Subnets prevent "broadcast" messages from being sent between areas, reducing the chances of traffic storms impacting substation operations. Subnets are also good for isolating high performance and high bandwidth traffic on separate networks, giving you easier ways to manage the network and increase performance. Many of these switch and router devices can also act as packet-filters, offering limited protection against cyberattacks.

Virtual Local Area Networks: VLANs create logical groups of Ethernet devices that cannot be physically grouped. They work by having Ethernet switches insert a "tag" (basically a 4-byte field) into each Ethernet message. Other switches on the network can read this tag and make decisions on whether a message should be forwarded or not.

VLANs are great traffic management tools as they allow devices to see only the data they need. They are frequently used to isolate high bandwidth traffic, such as video and voice, when subnetting is not possible due to the physical separation of equipment.

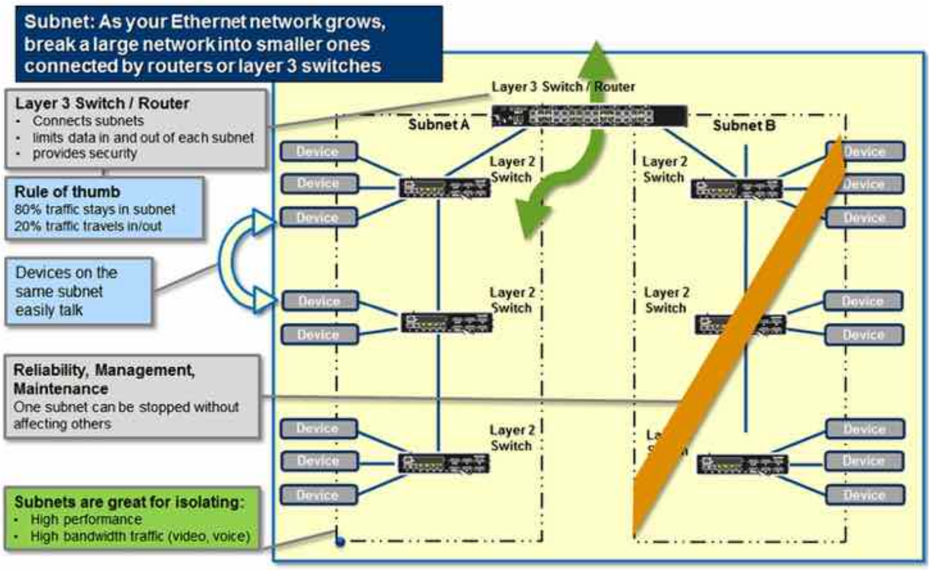
Similar to subnetting, Layer 3 switches and routers are used to configure and enforce the VLANs, limiting the data in and out of the VLAN. Devices from multiple VLANS may connect to a switch, and devices in the same VLAN can easily communicate between one another.

When Segmentation Is Not Possible: If you are unable to segment your network using one of the above technologies, possibly because it involves a process or protocols that cannot be maintained across a subnetted system, then you need to take extra care to secure your network. One way to do so is with the use of transparent firewalls.

Add serial communications devices

This best practice helps utilities connect legacy Intelligent Electronic Devices (IEDs) and other serial communications devices to an Ethernet network. This extends the useful life of the equipment and it can significantly reduce the cost of upgrading to a communications system that is "smart grid ready."

One may wonder if Ethernet is suitable for real-time control and information. In the past, Ethernet technology was 10 Mbps, half-duplex and hubs. Today's Ethernet is 100 Mbps and higher, full-duplex and switches. Switches eliminate collisions and other improvements make it a better choice technically than many of the fieldbuses it replaces.


Subnet: As your Ethernet network grows, break a large network into smaller ones connected by routers or layer 3 switches
Layer 3 Switch / Router
· Connects subnets
· limits data in and out of each subnet
· provides security
Rule of thumb
80% traffic stays in subnet
20% traffic travels in/out
Devices on the same subnet easily talk
Reliability, Management, Maintenance
One subnet can be stopped without affecting others
Subnets are great for isolating:
· High performance
· High bandwidth traffic (video, voice)
Layer 3 Switch / Router
Subnet A
Subnet B
Layer 2 Switch
Device

SOURCE: BELDEN

Subnets divide up devices into physical groups and make the network more manageable.

Importance of Power over Ethernet

What is Power over Ethernet (PoE)? It's the practice of using a single industrial Ethernet cable to provide power and Ethernet communications to devices. This best practice is vital when implementing physical security surveillance systems. It is not a simple process to wire and connect security cameras, card readers, routers, keypads and telephones, for example, together for substation security. Note that remote monitoring of substation security is an important element of an overall defense in depth protection strategy (more on this later).

Instead of using multiple cords or cables (one for power, one for pan/tilt/zoom control, and one for video), PoE gives you the ability to simplify your security installation and commissioning processes by replacing these with a single connection. This lowers costs as fewer components are needed and the replacement process is simplified.

Planning for PoE involves:

- Determining all the pieces to be used (cameras, telephones etc.).
- Identifying the power consumption (in watts) of each device.
- Totaling the power requirements of all PoE devices that will be wired to one PoE switch.

Note that most devices are "standard" PoE, requiring up to 13 watts, but some may be classified as "PoE+", ranging from 13 to 25.5 watts.

Time synchronization

As a utility operator, you need to know when events, such as faults, occurred, what happened throughout the event, and what pieces of equipment and substations were involved. This requires time synchronization, also known as fault event replay.

Examples of the equipment that must have accurate time stamping are IEDs, merging units (MUs), control units, Ethernet switches and any other system that requires synchronization within the substation automation system. Factors such as the protocols used, traffic load, communications media and cable distance of the network can affect the timing accuracy.

To ensure precision, we recommend using the IEEE-1588 protocol for devices on Ethernet requiring extremely high timing accuracy, that is, to less than one microsecond. IRIG-B is a similar, but older technology.

To implement time synchronization:

- Determine the timing needs of your application which can range from submicroseconds to milliseconds.
- Make sure that switches, routers and terminal servers in the path between devices needing to be synchronized support the timing technology used.
- Connect devices to a synchronized global positioning system or master clock.

Selecting switches and routers

Similar to power plants, substations contain valuable pieces of equipment typically housed in unconditioned control sheds inside the fence. While this provides some level of protection against the elements, temperature swings can be extreme, rodents and other pests can invade the shed, and dirt and grime can accumulate on the equipment. Other stresses can include humidity, corrosion and electromechanical noise.

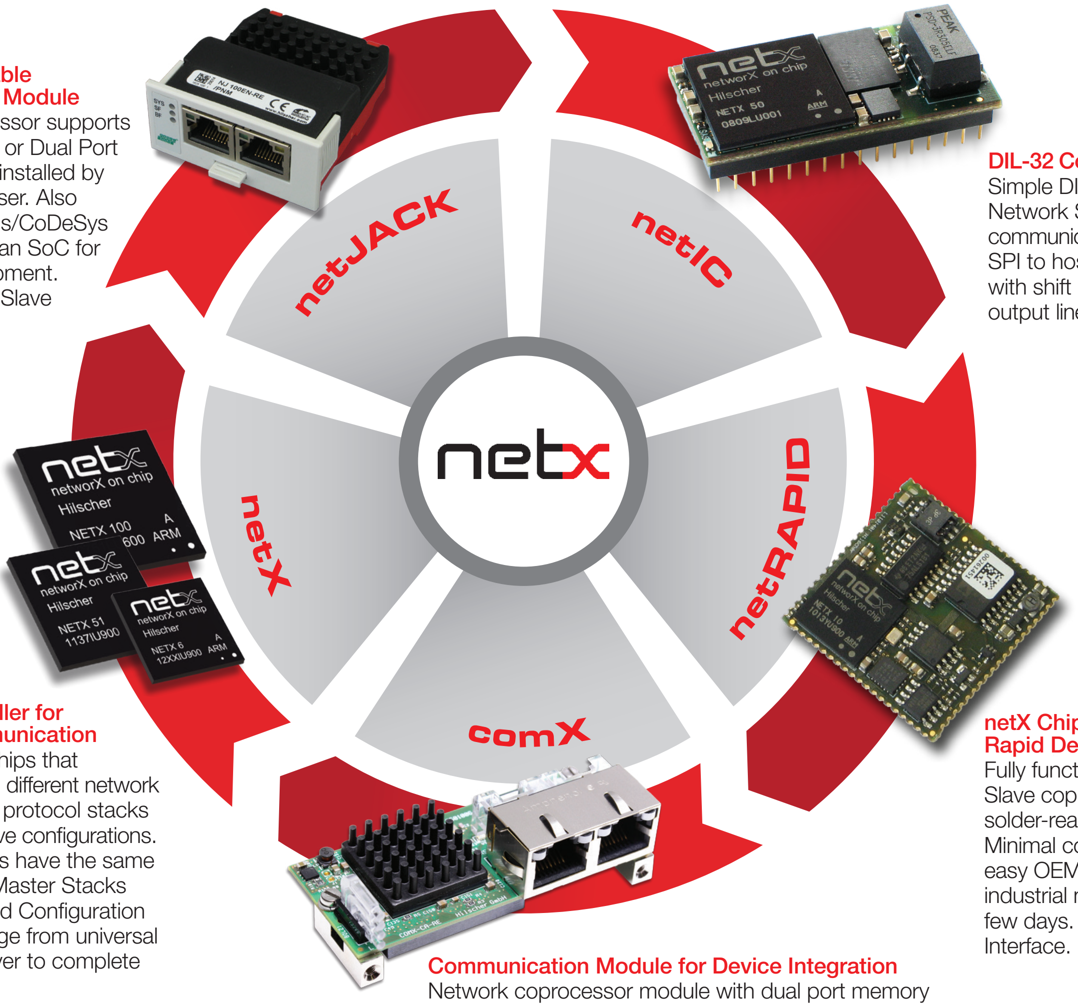
It is therefore important to select only

One Chip. One Company.

All the Network Hardware and Software Solutions You Need.

IP40 Exchangeable Communication Module
Network coprocessor supports SPI, PCI-Express or Dual Port Memory. Can be installed by supplier or end-user. Also available with QVis/CoDeSys and/or I/O, or as an SoC for your own development. Both Master and Slave Stacks available.

DIL-32 Communication IC
Simple DIL32-compatible Network Slave coprocessor communicates MB/RTU via SPI to host. Also available with shift register-based output lines to drive I/O.



Scalable Controller for Industrial Communication
Family of seven chips that supports up to 12 different network protocols and 24 protocol stacks in Master and Slave configurations. All protocol stacks have the same Driver Interface. Master Stacks include FDT-based Configuration Tool. Options range from universal network transceiver to complete System-on-Chip.

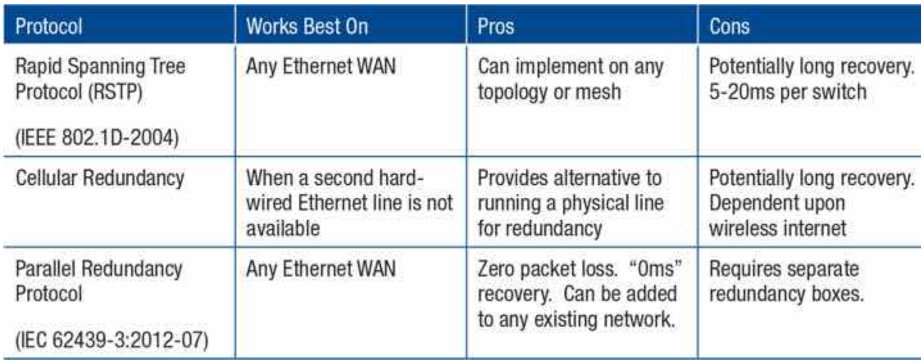
netX Chip Carrier for Rapid Development
Fully functional Network Slave coprocessor on solder-ready substrate. Minimal connections allow easy OEM integration of industrial networks in a few days. SPI or DPM Interface.

Communication Module for Device Integration
Network coprocessor module with dual port memory or SPI, for sophisticated high-performance network applications. Both Master and Slave Stacks available.

DeviceNet EtherNet/IP PROFIBUS PROFINET EtherCAT AS-Interface
Modbus CC-Link CANopen sercos the automation bus ETHERNET POWERLINK VARAN

To learn more about industrial communication solutions from Hilscher, call 1.630.505.5301, email: info@hilscher.us or visit www.na.hilscher.com.

hilscher
COMPETENCE IN COMMUNICATION



Protocol	Works Best On	Pros	Cons
Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1D-2004)	Any Ethernet WAN	Can implement on any topology or mesh	Potentially long recovery. 5-20ms per switch
Cellular Redundancy	When a second hard-wired Ethernet line is not available	Provides alternative to running a physical line for redundancy	Potentially long recovery. Dependent upon wireless internet
Parallel Redundancy Protocol (IEC 62439-3:2012-07)	Any Ethernet WAN	Zero packet loss. "0ms" recovery. Can be added to any existing network.	Requires separate redundancy boxes.

SOURCE: BELDEN

These three redundancy schemes and technology solutions are particularly useful for master-to-substation redundancy.

switches and routers that have the protection against the environmental and other hazards that exist in your substations. IEEE 1613 and IEC-61850 Part 3 describe the device standards that need to be met for environmental protection. As a utility operator you must ensure that network products meet or exceed all relevant industry standards.

Taking the time to select equipment with appropriate environmental and electrical ratings at the beginning of a project eliminates trouble in the future. You'll save yourself costly repairs and downtime.

Building multiple layers of security

Industrial infrastructure, especially critical infrastructure such as the electrical grid, is an increasing target for both sophisticated cyberattacks and for activists. Protecting substations is therefore vital. This best practice looks at how to design security measures that contribute to an overall security strategy.

Most engineers are aware that NERC CIP specifies the minimum requirements for security in the power industry. Unfortunately, NERC CIP uses an electronic security perimeter (ESP) philosophy based on hiding all critical assets behind a monolithic boundary. For example, a single firewall could be installed on the boundary between all critical control assets and the business network, with the hope that it will prevent all unauthorized access to the critical assets.

Industry experience has shown that monolithic designs present a single point of failure in a complex system. Few systems are so simple as to have single points of entry.

For example, this is what the U.S. Department of Homeland Security has found:

"In ....hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks.

In some extreme cases, we have identified up to 250 connections ..."

With the help of Murphy's Law, eventually all single-point solutions are either bypassed or experience some sort of malfunction, leaving the system open to attack.

A more realistic strategy is based on "Defense in Depth" (DiD) – multiple layers of defense distributed throughout the control network – as a strategy for securing operations. DiD maintains an ESP firewall between the business and control networks, but adds security solutions inside the control system that protect the substations if the main firewall is bypassed. The solutions work in parallel, with one technology often overlapping with others, to form a significant safeguard against either attack or human error.

There are two primary options for implementing network security technologies for a substation:

- Industrial firewalls that control and monitor traffic; comparing the traffic passing through to a predefined security policy, and discarding messages that do not meet the policy's requirements. Firewalls can be installed both at the ESP boundary and between internal zones.
- VPNs (Virtual Private Networks) are networks that are layered onto a more general network using specific protocols or methods to ensure "private" transmission of data. VPN sessions tunnel across the transport network in an encrypted format, making them "invisible" for all practical purposes.

A network protected using a DiD strategy responds to threats, such as a traffic storm (caused by device failures) or a USB-based virus, by limiting the impact to the zone where the problem started. Alarm messages from the firewalls would pinpoint the zone and even the source of the problem.

Routing firewalls guard perimeter

To create a security perimeter for the substation, a security control point can be used to restrict and monitor traffic flowing into and out of the substation. Typically, this will be a dedicated firewall, but in some cases a router or terminal server can be used.

These need to be able to filter large amounts of traffic and interface transparently to IT systems using security protocols, such as RADIUS and TACACS+. It is critical that this device is both security hardened and monitored for indication of attacks.

Transparent firewall protection

Transparent firewalls are security devices with special features for industrial use. At first glance they appear on the network like a traditional Ethernet switch, but they actually inspect network messages in great detail.

The "transparent" feature allows them to be dropped into existing systems without requiring readdressing of the station devices. This means that organizations can retrofit security zones into live environments without a shutdown. They also allow the installation of security controls within a single subnetwork; for example within a large process bus.

The "firewall" feature provides detailed "stateful"3 inspection of all network protocols so inappropriate traffic can be blocked. For example, rate limits can be set to prevent "traffic storms" while deep packet inspection rules can be set to prevent inappropriate commands from being sent to IEDs or controllers.

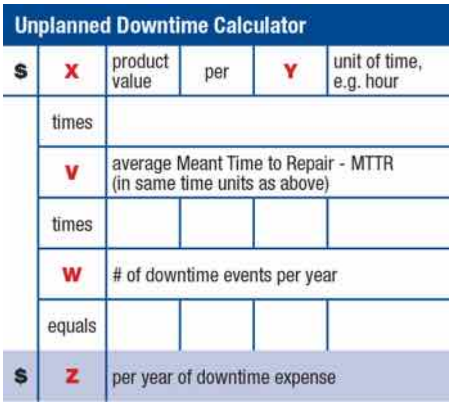
New communications infrastructure

As the design of the substation begins to come together, utilities must think about how all of the pieces will communicate with each other.

Substations can communicate with the master control station and the backup control station using a variety of networking technologies. These include Ethernet WAN, Cellular 3G or MPLS-PPP WAN. Whichever technology is chosen, consider making it redundant, such as adding yet another cellular backup. Robust communication keeps small issues small and ensures high availability of systems.

To evaluate your utility's need for redundancy, use the quick equation known as the Unplanned Downtime Calculator. It can help make the case for investing in redundancy.

While there have been numerous redundancy schemes developed over the years, there are three that are particularly useful for master



Unplanned Downtime Calculator

$	X	product value	per	Y	unit of time, e.g. hour
	times				
	V	average Meant Time to Repair - MTTR (in same time units as above)			
	times				
	W	# of downtime events per year			
	equals				
$	Z	per year of downtime expense			

SOURCE: BELDEN

Unplanned Downtime Calculator.

to substation redundancy. They are Rapid Spanning Tree Protocol (RSTP), Cellular Redundancy and Parallel Redundancy Protocol (PRP).

RSTP uses a physical ring, but logically disables one link to prevent messages from being forwarded on and causing message looping. If a break is detected on the network, the disabled link is re-enabled and messages then flow through the network using the new path. The main advantage of RSTP technique is that it can be used on any network topology. Its main drawback however is that recovery times may be as long as 5-20ms per switch.

When it is not possible or practical to add a separate physical hardwired Ethernet line, cellular redundancy can be used to provide a means of backing up communication. The cellular link remains in a standby mode until communications via the primary hardwired Ethernet line is lost. Communication is then transferred to the cellular link. The drawback of this approach is that recovery times will be dependent upon establishing the wireless internet connection.

Lastly, new redundant protocols have emerged that allow for zero packet loss and "0ms recovery." These protocols are defined by IEC 62439-3:2012-07. Parallel Redundancy Protocol (PRP) is one of these protocols and is particularly useful for master to substation communications.

PRP requires the addition of a switch that has dual attached nodes. This device is sometimes referred to as a "redundant box" or "red box" for short. As traffic comes into the red box, it duplicates the message packet. One packet is sent over one network, the second is sent over the other. The red box on the other end forwards the first message it receives to its destination and discards the duplicate when it arrives.

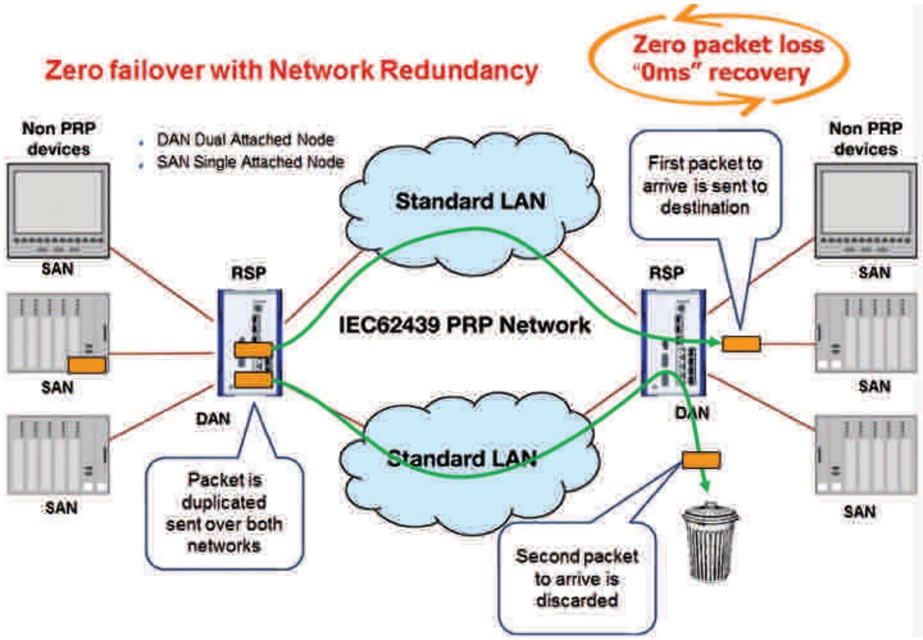
In the event of a network failure on one of the links, the message continues to be sent over the link that is still up. Thus, no packets are ever lost in the event of a communication failure on one of the links. Devices on either end see no delay in receiving packets. For the price of the additional hardware for the two red boxes, this provides the best method of implementing redundancy with no impact to operations.

Finally, consider providing redundant power supplies to critical communication devices such as routers.

Defense in depth is critical

This overall best practice depends on using a multi-layer defense model, which involves not just networking, computer and device protection technology, but things like physical security and policies and procedures.

The techniques used should be based on doing a risk assessment for critical assets and processes.


Zero failover with Network Redundancy
Zero packet loss "0ms" recovery
Non PRP devices
DAN Dual Attached Node
SAN Single Attached Node
Standard LAN
First packet to arrive is sent to destination
Non PRP devices
SAN
RSP
RSP
SAN
IEC62439 PRP Network
SAN
SAN
DAN
DAN
Standard LAN
SAN
SAN
Packet is duplicated sent over both networks
Second packet to arrive is discarded

SOURCE: BELDEN

Zero failover protection by implementing networking redundancy using Parallel Redundancy Protocol (PRP).

Security is covered in the Design Checkup, but you may require even more assistance in this area. If so, choose a partner who has experience in cyber security for substations and, in particular, securing industrial protocols.

Choosing cables, jackets, connectors

Often overlooked in complete communications infrastructure design are the physical cables themselves. More communication problems have been caused by improper cables or shoddy installation than one can imagine. Don't leave this critical portion of the design up to the whims of the installing contractor! It is vital to determine the proper cabling infrastructure that fully supports the system requirements.

These are specific steps to take to ensure successful implementation:

Determine Copper and Fiber Media Requirements: Plan the physical layout carefully considering distances and the data rate requirements to determine the need for copper and fiber media. Fiber is required for distances of greater than 100 meters and signal transmission rates of 10Gbps or higher.

Failures in the physical layer account for the largest problem area and are among the most difficult to troubleshoot and correct. In fact, according to Datacom's Network Management Special, 72 percent of all communication errors are introduced at the physical layers, such as cables and connectors.

Use Industrial Grade Cabling: After all of your planning, you want to be sure that your substation infrastructure will perform as designed in its harsh environment. Commercial grade cable is not designed nor intended to be used in industrial environments.

The Right Jacketing for the Location: Proper jacket material will provide the needed protection against the variety of environmental and physical challenges for both copper and fiber cables. Consult with the cable manufacturer about the jacket that would be most appropriate for the specific installation needs.

Choose High Performance Cable Designs: Copper cables with Bonded-Twisted-Pair technology are designed for high-balance performance for optimal signal transmission integrity. Proper fiber cable selection of multi-mode or single mode designs is critical to attaining system performance.

Consider Electrical Noise: EMI and RFI noise levels must be evaluated to determine if shielded or unshielded constructions need to be used. Highly balanced, bonded-pair cables in shielded or unshielded configurations provide the most robust noise immunity performance. Fiber cable provides the ultimate level of noise immunity. Make sure that the IEC 525 Substation cabling installation guidelines are followed. This will ensure that the cables are installed properly and will work properly for years to come.

Conclusion

While the smart grid promises vast improvements for the reliability, efficiency and economics of utilities, it will not meet the goal power producers envision without a robust communications infrastructure in place at transmission and distribution substations.

Investments in good network design and communications infrastructure will improve reliability and contribute to an economical energy delivery system.

***Tim Wallaert** is Director – Vertical Markets, Energy for Belden Corporation.*

SECURITY
WIRELESS
INFRASTRUCTURE

Maximum data transparency for lot size of one manufacturing

Series production integrating lot-size-of-one flexibility demonstrates the potential of Industry 4.0 at Nobilia, but a real benefit is the level of customization implemented at the same time. PC-based control offers a foundation for parts and production data, allowing kitchens to be supplied flexibly and efficiently.

AROUND 2,600 FITTED KITCHENS leave Nobilia's two production plants every day, making the company Europe's largest manufacturer. If this figure alone is any indication of the high demands placed on the manufacturing processes, it is made even clearer by the special market requirements.

"Despite series production, we manufacture fitted kitchens entirely in accordance with the customer's wishes which means in a lot size of 1," said Martin Henkenjohann, Nobilia's technical director. "In order to achieve this, we started way back in 1990 to keep all parts and production data transparent and universal over the entire manufacturing process – entirely in keeping with present-day Industry 4.0 concepts."

"That includes both the design data and the individual processing steps, so that we always know exactly where a particular piece of kitchen furniture is in the sequence of processes. This is the only way that we can meet the increasingly variable and specific customer requirements on the one hand and implement optimized and error-free freight transport with our own fleet of vehicles on the other," he added.

SOURCE: BECKHOFF

Nobilia produces a total of 580,000 individual kitchens per year and has concentrated on implementing a universally networked manufacturing environment since 1990.

Industry 4.0 requires real-time data

Modern Industry 4.0 concepts, and the higher flexibility in production that is attainable with them, are not possible without ensuring transparency of all machine and parts data.

"Real-time tracking capability over the entire process is the fundamental requirement. This starts by applying a barcode label that contains all necessary information about a piece of furniture, e.g. the front of a kitchen floor cupboard, as it moves from the anonymous prefabrication to the order-related production area," Henkenjohann said. "The production aspects with regard to further processing steps on various machines are just as important here as logistic details, such as the loading time and truck information or the delivery address. For example, each processing machine scans the barcode and retrieves the associated machining data from the central Oracle works database or from Web services."

It is the transparency of the real-time data that makes the daily produced volume of 2,600 individually manufactured kitchens possible. 88 different front designs form the basis for this process, and there are 250 different items behind each design.

Depending on the format of the front, plus such things as the fittings and handle or panel variants, this results in an extremely wide range of floor, wall and tall cupboards. The barcode of a drawer front, for example, contains the configuration of the entire drawer including its width and depth, the height of the rear wall and the type of handle.

The production facility accordingly supplies all required parts, initiates the correct processing sequences, and ensures that the desired drawer is placed in a just-in-sequence logistical train. The latter then drives to the assembly area, where the finished body of the cabinet is married to the drawer and other elements such as side-hung doors. Through real-time tracking, Nobilia knows exactly where each part is in the production process at any time, which corresponds precisely to the Industry 4.0 approach.

Time units and loading dates

Planning the production of Nobilia kitchen furniture is by no means traditional. In fact, production is controlled by time units. The tall, floor and wall cupboards are tracked to determine which production sequence they are in and whether these sequences are correctly parallelized.

Ultimately, all elements must enter the loading stream from a total of nine assembly lines with the right timing so that the individual fitted kitchen complete with all cabinets, electrical appliances and accessories can be loaded completely and on time onto the correct truck.

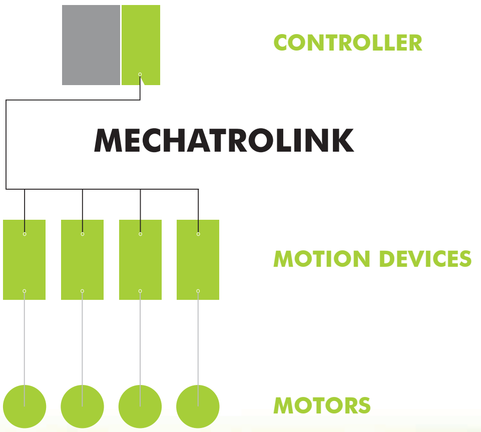
Henkenjohann said that the planning of an incoming customer order and production control is taken care of by the dispatch department, which is actually the final link in the chain. This means that the company's vehicle fleet optimizes the use of its truck volumes on the one hand and the route to the customers on the other.

The dispatch department finalizes the production plan just four days before the planned kitchen delivery date, so the usage of the production capacities must be extremely flexible. In order to properly take into account all customer requests within a short time, the construction data for the product variants are already stored to a large extent. In addition to

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

SOURCE: BECKHOFF

During the entire order-related production sequence, not only machine information, but also information on the production status of the furniture parts can be retrieved via the Beckhoff control panels and Panel PCs.

that, each of the three assembly lines for the tall, floor, and wall cabinets can also be used to manufacture one of the two other cabinet types within certain limits.

Dieter Grossekatthöfer, Sales Manager, Engineering at Beckhoff, illustrates this point: "Through the use of PC-based control technology and the units which are designed for as many different machining processes as possible, the machines cover a very wide range. For example, a drilling optimizer calculates a sequence in which, as a rule, as many holes as possible can be drilled simultaneously. When changing the product, however, it may be the case that consecutive drilling of the holes produces a better result so that, for example, it is possible to drive to intermediate gluing positions which are unavoidable for mechanical reasons. With these capabilities, the machines are optimally configured for maximum production flexibility."

Open and efficient system

The idea of data transparency at Nobilia was developed back in 1990 in order to meet the increasing demands on production.

According to Martin Henkenjohann, the decision in favor of PC-based control technology was clear from the outset: "Without the openness and high performance of PC Control, universal data storage would likely not have been possible at all, due to our heterogeneous manufacturing environment. "

With Beckhoff control technology and an Oracle works database developed in cooperation with Nobilia, a central closely meshing link between ERP and design software has been created. In this way, the requirements of a historically grown and accordingly heterogeneous production landscape can be satisfied. At the same time, it was and continues to be possible to continuously tap efficiency potential through the increasing integration of stand-alone solutions.

A technical move ahead coincided with the introduction of TwinCAT when an entire system no longer had to be completely controlled from one control computer. Today, for instance, it is straightforward to connect up to seven Industrial PCs together via TwinCAT and ADS communication, for example for several drilling machines, a distribution system and additional machining stations.

Larger production units are created using this approach, so that basically only a few equipment types such as a tall cupboard assembly belt or a drawer unit, have to be regarded. For each of these plant types there is a pre-defined, customized TwinCAT application available, which only needs simple parameterization to be adapted. On the one hand, this allows existing knowledge to be transferred to all plants without great effort, and on the other, software engineering can be much more efficient.

SOURCE: BECKHOFF

Each element can be very clearly assigned to the correct kitchen furniture via unique barcodes.

Grossekatthöfer regards the possibility to modularize the plant as a further advantage for this application: "As opposed to the earlier stand-alone solutions with no real overlapping communication, it is now possible to create individual function modules, for example, for the side or base area or a drilling unit.

This is an enormous advantage during commissioning, because these modules can be commissioned separately and then simply combined afterwards. This considerably reduces the commissioning time and facilitates the continuous modernization of Nobilia's production landscape," he said

Universal PC-based technology

Nobilia uses PC control throughout both of its manufacturing plants, from the EtherCAT I/O system and motion control through to the Control Cabinet Industrial PCs (IPCs) and Control Panels with TwinCAT PLC/NC.

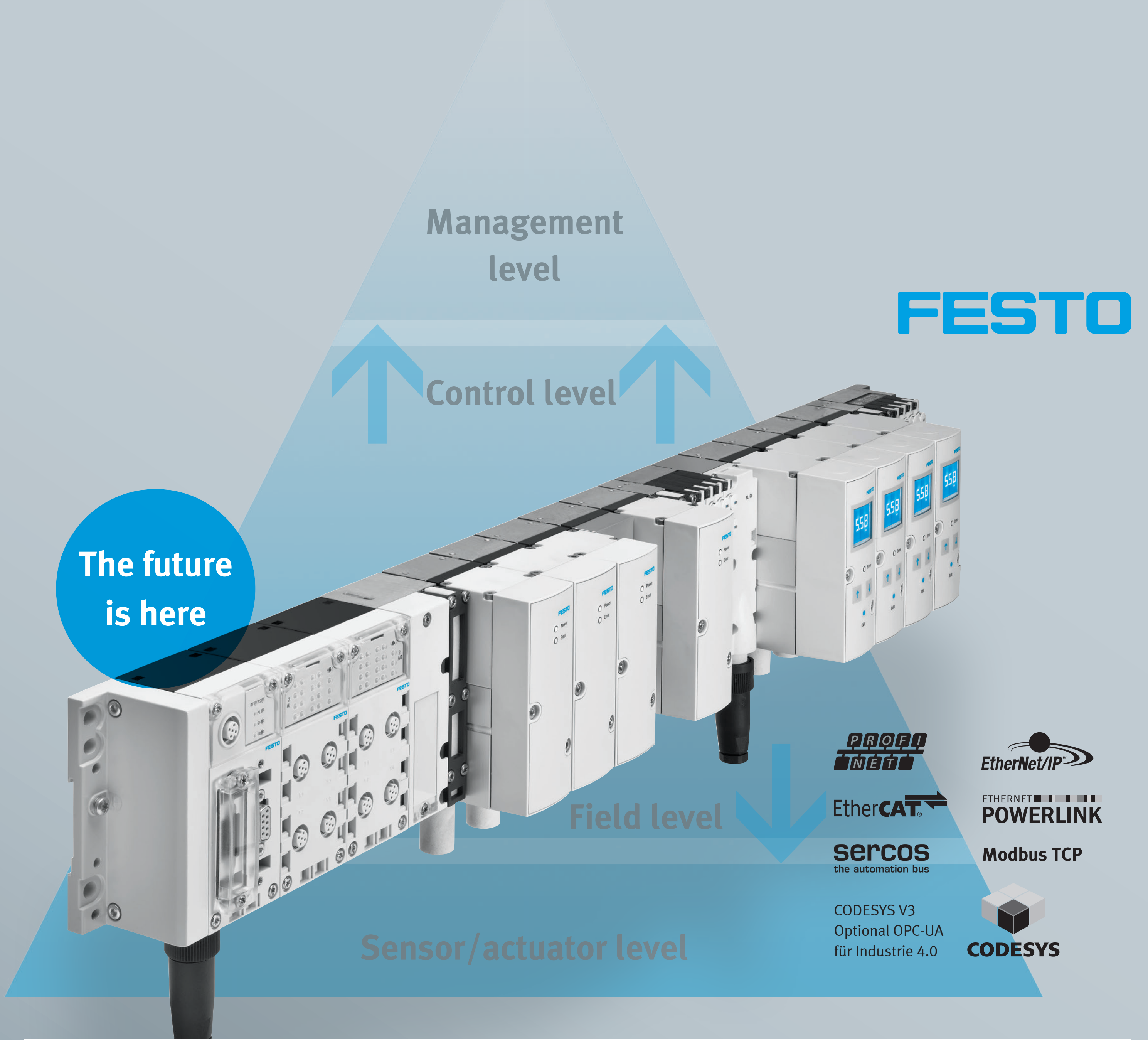
Even the few older machines with conventional PLC technology can be integrated with PC-based control. Matthias Gehle summarizes the results as follows: "A homogeneous data flow can be achieved despite the very heterogeneous machine pool. The data is held in the central Nobilia database. Special high-level language applications developed by Beckhoff that are implemented in the production plants communicate with this database and supply the respective plant controllers with adapted information. Over all these years that has been the key to the continuous improvement of efficiency in production."

Efficiency on way to Industry 4.0

Industry 4.0 is a concept that will only be fully implemented in the coming 10 to 20 years. Nobilia has already implemented it to a great extent today, but Henkenjohann sees some potential for further development in the short and mid-term.

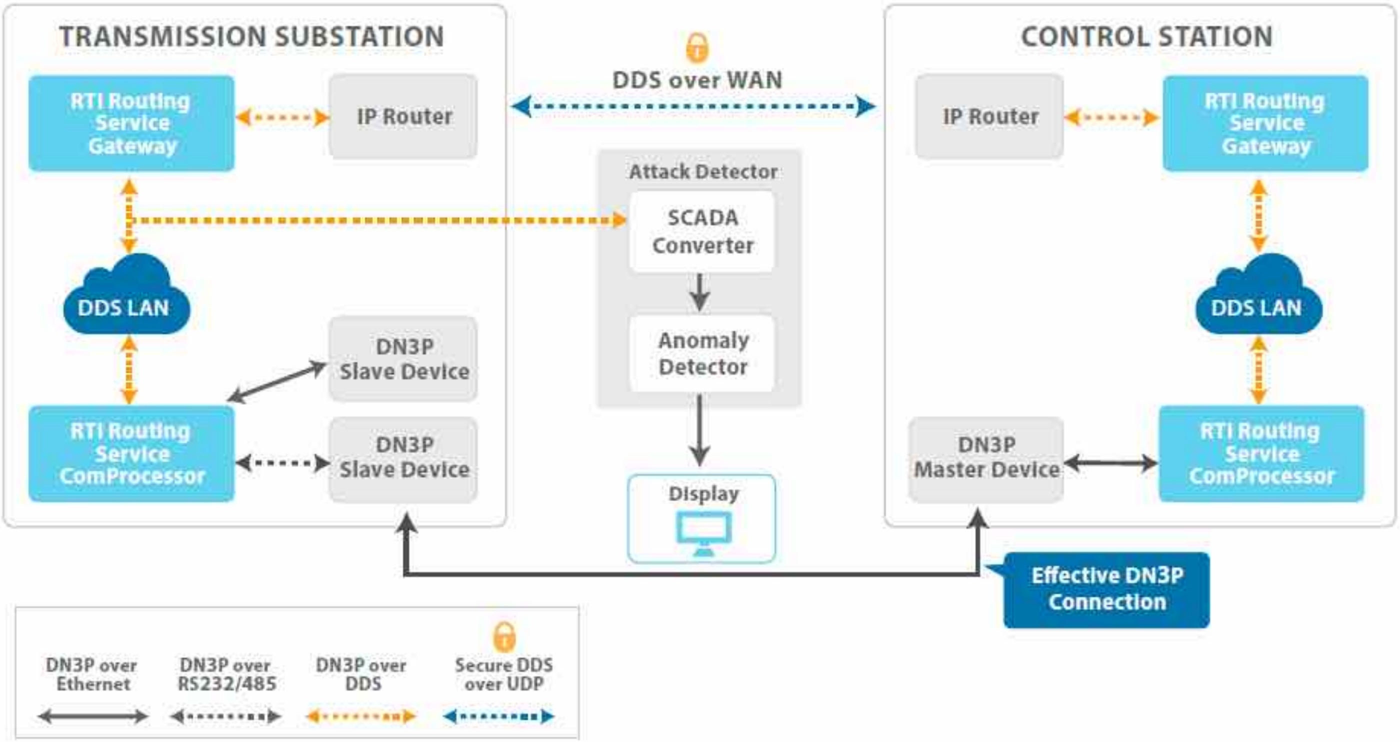
"Currently, we are using RFID and RTLS (real-time locating systems) on a test basis with the goal of making the identification of the furniture pieces more variable in comparison with the barcode system and also to provide them more clearly with all necessary information," he said "In addition, our production control will benefit from TwinCAT 3 and the multi-core IPC technology which it optimally supports."

***Shane Novacek** is Marketing Comnmunications Manager for Beckhoff.*


Management level
Control level
Field level
Sensor/actuator level
The future is here
FESTO
PROFI NET
EtherNet/IP
EtherCAT
ETHERNET POWERLINK
sercos the automation bus
Modbus TCP
CODESYS V3
Optional OPC-UA
für Industrie 4.0
CODESYS

Four keys to securing distributed control systems

At the core of critical infrastructure and industrial applications, control systems drive today's power grid, hospital clinical environments, factories and transportation systems. Because of their vital roles and the value of the information they exchange, these systems must be protected from both espionage and sabotage.



SOURCE: REAL-TIME INNOVATIONS

Retrofitting the power grid for boosted security and threat detection creates a complex system of data management and security. In partnership with RTI, Pacific Northwest National Laboratory (PNNL) has applied the DDS security standard to secure an electric grid. The use of DDS allowed a unique set of security policies to be introduced for each type of data flow which provides a high level of performance, reliability and service. Existing equipment and applications used the DNP3 protocol for as the connectivity option.

SECURITY HAS BECOME MORE CHALLENGING as millions of devices are moving to be ready to tap into the possibilities of today's Industrial Internet of Things. But the challenge is that more connections translate into more points of vulnerability, and security concerns and issues must not compromise other fundamental requirements including reliability, real-time performance, autonomy and interoperability.

This article presents an overview of industrial security requirements and the new security extensions to the Data Distribution Service (DDS) standard. Implemented as plug-ins, the security extensions introduce authentication, confidentiality and access control while still satisfying demanding reliability and performance requirements. A power grid use case is an important example that shows how DDS Security can be easily incorporated into existing systems — with or without prior adoption of the foundational DDS standard.

Control Systems

Industries that now depend on Internet connectivity cover the globe and relate to all aspects of modern life. As a result, the scope of the Internet has grown over time. The Industrial Internet of Things (Industrial Internet or IIoT) reflects the expanding requirements for connectivity at the heart of modern industry and commerce.

The control systems designed for the Industrial Internet have also evolved. Highly distributed in nature, a typical control system synthesizes live data streams from numerous sensors, actuators and other connected devices. Processed data then drives device control, and feeds other subsystems relating to operator interfaces, back-end systems, IT and cloud applications.

Because of their hierarchical nature, many modern control systems are referred to as "systems of systems." These highly complex systems, with smarter devices at the lower levels and broadened information sharing at the upper levels, pose unique security challenges. System designers must meet those challenges without compromising other vital requirements relating to real-time performance, safety and reliability.

Decentralized architecture

A secure IIoT needs a decentralized architecture, access control, elimination of TCP/transport layer dependencies and interoperability.

Industrial-strength data sharing can improve power generation and distribution, monitor and optimize use, and even power new business models and energy business systems. Most traditional IT systems and consumer Internet of Things applications rely on centralized intelligence and message routing. However, a central broker or server would severely limit industrial control systems in terms of:

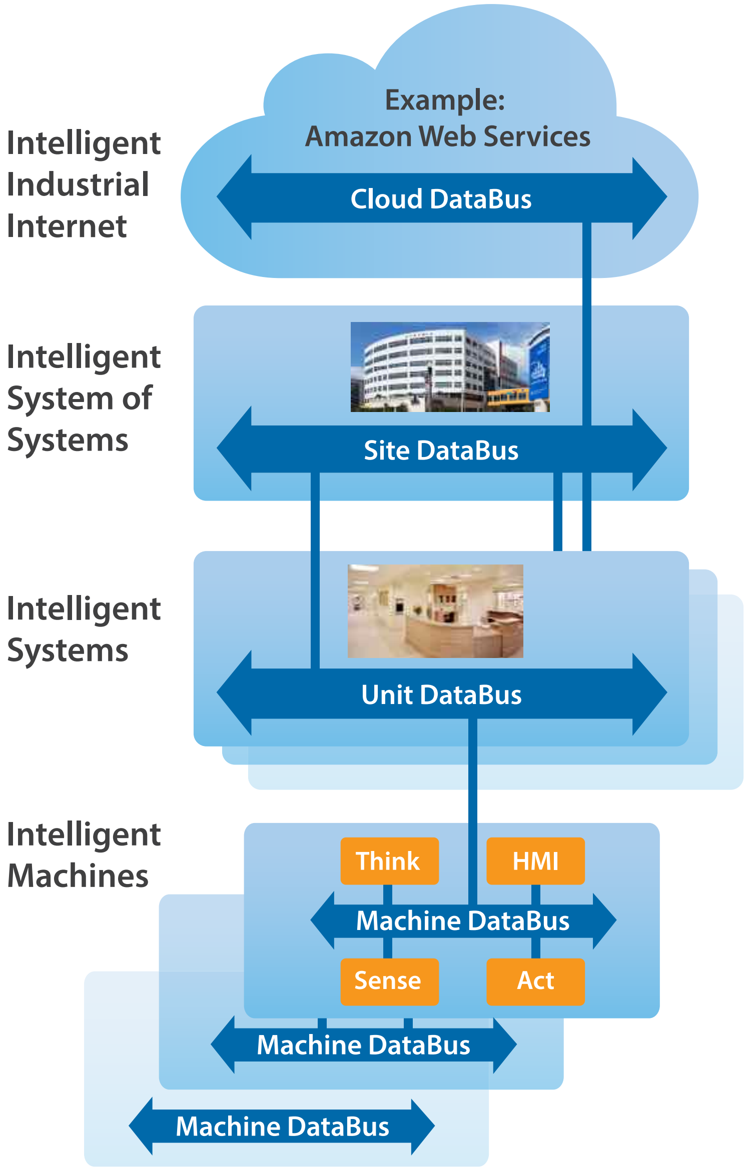
- *Performance*. A centralized messaging hub creates a bottleneck and choke point, which degrades latency and determinism as message volumes increase. Capacity and throughput are also constrained by the link speeds and switching performance at the hub.
- *Scalability*. The need to duplicate expensive hub servers drives up costs rapidly. Server cost grows with volume.
- *Robustness*. The hub creates a single point of failure or vulnerability, and system availability is directly tied to server maintenance and failures.
- *Capabilities and utility*. Centralized intelligence limits the autonomy and intelligence at the edge.

To overcome these limits, the vast majority of industrial control systems should adopt highly decentralized architectures. With distributed processing and more intelligence at the edge, overall systems can achieve lower latencies, higher resiliency and can analyze orders of magnitude more data.

Access control

Historically, physical site security or limited access to computer systems would serve to secure industrial control systems. Today, with higher levels of system connectivity, machines are much more accessible. More people — authorized and unauthorized — are attempting to access those systems. Access controls have become critical, and must address the physical layer all the way up through the application software layers.

Without adequate security, systems are vulnerable to increased threats and attack activities. These include both espionage (unauthorized access) as well as sabotage of equipment and infrastructure. Required protection must prevent unauthorized subscription (eavesdropping), unauthorized publication (introducing invalid data and corrupting behavior of a system), tampering and replay of information and unauthorized data access via infrastructure services.



SOURCE: REAL-TIME INNOVATIONS

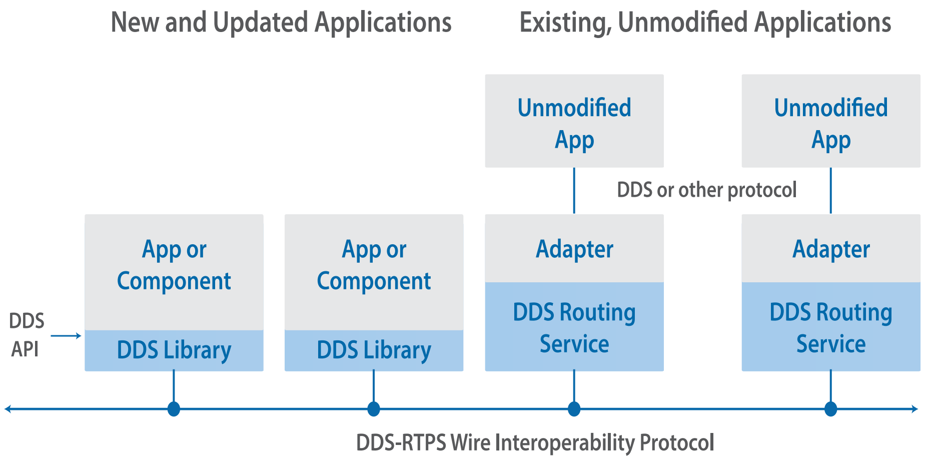
The Industrial Internet can be used to connect intelligent devices with applications that aggregate data from devices are themselves part of larger systems. The goal is to drive up overall quality with security at every level of the hierarchy.

TCP/Transport dependencies

At the transport layer, TCP provides no control over latency and lacks the control necessary for real-time behaviors. Since TCP is a unicast-only protocol, it also lacks the efficiency required in industrial environments that are traditionally multicast (one-to-many and many-to-many connections). TCP also assumes a reliable network, and can introduce a lot of overhead on less reliable networks.

IP can also be inefficient over very low-bandwidth networks such as satellite links. This protocol can introduce too much overhead compared to other high-speed interconnects such as shared memory and RDMA. In addition, transport layer security built on top of TCP or IP inherits other shortcomings such as a lack of fine-grained access controls. Once a connection has been established and keys exchanged between peers, peers can exchange any data without restrictions.

To address this shortcoming, message brokers are often introduced in an IT or consumer environment to enforce policies. But this requires a centralized architecture that does not accommodate industrial systems.



SOURCE: REAL-TIME INNOVATIONS

New and existing (unmodified) applications can co-exist on a Connext DDS DataBus.

Open architecture interoperability

Industrial systems encompass a broad range of components and subsystems from multiple vendors and must be supported over long lifecycles. Interoperability promotes modularity, which simplifies support of these components and therefore avoids spiraling costs over time.

Modular, interoperable components have become critical as system complexity has skyrocketed. Proprietary, hard-coded integration between components is impractical to maintain, difficult to evolve and limits design re-use. In contrast, well-defined interfaces and semantics simplify the evolution of very large scale systems.

IIoT data distribution service

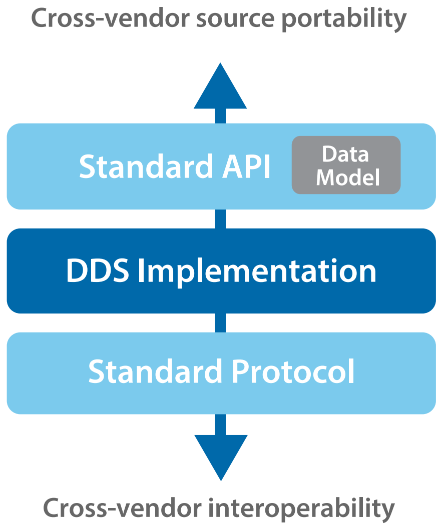
The Data Distribution Standard (DDS) emerged in conjunction with the evolution of the Industrial Internet of Things. For modern-day control systems, DDS addresses all four requirements for achieving secure, reliable, high-performance connectivity.

The standard provides connectivity between software modules, effectively creating a software DataBus. Well-defined interfaces and a standard interoperability protocol provide loose coupling between the modules in a system. The DDS protocol spans discovery (how modules locate each other), data routing, high-availability and real-time quality of service (QoS) enforcement.

The DDS application programming interface (API) enables portability across DDS implementations, and a DDS network wire protocol ensures interoperability. The standard also includes a discoverable data model. The DDS standard is published and managed by the Object Management Group (OMG).

Integrating existing components

A DDS implementation, such as RTI Connext DDS, is provided as a library. Each component of an application or system can be written or updated to incorporate DDS. This promotes a decentralized approach with low latencies and no single point of failure.


Cross-vendor source portability
Standard API
Data Model
DDS Implementation
Standard Protocol
Cross-vendor interoperability

SOURCE: REAL-TIME INNOVATIONS

Basics of the DDS standard.

RTI also provides a DDS Routing Service to protect existing investments. By building an adapter using an included software development kit, existing and unmodified applications or subsystems can be integrated into a DDS environment. This makes it easy to introduce DDS into any systems, and still allow peer-to-peer communication among all components.

To maximize connectivity, DDS can run on any device or system, from embedded systems and mobile devices to cloud services. Data can be shared seamlessly across applications that are geographically distributed anywhere in the world. The protocol supports many programming languages and is supported on all popular operating systems and platforms.

Simple publish and subscribe

On a DDS DataBus, components can rapidly and reliably share data. For mission-critical control systems, this provides many benefits:

- Simple, loose coupling. Adding a new sensor or actuator requires no changes to the other components and subsystems.
- Autonomous operation. Discovery is automatic, without a broker or centralized service.
- Non-stop availability. The decentralized approach avoids single points of failure.
- Visibility and control. QoS capabilities support real-time environments, and the DataBus provides status monitoring of system and component health.
- Flexibility. The DDS API is designed for embedded and enterprise systems, and the wire protocol also accommodates varying connectivity requirements.
- Low risk. Hundreds of thousands of devices successfully employ DDS today.

DDS security

In March 2014, OMG published security extensions to the DDS standard. Security capabilities are provided via plug-ins and require minimal or no change to existing DDS applications. Communication can be secured over any transport, including low-bandwidth and unreliable networks. Secure DDS does not require TCP or IP, and supports multicast for scalability and low latency.

The plug-in architecture, with built-in defaults, enables customizable security to suit unique requirements and take advantage of security-enabled hardware and firmware. Just like the foundational DDS features, the extensions support a completely decentralized architecture for high-performance and scalable control systems with no single point of failure.

An out-of-the-box implementation of these five security extensions supports common security algorithms for authentication and cryptography, and also supports fine-grained access control over which data users or devices are allowed to publish and subscribe.

For encryption, DDS provides control over which data and metadata must be encrypted and/or signed for authenticity and non-repudiation. It uses a hash-based message authentication code (HMAC).

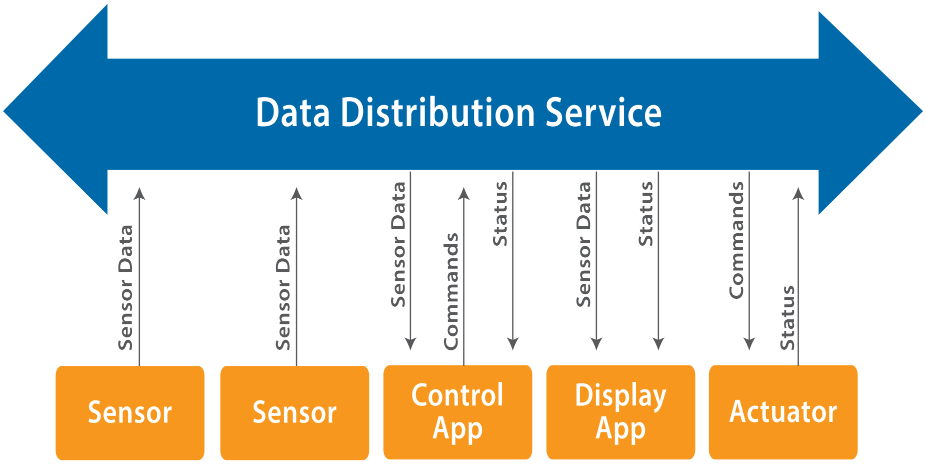
Encryption policies can be optimized for each data flow to restrict security overhead appropriately and balance security requirements against any impacts on performance. DDS security is well suited for time-critical control systems and CPU-limited devices.

Power grid use case

In partnership with RTI, Pacific Northwest National Laboratory (PNNL) has applied the DDS security standard to secure an electric grid. DDS allowed a unique set of security policies to be introduced for each type of data flow.

Existing equipment and applications used the DNP3 protocol for connectivity, which has been well documented in terms of security problems. Using a retrofit approach, secure DDS connections were added between the control station and the transmission substation.

Technology article by ***Real-Time Innovations****.*

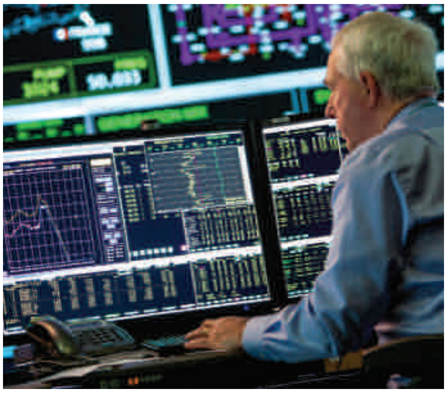


SOURCE: REAL-TIME INNOVATIONS

Publish and subscribe foundations of DDS.

National Grid prepares for the future

New system will handle emerging challenges through better monitoring of overall grid health, gathering operational data from a wide range of measurements and helping to identify potential problems earlier.



THE TRANSMISSION SYSTEM OPERATOR for nearly 20 million people in the UK faces the combined challenges of rapidly increasing demand, downgrading of fossil fuel plants and growing integration of renewable energy sources, an advanced measurement system has been developed to provide real-time data on power supply trends.

But a new system will help National Grid UK handle emerging challenges through better monitoring of the health of the overall grid. The ability to gather operational data from a wide range of measurements will help identify potential problems early, prevent power disruptions and better manage risks.

Selection of measurement system

Traditional measurement systems did not provide adequate coverage to overcome the challenges of the modern grid but new software-designed systems have enabled the creation of a customised solution that offers the flexibility to be upgraded in the future as measurement needs and data volumes evolve. National Grid UK selected the NI platform from National Instruments to develop a connected measurement system capable of gathering and analysing large amounts of data to better detect grid-wide trends. Compared to its existing infrastructure, implementing a smarter, more connected system allows National Grid UK to manage change, optimize energy sources and plan for the future grid.

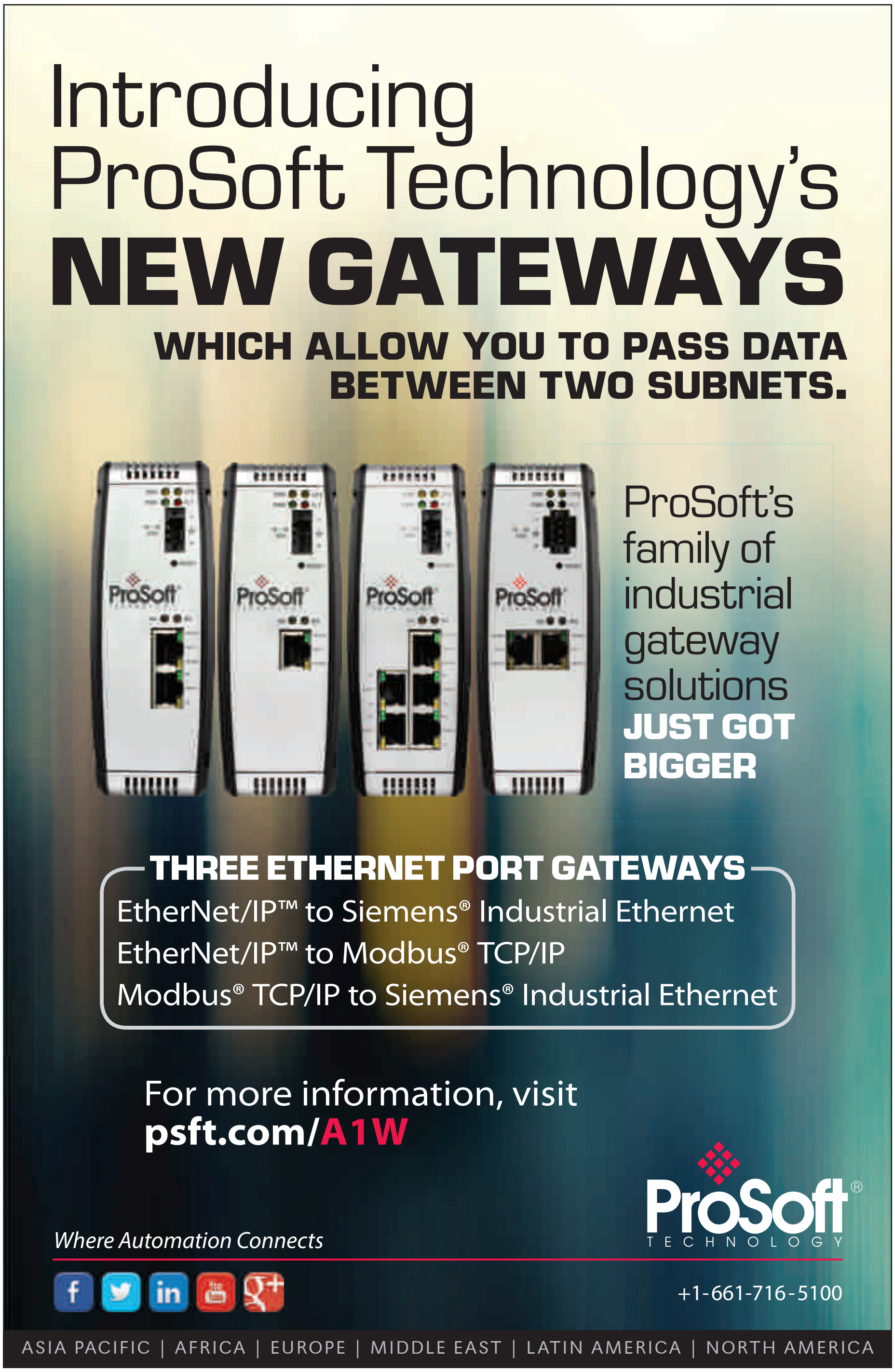
National Grid UK adopted a platform based on the CompactRIO controller that can provide more measurements and adapt with the evolving grid for generations to come. This interconnected network includes 136 systems, with 110 permanently installed in substations throughout England and Wales and 26 portable units that provide on-the-go spot coverage as needed.

The software application running on both versions is identical, which minimises the impact on system integration, training and support.

"Like many energy providers, National Grid UK is facing the challenges that come with a rapidly changing grid," said Peter Haigh, Senior Power Systems Engineer at National Grid. "The company is focused on developing a flexible solution that can be upgraded with new software as the measurement needs of the grid and amount of data available evolve."

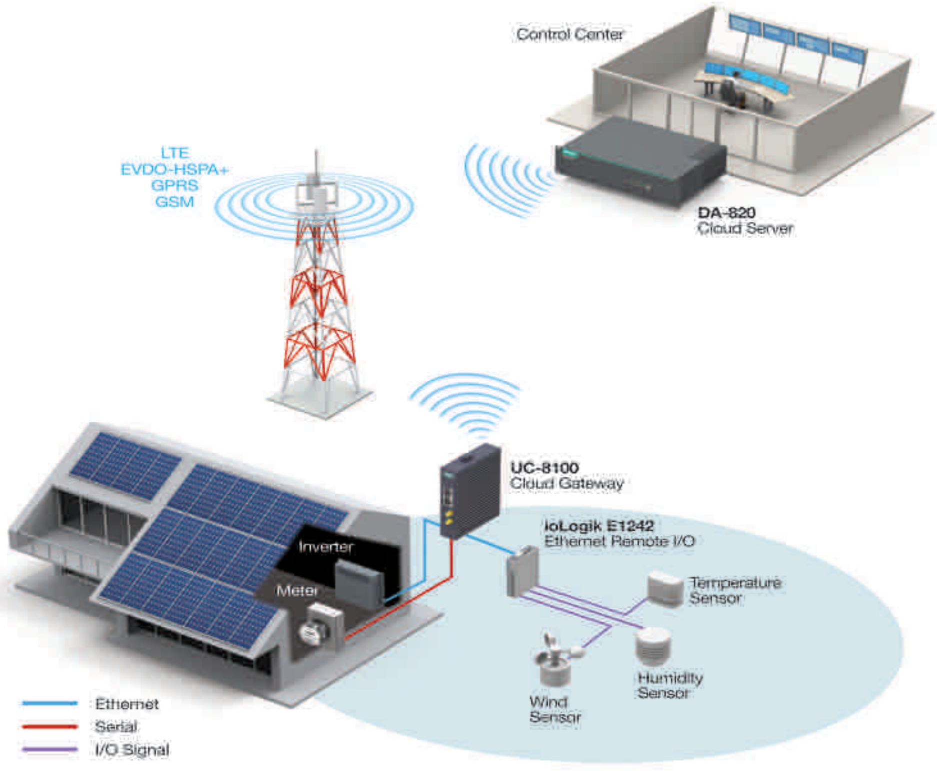
With an open, flexible, software-designed instrument, engineers can customise the information available for grid operation and make upgrades as needs change. This approach improves grid monitoring and reliability while reducing the amount of equipment needed.

Application story by ***National Instruments****.*



Building the industrial cloud: immediate future of M2M

If the Internet of Things is big news in general, it's even bigger news for the energy and power industries along with shipping and transportation. For these companies, the possibility of rolling out cheap, massively distributed networks that can collect and communicate consumer and process data offers tantalizing and easily understood business opportunities. The only challenge is finding the hardware that can do the work.



SOURCE: MOXA

If the Internet of Things is big news among retail manufacturers, it's even bigger news in heavy industries like the energy and power industries, or shipping and transportation. For these companies, the possibility of rolling out cheap, massively distributed networks that can collect and communicate consumer and process data offers tantalizing and easily understood business opportunities. The only challenge is finding the hardware that can do the work.

SECURITY HAS BECOME more challenging as millions of devices are ready to tap into today's Industrial Internet of Things. More connections translate into more points of vulnerability, but security must not compromise other fundamental requirements including reliability, real-time performance, autonomy and interoperability.

There is a pressing need amongst industrial automation suppliers for embedded computing platforms that are optimized for machine-to-machine (M2M) communications. The Internet of Things is poised to become a material reality, making great possibilities for industrial providers. Yet until the lack of specialized platforms is overcome, the building of IoT clouds for industries like traffic management or the smart grid will continue to be delayed.

Automation and IT challenges

The fundamental challenge in designing these systems involves negotiating the divide between IT and IA technologies. Industrial automation protocols are fundamental to the proper functioning of edge devices that make up the mass of mass deployments; fieldbus, Modbus, input/output configuration, serial interfaces, and the gateways that link all of these are common enough problems for industrial automation engineers, but for most IT engineers the entire field appears esoteric and mysterious. On the other hand, securing networks with firewalls and VPNs, protecting against dropped packets or node failures, and the multifarious problems introduced by wireless communications are all things typical for IT, but which IA engineers would rather avoid.

The biggest challenge today when building an industrial M2M network is its massively distributed nature: there is very little value gained by a gradual transition that takes years. IoT deployments must be rapid enough to sustain investment value, but the massive number and scope of the cloud of devices employed makes speedily completing the full installation pretty much impossible. Specialized technicians are required for every individual station, and these men and women must be both competent electricians as well as familiar enough with the network design to juggle the details of multiple protocols, interfaces, and communications media. Unfortunately, few IT professionals have ever worked with the protocols and interfaces that are most common to industrial automation networks, and setting up input/output stations, or configuring sensors, are things which IT people simply have no experience in.

At the outset, there are two important reasons why effective software automation at the connectivity layer is critical: first, to facilitate the deployment of a cloud of devices that may ultimately include hundreds of thousands of nodes, and second, to flatten the learning curve as much as possible for the men and women who will be installing these devices. Software tools that transparently automate the rollout of industrial automation devices and simplify overall network deployments are, therefore, a foremost consideration for anyone who will be managing the deployment of an IoT network.

Industrial and enterprise challenges

Yet another way in which IoT networks significantly differ from consumer networks are their strict availability and reliability requirements. Industrial M2M systems for intelligent transportation systems or the smart grid will, of necessity, operate 24/7, 365 days of the year. At literally any moment the network must be able to call upon remote stations at the network's edge and command them to make adjustments, return data, or perform maintenance checks. Obviously, devices which are not capable of reliably maintaining network connectivity for years on end will not be very valuable to network administrators. Similarly, all devices along the network must be able to deliver key information for preventive maintenance, and to respond to a wide variety of common network challenges such as failed nodes, network congestion, and wireless re-association. For the most reliable performance, network redundancy, automated connectivity checks, preventive maintenance routines, effective maintenance, monitoring, and control protocols must be integrated as deeply into the hardware level as possible.

Finally, there is the consideration of the related problems of data integrity and network security. Authorization, access, and accounting controls are as imperative for an M2M network as they are for any IT network. Authorization and access are easily understood: illicit access to a massively distributed industrial network by a hostile party has clear potential for disastrously lethal consequences. For this reason, IoT networks (especially those for traffic systems, the smart grid, or other power applications) must support the strongest possible encryption and access controls. Similarly, accounting controls over the entire network are important not only for the monitoring and management of the network itself, but also to aid in preventive maintenance, as well as to perform forensic analysis on suspected intrusions, or other security breaches.

Taken together, these imperatives amount to a lot of work that, until recently, had simply not yet reached a stage where machine-to-machine communication networks could be considered viable. Now, however, that has changed, and the IT/IA convergence of recent years has arrived at a point where integrating these two technological realms in a secure, reliable, cost-effective manner has become a relatively easily achievable reality.

Solutions for converging tech

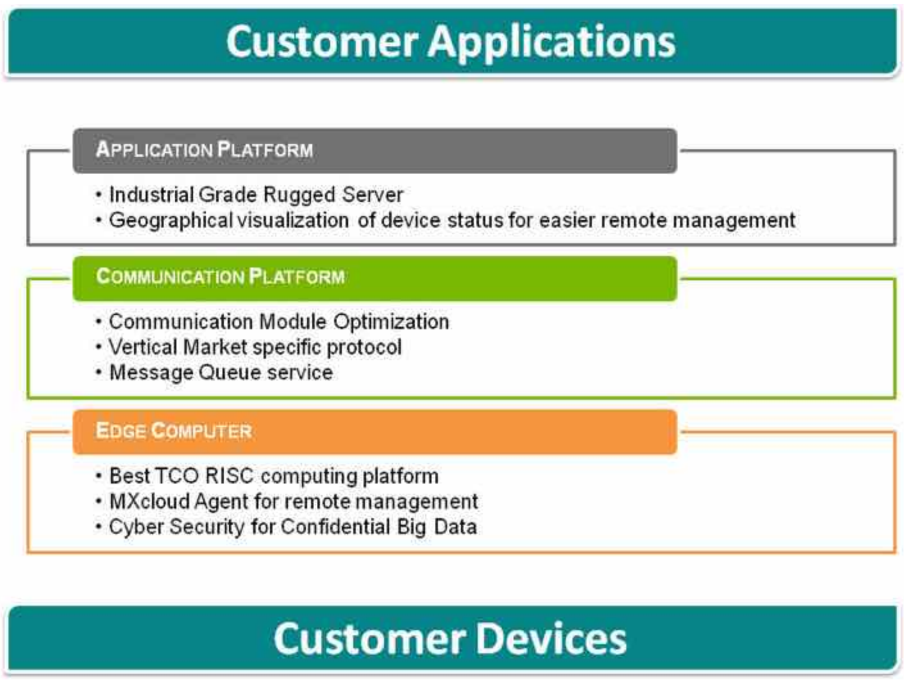
The overall technical challenge that must be addressed when building an industrial IoT network may be broken down into three key aspects:

- Network topology (and how that relates to device deployment, and engineering);
- Deployment, setup, and maintenance of network nodes and edge stations; and
- Overall monitoring and control

First, let us consider how an M2M network can be envisaged in terms of its topology, and how the technological implications of that structure affect the network's design and implementation. At first glance, it might be tempting to simply divide the network into two layers of two dimensions: network/process, edge/core. That, however, would neglect some important opportunities for automation and optimization. To begin with, the physical devices of the network are best broken up into three concentric layers, rather than two: the core, the connectivity layer, and then the terminal edge stations, where nearly all of the remote process data and events will be generated. Edge devices will necessarily include sensors, automatic metering infrastructure, embedded computers for control and monitoring, and gateways to bind all of these devices together, to allow effective communications between the various parts. The question then becomes: how can automation and effective device engineering speed up and simplify M2M deployments, monitoring, and management?

Simplified development

To guarantee that the network remains as customizable and flexible as possible, open platforms should be utilized wherever they are prudent. Linux/GNU and other open source solutions provide an excellent platform for IoT integration, and may reliably power



Customer Applications

APPLICATION PLATFORM

- Industrial Grade Rugged Server
- Geographical visualization of device status for easier remote management

COMMUNICATION PLATFORM

- Communication Module Optimization
- Vertical Market specific protocol
- Message Queue service

EDGE COMPUTER

- Best TCO RISC computing platform
- MXcloud Agent for remote management
- Cyber Security for Confidential Big Data

Customer Devices

SOURCE: MOXA

Successful applications create platforms to manage both customer applications and devices on the network.

both RISC and x86 platforms. These proven software solutions offer strong security (for both data integrity and AAA protocols) while providing a wide-open system that allows customization, optimization, and feature development on any subsystem process, no matter how low- or high-level it may be. Linux/GNU systems also offer two additional advantages: strong security in the form of packet filtering, firewalls, VPNs (and the strongest RSA encryption available), along with the important benefit that end users can escape the danger of proprietary lock-in, whereby a device may become useless should the manufacturer one day disappear, or decide to cease support for that particular line of hardware. Thus, system integrators and end users alike benefit powerfully when using open source / free software solutions like Debian.

Software optimizations are not, however, the only consideration. The physical devices that make up the IoT network must also be specifically engineered for customizability, security, reliability, and deployment flexibility. For embedded computers, features like a modular design are a critical feature that will allow end-users to adapt devices to specific roles within the network, or even to repurpose a device that is being used in an obsolete role. A wide variety of communications modules must be available as well including: ZigBee, Ethernet/IP, 802.11, cellular and fiber.

Principles of an IoT platform

Taking all of these observations, a clear vision emerges of what kinds of embedded computing platforms should be sought out when preparing to build an IoT solution.

1) IoT networking devices should conform to the strictest standards of flexibility, reliability, and security, starting with the physical hardware and then moving on up through every networking layer, right into user-space.

2) Software optimizations that automate configuration, setup, and the overall deployment of embedded computers and other edge devices are critical components of an effective IoT architecture.

3) All elements of an M2M networking platform should be able to be easily integrated into high-level, customized IoT customizations, to aid (rather than hinder) the optimal administration, maintenance, and management of the network as required by the particular vertical market it serves. At the highest central administrative layer, smart grid IoT solutions will share very little in common with intelligent traffic systems, while solar farm solutions will be distinct from both. IoT networking platforms must not intrude on the work of building the final solution envisaged by the customer, but should assist in achieving that goal in every possible way.

SOURCE: MOXA

Cloud services are integral for future connectivity options.

4) An IoT networking platform must make the connectivity layer as transparent as possible, effectively turning the intermediate portion of the network between the edge and the core into a black box, with which system integrators and application engineers never need concern themselves.

5) Communications between the edge and the core must reliably process all data, regardless of the health of the network as it is accumulated. This means asynchronous, encrypted transmissions between the edge and core, with strong failsafes to guarantee the physical integrity of the data.

As these considerations reflect, any computing platform or other networking device intended for use in IoT deployments should be engineered from a system-wide perspective, where each device is viewed as part of a mutually-supportive interlocking whole, rather than as a single, one-off network tool. A recent solar power deployment for the smart grid is useful as an example, here. Consider a solar station where an embedded computer is used as a gateway and station controller for a residential solar generator system. In this system, the inverter, meter, and remote I/O system are all connected to an embedded RISC platform that manages local automation and data logging, while maintaining remote wireless communications with the central control station. This residential system must maintain network communications over serial, Ethernet, and fieldbus interfaces, as well as either 802.11 or perhaps cellular wireless.

Looking ahead

Strong initial steps have been taken towards creating a virtualized connectivity layer specifically engineered for industrial cloud solutions. The automation involved vastly simplifies the deployment, setup, and management of industrial networking and edge devices, while consolidating and simplifying their management at the central core. By calling upon tailored software solutions carefully integrated with key hardware optimizations in networking, I/O, and embedded computing platforms, industrial cloud engineers will be able to set aside the work of connectivity integration and low-level coding to concentrate on the work of developing the most effective system for their needs.

__Johnny Fang__ and __Patrick Bor__ are Product Managers at Moxa, Inc.

Unmanned aerial vehicles & Big Data

Unmanned aerial vehicles (UAVs) are making surveying of landscapes and creating massive amounts of data that will need to be managed and stored efficiently using always-on database management systems.

TODAY'S UNMANNED AERIAL VEHICLES (UAVs) are small, simple, cheap to operate, and can carry multiple types of surveying equipment. They allow survey data to be collected in a continuous stream throughout the flight and instantly uploaded to a server for immediate analysis.

As well as conventional cameras, UAVs can carry specialized equipment such as ultraviolet, infrared and thermal imaging cameras, hyperspectral sensors and lidar scanners. These data streams will have to be accurately married with GPS (global positioning systems) and other information for complete analysis.

Transferable technology

Embedded data management technology already has a proven track record in big data applications across many industries. Its solutions offer specialised capabilities that enable intuitive management and manipulation of real-time information.

Designed for distributed architectures in resource-constrained applications, RDM technology from Raima can store data locally on a mobile or embedded device, which may be disconnected from any networked database servers, and then replicate this data to a server when a connection becomes available. This capability also allows buffering of data on a mobile device during a phase of rapid data acquisition, and then transmitting it across a network with relatively low bandwidth.

Because RDM provides sophisticated data management on the embedded device itself, it is also possible to filter the data in real time on the embedded device, thereby reducing the amount of data that has to be transmitted to remote servers. It also provides a SQL implementation that is small enough for resource-constrained systems, while providing the features most needed by an embedded application, such as pre-compiled database schemas, pre-compiled stored procedures, user-defined functions written in C and "virtual tables" for accessing any kind of source data through SQL (e.g. real-time data fed from sensors).

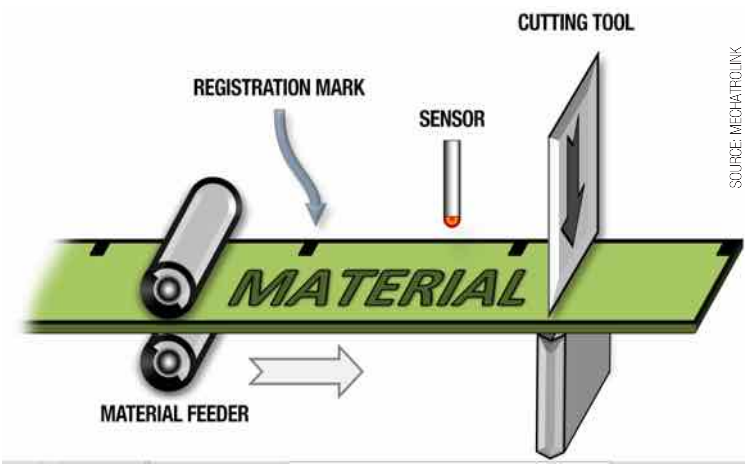
The system's modular structure, and support for distributed data and scalability through data partitioning. As well as enabling it to run on small systems these characteristics allow it to handle larger databases, supporting data mining applications.

Data mining allows users, such as farmers, to look beyond simple factual information and consider the consequences of each decision in a wider context. There is no doubt that in the future, data and the information and knowledge that can be drawn from that data will be one of the greatest assets available to farmers.

Application report by ***Raima****.*

Using a motion network for external positioning

Distributing processing from the main controller into field devices can improve the repeatability and performance of applications. Using external positioning allows additional tasks to be handled by the servodrive to perform latching of the registration mark, feeding to a stopping position and stopping the feed.



SOURCE: MECHATROLINK

Cut-to-Registration application

MOTION CONTROL APPLICATIONS benefit from having more repeatability, faster operating speeds and more compact solutions. Applications that require sensing a registration mark, and then stopping a distance from that mark, may be restricted from those benefits due to controller processing variances and communication delays. By moving the processing into field devices, the variances and communication delays become virtually eliminated so that applications can achieve higher performance operation.

Cut-to-registration application

The application known as "cut to registration" is where a feed of material has registration marks of where to be cut. The steps are as follows:

1) Machine feeds material.
2) Latch sensor detects registration mark.
3) Material continues to feed until mark is located under a cutting tool.
4) Material feeding stops.
5) Cutting tool cuts the material.
6) Machine feeds again, repeating at the first step.

In motion control architectures that give the controller the tasks to latch the registration mark, calculate the stopping position, and stop the feed, processing variances and communication delays exist that can result in poor repeatability.

Processing variances exist due to the timing of the latch sensor input is processing. The controller latches the sensor input at the end of the controller processing cycle, rather than at the moment the latch sensor input occurs. This means that the latch sensor can trigger at a specific position, but the actual position recorded by the controller occurs at a later time.

Also with this architecture, operating at a higher speed would result in a higher difference in position between sensor input and position recorded by the controller. To avoid controller processing variance, the processing can be moved to the field devices by means of a digital network.

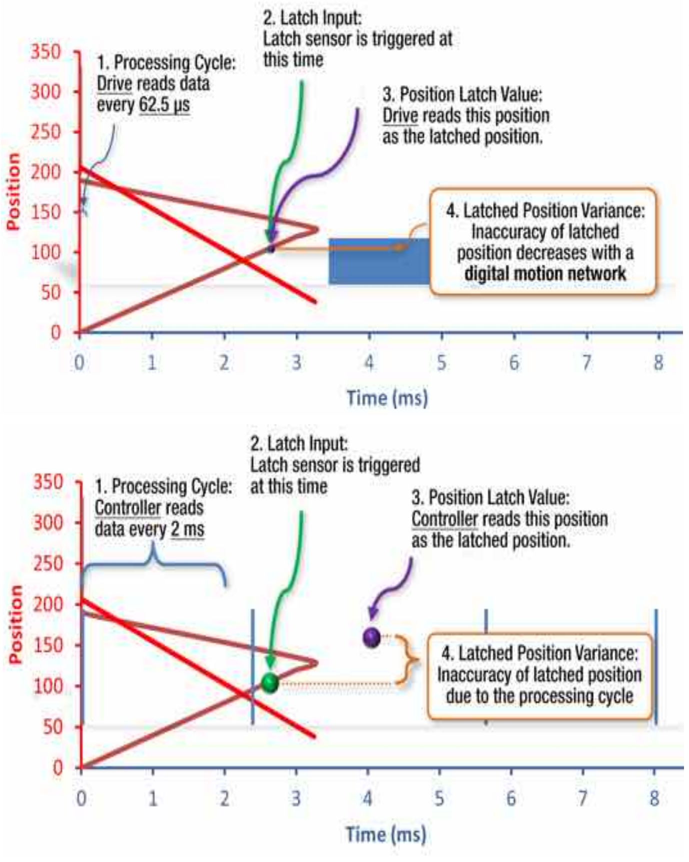
Digital networks

Latch processing can be moved to field devices like servodrives by using a digital network. For Ethernet-based field networks that implement device profiles like CANopen or Mechatrolink, the latching of the position value occurs on the servodrive, rather than on the controller. Through the digital network, the latched position value is communicated to the controller. The controller calculates the final stopping position, and then communicates to the servodrive to stop at that position.

Because the servodrive's processing cycle is several times faster than a controller, the latched position value is several times more precise. As an example, modern servodrives can operate at a processing cycle of 62.5µs, where the controller processing cycle for most machines is 2ms.

The result of the increased latched position precision gives the machine more repeatability and allows for faster machine operation. In the example of a "cut to registration" application, repeated cuts will fall into a smaller range on the registration marks while also operating at a higher speed. This allows the machine to output more uniform pieces, and more total cut pieces over time.

While latch processing by the servodrive improves precision, the controller still needs to perform the tasks of calculating the stopping position and commanding the motion stop. For a controller to perform



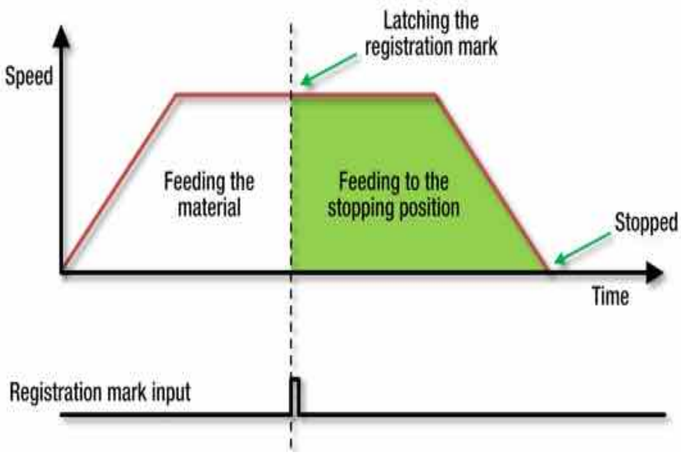
SOURCE: MECHATROLINK

Variability in latched position occurs due to the controller processing cycle.

these tasks, the sensor input must be located away from the cutting tool at a distance far enough to allow the tasks to complete. Moving these tasks to the servodrive would allow the sensor to be located closer to the cutting tool, resulting in a more compact machine.

External positioning solution

Servodrives can perform the task of calculating the stopping position and stopping at that position by the use of the Mechatrolink command "External Positioning" (EX_POSING). The controller only needs to send the "External Positioning" command to the servodrive, and the servodrive performs all time-critical tasks to perform the "cut to registration" application: latching the registration mark, feeding to the stopping position, and stopping.



SOURCE: MECHATROLINK

The Mechatrolink "External Positioning" command allows a servodrive to perform the tasks of latching the registration mark, feeding to the stopping position, and stopping.

SOURCE: MECHATROLINK

Task	Without Digital Network	With Digital Network	Using "External Positioning" Command
Feed material	Controller	Controller	Controller
Latch registration mark	Controller	Servodrive	Servodrive
Feed to stopping position	Controller	Controller	Servodrive
Stop	Controller	Controller	Servodrive

Tasks performed by the controller or servodrive, depending whether or not a digital network is utilized, and if the Mechatrolink digital network is utilized.

This command improves upon modern motion control architectures that use digital networks by decreasing the distance between the registration sensor and the cutting tool. Because the distance can be decreased, the machine can be built smaller.

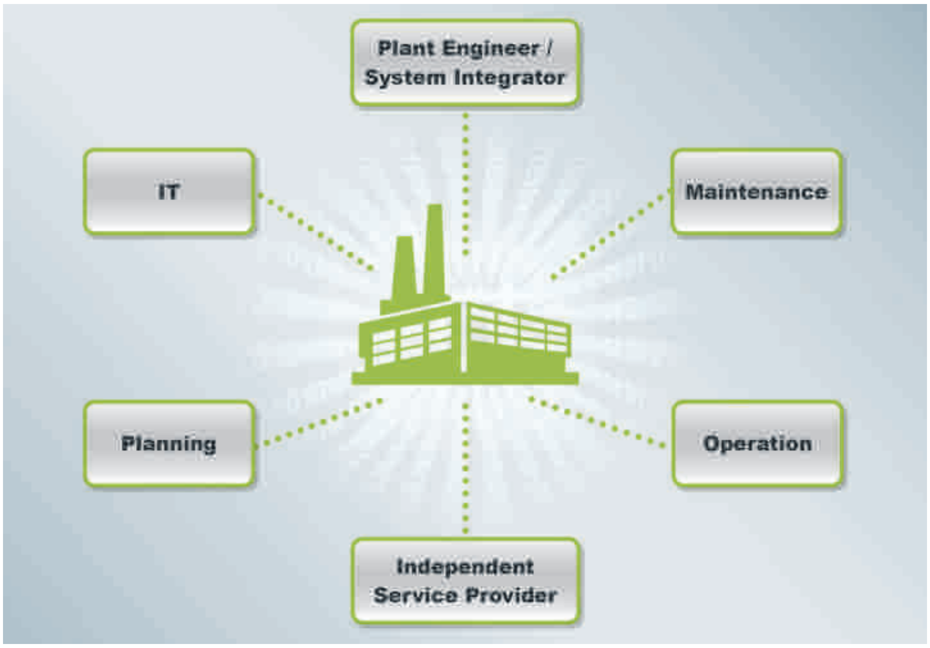
Summary

By moving as many tasks as possible away from the controller and into the field devices like servodrives, machines benefit from having more repeatability, operating faster, and being more compact. Digital networks open the possibility of moving tasks to the field devices. The "External Positioning" command allows additional tasks to be moved to field devices. In "cut to registration" applications, the command "External Positioning" can allow the servodrive to perform the tasks of latching the registration mark, feeding to the stopping position, and stopping the feed. This results in more uniform cut pieces, more total pieces over time, and a smaller machine.

***Derek Lee** is a Motion Product Engineer for Yaskawa America, Inc.*

PROFINET diagnostics: flying blind or efficient maintenance?

Diagnosing problems with PROFINET networks and other TCP/IP-based Industrial Ethernet systems raises technological and organizational challenges. Issues span from routine checks of open networks through to complex technical troubleshooting of persistent faults, and require additional training within the enterprise.


Plant Engineer / System Integrator
IT
Maintenance
Planning
Operation
Independent Service Provider

SOURCE: SOFTING

Potential participants in PROFINET network diagnostics. Who does what tasks?

PROFINET IS AN ESTABLISHED COMMUNICATION standard in industrial automation, and the development and installation of PROFINET networks presents no problems in the majority of cases. If a diagnosis of the PROFINET network is needed, however, many users venture into new territory. A network acceptance test, for example, is often not included in the plant commissioning procedure, and plant operators and maintenance staff are looking for clear best practice guidance on how to monitor PROFINET networks during operation, how to reliably keep them up and running, and how to react quickly and efficiently if problems occur.

The reason for this situation lies in the profound changes brought about by the shift from traditional fieldbus systems to PROFINET, or to TCP/IP-based Industrial Ethernet systems, in general. One thing that becomes particularly apparent is that these changes not only raise technical but also organizational issues and their effects on plant organization.

Before delving into the subject, it is necessary to clarify what is meant by the terms “diagnosis” and “network diagnostics”. In this context, Softing uses a comprehensive approach that not only covers fault localization and correction in the case of failure, but also includes general action and measures ensuring proper operation of a PROFINET network throughout the life cycle of a plant – from installation to commissioning and operation. The table below illustrates the individual diagnostic measures taken for each of the three life cycle phases of a plant or network. The transition to a plant’s “network management” or even “system management” is seamless.

TCP/IP brings change

What changes does the use of PROFINET, as an example of TCP/IP-based Industrial Ethernet communication, actually bring to industrial automation? TCP/IP is an open, extremely widespread standard protocol. Users are looking to profit from this openness and the possibilities it offers. As a result, the conditions on PROFINET networks frequently change in the field. For example, users regularly modify the network configuration and exchange the nodes connected to the network. The use of a TCP/IP protocol therefore also means that the boundaries between industrial automation and enterprise IT are becoming more and more blurred and permeable.

Even if a network can be kept stable, the configuration of the network and nodes is still more complex. Regardless of whether faults in the network occur right at the beginning during commissioning or later on, e.g. after the replacement of a defective device during operation of the plant, they are often caused by configuration errors. Faults resulting from physical causes, in comparison, are far less frequent than in PROFIBUS networks, for example. (This is the current state of knowledge. The future will show how PROFINET networks will age in practice.) The lower protocol levels of PROFINET communication are complex. Depending on the cause of the fault and the necessary analysis to be performed by the user, it may take in-depth knowledge of communication technology or IT to identify and correct the fault.

	Installation	Commissioning	Operation
Cable test	X		
Acceptance test		X	
Continuous monitoring			X
Troubleshooting		X	X

SOURCE: SOFTING

The individual phases of a plant’s life cycle require different diagnostic functionalities for PROFINET networks.

All in all this means that, on the one hand, users of PROFINET technology are faced with the technological challenge of adapting network diagnostics to the new conditions brought about by TCP/IP-based communication. But on the other hand, users need to address organizational issues. These reach from routine checks of open networks that are basically running stably but are subject to changes, through to the complex technical troubleshooting of a persistent fault. The first question that needs to be answered here is how the wide range of diagnostic tasks can best be fulfilled and who is to take care of what tasks.

Organizational matters

The following three example questions illustrate the organizational challenges facing

PROFINET technology users attempting to maintain plant networks.

1) Who does the maintenance staff call if they are unable to locate and correct a fault with their standard tools? A specialist from their own department? The in-house IT department? An external service provider? Are there in fact any clear criteria by which the maintenance staff can decide at which point external experts are to be called in?

2) How can users obtain a transparent, reliable acceptance test for a PROFINET network as part of plant commissioning? Is acceptance testing performed by the plant vendor? Is it performed by the in-house planning department? Or is an independent third party called in?

3) To what degree does the planning department take the responsibilities, processes and tool selection for network diagnostics into account at an early stage? If this is not the planning department's job, then whose is it?

It is striking how differently these organizational questions are currently answered by PROFINET technology users and how widely the assignment of responsibilities and tasks to different roles varies. Even within a single company, there are great differences between individual production sites.

It is largely undisputed that maintenance plays a key role. The maintenance department is responsible for first-level support for the entire plant, which is now based on complex PROFINET technology. Maintenance staff needs processes and suitable tools that enable them to efficiently work on PROFINET networks without having to "fly blind".

At the same time, it is neither necessary nor practical to have every member of the maintenance staff become an IT and communications expert able to detect and identify such difficult errors as an internal error in the device vendor's protocol stack.

Consequences for diagnostic tools

Against this background there are a number of basic requirements that need to be met by network diagnostic tools. The fact is, there is no ultimate all-in-one tool that can automatically perform all conceivable diagnostic tasks for any conceivable user in the best possible way. What can be used instead is a set of individual tools which each fulfill a specific diagnostic task in reference to the assigned responsibility. The other way round, users should select their tools with a view to the precise role and tasks they have been assigned.

Back to the technological challenges, two working group initiatives in standards bodies (one current and one recently completed) are worth mentioning. The first initiative, a PROFIBUS+PROFINET International (PI) working group headed by Karl-Heinz Niemann, has revised and extended both the PROFINET Design Guideline and the PROFINET Commissioning Guideline (PROFINET Design Guideline Version 1.14, PROFINET Commissioning Guideline Version 1.36, both released in December 2014). In the second, the GMA Technical Division 6.15 (VDI/VDE) headed by Jürgen Jasperneite is currently preparing a guideline entitled "Reliable Operation of Ethernet-Based Bus Systems in Industrial Automation". These documents provide many detailed descriptions accompanied by concrete recommendations, in particular also for PROFINET network diagnostics.

Exactly what tasks are involved in the operation and diagnosis of PROFINET networks during the different phases of the plant life cycle? What functionality is needed during installation, commissioning or operation of the plant? And how can tools assist the different user groups in fulfilling these tasks? A second article on this topic will address these questions in detail in an upcoming issue.

Dr. Christopher Anhalt *is Senior Product Manager, Diagnostics, at Softing.*

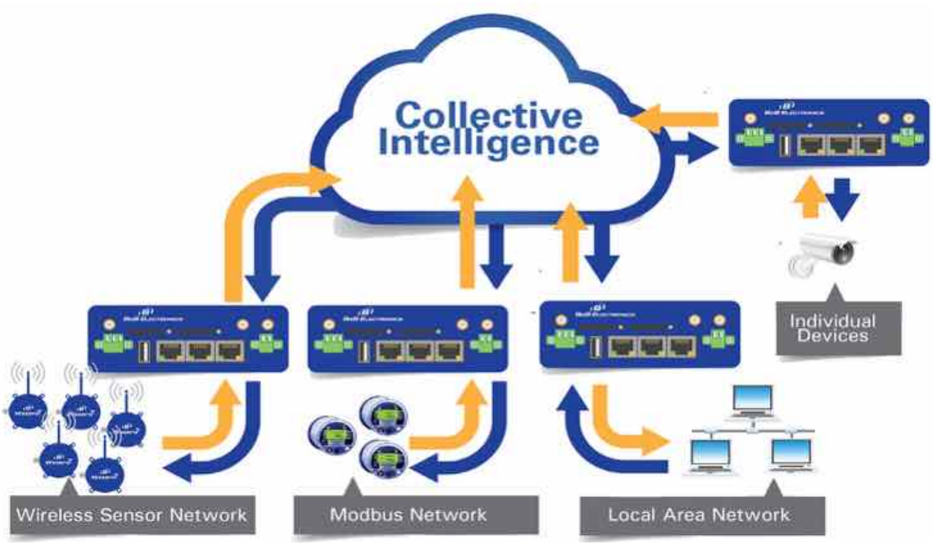
SWARM intelligence for IoT: greater than sum of its parts

SWARM intelligence is visible in nature where the collective efforts of simple creatures like ants, bees and termites can produce highly sophisticated results. Termites build enormous mounds, and bees successfully build hives. But now, SWARM technology principles are being applied to data networking and the IoT.

THE SAME PRINCIPLES that make natural collectives successful, such as bees building hives, can be put to work in modern data networking. The sum of the knowledge embedded within thousands of relatively simple devices, if efficiently and effectively communicated between network nodes and applications, can produce benefits above and beyond those provided by the individual pieces of equipment. This can help address the problems that occur out at the network edge, and have specific future relevance to the Internet of Things.

In nature, termites build enormous mounds in which internal temperatures are regulated to within a degree, even when temperatures outside of the mound vary by 40oC or more. Individual ants forage at random, but the overall motion of the collective produces highly efficient search algorithms that researchers have compared to those used in Google Maps.

Bees successfully build and defend hives, forage for food, protect the queen, and raise their young, even though the drones themselves possess very little personal intelligence. Individual members of these collectives have no knowledge of the overall aims of the colony; they merely follow simple rule sets. The collective itself exhibits characteristics that are not present in its individual members, and can almost be viewed as an organism in its own right.



SOURCE: B&B ELECTRONICS

The network gateways can connect many devices and accommodate many different interfaces. All of these resources are available to the collective. No single network gateway is responsible for every task.

Intelligent SWARM networking

With SWARM intelligence applied to data networking, an edge device does not have to be a single physical device with implicit limitations on interfaces, resources and expansion. Instead, it can be made up of a number of discrete physical devices, with each one contributing its interfaces and processing capabilities to the collective. Together, these individual devices can then be viewed, in architectural and functional terms, as a single entity.

This approach solves the scalability problem which has been the “elephant in the room” when discussing previous edge architectures. Doing so results in a quantifiable reduction in the total cost of ownership of an edge SWARM compared to other current solutions.

There are five distinct ways that SWARM intelligence reduces the cost of ownership for industrial systems.

Service oriented

Conventional edge devices are typically either relatively limited in their programmability providing, for example, simple scripting support, or may require detailed user programming that requires a high level of familiarity with the device and its underlying hardware and software structure. SWARM devices support both scripting and detailed programming, but dramatically reduce the time and risks involved in business logic development by providing fully rewireable services, coupled to an ontology engine that allows services to be broadcast throughout the SWARM. User programming becomes, to a much greater degree, an exercise in the binding of trusted services and user modules, while also allowing for the extension of the available services and modules for inclusion in the local SWARM.

The generation of local business intelligence is further simplified by the provision of an internal continuous query engine, allowing users to filter and enrich underlying data passing through the SWARM by invoking calls using a comprehensive high level query language which includes the concepts of both time and number bound operations.

This combination of features dramatically reduces the time and risk involved in the development and deployment of the business logic, analytics or other user programming required at the edge. This shortens the overall time to revenue for systems based on SWARM.

Future interfaces and resources

In traditional edge devices it is necessary to define the characteristics of the device prior to installation. Parameters may include the number and type of physical interfaces to be provided, the bandwidth of the processor, the amount of RAM and the persistent storage required. This often leads to the deployment of devices that are more expensive than is really necessary, as a means of “future-proofing” the installation. Even then, an installation may prove to be inadequate for some future task, calling for replacement with more advanced equipment, potentially also incurring costs for retest or recertification of the installation.

A SWARM edge is already future proof. If a new interface is required, or if a new edge application calls for more processing power, memory or storage resources, additional nodes with the necessary features can simply be added to the pre-existing SWARM, with no effect on any of the existing interfaces or the applications built upon them. As new classes of device emerge, the SWARM will absorb and incorporate them, thus increasing the overall capabilities of the collective.

This means that deployed devices can be sized for the known requirements at the point of deployment, without risk to the investment being made at the time.

Installation costs

SWARM technology can directly reduce the cost of integrating remote sensors and devices. In a traditional architecture, where the edge is a single physical device in a single location, connecting each sensor or subsystem requires another cable run. That can be made even more expensive if trenching is required, or there is a need for armored or specialist cables.

In a SWARM-based system, a wireless node is connected to a sensor or device. The node then makes its data available to all of the SWARM, which provides a wireless path to the network gateway. This makes a cable run unnecessary.

Redundancy

The ability to add and use new interfaces and resources, along with the routing capabilities built into each SWARM device, makes SWARM incredibly flexible technology to implement. It is easy to set up strategies to attach business logic to multiple interfaces, providing redundancy of outputs, or x-out-of-y voting on input data. Redundancy need only be added to those interfaces that truly require it. This is far cheaper and far less complicated than the process of creating redundancy by duplicating the entire edge.

Managed device infrastructure

Each device within the SWARM supports local configuration and management. More importantly, SWARM also supports remote management from a central location. This dramatically reduces the number of site trips required for system maintenance.

A SWARM reports the status of connected devices and allows for the download of user programs to both individual devices and groups of devices. User programs are deployed in protected containers within the edge devices, and no user program can negatively impact services, interfaces or programs that are running outside of those containers. If a user downloads a program that contains bugs, the program itself may crash. But the edge device remains operational, and the user can remotely recover the situation.

SWARM devices also include the ability to support "zero touch" provisioning, automatically contacting a central server to obtain their initial configurations and user modules on initial power up. To bring an unconfigured SWARM device into service, the device need only be physically installed and switched on. This reduces the number of operational spares needed to support a system, as standard SWARM devices can be substituted without any pre-configuration process. Additionally, the installer needs no special skills.

Conclusion

Like a beehive or an ant colony, SWARM technology lets individual devices contribute their abilities to the collective, even legacy equipment that was never designed to be a part of the Internet of Things.

In doing so, SWARM technology provides massive scalability and the ability to easily integrate future, as yet undefined, interfaces and devices. SWARM can drastically reduce the costs of application development and deployment, installation, commissioning and maintenance out at the network edge.

Tim Taberner *is Global Project Manager, Advanced IoT Gateways for B&B SmartWorx.*

Industry 4.0 impact on PLC system design

The promise of Industry 4.0 will be realized through greater levels of integration across PLC system design. Engineers can no longer ignore obvious problems on their boards. Many analog and discrete components that have worked so well in previous systems are simply too big for micro PLCs and embedded controllers.

MANUFACTURERS ARE DEPLOYING the latest sensor technologies, adopting new control architectures, and starting to discover the potential of "big data" and analytics. Often called Industry 4.0, what's happening in manufacturing is nothing short of a revolution.

For equipment OEMs, this represents a massive opportunity. The number of sensors used to track environmental and process variables continues to increase. This is accelerating the transition to distributed control architectures, as plant operators seek to reduce bottlenecks and shorten control loops by moving PLCs closer to the processes they control. Ultimately, the promise of improved operational efficiencies and yields will lead to the largest overhaul of plant operations since the invention of the PLC.

This poses a considerable challenge for PLC engineers. System designers will need to pack more I/O and functionality into enclosures that keep getting smaller, and there's relatively little space to be gained from digital scaling of the microprocessor. In today's advanced PLC modules, analog and discrete components consume approximately 85% of board space.

Next industrial revolution

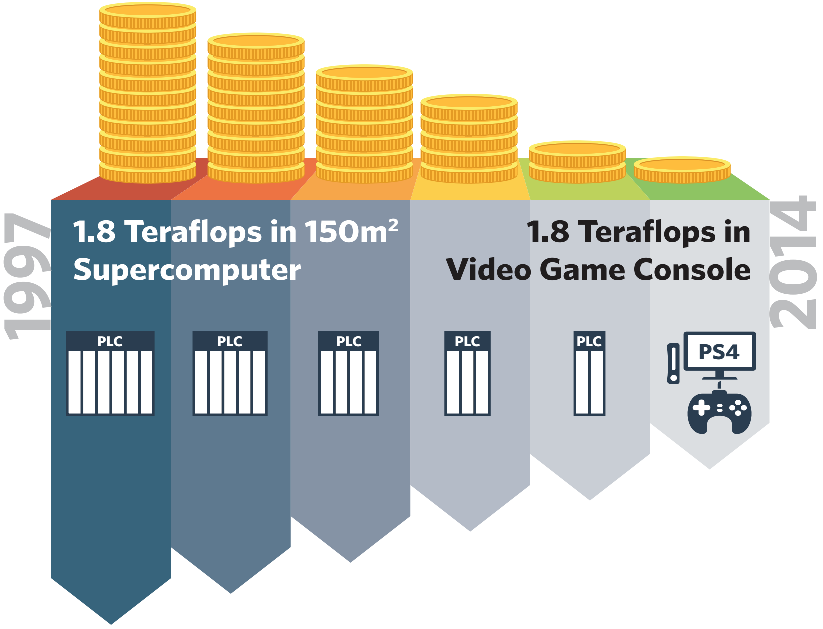
PLCs have been at the nexus of industrial transformation ever since the introduction of the Modicon 084 in 1969. But they have become progressively more powerful over the years, capable of handling more inputs, larger words, and more complex instruction sets.

Today, innovations in analog and sensor technology are helping manufacturers take full advantage of the massive compute resources available, both in the factory and the cloud. Industry 4.0 represents a vision for what's possible when you combine this intelligence with pervasive sensing, distributed control, and seamless connectivity. And once again, the PLC finds itself at the center of a revolution. This is creating new business opportunities for PLC OEMs as manufacturers increase capital expenditures to take advantage of these technologies. However, it also raises a variety of challenges for system designers.

The promise of Big Data

Thanks to Moore's Law, massive amounts of processing power enables enterprises to crunch terabytes or even petabytes of data. For manufacturers, the biggest challenge is collecting and acting on this data. Three trends have emerged to address this problem:

- **Pervasive Sensing**. The cost of sensors and their interfaces continues to decline, enabling manufacturers to track more variables and types of data.
- **Distributed Control**. Moving process controllers closer to the machines they control eliminates bottlenecks to improve manufacturing throughput and flexibility.
- **Seamless Connectivity**. Manufacturers are connecting the factory to the enterprise network to unlock the potential of big data and analytics.



SOURCE: IMAXIM

In 1997, a supercomputer offered 1.8 TeraFLOPS of processing power in 150m^2. Today, it's in a video game console.

New integration problems

A recent market study revealed that engineers still believe that digital technology offers the best opportunity for spacing savings. Yet, digital chips consume just 15% to 20% of board space in PLC modules.

The problem is the amount of PCB devoted to analog and discrete components. These devices consume as much as 85% of available board space in PLC modules. But they don't scale like digital chips, so greater levels of integration are needed to conserve PCB space while delivering the required functionality.

Today's market requires a step-function improvement in space and energy efficiency. To be successful designers will need to systematically look for opportunities to streamline analog circuitry and reduce power dissipation. Fortunately, new solutions are being developed that combine multiple discrete functions in a single IC that can provide system designers with significant advantages in size, power consumption and cost. New Micro-PLC technology demonstrates how analog integration can enable a 10x smaller PLC footprint, 50% cooler operation and 70x faster throughput for digital I/O.

Increasing I/O Density

I/O are the essential link between PLCs and the countless sensors and actuators required by Industry 4.0. The I/O isolation architecture offers an opportunity for significant space savings. The traditional approach is to use one optocoupler per channel, connecting each optocoupler output to a digital input on the microcontroller. This approach is costly in parts count, board space, and use of digital I/O pins. Today, multichannel serializers can translate, condition, and serialize the 24V digital outputs of sensors and switches to the 5V, CMOS-compatible levels required by PLC microcontrollers and reduce the number of necessary isolated channels to three. An eight-channel industrial interface can support SPI daisy chaining, so larger numbers of inputs from multiple serializers can share the same three isolated signals. There can be dramatic savings in power dissipation, parts count, overall PCB real-estate footprint, optocouplers, and cost for a 32-channel implementation, compared to the nonserialized approach.

Lower heat dissipation

Higher I/O density and smaller form factors also add to the design challenge in another basic way, a consequence of the inevitable power dissipation. The system must be more power efficient than ever to keep the PLC from overheating, especially in an application where fans and vents are generally not acceptable.

An often-overlooked source of heat in PLCs is I^{2}R losses in the DC power-distribution feeds. Frequently, 24V is used for PLC backplanes, while 12V is used for on-board distribution. A better approach is to use 48V across the board to reduce current by a factor of 4 and PCB copper losses by a factor of 16.

Using high-voltage point-of-load DC-DC converters eliminates the need for intermediate DC-DC conversion stage. Converters operate directly with up to 60V inputs to enable single-stage conversion for digital, analog, and mixed-signal loads at low voltage, freeing valuable board space while avoiding the cost and energy losses of the interstitial stage. They minimize copper losses, reduce connector contact current ratings, and increase reliability while maintaining cool operation using a synchronous switch architecture.

Power subsystem complexity

Today's signal-conditioning, processing and communication circuits require a diverse set of power rails, often differing by a few volts or only fractions of a volt. This exacerbates an already complex electrical environment. Add to this the increasingly sophisticated methods of energy savings through various power-control methods, and the cost and complexity of power subsystems only increase further.

SOURCE: IMAXIM

One way to supporting Industry 4 Micro PLC Reference Design shows how much space can be saved when engineers take advantage of new analog integration.

Maxim's Beyond the Rails products simplify the signal chain, enabling a design that allows ±10V bipolar inputs to be multiplexed, amplified, filtered, and digitized, all with a single 5V supply. This eliminates the need for additional ±15V power supplies, thus reducing component count, system cost, power dissipation, and footprint.

Countering security threats

When factory networks were closed to the outside, IT security issues usually involved rogue employees and internal data theft. Those "good old days" are gone, and are not coming back. Today's Internet-connected PLCs must be protected against multiple threats, including hackers, malware, and viruses.

System-level software provides an initial level of protection, but it isn't enough. Hardware-based security protects against:

- **"Cloned" or counterfeit components**. Counterfeit field sensors and I/O modules pose a real threat to your bottom line, but the bigger danger is that they could be used to execute an attack on the industrial environment. Using a secure authentication IC is the only way to guarantee that you can trust the temperature readings being sent from a boiler and other critical components.
- **Malware injection**. Stuxnet was a wake-up call to industry. System operators must ensure that all equipment upon which a SCADA or DCS system is built runs genuine software. Secure boot and secure update management are the best ways to protect a device from malware injection. A secure coprocessor can be used to implement an encryption design that fully addresses issues with minimal design-in effort.
- **Eavesdropping**. As concern over industrial espionage increases, manufacturers must ensure that unauthorized users cannot steal trade secrets off of industrial networks. Encryption and authentication ICs can protect against such eavesdropping, and go further with active tamper detection to prevent brute-force attacks on the hardware components.

Integration advantage with PLCs

Industry 4.0 is fundamentally transforming what it takes to win in the PLC market. Smaller form factors, higher I/O density, and advanced capabilities—success today necessitates new strategies for managing competing demands for more functions in less space.

Engineers who seek out higher levels of component integration will be well positioned as manufacturers pursue the benefits promised by Industry 4.0.

Suhel Dhanani *is Principal Strategic Marketing Manager for Maxim.*

SOURCE: INDUSTRY 4.0

New UHF RFID projects overcome technical challenges

RFID systems in accordance with the UHF standard provide key advantages when identifying objects along the supply chain. Often, UHF projects are considered challenging due to technical reasons. A new generation of readers offer important functions to implement UHF projects quickly and at low cost.

THE MAJOR COST DRIVERS IN RFID projects, besides the hardware (reader and transponder), are the effort expended in integration and commissioning. According to a study by ARC Advisory Group, the costs for software and integration are about twice as much as the expenditures for the reading technology.

But now, new UHF reader technology is lowering the cost of projects and reducing downtime as well. Integrated software provides commissioning and diagnostic tools, and hardware options such as adaptive antennas have improved acquisition rates.

SOURCE: SIEMENS

New RFID readers with adaptive antennas are easy to configure for different environmental conditions.

Software speeds commissioning

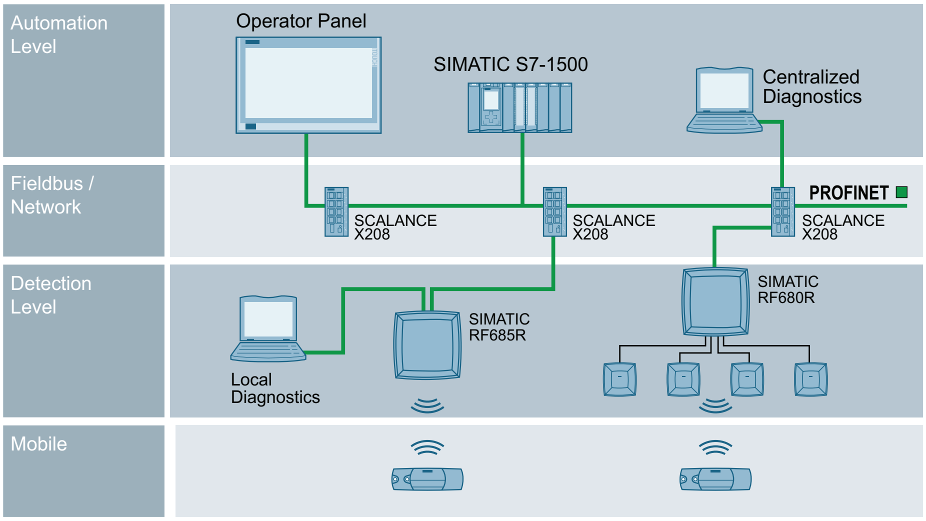
In commissioning UHF RFID systems, important parameters such as an ability to transmit power have to be defined. Using functions such as Determine Pickup Power, new UHF readers can deliver tools that enable users to determine the least amount of radiated power required at the push of a button. The function also supplies information about tags acquired due to overshooting, which allows the integrated filter algorithms to be optimized accordingly.

Orientation of antennas can be setup in a few minutes with the aid of software tools. The RFID system gives the user immediate feedback, if changing the antenna position or orientation affects acquisition. The same information is also shown via a brightly lit LED row on the housing of the reader – so that the setup can also be performed in obstructed installations. During commissioning or diagnostic, software installations have been eliminated, and the user interface is easily accessible using a web browser.

First class reading results

Combining a high-quality radio module and extensive evaluation algorithms, first-class reading results can be achieved. The algorithms, such as the automatic control of the transmitting power, not only lead to a high reading rate, but also to the least amount of energy emitted – to prevent interference at neighboring readers. At the same time, overshooting is reliably avoided with them. Many functions are designed to automatically adapt to changing environmental conditions (such as moving objects or tolerances in transponder sensitivity).

For the first time, the SIMATIC RF685R reader is shipped with a built-in antenna, whose polarization can be configured by the user via software command as either circular, linear-vertical or linear-horizontal. The advantage is that the same device can be utilized for different applications. This not only simplifies commissioning, but also the planning and management of spare parts. A strength of the antenna is that the reader automatically selects the best antenna configuration for each individual reading operation based on special algorithms.



SOURCE: SIEMENS

Thanks to the use of different protocols, the readers can be seamlessly integrated into IT and automation systems.

Reducing downtime

To reduce downtimes, it is very important to have meaningful diagnostics. In a "Tag Monitor" menu, information necessary to assess the quality of the reading results during operation is displayed. Even the tags filtered out on the basis of the "UHF for Industry" algorithms used are shown. With that, the effect of these filter functions can be easily analyzed and their parameters be quickly optimized.

A built-in diagnostics log records all events including read and write errors or changes made to the parameters of the reader.

Application report by ***Siemens****.*

Wireless radios for monitoring/control

Wireless radios communicate with infrastructure to supply water to mountainous West Virginia terrain isolated from such amenities as high speed internet and/or cell phone coverage in most of the region.

EXTREME ENDEAVORS WAS CREATED to design reliable and robust equipment for the harshest conditions found anywhere on Earth. The company specializes in taking technology into the most remote and dangerous places imaginable.

West Virginia (USA) may not be a place most people think of as dangerous, but it presents utilities and other businesses with a unique set of challenges. It is known for its beautiful rolling hills, thick vegetation and isolation from such amenities as high speed internet and/or cell phone coverage in some regions.

Water supply system monitoring

One of Extreme Endeavors' projects is with Central Barbour Public Service District (Central Barbour PSD), a large network of five water tanks and five pump stations in a remote area of Northern West Virginia.

Central Barbour PSD stretches from the town of Philippi up to Backbone Mountain, a ridge of the Allegheny Mountains of the central Appalachian Mountain Range. It is situated in the U.S. states of West Virginia and Maryland and forms a portion of the Eastern Continental Divide. Extreme Endeavors looks to AvaLAN Wireless products to perform critical infrastructure monitor and control in this region.

By utilizing wireless radios to fabricate the Node Extender and repeater product lines, that communicate with the sensors and controllers. These solutions have an excellent history of dependability in mountainous terrain for SCADA applications.

The system uses the high speed network connectivity to sense water tank levels, grid power conditions, pump motor current levels and a variety of other parameters. Not only does the system bounce around the mountains sensing parameters, it also controls the pumping system which distributes water throughout the mountainous region.

"By using a high speed network, we can acquire high sample rate sensor data with greater precision and timing accuracy allowing us to use this information to perform advanced calculations which describe the systems state and conditions that could become costly," said Mike Masterman, president of Extreme Endeavors.

Wireless radio technology provides an effective connectivity solution for remote water supply system.

This system has proven beneficial in other facets as well. Recently an Intelligent Power and Control (IPAC) system manufactured by Extreme Endeavors detected an over voltage condition on the power grid.

IPAC provides a network based power monitoring and control system suited for control of industrial facilities or remote locations. The solution proved its worth early on when the power company could be notified to replace a faulty transformer before any critical potential problems could occur.

Critical infrastructure monitoring between AvaLAN Wireless and Extreme Endeavors will continue with leak detection algorithms and real time chemical analyses of drinking water quality. The analytics of power grid monitoring is also an area that is rapidly expanding. Using the intelligent priority based power control of the IPAC modules with the connectivity support by the wireless solution, Extreme Endeavors is looking at power control of remote locations, creating a microgrid within a building and or other locations.

*Application report by **AvaLAN Wireless**.*

Implementing more intelligent OT/IT networking solutions

Manufacturing will change more radically in the next five years than it has in the last twenty. In the "Internet of Things" (IoT), almost every object can use embedded technology to gather and transmit information. Machinery on a factory floor will be able to manage its own quality control and energy usage.

THE ACCELERATED CONNECTION OF OPERATIONS technology (OT) and information technology (IT) is enabling unprecedented collaboration across the enterprise, linking processes and facilities to suppliers and customers in new ways.

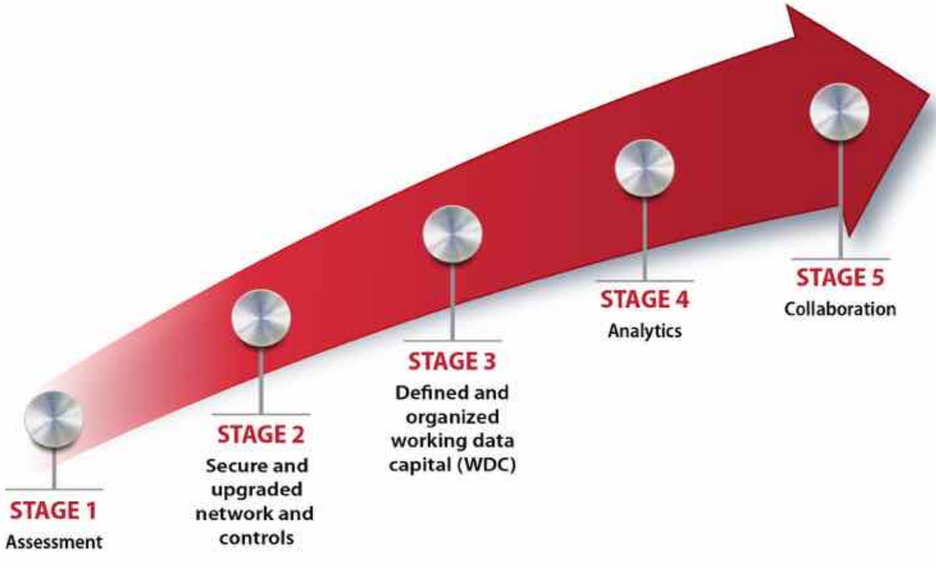
Manufacturers, industrial operators and Original Equipment Manufacturers (OEMs) can take advantage of real-time decision-making that drives profitability, but they also face new challenges in securing the data and infrastructure that underlies that opportunity.

A new path to productivity

The rapid convergence of OT and IT, thanks to the proliferation and affordability of plant-floor Ethernet and smart devices, powerful local computing solutions and multiple network technologies merging into one is transforming information into insight. This gives decision-makers across the enterprise new visibility into operations — and new opportunities to make them better in response to:

- *Internal measures:* Real-time monitoring and sharing of key performance indicators (KPIs) so that staff (senior executives down through frontline employees) can identify problems and resolve issues before they escalate or even occur. You cannot improve what you don't measure.
- *External business activities:* Incorporate customer-demand information and/or supplier performance data (e.g., late deliveries, out-of-stocks) as they happen to trigger revised production scheduling, staffing changes, procurement alternatives, etc.
- *Market changes:* Supply-chain planners and purchasing managers now rely on anarray of vendors from around the world, complicating management of lead times, quality, and cost control (e.g., additional staff time to work with distant suppliers, inventory carrying costs, obsolete materials due to overstocking).

The connection of people and processes via technology allows executives and their continuous-improvement (CI) teams to implement real-time decision-support tools that boost productivity and profits — often without direct intervention or additional staff.


STAGE 1
Assessment
STAGE 2
Secure and upgraded network and controls
STAGE 3
Defined and organized working data capital (WDC)
STAGE 4
Analytics
STAGE 5
Collaboration

SOURCE: ROCKWELL AUTOMATION

Looking at the progressive stages of a Connected Factory Model provides a framework for managing improvements.

"Making data the basis for automation and control," said a recent McKinsey Quarterly, "means converting the data and analysis collected through the Internet of Things into instructions that feed back through the network to actuators that, in turn, modify processes. Closing the loop from data to automated applications can raise productivity, as systems that adjust automatically to complex situations make many human interventions unnecessary."

Intelligent networks are also improving optimization of assets including energy usage, equipment reliability, longevity and expanded capacity from existing assets. The information delivered by the network also helps executives to plan strategically, scheduling production within their portfolio of facilities based on performance trends, logistics patterns, market demands, etc.

Lastly, when baby-boomer executives and experts throughout the organization including engineers, OT specialists and maintenance personnel retire, their lost knowledge becomes a significant danger to the organization. (Some 10,000 baby boomers will turn 65 every day until 2030.)

Improved information flow and availability can help to mitigate this risk, especially in industries facing increased customer demands, regulatory requirements, and a decrease in skilled labor.

Information and profitability

Most industrial infrastructures today were not designed to take advantage of the Internet of Things. According to the 2013 Next Generation Manufacturing Study, surprisingly few manufacturing executives indicate that their business systems and equipment are state-of- the-art and able to provide long-term support for six key strategies that will drive organizations into the next generation.

A study of manufacturers found surprisingly low levels of integration, both on the plant floor and throughout the enterprise:

- Only 14% of executives indicated that all plant-floor data is integrated with enterprise systems.
- About one-quarter of executives indicated that nearly half or more of their plant-floor machinery (not including computers) is Internet-enabled (Ethernet or Wi-Fi); 30% report none of their equipment is Ethernet-enabled.

The opportunity clearly exists for manufacturers to bring their equipment and systems into the modern information-enabled world. The American Society for Quality (ASQ) surveyed manufacturers about their use of smart manufacturing — defined as the integration of network-based data and information that provides real-time understanding, reasoning, planning, management and related decision making of all aspects of a manufacturing and supply-chain enterprise. Only 13 percent said they use smart manufacturing within their organization. Of those organizations that claim to have implemented smart manufacturing, 82 percent say they have experienced increased efficiency, 49 percent experienced fewer product defects, and 45 percent experienced increased customer satisfaction.

Attacks on enterprise networks can come from anywhere, anything, and anyone, including via legacy OT devices. As employees or contractors monitor production via wireless smartphones and tablets, these hand-held devices can become entry points for both intentional and unintentional internal attacks or, externally, through authorized or unauthorized remote access. Unauthorized access could indicate an attacker's intent to capture proprietary data or information, or to fully stop production at a facility. More malicious actions could impair plants in ways that put public health and welfare in danger.

Security policies must now reach from enterprise to end point, areas in which IT has not traditionally ventured and which require IT and OT collaboration to securely address the needs of the operation. Aging systems connected to modern OT or modern systems connecting to aging OT also can pose significant risks, such as flawed transmissions that change processes and result in incorrect product specifications, poor quality, or equipment and work stoppages.

A production stoppage in industries such as the automotive sector, can exceed $20,000 per minute. Networks also can incorrectly interpret data, building reports that misrepresent operations information for customers, stakeholders, regulators, and/or corporate reporting and planning. These older legacy systems also are becoming harder to integrate and maintain for improved efficiencies.

Stage 1: Assessment

The Assessment Stage of the Connected Enterprise Maturity Model evaluates all facets of an organization's existing OT/IT network:

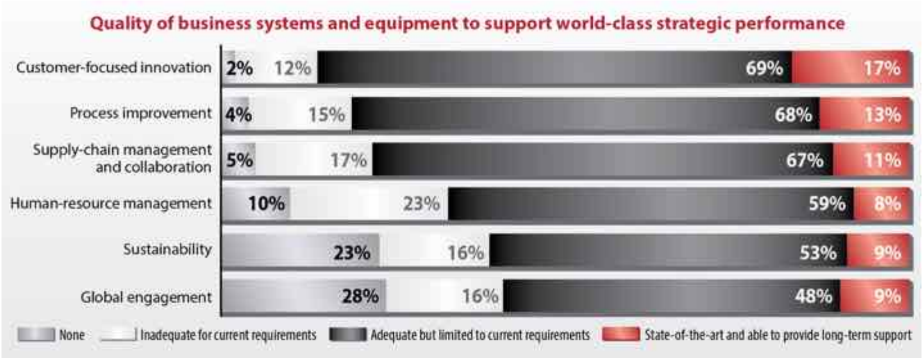
- Information infrastructure (hardware and software)
- Controls and devices (sensors, actuators, motor controls, switches, etc.) that feed and receive data,
- Networks that move all of this information, and
- Security policies (understanding, organization, enforcement).

Especially critical is an examination of the people and processes that manage this framework, if a recognizable framework even exists.

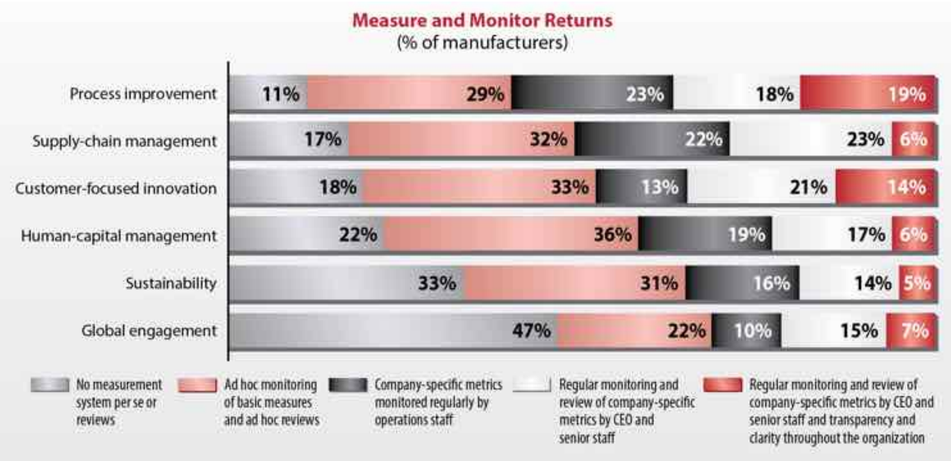
A major challenge during the Assessment Stage is potential hesitation to invest time in questioning practices that they have relied upon for years. Even more pressing, though, is to understand how to manage the transition to a more intelligent OT/IT network without disrupting operations or causing customer delays. That transition will depend, in large part, on the extent of the gap between the current state and the desire state — i.e., can the capability of the existing network be upgraded, or will it need to be replaced?

A thorough assessment identifies and catalogs problems with the existing OT/IT network, to help create a "wish list" for the new network and operations, laying the foundation for more advanced technologies, such as business intelligence software or cloud-computing capabilities. More than half of manufacturers (56%) report that none of their applications or systems use cloud computing; another 23% have just 1–10% of applications and systems in the cloud. On average, just 10% of applications and systems are in the cloud, however, cloud computing falls among the top three technologies CIOs selected as a priority in 2013 as it is predicted to disrupt business fundamentally over the next 10 years. These statistics are likely driven as much by technology capabilities as by executive preference.

Just as important as understanding the ability to move to improved technologies, the assessment will uncover network security issues, allowing for risk-mitigation procedures to begin. No two manufacturers are alike, and each will define the level of risk they are willing to accept, and the level of action they



Surprisingly few manufacturing executives indicate that their business systems and equipment are state-of-the-art and able to provide long-term support for key strategies that will drive the next generation.



SOURCE: THE MPI GROUP

An effective OT/IT network incorporates data from OT devices across the enterprise to deliver performance-critical information (costs and downtime, for example) that can be used for improving the quality of real-time decision-making.

are willing to take on to get to that sense of security. The precise definition of those "consequences" is another outcome of the Assessment Stage.

Stage 2: Secure and upgraded

After gaps and weaknesses have been identified in the current OT/IT network and operations, upgrades begin with a long-term view that contemplates facility expansions and new technologies. During this stage the organization evolves and/or builds an OT/IT backbone that will deliver secure, adaptable connectivity from plant-floor operations to enterprise business systems.

It's this phrase "from plant floor to enterprise network" that surfaces as one of the largest challenges manufacturers face in designing more intelligent network. Who has responsibility for managing the new OT/IT network? Is it OT, or IT, or both? During Stage 2, upgrades to hardware begin, along with planning for how OT and IT engineers will collaborate. In a workshop environment, cross-functional teams assess new technology options, establish vendor roadmaps, and plot out future-ready, scalable design of the OT/IT network.

The objective is to guide the intersection of OT and IT in a controlled, virtual environment, rather than wait and hit those problems in the real world, with real customer orders on the line. This process also allows companies to map out business processes and workflows that are acceptable to both sides of the house and appropriately distribute management of the intelligent network.

A frequent challenge, especially in larger organizations, is the sheer volume and variety of outdated controls and networks in place. Savvy executives plan for systematic replacements, with priorities determined by cross-functional teams that include representation by location, function, etc. It's also not uncommon for an OT/IT upgrade to encounter hesitation from executives and engineers who feel that current systems remain viable. If a network cannot acknowledge equipment, it cannot secure it. Senior leadership will be responsible for the culture change that persuades or removes these obstacles to change.

Even as an organization moves through Stage 2, a more secure network emerges, providing accessible data with built-in security authorizations and authentications. For many companies, it will be the first time they've ever had an integrated OT/IT network and the first opportunity to control equipment performance in real time (e.g., demand responsiveness). Developing a security policy to accompany the more secure, productive network also begins in Stage 2.

Stage 3: Defined and organized

In Stage 3, teams organized for the OT/IT upgrade, define, and organize the company's Working Data Capital (WDC) including all the available data for improving business processes and improvements, and determine how to leverage it for optimum gains. Note that none of the stages are completely separated from others, and this is especially true with organizational changes in Stage 2 (new data capabilities emerging) and Stage 3 (identifying how to harness and leverage the data). In Stage 3, the team also "contextualizes" the data by scoping new workflows, schedules, and responsibilities. Data must be standardized and normalized between systems.

A WDC plan prevents manufacturers and industrial operations from drowning in data while they starve for information. The plan helps companies establish systems that allow them to identify how to turn data into tangible triggers for change, and to evaluate how C-level strategic decisions benefit the bottom line.

Even with the most basic of business strategies, few manufacturers can clearly see as an entire organization the return from their efforts. For example, just 14% of manufacturers describe their measurement systems for reviewing return from customer-focused innovation efforts as regular monitoring and review of company-specific metrics by CEO and senior staff and transparency and clarity throughout the organization. Many manufacturers have no systems to monitor returns from strategic efforts.

An effective OT/IT network incorporates data from OT devices across the enterprise to deliver performance-critical information (e.g., costs, downtime) that can be used for real time decision-making, even as IT supports more locations via remote monitoring. Just as important, documentation also is being compiled in real-time necessary for customers, certification programs (e.g., ISO), and regulatory compliance programs.

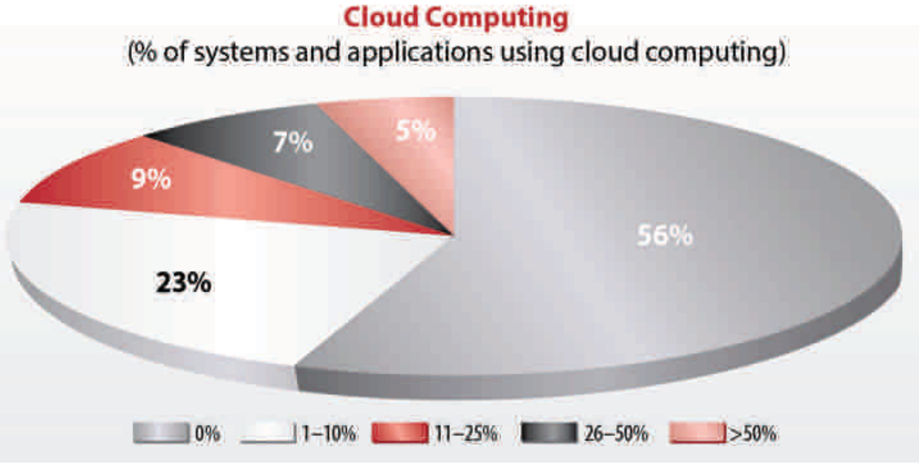
Stage 4: Analytics

During Stage 4, the focus shifts from hardware, devices, software and networks to continuous improvement. How best to leverage the newfound OT/IT capabilities? A changing culture within the company now recognizes the ability of the OT/IT network to surface problems and opportunities in real-time. At an operational level, analytics utilizing the WDC identified will help to pinpoint the greatest needs for real-time information (e.g., persistent problems by location, process, product, machine); authorized recipients of the information who have the ability to act on the information; and standardized protocols that the information will trigger (many proactive and automatic).

At the senior executive level, analytics inform asset management. According to Sujeet Chand, senior vice president and chief technical officer at Rockwell, "the OT/IT network has evolved into an ecosystem," said "It allows executives to optimize their global plant operations and achieve significant long-term savings via capital-avoidance. They can make better decisions on which plants produce which products, and when."

During Stage 4, the challenge continues to be in scope, and avoiding data overload. Some managers will want to capture and review all available data, even though there is little benefit in doing so. Others will fall victim to "data disbelief" and will be hesitant to accept data emerging from the plant floor because it contradicts long-held beliefs regarding how processes, lines and equipment operate. Again, senior leadership will be responsible for culture change that persuades or removes these obstacles to change, furthering development of an organization focused on operational excellence.

Once cultural change begins to occur, built-in mechanisms will proactively respond to issues and problems as they arise, often based on lead metrics that minimize cost training losses. So rather than wait for lag measures that lead to an accumulation of



SOURCE: THE MPI GROUP

More than half of manufacturers (56%) report that none of their applications or systems use cloud computing; another 23% have just 1–10% of applications and systems in the cloud.

wastes (inventory, resources, energy, etc.) and that typically spur short-lived firefighting improvements, WDC and analytics help the organization rapidly identify and prioritize continuous-improvement/kaizen projects before problems escalate. And through this progression of ongoing operational improvements via lean, six sigma, and/or other improvement principles — productivity, efficiency, and quality improve in lockstep. Rockwell itself has achieved operational improvements over multiple years of the company's progression through the model.

Stage 5: Collaboration

Stage 5 of the maturity model is creating an environment that anticipates activities throughout the enterprise and through the supply and demand chain. Predictive capabilities emerge within the enterprise that make for more efficient production planning and asset management; timely and leveled order execution; improved quality; and streamlined plant-to-plant performances. Real-time information brings the ability to sense and manipulate plant processes on the fly.

The external objectives are to develop responsiveness to external events (supplier and customer activities, business trends, markets, political events, and even weather patterns) to minimize losses from negative events (for example, foreign currency collapse and its impact on inventories in the country) and leverage new opportunities (the effect of a heat wave on product demand). The OT/IT network begins to coordinate activities from furthest suppliers to end customers.

Although the opportunity to improve supplier and customer relationships is available to all manufacturers, only 21% have developed "partnership" relationships with customers, and only 13% describe their supplier relationships as "partnerships".

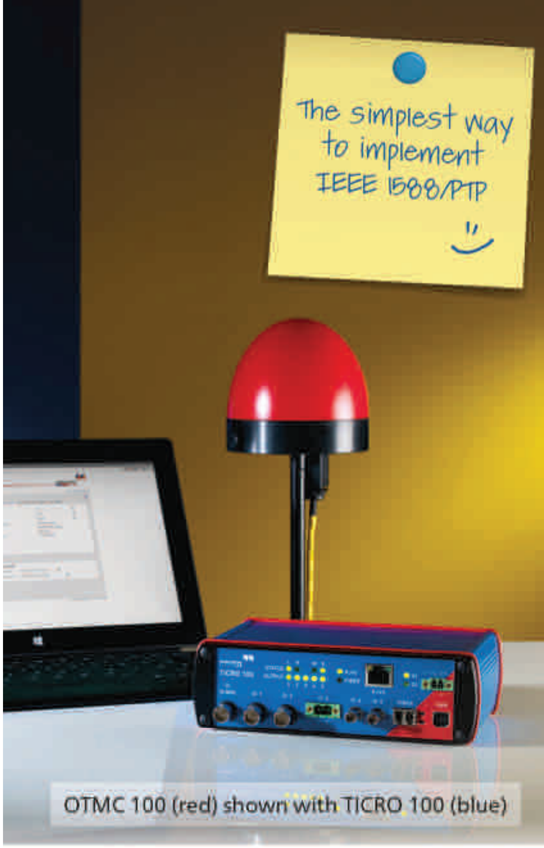
During Stage 5 improvement continues internally, but focuses on advanced performance targets with innovative methods to reach once-unrealistic goals. One major challenge during this stage is tempering the belief that the organization can now "do anything," which can unnecessarily burden staff.

Limitations of OT/IT networks at suppliers and customers also can prevent optimum collaboration and performance. Supplier criteria can be established to "encourage" vendors to move forward with their own maturity models, but customers may remain resistant until they understand how collaboration can improve products and prices. For suppliers, customers and business units capturing or contributing data to the OT/IT network, access should be scoped both for network-security reasons and to protect proprietary processes.

The benefits from being able to react rapidly and accurately to emerging supply-chain and market conditions drive operational excellence and cost savings in countless ways:

- Improvement of supplier performances in delivery, quality, and costs, as well as improved vendor documentation for regulatory compliance.
- Integrated production with the enterprise via manufacturing execution systems that drive and track consistent workflows, materials consumption, inventories, etc.
- New partnering opportunities, such as collaboration tools in use across an extended OT/IT technology framework (e.g. remote access, instant messaging, video chat, file sharing, etc.) that unleash unprecedented innovation.
- Centrally located domain experts that can be leveraged across countries and companies, sharing best practices and enlisting the knowledge base of an entire supply chain to address challenges.

Technology article by ***Rockwell Automation****.*



Secure cloud-based remote maintenance and engineering

Plants that work efficiently must be continuously available. When disturbances occur, quick assistance via remote maintenance is essential, but operators often avoid maintenance access for security reasons. Manufacturers shy away from investing in a infrastructure that constantly needs to be state-of-the-art.

SOURCE: INNOMINATE

The equipment manufacturer STOPA ensures the highest possible availability of its storage systems via remote service.

A SECURE CLOUD PLATFORM can address this conflict between plant operators that avoid remote maintenance access for security reasons, and the need to invest in a state-of-the-art security infrastructure. New solutions can now offer the latest security standards, meaning that plant manufacturers do not require their own infrastructure.

"As an equipment manufacturer, our core competency does not lie in constructing complex IT infrastructures, but service-friendly plants for our customers," said Ettore Caurla from the Customer Service Department at STOPA Anlagenbau GmbH, a leading European provider of automatic storage and retrieval systems.

Avoiding 80% of the disruptions

STOPA's storage systems need to ensure a quick and efficient material flow for operators. If a storage system is disrupted, the entire production process can be quickly compromised. Common causes of disruptions include plant and operative problems, including a proper handling under Windows or the configuration of Interbus or Profibus applications. Many of the problems can quickly be solved online or by telephone.

Service and system availability have always played a decisive competitive role for the manufacturer. For this reason, remote service has been a common means of support at STOPA for 20 years. Initially, customer plants were remotely accessed using analog modems. However, with the rising scope of automation technology services and data volumes, this was no longer enough. Slow connections led to a situation in which the sensor data status changed during transmission, for example. So the modems were replaced by broadband IP connections. One service employee reported that 1,000 of its 1,600 plants are connected via remote service. Only smaller and older plants have not been included, and new plants are fully equipped with remote service features.

The STOPA Customer Service Department systematically evaluates the duration and success rate of the remote service. It received 5,000 calls last year. These included requests for appointments, documents or other service information. Remote support was initiated for 600 calls to resolve disruptions. In 78% of these cases, the problem could be conclusively resolved within 24 hours. Only the remaining 22% required longer processing times, for instance due to spare parts for defective devices not being available locally.

Reducing fault-clearing times

Previously STOPA had used a modem-based service solution for remote support. The average connection time per assignment was 75 minutes. Establishing the connection and exchanging extensive program files with Siemens Step 7 alone required 20 minutes, and more complicated handling extended the support time.

With the conversion to mGuard VPN (virtual private network) technology from Innominate, the average connection time was reduced to just 37 minutes. Here, establishing the connection initially required 30 seconds, but was reduced to just a few seconds after a software update. Basically nothing was changed in terms of the accessibility of the Simatic S7 or S5 systems. The processes merely became more streamlined due to the intuitive operation. "The connection time for remote service is an important variable, because the faster we can help the customer, the more cases the support team can attend to," said Caurla. Not only was the IP connection technology replaced, but with the cloud platform "mGuard Secure Cloud", a new remote service approach was introduced.

The operator retains control. VPN connections can only be established from the machine outwards using a hardware key switch.

SOURCE: INNOMINATE

Remote cloud platform

"We were looking for an easy-to-manage and economic solution. It had to ensure the highest security standard for our customers. At the same time, we did not want to deal with complex security architectures or the configuration of VPN clients, proxies and firewalls," explains the STOPA service technician.

From the perspective of the plant manufacturer, setting up an in-house security infrastructure would be too costly: "State-of-the-art security requires a reliable and fail-safe infrastructure, disaster recovery and ongoing updates. Due to the high infrastructural and personnel costs involved, these factors are not economically feasible for a medium-sized manufacturer," said Caurla.

According to a service technician working on the system, "The cloud solution is the perfect approach. The hardware is already pre-configured for use. Just two outgoing ports need to be set up once for customer-side integration. That's it. We do not intervene in the customer's IT, nor does the customer have to install any software."

Using this solution, a bug and tamper-proof VPN tunnel is established with hardware-based encryption between the customer's plant and the service technician. The connection is established via the company's Secure Cloud, a turnkey VPN infrastructure for operators and plant and equipment manufacturers. The cloud platform is operated in a German data center implementing high security and privacy standards.

Operator retains control

Having set up 1,000 installations, the STOPA service technician names the most important requirements for a remote service solution: "For the operator, system availability has become even more important in recent years. For this reason alone, operators are willing to allow external access. At the same time, they want to retain control. For us as a manufacturer, the costs and efficiency level are decisive factors."

From a previous job as an IT administrator, Caurla has extensive experience with various VPN technologies: "Centralized IT demands reliable protection of one's own plants. Especially in large companies, access to the in-house network is therefore largely restricted. In addition, many security requirements for authorization of remote service connections make handling extremely inefficient."

He cites the example of security tokens that generate a new, one-time password every ten seconds. Once the connection is made, the password has often already expired. In other cases, an IT employee or the supervisor must be called in to enter the password. Such processes make customer support difficult and ineffective.

The STOPA service technician finds the secure cloud approach much more efficient – yet still very secure. "The machine operator must first enable the connection with a VPN hardware switch. It can only be initiated from the plant operator's network. While the connection is being established, an indicator light blinks. Once the connection has been made, this light is permanently illuminated. One push of the switch button is enough to interrupt access. "This ensures that there is always an operator on site. For service access, no one can be endangered (safety). What's more, the operator always maintains control over access to his network, because a connection is only possible after his consent with the hardware switch (security).

Cost-effective and efficient

The service technician emphasizes that with over 1000 plants, customized solutions are impossible. Acceptance for the uniformly utilized mGuard technology is also very high due to the operator's exclusive and permanent control over the VPN connection. Even 20-year-old Simatic S5 systems can be remotely serviced via Ethernet adapter. "This cloud approach is perfect for manufacturers who want to maximize their efficiency: quick connection establishment, ease of use and a security level that only large companies could otherwise attain. Because no in-house infrastructure is required with the cloud platform, we save about 30 – 40% of the costs," said Caurla.

Application case study by ***Innominate Technologies****.*

While others think
about the IIoT
... we enable the change.
Networks and computers for a smarter industry.
• From small to big data to cloud
• Wired, wireless, remote – anywhere, anytime
• Vertical integration from SCADA to field device
Moxa. In the middle of innovation.
www.moxa.com
MOXA
Reliable Networks ▲ Sincere Service

Beckhoff – New Automation Technology

Beckhoff implements open automation systems based on PC Control technology. The product range covers Industrial PCs, I/O and Fieldbus Components, Drive Technology and automation software. Products that can be used as separate components or integrated into a complete and seamless control system are available for all industries.

THE BECKHOFF "NEW AUTOMATION TECHNOLOGY" philosophy represents universal and open control and automation solutions that are used worldwide in a wide variety of different applications, ranging from CNC-controlled machine tools to intelligent building automation.

Worldwide presence on all continents

The central divisions of Beckhoff, such as development, production, administration, distribution, marketing, support and service are located at the Beckhoff Automation GmbH & Co. KG headquarters in Verl, Germany. Rapidly growing presence in the international market is taking place through 34 subsidiaries. Through world-wide co-operation with partners, Beckhoff is represented in more than 70 countries.

Innovative products and services

Since the foundation of the company in 1980, continuous development of innovative products and solutions using PC-based control technology has been the basis for the continued success of Beckhoff.

The Beckhoff PC Control philosophy and the invention of the Lightbus system, the Bus Terminals and TwinCAT automation software represent milestones in automation technology and have become accepted as high-performance alternatives to traditional control technology. EtherCAT, the real-time Ethernet solution, makes forward-looking, high-performance technology available for a new generation of leading edge control concepts.

Beckhoff | The Automation Company

Beckhoff offers comprehensive system solutions in different performance classes for all areas of automation. Beckhoff control technology is scalable – from high-performance Industrial PCs to mini PLCs – and can be adapted precisely to the respective application. TwinCAT automation software integrates real-time control with PLC, NC and CNC functions in a single package.

All Beckhoff controllers are programmed using TwinCAT in accordance with the globally-recognised IEC 61131-3 programming standard. With TwinCAT 3 C/C++ and Matlab®/Simulink® are available as programming languages in addition to IEC 61131-3.

Beckhoff | The IPC Company

Beckhoff supplies the right Industrial PC for every application. High-quality components based on open standards and the rugged construction of the device housings mean that the Industrial PCs are ideally equipped for all control requirements. Embedded PCs make modular IPC technology available in miniature format for DIN rail mounting. In addition to their application in automation, Beckhoff Industrial PCs are also ideally suited to other kinds of tasks – wherever reliable and robust PC technology is required.

Beckhoff | The I/O Company

Beckhoff has the right technology for every signal and every fieldbus. Beckhoff supplies a complete range of Fieldbus Components for all common I/Os and over 15 major fieldbus systems. With the Bus Terminals in protection class IP 20, and the Fieldbus Box modules in IP 67, a complete range is available for all important signal types and fieldbus systems. In addition to conventional bus systems, Beckhoff offers a complete EtherCAT I/O range for the high-speed Ethernet fieldbus based on EtherCAT Terminals and the EtherCAT Box.

Beckhoff | The Motion Company

In combination with the Motion Control solutions offered by the TwinCAT automation software, Beckhoff Drive Technology represents an advanced and complete drive system. PC-based control technology from Beckhoff is ideally suited for single and multiple axis positioning tasks with highly dynamic requirements. The AX5000 Servo Drive series with high-performance EtherCAT system communication offers maximum performance and dynamics.

Servomotors with One Cable Technology, which combines power and feedback system in a standard motor cable, reduce material and commissioning costs. The drive system XTS (eXtended Transport System) replaces classic mechanical systems by innovative mechatronics. It enables individual product transport applications with a continuous flow of material.

BECKHOFF

Beckhoff Automation GmbH & Co. KG
Email: info@beckhoff.com
Phone: +49 5246 963-0
www.beckhoff.com

CC-Link Partner Association - Automation Networks

CC-Link is a family of open-technology industrial automation networks that process control, information & diagnostics to provide efficient, integrated factory-wide industrial and process automation. CC-Link provides high speed, deterministic communication seamlessly linking a wide assortment of multi-vendor automation devices over a single cable.

THE 'FAMILY OF CC-LINK NETWORKS' is ideally suited for machine automation, cell or process control in a wide variety of industries. The CC-Link family includes fieldbus and Safety networks: CC-Link & CC-Link Safety; and the most advanced Industrial Ethernet networks; CC-Link IE Field & CC-Link IE Control. This family of networks is managed by the CC-Link Partner Association (CLPA). The Ethernet-based networks operate at 1 Gigabit speed to provide extremely fast and inherently deterministic communication from the field/sensor/actuator level to the control level of a manufacturing or process operation.

CC-Link is a family of industrial open-technology integrated automation networks:

CC-Link IE Field - Ultra-fast 1 Gigabit Industrial Ethernet network linking field level devices to controllers, as well as controllers to controllers and providing absolute deterministic communications without the need for detailed knowledge of Ethernet networking. CC-Link IE Field is IEC approved for safety communications and can provide integrated motion control and/or energy management functions all on a single Industrial Ethernet network.

CC-Link - Open-technology fieldbus network with performance up to 10 Mbps providing absolute deterministic behavior and cost effectiveness, flexibility and ease of use.

CC-Link Safety - Open-technology fieldbus safety network that is IEC / ISO approved and meets or exceeds industry safety network standards. It provides cost effectiveness, flexibility and ease of use to automation safety networks, all while delivering full compatibility with the CC-Link fieldbus network.

"Why choose CC-Link?"

Primary reasons include CC-Link and CC-Link IE Field are high-performance, cost effective, flexible, as well as easy to install and use. These networks are globally accepted and CC-Link IE is an industry leader with Gigabit Ethernet networking. Independent market research has shown that CC-Link is the market leading choice for automation networks in Asia, the fastest growing market in the world. Combine that with the world leading productivity features of the network, and CC-Link can offer a solution that can bring significant improvements to any manufacturing enterprise anywhere. If that's not enough; there are over 12 million installed nodes & over 1400 CC-Link certified products on the market. Many export oriented American and European manufacturers are incorporating CC-Link compatibility because of its strength and market leadership in Asia.

CC-Link - Your Gateway to Asia

Access markets closed to your current network strategy. 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? Adding CC-Link 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 help you capture this additional market share.

CC-Link Partner Association (CLPA) is a Global organization with offices in the Americas, Europe, and across Asia.
www.cc-link.org

CC-Link Partner Association-Europe
Email: Partners@CLPA-Europe.com
Phone: +49 2102 486 1750
www.CLPA-Europe.com

CC-Link Partner Association-Americas
Email: Info@CCLinkAmerica.org
Phone: +1 (847) 478-2647
www.CCLinkAmerica.org

CC-Link Partner Association-Japan
Email: cc-link@post0.mind.ne.jp
Phone: +81-52-919-1588
www.cc-link.org

Ethernet POWERLINK - One Network for all applications

POWERLINK is a real-time Industrial Ethernet solution designed to give users a single, consistent and integrated means for handling all communication tasks in modern automation. It is suitable for all conceivable applications in machine and plant engineering as well as for process industry applications.

A POWERLINK NETWORK INTEGRATES all of the components used in industrial automation, from PLCs, sensors and I/O modules to actuators such as inverters, motion controllers and servo inverters, as well as hydraulics, pneumatics, safety controllers, safety sensors and actuators and HMI systems.

PLC
Safety
Fieldbus
Vision System
ETHERNET
POWERLINK
Motion
I/O
Visualization
Sensors

With impressive performance characteristics including high bandwidth and fast cycle times as well as exceptional versatility, POWERLINK is perfectly suited for both centralized and decentralized automation architectures. Machines and plants with decentralized architectures give users increased flexibility for adapting and expanding, but demand a communication system that is up to the task.

free choice of topology

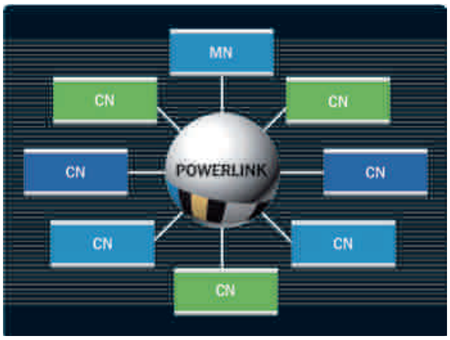
POWERLINK offers the free choice of topology that is virtually indispensable for modular system expansion. Not least due to its excellent scalability, POWERLINK allows for limitless system expansion without negative effects on the network's real-time performance. Unlike other real-time Industrial Ethernet systems, POWERLINK is a purely software-based open source solution that complies 100% with the IEEE 802.3 Ethernet standard.

By providing such close standard compliance without any proprietary hardware, POWERLINK ensures that all of the benefits and flexibility of Ethernet technology are carried over into the real-time protocol. Users are therefore able to draw on the same standardized hardware components and use the same tools for diagnostics.

Focus on pplication requirements

In order to achieve real-time capability, POWERLINK relies on a highly effective mixed polling and time-slot procedure. Unlike with standard Ethernet, no arbitration is required. In the POWERLINK communication structure, one node in the network, such as a PLC, motion controller or industrial PC, is arbitrarily designated as the managing node (MN) and serves as a "moderator of the conversation".

All other devices operate as controlled nodes (CN). The MN defines the clock pulse for the synchronization of all devices and manages the data communication cycle.



In the course of each cycle, the MN successively polls each CN. This polling is done via a poll request message (PReq), which additionally conveys data from the MN to the polled CN. In response, the CN then sends its own data to all other nodes by broadcasting a poll response message (PRes). This mechanism is what allows POWERLINK to achieve the fastest cross-communication available on the market.

PRC and multiplexing

Depending on the requirements of the application, it is possible to choose between poll response chaining (PRC) and multiplexing modes. When the cycle is run in PRC mode, the MN sends out a frame containing the output data for all CNs. The CNs respond to this signal in a time-triggered, synchronized manner and send their chained poll responses back to the MN.

In applications that contain synchronized axes and temperature sensors, for example, it is possible to multiplex the network nodes.

In short, POWERLINK offers the best performance for your application by optimally adapting to the requirements at hand.

Maximized utilization

A POWERLINK cycle consists of three periods. In the first period, the MN sends a "Start of Cycle" frame (SoC) to all CNs, which synchronizes the devices. The second period, or isochronous phase, is used for cyclic exchange of process data.

The third period of a cycle is the asynchronous phase, which allows for the transfer of data packets that are not time-critical, such as TCP/IP, FTP, HTTP, parameterization data, etc. Likewise, devices that do not belong to the immediate automation level can be included in the network environment as well, as in the case of video cameras for site surveillance and access control. Moreover, a proper gateway allows for the transmission of other, non-POWERLINK fieldbus data within the asynchronous portion of a cycle, making it possible to integrate a variety of different networks.

Prepared for future challenges

The ability to send multiple asynchronous frames per cycle (MultiASnd) helps POWERLINK guarantee best-in-class utilization of the physical network's bandwidth. Clearly, POWERLINK is well-prepared to meet any challenges posed by digitalization well into the future.

ETHERNET POWERLINK

Ethernet POWERLINK Standardization Group
Email: info@ethernet-powerlink.org
Phone: +49 33439 539270
www.ethernet-powerlink.org

Smart, secure and flexible M2M/IoT Integration Platform

As a leading supplier of embedded systems, Machine-to-Machine (M2M) platforms and Internet of Things (IoT) solutions, Eurotech delivers leading-edge M2M and Industrial IoT solutions.

EUROTECH (WWW.EUROTECH.COM) IS A global company that integrates hardware, software, services and expertise to deliver embedded computing systems, M2M Integration Platforms and IoT enabling solutions to leading OEMs, system integrators and enterprise customers for successful and efficient deployment of their products and services.

EUROTECH headquarters in Amaro, Italy

Drawing on concepts of minimalist computing, Eurotech lowers power draw, minimizes physical size and reduces coding complexity to bring embedded platforms, sub-systems and ready-to-use devices to market, specializing in transportation, industrial, security, logistics and medical industries. By combining domain expertise in wireless connectivity and communications protocols, Eurotech architects platforms that simplify data capture, processing and transfer over unified communications networks.

Everyware Device Cloud

Eurotech's offer is built on Everyware Device Cloud (EDC). This end-to-end IoT solution includes purpose-built hardware, connectivity and embedded device management through the Everyware Software Framework (ESF), the EDC Client and the Everyware Cloud (EC) platform of M2M cloud-based services.

It enables customers to deliver actionable data from the field to downstream applications and business processes, dashboards, reports and sophisticated data analysis.

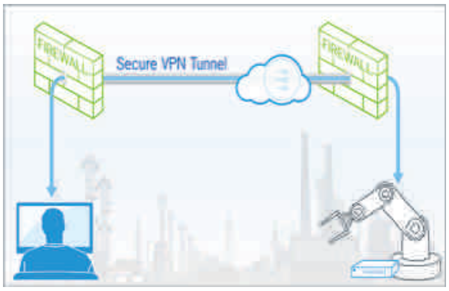
Quickly develop IoT applications

ESF is an inclusive and targeted Java OSGi software framework for M2M multiservice gateways and smart devices, which allows Eurotech and its customers to deliver latest generation pervasive/embedded computer hardware platforms, and all the fundamental components needed to quickly develop IoT applications.

ESF acts as the bridge between the private device network and the local network, public Internet, or cellular network.

M2M Integration Platform

EC is an M2M Integration Platform that simplifies device and data management by connecting distributed devices over secure and reliable cloud services.



Secure connection between remote devices and your PC, tablet or smartphone.

Once devices are deployed, EC allows users to connect, configure and manage devices through the lifecycle, from deployment through maintenance to retirement.

Secure data exchange

To connect remote devices within secure networks, Eurotech has developed Everyware VPN, a software agent that creates a secure connection between remote devices and your PC, tablet or smartphone.

It is the ideal solution for all those applications where firewalls block access to the devices, such as remote support, data collection and device administration. No special requirements are needed to access the remote device: simply run an OpenVPN client to reach the remote device and access rights are managed from a secure portal running in the cloud.

EUROTECH

EUROTECH S.p.A.
Email: sales.it@eurotech.com
Phone: +39 0433 485411
www.eurotech.com

Festo: Significantly increasing productivity

Automation technology in the 21st century offers perfection in speed, precision and quality – and is flexible, smart and intuitive too. In addition to pneumatic automation technology, applications with electric automation technology, and above all those featuring customer-specific combinations of the two technologies, are bringing the automation of the future into new dimensions of productivity.

Setting your sights high?
Want to achieve more?
We show you new ways forward.
→ WE ARE THE ENGINEERS OF PRODUCTIVITY.
21st century factory automation: Festo CPX.
An automation platform for excellent productivity

FESTO RESEARCH PROJECTS, SUCH AS the Bionic Learning Network, Industry 4.0, or the industrial use of superconductors, will allow completely new applications for the contactless transport of workpieces within self-learning, self-adapting and totally flexible systems.

Let's point out three enablers of productivity increase:

1. IE and Industry 4.0

Even today, Festo is a market leader in networked and intelligent components and system solutions which make it an enabler of productivity. Only with sophisticated automation solutions will it be possible to meet the challenges of the future such as the desire for individualised and personalised products, the diversification and atomisation of markets, rising energy costs and the enormous pressure on costs resulting from globalisation and continuous technological change.

As a global player, Festo supports various Industrial Ethernet protocols as well as the established fieldbus protocols. But we hope to see a more harmonised standard as part of the Industry 4.0 discussion and standardisation processes, like the OPC-UA definition.

2. Electric automation

Festo is constantly making life easier for users with regard to electric automation. In addition to pneumatics, Festo is also continuously expanding its portfolio of electric axes, motors and controllers. Software allows electric actuators to be configured quickly and easily.

Festo's automation platform CPX provides a simple means of networking several levels of the automation pyramid.

Customers' design engineers can draw on the extensive Festo product portfolio, including mechanical drive components, motors, axis controllers and firmware, as well as diagnostic and operating equipment for motion control systems or their PLC.

There is a wide range of toothed belts, spindles, recirculating ball bearing guides and linear motor axes available in the case of electric drives. Everything comes from a single source and is perfectly coordinated. This means there are no interface problems.

3. Ready-to-install robotics

In recent years, Festo has surprised the automation market with groundbreaking ready-to-install innovations for handling and assembly operations based on electric drive technology. This include the delta robot EXPT, the high-speed H-gantry EXCH, the high-speed T-gantry EXCT and the mini H-gantry EXCM.

A common feature of all of Festo's ready-to-install handling solutions is their highly dynamic operation thanks to low moving masses, and the fact that the solutions are built using standard Festo components.

All standard handling systems can be easily configured and ordered by customers (even without in-depth design knowledge) with the latest innovation called "Handling-Guide-Online"– including IE integration later on.

Festo AG & Co. KG
Email: info_de@festo.com
Phone: +49 711 347-0
www.festo.de

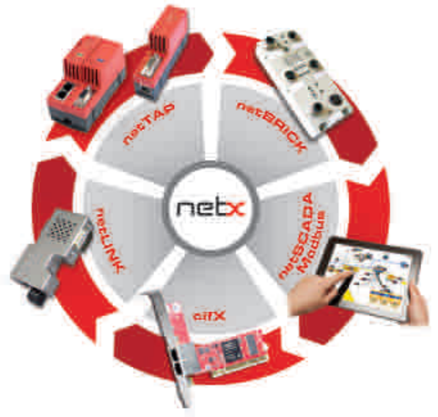
Got Networks? Think Hilscher

Hilscher is your one-stop solutions provider for industrial communications. Our gateways, chips and embedded solutions provide multi-protocol support to end-users and device manufacturers.

IN THE PAST THREE DECADES, multiple generations of networking technologies have been adopted in the marketplace.

As a result, most plants have a variety of industrial protocols in their manufacturing systems that need to be inter-connected.

Hilscher, a leading global specialist in network connectivity, provides solutions to bridge these various networks together.



Hilscher's networking solutions for end-user customers include gateways, PC cards and visualization platforms, all built on Hilscher's highly flexible netX technology.

Multiple protocol support

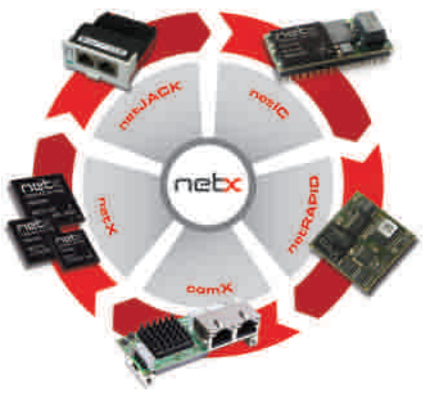
At the heart of the Hilscher product portfolio is the netX system-on-a-chip, a highly integrated network controller that can support multiple communication protocols simultaneously.

Optimized for maximum data throughput, the netX chip provides the universal connection to all popular communication protocols. These include traditional fieldbuses (ASinterface, CANopen, DeviceNet, PROFIBUS, SERCOS, Modbus and CC-Link) and the latest generation of industrial Ethernet technologies (EtherNet/IP, PROFINET, EtherCAT, Modbus TCP and POWERLINK).

Custom serial protocols can be easily written using the Hilscher netSCRIPT scripting tool.

Products support end-users and OEMs

Built on the netX core technology are Hilscher's communications products for end-users and OEMs. The product portfolio includes gateways, PC cards, embedded modules, chips, controllers and supporting software stacks.



Core products for OEMs and device manufacturers include chips, embedded modules, controllers and supporting software stacks that implement all proven fieldbus and Real-time Ethernet systems.

Convert data between networks

For end-users, Hilscher's gateway products, such as the netTAP, netBRICK and netLINK families, are self-contained protocol converters with simple plug-in connections to connect and convert data from one network to another.

The netTAP and IP67-rated netBRICK gateways have Master and/or Slave configurations.

The netLINK Proxy allows any PROFIBUS DP Slave to be easily integrated into a PROFINET network. For PC-based applications, the cifX family includes Master/Slave cards in various configurations (PCI, Compact PCI, PC/104 and others) that use a common dual port memory so a single driver works with all form factors.

Visualization and monitoring

Hilscher's netSCADA solutions add low-cost visualization and monitoring to your networks. Point-and-click tools create visualization screens that can be viewed on any web browser-enabled platform, such as smart phones and tablets. Our netSCADA solutions support Modbus, Modbus TCP, PROFIBUS, MPI and PROFINET applications.

For OEMs and device manufacturers, Hilscher offers a wide variety of netX chip and embedded products.

The netRAPID is a stamp-sized network coprocessor that speeds custom development and integration of netX solutions. The netJACK module is designed to quickly and easily add or change fieldbus and Ethernet protocols in an automation device.

Custom solutions

Hilscher also offers extensive engineering services to develop custom solutions tailored to your exact specifications. Contact Hilscher for more information on how we can support your application.

hilscher
COMPETENCE IN
COMMUNICATION

Hilscher North America
Email: info@hilscher.us
Phone: +1 630 505 5301
www.na.hilscher.com

MECHATROLINK Members Association

The MECHATROLINK Members Association (MMA) is a group of product developers and users who promote the use of the MECHATROLINK motion field network. All members support the construction and promotion of a larger MECHATROLINK family.

MECHATROLINK IS AN OPEN FIELD network that connects a controller with a variety of devices. High-speed communications and data synchronization are provided to increase system speed and provide advanced functionality.

Moreover, it uses simple cable connections to reduce wiring, downsize the system, and enable easy system expansion. Because it is an open network, there are many different MECHATROLINK compatible devices available on the market that can be flexibly combined to suit your application.

You can also freely develop your own master and slave devices to quickly achieve a variety of mechanical operations simply and at a low cost.

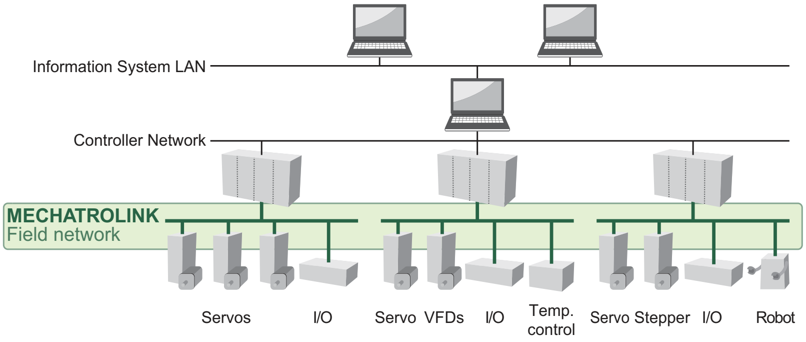
In August, 2014, MECHATROLINK obtained IEC Certification.

MECHATROLINK Applications

MECHATROLINK has been used in diverse applications, such as those for machine tools, industrial robots, machines for mounting electronic parts and machines for transferring. It is especially suitable for synchronous and interpolated motion control. MECHATROLINK enables control of torque, positioning, and velocity, all of which are necessary to control your machine. Also, the control modes for velocity, torque, and position can be switched while the machine is running, so you can perfectly control the machine's complex motions.

Network Reliability

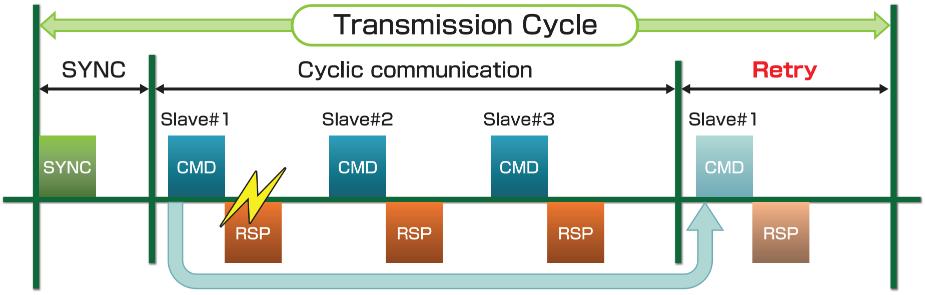
MECHATROLINK is the only field network that utilizes a "data retry" function processed and executed by the communications chip.



Positioning of MECHATROLINK

MECHATROLINK is positioned as a Field Network. A Field Network is a network that drives control elements of control system such as I/Os and actuators, and allows devices for input control information to be connected.

The communication chip resends data that has become corrupted by noise, within the same communication cycle. This results in the communications having a strong resistance to noise. Since this "data retry" function is processed and executed by the communications chip, application-sided code is not necessary to take advantage of this feature.



Membership

MMA has grown to over 2300 members globally and membership is free of charge.

Join MMA as a Registered Member today to download the communication specification and access all the technical materials at www.mechatrolink.org

MECHATROLINK Members Association
Email: mma@mechatrolink.org
Phone: +81-4-2962-7920
www.mechatrolink.org
Regional Offices
MMA Germany
Email: mma@mechatrolink.de
Phone: +49-6196-569420
MMA Korea
Email: mma-kr@mechatrolink.org
Phone: +82-2-368-8875
MMA China - Shanghai
Email: mma-sh@mechatrolink.org
Phone: +86-21-53852070
MMA China - Shenyang
Email: mma-cn@mechatrolink.org
Phone: +86-24-24966008
MMA USA
Email: mma-us@mechatrolink.org
Phone: +1-847-887-7231
MMA Taiwan
Email: mma-tw@mechatrolink.org
Phone: +886-2-8913-1778
MMA India
Email: mma-in@mechatrolink.org
Phone: +91-80-4244-1920

Perfection often evolves out of sight.

Moxa was founded in 1987. Since then, we have constantly expanded - both geographically and technologically – and today we are one of the leading global manufacturers of industrial networking technology.

OUR INTERNATIONAL CLIENTS READ like a "Who's Who" of the transport, energy, production, shipping, as well as oil and gas industries. On both the technical and the entrepreneurial front we embrace the philosophy of reliability and sincerity.

"Reliable Networks. Sincere Service" is thus simultaneously the approach we take and the aim of our endeavours.

Moxa Europe

Since the foundation of our Moxa Europe headquarters in Unterschleißheim near Munich, Germany, in 2007, we have been growing steadily both in terms of resources and revenue.

Today, we have about 50 experts in 3 different locations, and the European success story is reflected in our year-on-year double-digit growth.

Shaping the future now

Moxa has always been a forerunner in industrial networking and computing. In close cooperation with our customers and partners we are shaping the future of industrial automation day by day. This includes the further development of current industry topics like "Industrie 4.0", "Big Data", "Industrial Internet of Things", and "Industrial Cloud".

Therefore, we are member of the relevant industry committees and associations, such as IEEE, CIRM, Cigré, or the Industrial Internet Consortium.

Thus, we ensure that we create innovative products which guarantee that our European customers and partners receive the right products and solutions for their specific requirements.

Experts in the IIoT and Industrial Cloud Computing

Moxa offers proven solutions that allow customers to take advantage of the Industrial Internet of Things (IIoT) for industrial applications. Our solutions help to ease device connectivity and network deployment, leaving customers to focus resources on infrastructure design and software development.

DA-820: Rugged cloud server for distributed, high-availability cloud applications

Rugged Cloud Servers

An essential ingredient for cloud connectivity is high computing performance. Moxa's DA-820 series delivers superior processing power with reliability and efficiency that meet the demands of distributed, high-availability cloud applications in any harsh environment.

Edge Gateways and Devices

UC-8100: Cloud gateway designed for big data computing applications

Moxa's UC-8100 RISC computer is a cloud gateway designed for big data computing applications.

Its versatile communication capabilities let users efficiently adapt the UC-8100 to a variety of complex communication and processing solutions.

The flexibility of the UC-8100 facilitates the development and deployment of custom applications, making it ideal for distributed peer-to-peer (mesh) wireless communications. This frees the edge of the network from the constraints of wired connections for greater mobility and intelligence.

MXcloud: M2M Connectivity Services

MXcloud is a cloud connectivity solution that uses a highly secure, asynchronous architecture to automate management, monitoring, and data acquisition on edge devices in the field.

The open platform allows users to build complex, customized edge applications for private, personalized networks.

MOXA®
Reliable Networks ▲ Sincere Service

Moxa
Email: europe@moxa.com
Phone: +49-89-37003-99-0
www.moxa.com

We started by revolutionizing the design of a cable.

We evolved to change the way the world communicates. Founded in 1983, OCC was among the first companies to offer some of the most reliable, rugged and innovative cable products in the world. Our engineers were at the forefront of the development of the tight-buffered, tight-bound cable technology that met the stringent standards of the U.S. Military.

OUR SUCCESS IN THE battlefield was the foundation for our broad fiber optic cable offering. Today, OCC has evolved into a world-class provider of a complete line of fiber optic and copper cabling and connectivity. While our heritage started with the military, our expertise now extends into the enterprise, broadcast, industrial, harsh environment and various specialty markets, and reaches worldwide through our network of distributors with customers in more than 70 countries.

Helping the world communicate faster

Today OCC products are at work from mission critical data center applications to broadcast cables transmitting on location; consistently meeting the demanding survivability standards for the toughest environmental stresses. From extreme temperatures to dust, chemicals, and vibration - even in mining applications where installations stretch for miles - OCC products are relied upon time and time again for successful environmental and safety monitoring; equipment control; security; and voice, data and video communications.

We are proud that our products provide the conduit that helps businesses, government, and the military communicate with speed and clarity.

MIL-STD-790F certified

OCC is headquartered in Roanoke, Virginia, and each of our three manufacturing facilities is located in the U.S. OCC's quality management system and manufacturing facilities in Roanoke, Asheville, and Dallas are ISO 9001:2008 registered, and our Roanoke and Dallas facilities are certified by the U.S. Department of Defense as MIL-STD-790F, a reflection of strict compliance with government requirements.

It's a new world. OCC is helping keep it connected.

The future holds new opportunities, and efficient communication will play a critical role in realizing the promise of a world where connections are instantaneous, communication is clearer and people are more connected. And OCC will be there.

OCC continues to drive standards for emerging technology such as 10GbE over copper connectivity and cabling, Category 6a cabling standards and Extended Power over Ethernet. Our dedication to designing exceptional fiber optic and copper cable and connectivity components keeps us at the forefront of the telecommunication industry.

Gigabit Ethernet, 10 Gigabit Ethernet and emerging technologies, like 40/100 Gigabit Ethernet are placing new stresses on communications systems and presenting new challenges to our industry. OCC is making the most of these opportunities with one of the industry's widest array of structured communications product and solutions.

We pledge to stay at the forefront of innovation- keeping pace with the growing demands of an increasingly connected world.

OCC®
OPTICAL CABLE CORPORATION

OCC
Email: marketinginfo@occfiber.com
Phone: +1 800 622 7711
www.occfiber.com

Opto 22 makes automation simple

Founded in 1974 by engineers who designed a better solid-state relay, Opto 22 has designed and built reliable SSRs, controllers, automation software, and I/O systems for over 40 years. As a vertically integrated company with a flat organizational structure, we can respond quickly to customers' needs and develop cutting-edge products fast.

BASED ON OPEN STANDARDS and four decades of experience in automation, all Opto 22 products are manufactured and supported in the U.S.A. and available worldwide. We individually test our products before we ship them to you. That's why we can afford to guarantee most SSRs and I/O modules for life.

Meet *groov*: Your system on your mobile™

groov is all you need to build effective operator interfaces for your system and securely view them from virtually any mobile device, anywhere.

Mobility. What would you like to be able to see or control from your smartphone? Machine status? Factory production? Energy usage? Facility security? Key performance indicators?

Now you can. Your *groov* interface works on virtually any authorized, web-enabled device regardless of manufacturer or screen size: smartphones, tablets, and more. Gauges, buttons, labels, even live video all scale to match the device you're using, but never become too small to use.

Simplicity. With *groov*, all you need to build interfaces is a web browser. No plugins; no extra software. And there's no coding or programming.

Just drag and drop touchscreen-ready indicators and controls onto the screen, then tag them. Your interface includes only what you need. Interface updates are simple, too. No user or device keys; no reinstallations. Just have users refresh their screens.

Connectivity. What equipment do you have: Modbus/TCP devices, Allen-Bradley systems, Siemens, Yokogawa, ABB? With *groov*, you can build mobile interfaces to all of these and many more.

Mix equipment from different manufacturers in the same interface if you want. Your authorized users can securely monitor and control equipment from anywhere.

Get your *groov* free trial today. Find out more at groov.com.

SNAP PAC System: Automation simplified

It can be confusing to choose and apply an automation system. Opto 22's SNAP PAC System simplifies the process. Four flexible components—software, controllers, brains, and I/O—form a system that can handle any application from basic equipment monitoring to complete factory automation.

Grows with you. With distributed intelligence, it's easy to add I/O where you need it. The modular SNAP PAC System is well suited for process control, discrete automation, energy management, data acquisition, and remote monitoring.

Plays well with others. SNAP PAC controllers and brains include built-in support for OPC, Modbus®/TCP, and EtherNet/IP™. Free integration kits connect with building automation, utilities, and telecommunications protocols.

Lower costs. The SNAP PAC System costs less than many single-purpose PLC systems, and software is included with your controller purchase. With FREE product support and free training, lifetime costs are significantly lower.

Learn more at http://op22.co/pacchecklist

OPTO 22
Automation made simple.

Opto 22
Email: systemseng@opto22.com
Phone: +1 800 321 6786
www.opto22.com

Phoenix Contact: Automation for the future

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

TODAY, THE FAMILY-OWNED COMPANY employs 14,000 people worldwide and had a turnover of 1.77 billion euros in 2014. The corporate headquarters is located in Blomberg in North Rhine-Westphalia. The Phoenix Contact Group has ten companies as well as 50 sales subsidiaries. In addition, the worldwide presence is consolidated by 30 representations in Europe and Overseas.

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

Wide product range

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

Electronic interfaces and power supplies, automation systems on the basis of Ethernet and Wireless, safety solutions for man, machine and data, surge protection systems as well as software programs and tools provide installers and operators of systems as well as device manufacturers with comprehensive systems. The automotive, renewable energy and infrastructure markets are supported with holistic solution concepts including engineering and training services and further service features according to their specific demands.

Product innovations and specific solutions for individual customer requests are developed at the locations in Germany, China and the United States. Numerous patents underline the fact that many developments from Phoenix Contact are unique in their own. In close cooperation with universities and science, future technologies like e-mobility and environmental technologies are explored and integrated into products, systems and solutions for the market.

Ethernet switches in 19" rack format

In addition to the broad portfolio of products for Industrial Ethernet communication in DIN rail mounting technology Phoenix Contact now offers new rugged managed switches for deployment in 19" racks as used in control centers and data centers. In the past, these types of systems frequently relied on devices designed for office environments, which made them of limited use in industrial applications. The new switches offer all the advantages of Industrial Ethernet in a suitable 19" rack format. They are designed for extreme electromechanical and climatic conditions and fully comply with the IEC 61850-3 and IEEE 1613 requirements for deployment in energy systems. The switches provide fanless operation and can handle a wide temperature range extending from -40 °C to 70 °C. This ensures ongoing availability even when the heating or air conditioning system fails. Redundant power supplies offer additional system stability and permit maintenance and replacement during live operation. Despite a high port count of 28 Ethernet ports, the units only take up one rack unit in the switching cabinet. Depending on requirements, the switches are available with copper or fiber-optic ports.

Infrastructure components

In addition to managed switches, Phoenix Contact offers a wide range of infrastructure components for 19" racks in control systems and data centers. These include solutions for structured cabling, network security, power supply, and surge protection. Using a special adapter, compact industrial devices designed for DIN rail mounting can be easily installed in 19" racks.

PHŒNIX CONTACT

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

Red Lion Controls: Connect. Monitor. Control.

As the global experts in communication, monitoring and control for industrial automation and networking, Red Lion has been delivering innovative solutions for more than forty years. Our award-winning technology enables companies worldwide to gain real-time data visibility.

RED LION'S INDUSTRIAL networking products include:

- **Unmanaged Switches:** compact IEEE 802.3 Layer 2 industrial switches with automatic speed, duplex and cable sensing
- **Monitored Switches:** Layer 2 unmanaged industrial switches provide network performance monitoring via N-View software
- **Managed Switches:** Layer 2 and Layer 3 Ethernet switches provide enterprise-class networking in a rugged package
- **PoE Solutions:** designed to transmit power and/or data over an Ethernet network
- **Wi-Fi Radios:** IEEE802.11a,b,g,n hardened radios support data bandwidths up to 300 Mb/s
- **Cellular M2M Routers:** provide uninterrupted, secure communication for remote sites

We also offer the following industrial automation offerings to collect, present and process data:

- **Controllers:** a broad line of PID controllers, signal conditioners and data acquisition devices for machine and process control
- **Protocol Conversion:** extensive protocol library connects otherwise incompatible devices on wired or wireless networks
- **HMIs:** seamlessly combine protocol conversion, data logging and web server capabilities with visualization functionality for PLCs, motor drives and other communications-capable devices
- **Panel Meters:** a wide range of models and sizes with expansion capabilities that easily adapt to changing requirements
- **Visual Management:** enables the display of real-time KPI data and Andon messages on large televisions to drive productivity
- **RTUs & I/O Modules:** provide a simple yet powerful monitoring and control system for remote sites

Connect, monitor and control

Together our industrial automation and networking solutions provide critical information and controls to improve productivity, working with numerous devices and diverse protocols to access data. The end result helps organizations connect, monitor and control operations.

The global experts

With headquarters in York, Pennsylvania, the company has offices across the Americas, Asia-Pacific and Europe. Red Lion is part of Spectris plc, the productivity-enhancing instrumentation and controls company.

red lion®

Red Lion Controls
Email: info@redlion.net
Headquarters: +1 717 767 6511
EMEA: +31 33 4723 225
www.redlion.net

Dependable Communications for Critical Infrastructure

Schweitzer Engineering Laboratories, Inc. (SEL), is a recognized world leader in electrical protection, communications, monitoring, cybersecurity, automation, and control solutions for mission-critical utility and industrial applications. Founded in 1982 in Pullman, Washington, by Edmund O. Schweitzer, III, SEL revolutionized the power protection industry.

SCHWEITZER INVENTED THE world's first digital relay, which provides fault locating and real fault data at a much lower cost to the customer than traditional electromechanical relays. Today, SEL delivers products, services, and solutions to both utility and industrial customers. Our communications and networking products support instrumentation and control operations in a wide variety of industries, such as gas, water and wastewater, oil and petrochemical, and information technology.

SEL strives to exceed customer expectations in all aspects of product and service design, manufacture, and delivery. Our robust design practices build quality into our products from the moment they are conceived. We select the best components, design for simplicity and wide-operating margin, and perform qualification tests to meet or exceed national and international performance standards. Through our relentless focus on customer expectations and continuous improvement, SEL achieves ever-improving levels of quality, delivery, and service.

SEL understands the importance of local support, which is why we have application and integration engineers, customer service representatives and sales managers in more than 55 offices in the United States and 45 offices internationally.

Industries like oil and gas, mining, and pulp and paper depend on SEL products to control and monitor power, minimize downtime, and provide a steady, reliable flow of electricity.

ISO 9001 Quality Management

SEL's Quality Management System is certified to the International Organization for Standardization (ISO) 9001:2008 American National Standard for Quality Management Systems. This certification provides evidence that our critical design, manufacturing, and business processes meet the exacting requirements of this internationally recognized ISO program. Likewise, our manufacturing processes comply with workmanship standard IPC-A-610 Class 3 for products requiring high reliability, such as those used in life-support and aerospace systems. SEL's approach to quality includes the following key differentiators:

- Twenty-five-year product design life
- Ten-year, worldwide, no-questions-asked warranty
- Technical support included in purchase price; no support contracts required
- SEL ownership of the complete design, testing, and manufacturing process

The SEL ten-year, worldwide product warranty is proof of the confidence we have in the quality of the products we manufacture while following the strictest industry standards. This commitment extends throughout a product's installation and life as part of our customers' critical infrastructure. SEL consistently strives to find new ways to make our products more reliable, reduce early product replacement, and eliminate waste. To ensure superior, reliable functionality, we test our products thoroughly and verify that they will perform under demanding conditions for decades. Customers rank SEL's personalized service and ongoing technical support as the best in the industry. Our engineers have the field experience and expertise to create application-specific solutions for a variety of electric power systems. With application and integration engineers, customer service representatives, and sales managers in over 55 offices in the United States and more than 45 internationally, SEL truly understands the importance of local support.

Innovative SEL communications technology enables customers to monitor, control, and automate the operation of power systems.

For complete information on SEL communications equipment, visit www.selinc.com/3ieb.

SEL® SCHWEITZER ENGINEERING LABORATORIES

Schweitzer Engineering Laboratories
Email: info@selinc.com
Phone: +1 509 332 1890
www.selinc.com

More Efficiency Based on Proven Standards

Setting trends, opening up new areas, breaking down barriers – industrial communication is the basis for automation today and in the future. Siemens is the specialist for small, medium and large industrial network infrastructures.

SIEMENS OFFERS A WIDE RANGE of services and products for this purpose, enabling comprehensive and innovative solutions to meet your individual requirements.

Developing field-proven technology even further, breaking new ground, and opening up new media for industrial communications.

Setting trends

Today Siemens fully relies on Industrial Ethernet and PROFINET, the open Industrial Ethernet Standard of PROFIBUS & PROFINET International (PI), with about 10 million installed nodes in the field already today. This is demonstrated by Siemens by means of a comprehensive range of products for PROFINET such as automation systems, drive systems, identification systems , and network components such as Industrial Ethernet Switches, Industrial modems and routers, Industrial Security Modules as well as Industrial Wireless LAN (IWLAN) Access Points.

With IWLAN from Siemens based on PROFINET (PROFIsafe) wireless communication also can be realized for safety applications.

Future proof network designs

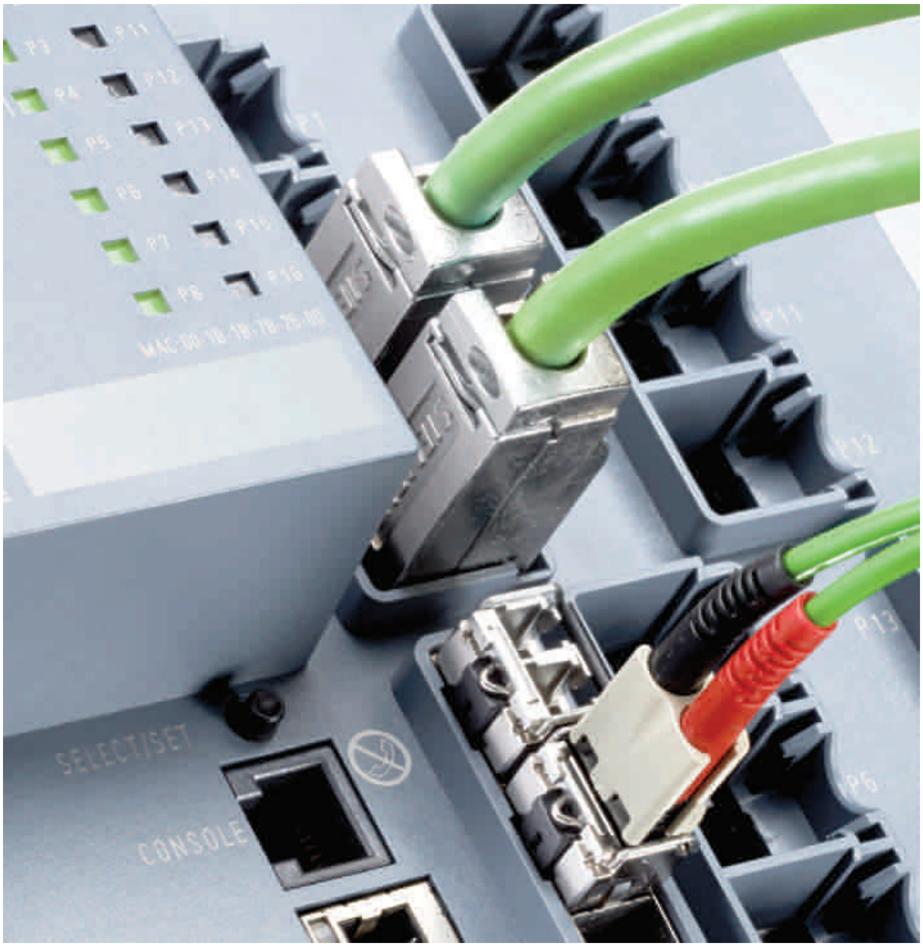
Siemens designs industrial network structures to master both today's challenges and future customer requirements. Data networks for rough environments, high availability and redundancy, connectivity to existing office IT are Siemens' daily business.

Breaking down barriers

Industrial Wireless LAN (IWLAN) replaces obsolete communication paths via contact conductors or tow chains and permits applications such as mobile operation with integrated emergency stop functionality. Experience with Industrial Wireless LAN devices has shown that time critical, cyclical communication is possible. Even safety signals can be exchanged wirelessly.

Integrated communication

Industrial Ethernet and PROFINET permit a unique integration from the field level all the way up to the control level. For example, the SCALANCE M industry router and the SCALANCE S security modules permit secure access to a plant network via mobile radio and the internet.



The plant's Industrial Ethernet is connected by means of SCALANCE X switches and thus permits access to controllers and PROFINET field devices, for example via web servers. Specific tools for servicing and diagnostics e.g. Sinema Server complement the portfolio.

Rugged Communications

With RUGGEDCOM, Siemens has enhanced its portfolio of network components for Industrial Ethernet with solutions for mission-critical applications even in the harshest environments. The highly specialized, robust RUGGEDCOM switches fully comply with both IEC 61850-3 and IEEE 1613. They meet thetoughest EMC, shock and vibration resistance standards, while operating at a temperature range from -40°C to +85°C. RUGGEDCOM WIN series of products is the first broadband wireless product portfolio designed for private networks, delivering the benefits of carrier-grade 4G technology to critical infrastructure applications in harsh environments.

SIEMENS

SIEMENS AG
Phone: +49 911 895-0
www.siemens.com/industrial-communication

Maximize Availability Without Compromising Safety

TTTech is delivering products and technologies to maximize the availability of industrial control systems and do so without compromising system safety. System availability is vital as process control, safety systems and security capabilities become more integrated, and TTTech's offering is now extended to distributed control systems in autonomous driving vehicles and open IoT infrastructures.

Industrial Safety and High Availability

TTTECH'S CHRONOS INDUSTRIAL 24 port switch is designed to address a key concern of industrial customers: safety and availability of systems. By utilizing industry-proven components and architectures, the Chronos switch provides fail-operational performance which guarantees safe communication whilst maximizing system uptime.

In addition, the switch is developed according to IEC 61508 SIL 2 standards, which can significantly reduce the time and cost of system certification for the integrator or end-user. The switch offers Deterministic Ethernet connectivity, which includes the IEEE 802.3 and 802.1Q standards, rate-constrained mechanisms and time-triggered scheduling for synchronous communication.

Guarantee of Service for IoT

The IoT product portfolio from TTTech includes the core elements required for integrating critical control systems in open IoT infrastructures. TTTech's industrial IoT switches can be used to converge all controls, streaming and data traffic over a Deterministic Ethernet network and support the upcoming time-sensitive networking (TSN) enhancements to the IEEE 802.1 standard. This convergence also include existing Industrial Ethernet protocols which can share the network infrastructure, and also benefit from the Guarantee of Service enabled by Deterministic Ethernet. Guarantees for traffic delivery in open systems can be extended to endpoint devices by using a standard PCIe card from TTTech with Deterministic Ethernet capability.

Enabling Autonomous Driving

With TTTech's Advanced Driver Assistance System (ADAS), car makers are now able to integrate multiple driver assistance functions onto a single platform ECU. This is especially useful for Autonomous Driving applications where a huge amount of video, sensor and control data is now being generated.

The ADAS enables central diagnosis of all systems and has a scalable architecture with flexibility to grow as systems become more complex. The use of Deterministic Ethernet in ADAS allows seamless integration of functions and co-simulation on PCs.

Automotive Ethernet

TTTech is delivering its Deterministic Ethernet switch IP supporting AVB and TSN for automotive networking solutions.

One example of this is the NXP manufactured switch chip which is specifically designed for the automotive market, but will also be suitable for various demanding industrial real-time applications. It is the first Ethernet switch chip with three incorporated traffic classes including standard Ethernet traffic for diagnostics and ECU flashing, asynchronous rate-constrained traffic for audio/video streaming and sensor fusion, as well as synchronous traffic for hard real-time control and fail-operational systems.

Hence, this new automotive switch chip will enable unified Ethernet networks and the convergence of critical and non-critical application data streams in vehicles.

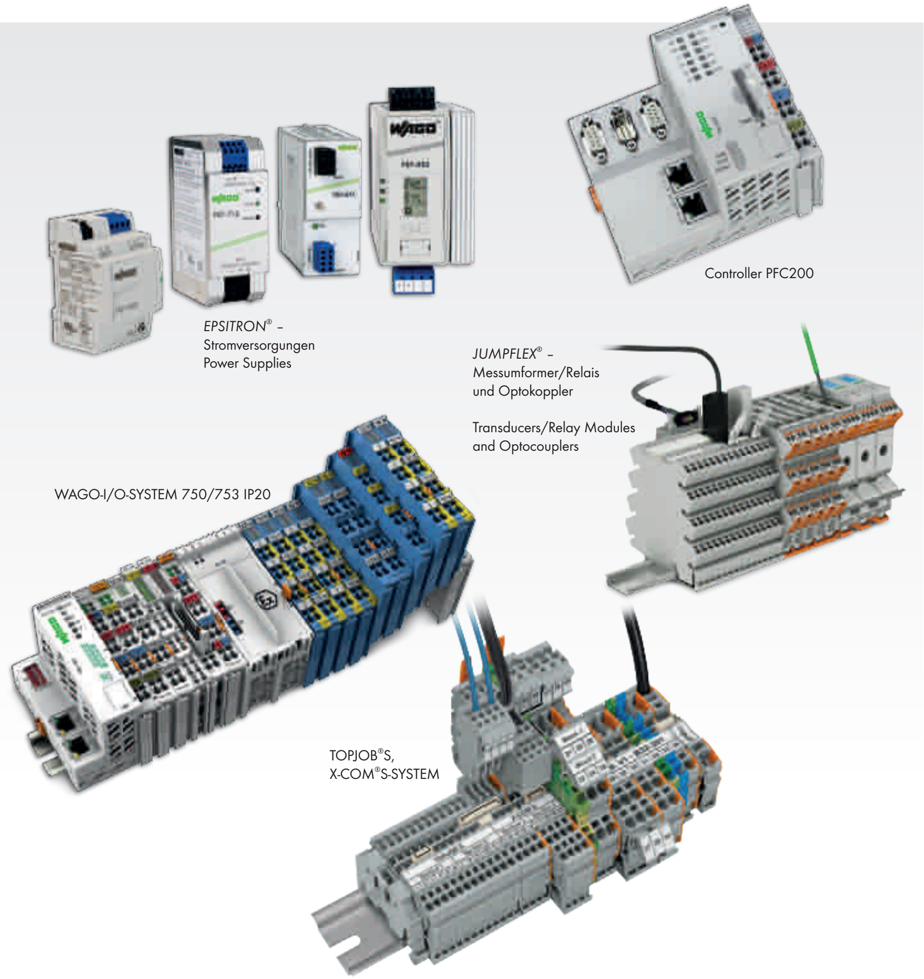
Ensuring Reliable Networks TTTech

TTTech Computertechnik AG
Email: office@tttech.com
Phone: +43 1 585 34 34-0
www.tttech.com

WAGO: Innovations that make industry safer and more efficient

Founded in 1951, WAGO Kontakttechnik GmbH & Co. KG changed the way electrical connections are made with the invention of Spring Pressure Connection Technology. Headquartered in Minden (Westphalia), Germany, WAGO leads the industry with innovations that make industry safer and more efficient.

IN 1995, FOR EXAMPLE, WAGO became one of the world's premier automation suppliers with the introduction of the first modular, fieldbus-independent control system. WAGO products are used in more than 30 countries for a wide range of applications (e.g., power and process technology, building automation, machinery and equipment, as well as industrial and transportation applications). As of December 31, 2013, the WAGO group employs ca. 6,300 people internationally and has an annual turnover of €606 million.



Simple, but revolutionary

WAGO's success story began with the simple, but revolutionary spring clamp. Known worldwide as CAGE CLAMP®, this innovation is renowned for user-friendly operation and ability to reliably provide a gas-tight connection between conductor and current bar. Because the clamping force automatically adjusts to the conductor size, it is absolutely maintenance-free. In contrast to screw-type connections, connection quality is virtually independent of operator skill, while providing faster operation.

Today, WAGO offers the broadest range of spring pressure termination products thanks to continuous innovations and advancements in Spring Pressure Connection Technology used in new products. Both well-known products and all-new innovations featuring this technology include: 273 Series PUSH WIRE® connectors for junction boxes and 2273 Series, TOPJOB® S, X-COM®-SYSTEM and *WINSTA®* connectors for building installations.

Distributed control systems

The beginning of the 1990s signaled a shift from centralized to distributed control systems. In 1995, WAGO launched the WAGO-I/O-SYSTEM 750 — a completely new, finely modular control solution.

The open and flexible architecture of the WAGO-I/O-SYSTEM laid the foundation for further innovation in automation. Recent examples include: DALI or IO-Link Master modules, KNX and BACnet controllers, 16-channel modules or safety modules for monitoring and controlling safety functions.

WAGO's modular *SPEEDWAY 767* system was introduced in 2006 for in-the-field control applications. With its IP67-rated housing, it is ideal for fast process control or cabinet-free automation in harsh industrial environments.

WAGO's range of interface modules includes a wide variety of relays and transducers. The newest addition to the line is the *EPSITRON®* family of power supplies, which features a diverse range of power ratings.

WAGO Kontakttechnik GmbH & Co. KG
Email: info@wago.com
Phone: +49 571 887 0
www.wago.com

Smart Sensing: Intelligence at the Network Edge

Machines have been talking to machines for decades, but IoT technology is transforming the conversation. In traditional SCADA applications, sensors were passive devices that steadily transmitted all of their data, whether that data had value or not. In many cases, they could only report to PLCs or HMIs.

IOT TECH, LIKE THE Wzzard™ Intelligent Sensing Platform, can turn virtually any device into a node on a modern network. The platform also makes networks faster and more efficient by bringing decision making out to the network edge.

The Wzzard platform creates a complete connectivity stack between remote sensors and applications at the network core or in the cloud. It begins with Wzzard Intelligent Edge Nodes, which connect to industry standard sensors providing them with wireless connections across resilient, reliable mesh networks.

The nodes can be configured to report data only when specified parameters are exceeded, reducing network traffic. They use a publish/subscribe protocol to ensure that data is only transmitted to the appropriate applications. And, because every Wzzard Intelligent Edge Node has routing functionality, individual nodes need not be within range of the network gateway. They can communicate with the gateway via fellow nodes, making Wzzard mesh networks incredibly scalable. The Wzzard Network Gateway then provides secure Ethernet connections via either wired infrastructure or cellular data networks, extending the network edge to include any location that has cellular service.

Together, the Wzzard nodes and the Wzzard network gateway provide IoT connectivity for virtually any sensor, in virtually any industry.

B+B SMARTWORX®

B+B SmartWorx
Email: orders@bb-elec.com
Phone: +1 (800) 346-3119
www.bb-smartsensing.com

DINSpace: Patch Panels for Industry

Ethernet has won. Fiber optic and CAT5/CAT6 cabling can now be found in almost every industrial automation environment on the planet. Keep in mind, though, that there are probably more Ethernet connections in California's office buildings than there are Industrial Ethernet end points in the world.

HENCE, MAJOR COMMERCIAL IT manufacturers have seen little need to design and market solutions for Industrial Ethernet cabling needs. Case in point: Patch Panels.

Commercial IT patch panels are generally large contraptions, designed for spacious wiring closets and racks, not tight control cabinets, and certified to comply with commercial rather than industrial electronics regulations.

DINSpace to the rescue...

DINSpace released its compact and rugged SNAP® line of patch panels in 2012 for space-constrained control cabinetry.

SNAP® patch panels feature DIN-Rail and surface mounting options, durable metal construction, and UL and CE ratings to comply with control cabinetry requirements. The product line supports ST, SC, FC, and LC connectors for fiber optic cable, and CAT5 and CAT6 shielded connectors for copper cabling. The SNAP® has been used to solve cabling termination needs in industrial environments ranging from wind farms to pipelines, refineries to water treatment facilities and intelligent traffic systems.

SNAP® patch panels have even been launched into space!

DINSpace

DINSpace
Email: sales@dinspace.com
Phone: +1- 214 613 0349
www.dinspace.com

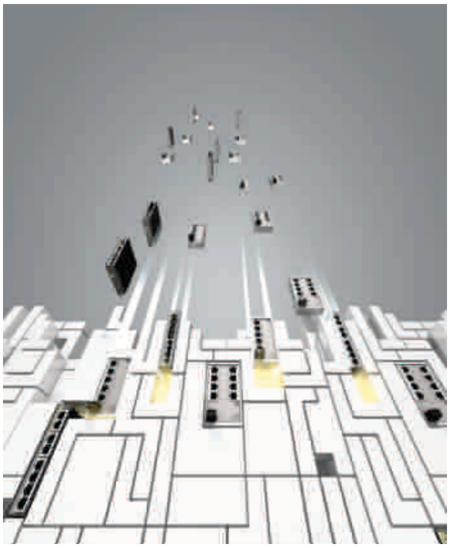
Make a Lasting Connection with HARTING USA

HARTING USA is the North American subsidiary of HARTING, a German-based global leader in the connector industry. We develop, manufacture and sell the world's most durable and reliable products and solutions for use in mechanical and plant engineering, broadcast and entertainment, factory automation, power generation and distribution as well as industrial electronics and telecommunication.

FOUNDED IN 1986 AND based in Elgin, Illinois, HARTING USA continues the proud tradition of our parent company, first established in 1945, delivering unrivaled reliability, efficiency, performance and innovation. That includes our own facility, where we manufacture circuit board technology and customized cabling solutions.

At HARTING, we are as invested in our customers as we are in our products, knowing that confidence comes from dependable connections that stand the test of time.

Although HARTING is known for our pioneering work in rectangular connections, we make the ideal shape, including circular, needed for the application. We develop solutions that are responsive to real-world issues with a record of innovation that to date has resulted in more than 915 registered designs and 318 trademarks.



Our products include electrical and electronic connectors, device terminations, backplanes, network components, as well as cable harnesses for networks and machinery, and for power and data application in factories.

HARTING®

Pushing Performance

HARTING USA
Email: stkcheck@HARTING.com
Phone: +1 (866) 278-0306
www.HARTING-usa.com

MICROSENS fiber optic solutions Innovation from conviction

Transmitting information via fiber optic connections offers numerous benefits. MICROSENS recognised this very early on. As one of the pioneers, the company has developed and produced high-performance glass fiber transmission systems in Germany since 1993.

INDIVIDUALLY MATCHED TO THE demands of diverse business fields and embedded in comprehensive concepts for individual sectors. But, above all, close to the customer.

Technical challenges from customer projects are incorporated directly into product development.

Industrial Solutions

In production, in the rail sector, in traffic control technology or in other industrial environments – network technology has long-since become indispensable in these fields too. Robust and reliable products from MICROSENS guarantee secure data transmission even under adverse conditions. Products from the Profi Line and Profi Line Modular series are the ideal solution for high availability areas like industrial automation, traffic information/control systems, energy technology, Wireless LAN and IP video surveillance. The Entry Line series from MICROSENS stands for powerful Industrial Ethernet components with a particularly compact design. It offers especially space-saving, reliable while cost-effective product solutions.

MICROSENS

MICROSENS GmbH & Co. KG
Email: info@microsens.de
Phone: +49 2381 9452 0
www.microsens.de

Smart Measurement Solutions and Smart Time Synchronization

OMICRON Lab is a division of OMICRON electronics GmbH specialized in providing Smart Measurement Solutions and Smart Time Synchronization to professionals such as scientists, engineers and teachers engaged in the field of electronics.

OMICRON LAB SIMPLIFIES measurement and time synchronization tasks and therefore provides its customers with more time to focus on their real business.

By utilizing the Precision Time Protocol (PTP) according to the IEEE 1588 standard OMICRON Lab is offering precise, cost efficient and easy-to-use time synchronization solutions to industries, where time accuracy is mission critical. Typical applications are the synchronization of protection relays and other intelligent electronic devices (IEDs) in the electrical power industry, as well as synchronization of measurement devices, computers and sensors for industrial applications.

OMICRON Lab was established in 2006 and is meanwhile serving customers in more than 50 countries. Offices in America, Europe, Asia and an international network of distributors enable fast and extraordinary customer support.

OTMC 100 – Grandmaster Clock and

TICRO 100 – IEEE 1588/PTP Time Converter

OMICRON Lab products stand for high quality offered at the best price/value ratio in the market. The products` reliability and ease of use guarantee trouble-free operation.

Close customer relationship and more than 25 years in-house experience enable the development of innovative products close to the field.

OMICRON Lab
Email: info@omicron-lab.com
Phone: +43 59495
www.omicron-lab.com

ProSoft Technology: Where Automation Connects

ProSoft Technology specializes in the development of industrial communication solutions for automation and control applications. Our focus is to provide connectivity solutions that link dissimilar automation devices as seamlessly as if they were all from the same supplier.

OUR PRODUCTS ACT AS AN interpreter so data can flow easily between machines that speak different languages. ProSoft Technology products include in-chassis interfaces for large automation suppliers' controllers such as Rockwell Automation® and Schneider Electric®, as well as stand-alone gateways and industrial wireless solutions. ProSoft Technology products can be found in nearly every industry that employs automation.

Starting with one computer chip in 1988, ProSoft Technology now has over 400 products supporting more than 60 different industrial automation languages. With 500 distributors in 52 countries and Regional Offices in Asia Pacific, Europe, the Middle East, Latin America and North America, ProSoft Technology is able to provide quality products with technical support to customers worldwide.

Brand Statement

ProSoft Technology strives to provide customer-centric communication interfaces for industrial automation. By thinking globally and acting locally we provide our customers worldwide with products and support, allowing them to produce more, and work faster and more efficiently in whatever industry they are in.

Products Sold

- In-chassis protocol interface modules, flow computers and C/C++ development modules for Rockwell Automation PLCs
- In-chassis protocol interface modules for Schneider Electric PLCs
- Stand-alone communication gateways
- Wireless industrial radios

ProSoft Technology
Phone: +1 661-716-5100
http://psft.com/A1U

New UX vision processors

Datalogic Automation: New low-consumption, high-performance Automation PC 910 systems from B&R are being incorporated into Datalogic's new UX series of vision processors.

Equipped with state-of-the-art technology like Intel's third-gen Core i-series processors and a wide range of standard video interfaces, the Automation PC 910 becomes a choice for demanding applications including high-speed, high-resolution inspection and analysis. Combined with Datalogic's IMPACT software, the system can manage up to four USB 3.0 cameras to deliver unrivalled machine vision solutions.

UX vision processors support a wide portfolio of USB 3.0 vision cameras, and can handle different camera formats and resolutions with the same vision processor. With three configurations for high-powered image processing, they can be seamlessly integrated into standard factory networks as well as secondary software packages.

PFC200 Telecontroller

WAGO: The PFC200 Telecontroller enables bidirectional communication in smart grid applications. The creation of a smart grid requires additional open-loop and closed-loop control technology, in addition to measuring applications. So-called control boxes, which are currently still in development, are meant to provide these functions in the smart grid.

The WAGO-I/O-SYSTEM 750 already provides a solution today that can be placed on Metering System 2020 control boxes in the future. Its Linux environment makes it possible to implement encryption technologies via TLS 1.2. (Transport Layer Security). This allows a TLS connection to send encrypted data to be implemented directly from the controller. Besides the security features, the platform of the PFC200 Controller also provides a fieldbus-independent transmission protocol. This enables bidirectional communication via IEC 60870/61850 or Modbus TCP, for example.

The I/O system can also be expanded with various master modules in order to serve a wide range of different bus systems.

HiLCOS 9.0 Software

Belden: Hirschmann HiLCOS version 9.0 software includes new security features and simpler deployment for industrial networks.

HiLCOS 9.0 helps ensure the highest-available wireless connection while also protecting industrial networks from malicious behavior. Many markets such as transportation (railways), power transmission and distribution, oil and gas, renewable energy, machine building and other hazardous environments, can benefit from the software's newest features.

Options include simple deployment through an Automatic Wireless Distribution System (AutoWDS) and enhanced security through a Wireless Intrusion Detection System (WIDS), Protected Management Frames (PMF), Layer 2 firewalls with stateful packet inspection and Wi-Fi Protected Access (WPA). Zero network failover due to Parallel Redundancy Protocol (PRP) is provided even in situations with high latency and traffic congestion.

Data acquisition system

Yokogawa: The SMARTDAC+ GM data acquisition system improves operational efficiency due to a modular design which facilitates the mounting and removal of modules. In addition, the SMARTDAC+ GM system supports Bluetooth wireless communications for use with handheld mobile devices.

Depending on the application, most data acquisition systems utilise a variety of modules to acquire a wide range of data. Historically, many of these systems were equipped with a base plate for the mounting of modules. Base plates are now less common, as users prefer designs that allow easy mounting and removal of modules.

The data acquisition systems in use today can be classified into two types: those that are equipped with a monitor and those that are not. In the latter case, the systems must be hooked up to a PC and operated using its screen and keyboard. To better accommodate the needs of its customers, the company developed the SMARTDAC+ GM modular data acquisition system. With modular I/O, users can scale their data acquisition system based on their process requirement, with the ability to upgrade as their needs evolve. In addition, wireless Bluetooth connection allows wireless communication with mobile devices.

Managed PoE switch

Antaira Technologies: The LMP-0600 series is a six-port industrial PoE+ managed Ethernet switch that supports a 48~55VDC high voltage power input. Each unit is designed with four 10/100Tx Fast Ethernet ports that are IEEE 8023.at/af compliant (PoE+/PoE) and have a PoE power output of up to 30W per port. There are also two 10/100Tx Fast Ethernet ports.

The dual power input designed product series provides reverse polarity, EFT, surge (2,000VDC) and ESD (6,000VDC) protection. There is also a built-in relay warning function to alert maintainers when power failures occur. This makes the units well-suited for applications requiring a high reliability, distance extension capability and harsh environment flexibility.

The product is pre-loaded with Layer 2 network management software, of which, it supports an ease of use Web Console or Telnet using a serial console with CLI configuration. All Antaira managed switches provide a redundant ring network function with RSTP and the ITU-G.8032 support, which eliminates the compatibility issue for any existing network concern.

In addition, the built-in SNMP, VLAN, IGMP, and QoS features support the network planners to increase data transmission performance within the network. An external USB 2.0 port allows users to export and save all the configuration settings.

Handheld Bluetooth Transmitter

OMEGA: The UWBT Series of Bluetooth transmitters combine the accuracy of an industrial sensor/transmitter with the convenience of smartphones and tablets.

The unit measures different sensor inputs such as thermocouple, RTD, relative humidity, and pH and transmits the data to your smart phone or tablet via wireless Bluetooth communication from the free UWBT app running on an iOS or Android smart phone/tablet.

The free app has many features including the ability to be configured in nine languages, can be paired with multiple transmitters simultaneously, monitors and logs sensor data on your smart phone or tablet, and displays sensor data in digital, graph, or gauge format.

This CE compliant product has the capability to download logged data to your smart phone or tablet and email the data to an email address or to the Cloud. The UWBT logs up to 10 samples per second and logs data to the handheld transmitter with date/time stamping, or directly to a smartphone/tablet. It works with mobile devices and computers by using USB communications.

Deterministic Ethernet connectivity

TTTech: The launch of the TTEPCIe Rugged network interface card allows industrial PCs to be easily integrated into a fault-tolerant Deterministic Ethernet network architecture.

The TTEPCIe Card Rugged is specifically designed for distributed control systems, and for use in a wide range of industrial applications and harsh environmental conditions. Two SFP ports can be used for redundancy management, utilizing the unique fault-tolerant capabilities of TTTech's Deterministic Ethernet solution including TTEthernet. This enables simple and cost-effective high availability in safe systems.

Deterministic Ethernet is a standards-based industrial Ethernet solution that allows users to simplify their network architecture through safe and guaranteed convergence. The TTEPCIe Card Rugged acts as an endpoint interface for the Deterministic Ethernet network, which supports three traffic classes: best-effort Ethernet traffic for non-critical applications, rate-constrained traffic for streaming and synchronous (TTEthernet) traffic for mission-critical and safety-critical real-time applications.

iQ-R Controller series

Mitsubishi Electric: The new MELSEC IQ-R, controller series enables manufacturers to achieve high speed, information-driven operations.

The iQ-R controller is designed with protective features such as IP address filtering to prevent unapproved access to the system. It is protected with strengthened password and program encryption options, and production can be protected using flexible and cost effective system configuration for redundant CPUs using standard CPU technology.

System processors have been optimized for consistent, reliable manufacturing operation, and are up to eight times faster than the preceding Q CPU. When combined with the new high speed bus, users will see an increased throughput of around 40 times the current iQ Platform.

The GX Works3 programming interface increases program reusability while at the same time provides advanced options for monitoring and fault diagnosis, but also increased options for protecting and managing the user's programming assets.

DH+ for PanelViews

ProSoft Technology: The company's Migration Gateway has added DH+ for PanelView upgrades. The gateway allows customers to take a phased migration approach to replacing or upgrading legacy DH+ and remote I/O PanelViews.

Prosoft has also added the EtherNet/IP to Square D Remote I/O Gateway to its Migration Gateway family. This gateway allows Rockwell Automation PACs to control Square D Remote I/O devices, minimizing the downtime required to upgrade the system. An Autoscan feature reduces configuration time, allowing users to get systems up and running quickly. The gateway's configuration data is stored on a micro SD card, which can be used for disaster recovery.

The Migration Solutions family provide users the freedom to migrate legacy control systems in phases, minimizing the risk of extended downtime including solutions for GE Genius, Texas Instruments 505, Modicon S908 I/O networks and more.

New managed switches

Red Lion Controls: New compact Industrial Gigabit and PoE+ DIN-Rail switches have been added to the company's NT24k platform. The new managed switches maximize port, speed and power options for demanding network operations.

The expansion of the NT24k platform includes the addition of compact DIN-rail mountable switches. All-Gigabit and Power over Ethernet Plus (PoE+) IEEE802.3af/at switches deliver wire-speed performance in harsh environments where space may be limited.

A compact NT24k hardened metal housing provides shock (200 g) and vibration (50 g) tolerance coupled with an up to -40° to 85°C operating temperature range to ensure optimal network performance in the harshest industrial environments.

All NT24k models feature N-Ring technology with ultra-fast (30 ms) recovery for rings containing up to 250 nodes, automatic configuration, and backup and restore capability to provide reliable plug-and-play solutions for critical monitoring and communication applications.

Designed for industrial manufacturers, OEM machine builders and system integrators, the rugged NT24k platform is targeting alternative energy, water/wastewater, transportation and intelligent traffic applications.

Compact advanced controllers

Siemens: New advanced controllers combine small size with high performance. The company has expanded its portfolio of controllers in the Simatic S7-1500 family with the addition of two small footprint controllers. The Simatic S7-1511C and S7-1512C combine CPU (including front display) with inputs and outputs in one enclosure.

The compact design of a Simatic S7-1511C providing 32 digital IO ports in a format that is just 85 millimeters wide; the Simatic S7-1512C with 64 digital IO connections is only 110 millimeters wide. Both models can be expanded to include additional connections using signal modules if required.

Key technology functions such as metering, measuring and positioning are already integrated into the hardware. The new controllers are suitable primarily for compact designs, such as those used in series production machines. Other benefits for applications include low cost compared with modular controllers with processing units along with easier storage or warehousing.

ioLogik 2500 4-in-1 I/O device

Moxa: A single IP address can communicate with multiple I/O devices, using the new ioLogik 2500 device to accelerate daisy chain expansion.

Leveraging the company's Click&Go Plus logic technology to control the I/O array, the ioLogik 2500 empowers engineers to reduce the number of system components and connections, and to eliminate the need for extensive rewiring during a daisy chain expansion. As a result, it minimizes overall system cost and complexity, while increasing data acquisition efficiency and accuracy.

Key technology is the ability to communicate with multiple remote I/O devices under a single IP address, simplifying daisy chain expansion of industrial networks and providing for the most efficient data acquisition at the lowest cost, especially for industrial field sites that have an insufficient number of IP addresses.

The ioLogik's slave Ethernet port can link up to 8 daisy-chained ioLogik E1200 expansion modules and convert more than 100 channels to one IP address. Meanwhile, the other three Ethernet ports can be used to connect to any Ethernet-driven field device.

Wireless USB DNC unit

eNETDNC: New Wireless USB DNC units can connect directly to the USB Port on a machine tool while communicating via the plant's wireless network.

DNC technology gives customers the option of not having to run CAT5 cabling to use the tools that the eNETDNC provides such as file revision control and 20,000V of surge protection while still being able to control the DNC from the office. Operators can view a directory listing at the CNC Control, and transfer files with functionality that mimics a thumb drive for easy training.

Surge protector product line

EtherWAN Systems: The PD Series Surge Protection Device (SPD) product line offers total surge protection current up to 10kA.

The PD1041 features two RJ45 ports compatible with pass-through data/ power of standard Gigabit Ethernet/ Power over Ethernet, and a wide operating temperature range (-40°C to 75°C under 100Mbps throughput). It also passes CE, FCC, VCCI, UL497B and RoHS compliance requirements.

High electromagnetic interference, unstable electricity, and indirect lightning often generate undesired voltage surges toward the network equipment. When a surge occurs, the PD1041 will isolate the surge to the ground, and the network devices, cables and data communications are free from additional damage. The PD1041 can be DIN-rail mounted in a rooftop cabinet to connect with outdoor PoE speed dome cameras, wireless APs, or PoE switches, protecting the LAN devices and cables.

EtherWAN's products are already designed in compliance with EN61000-4-5. The PD1041 can work with all company products when higher level of data port protection is needed. Testing with PoE under 1Gbps transmission rate, the PD1041 has proven itself without CRC errors under 50°C temperatures.

EtherCAT controller

Galil: The DMC-500x0 EtherCAT controller is the newest entry in Galil's latest generation of digital motion controllers. The controller allows integration of remote EtherCAT drives with just a handful of configuration commands.

The DMC-500x0 is offered in 1 through 8 axis formats. Axes 1-4 can be configured as either local or EtherCAT drives while axes 5–8 can be configured for additional EtherCAT drives. Unique to the motion control industry, this ability to mix and match local and EtherCAT drives on the same controller provides increased flexibility for any application. In addition, the DMC-500x0 is fully compatible with Galil's internal servo and stepper motor amplifiers as well as third party external drives.

Once enabled, an EtherCAT axis replaces a local axis and can be controlled in the same manner. This transparency means access to Galil's library of coordinated motion functions that can be mapped to any combination of local and EtherCAT axes. Standard modes of motion include jogging, point to point, electronic gearing and cam, linear and vector interpolation, contour and PVT modes.

Smile! Cool camera accessories for your smartphone

Most people use their smartphone as their only camera because it's always with you and you don't have to carry a second device. The integrated cameras are are constantly getting better, but there is still room for improvement. If you love shooting pictures and want to do more with the technology you have, here are some essential accessories.

Tripod

UNLESS YOU HAVE THE STEADIEST hand since Wyatt Earp, a camera mount proves very useful in many situations.

The Joby GripTight GorillaPod is a flexible tripod that will make sure the pictures you take with your smartphone are as steady as possible.

PHOTO: JOBY

This tripod is compact and foldable, and uses rubber grip pads to secure your phone in place, even when turned sideways. The stand's legs consist of 24 joints that bend and rotate, so you can place your phone anywhere, not just on flat surfaces. With the camera securely mounted you can shoot from new perspectives, give night photography a go, or make a timelapse video.

www.joby.com

Remote Shutter

Now you have your camera perfectly placed, but how do you get yourself in the picture? You can use a self-timer and rush in front of the camera, but that often results in half-body shots when you were aiming for full ones.

A smarter option is the Muku Shuttr, a wireless remote for triggering your smartphone's camera shutter from a distance. It comes in a small and unobtrusive housing that you can hook to a keychain. As it only has one function, it only features one button, making it a no-brainer to use. Since it uses Bluetooth to connect with your iOS or Android phone, it doesn't require a line of sight for operation, so you can keep the remote concealed in your pictures.

PHOTO: MUKULABS

mukulabs.com

Flash

Even amateur photographers know that natural lighting isn't always adequate.

While smartphones have evolved and mostly offer an integrated flash, that often creates more problems than it solves.

Win a flexible camera stand

Enter our contest for a chance to win a GripTight GorillaPod. It adapts to even the most uneven terrain and so the entire world can become your photography studio.

www.iebmedia.com/quiz

The winner will be announced May 7.

Contest sponsored by:

CC-Link
CLPA
PARTNER ASSOCIATION

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

PHOTO: NOVAPHOTOS

Firstly, you can't position the flash anywhere else to shed better light on the subject. As the flash triggers only when you hit the shutter, you can't tell from the viewfinder how the results will be. And lastly, you cannot control the amount or temperature of light. This often results in under- or over-exposed images.

All these problems can be overcome with the Nova, a credit-card sized Bluetooth off-camera flash for the iPhone. It features 40 points of gently diffused light, with temperature and brightness controlled from the free Nova Camera app.

www.novaphotos.com

Lens kit

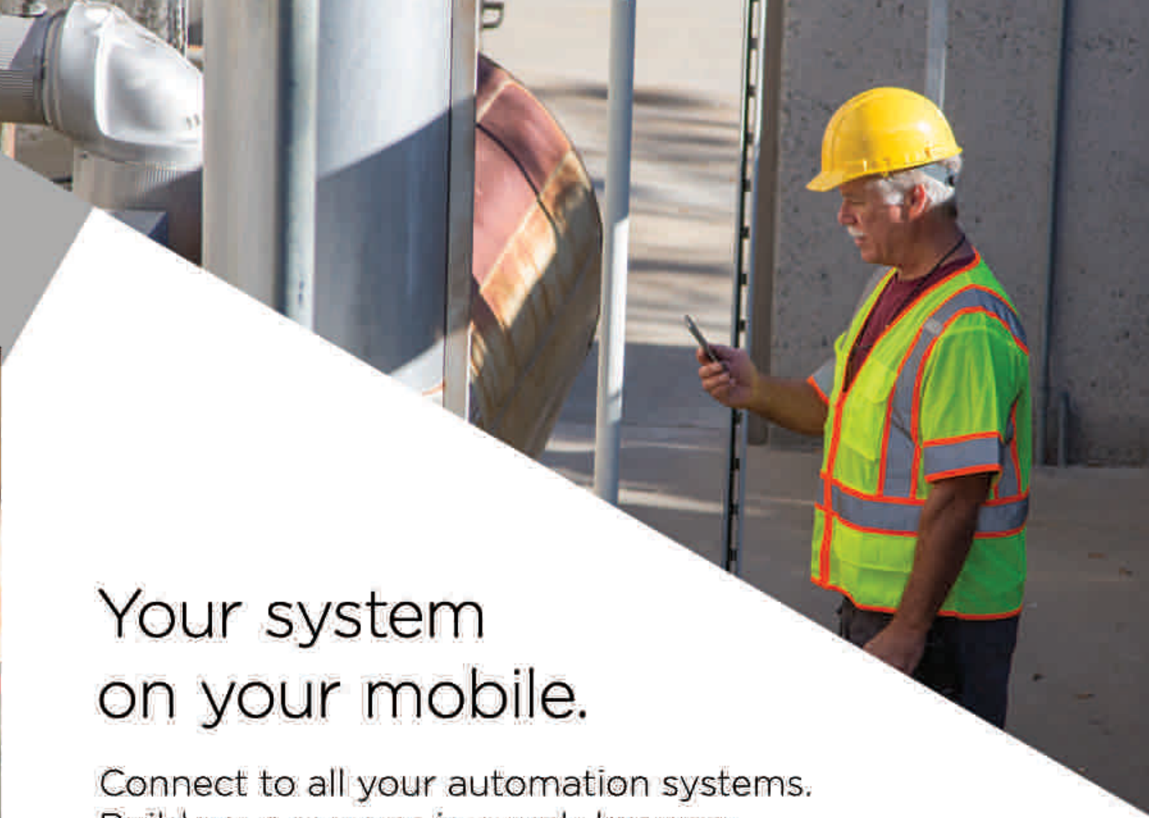
PHOTO: OLLOCLIP

The olloclip 4-IN-1 Photo Lens delivers a wealth of creative options. In one compact design it features four quick-change photo lenses: fisheye, wide-angle and 10x and 15x macros. The lens systems are made of precision ground multi-element coated glass optics. Because of olloclip's patented design, the lens system clips on and off your smartphone in seconds with no extra mounting plate or case needed.

www.olloclip.com

Leopold Ploner

CC-Link
CC-Link IE
G2A PARTNERS
BALLUFF sensors worldwide
messtec drives Automation
DATALOGIC
Industrial Ethernet Journal
IDEC
molex one company > a world of innovation
FESTO
Pro-face
ABB
上海电气菱电
frontline
Weidmüller
COGNEX
3M
MITSUBISHI ELECTRIC Changes for the Better
Automazione industriale
Bihl + Wiedemann
WAGO
Fieldbus Networks
HMS
METTLER TOLEDO
PEPPERL+FUCHS
hilscher COMPETENCE IN COMMUNICATION
RENESAS
SCHAEFFLER
LuK INA FAG
Empowered by Innovation
NEC
CC-Link
CC-Link IE



Your system on your mobile.

Connect to all your automation systems.
Build your screens in a web browser.
View on your mobile devices.
groov on.

Compatible with:

OPC UNIFIED ARCHITECTURE

Modbus

See it now!
Visit op22.co/trial-demo
or scan this QR code.
Username: **trial** Password: **opto22**

Get the *groov* View app for free:

Available on the App Store

ANDROID APP ON Google play

MADE IN THE USA

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

groov

from OPTO 22