2.2016 Issue 92
ISSN 1470-5745

industrial ethernet book

The Journal of Industrial Network Connectivity

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

industrial ethernet book

Reader Service Card

IEB issue 92 - February 2016

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

Return by mail to:
IEB Media
Bahnhofstr. 12
86938 Schondorf
Germany

Or fax back to:
+49 8192 933 7829

Or use our online reader service at:
www.iebmedia.com/service

Please enter your contact details below:

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

I want to:

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

Signature: ______________________________

Date: ______________________________

Company Activity (select one)

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

Job Activity (select one)

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

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

The Rise of TSN

When IEB covered "Deterministic Ethernet & TSN for Automotive" as the cover story in our July 2015 issue, we really didn't fully understand the potential impact of Time-Sensitive Networking (TSN). But now it is becoming increasingly clear that the TSN technology is part of the conversation on the direction of Industrial Ethernet networking.

ODVA recently announced that its technical work for 2016 includes the adaptation of time sensitive networking along with cybersecurity, application data models and communication integration standards.

"One area of focus will be the adaptation of certain emerging standards for Time-Sensitive Networking (TSN) to EtherNet/IP," ODVA wrote in a recent press release. "In particular, ODVA will create enhancements to the EtherNet/IP specification for frame preemption and stream reservation based on the standards being defined in the IEEE-802.1 projects."

"ODVA's adaptation of TSN technologies is a straightforward evolution of the EtherNet/IP technology, which relies on commercial-off-the-shelf (COTS) technologies for Ethernet and the Internet to solve demanding applications in industrial automation. Users of EtherNet/IP will be able to realize performance improvements in systems using EtherNet/IP by as much as two orders of magnitude by combining TSN with existing standards already included in the EtherNet/IP specification, such as Quality of Service, Gigabit Ethernet and CIP Sync -- ODVA's adaptation of IEEE-1588."

The AVnu Alliance (www.avnu.org) is a consortium of leading technology companies with a charter to assure an interoperable ecosystem for applications that need precise timing and low latency on a network. Readers may want to visit their website to learn more about TSN technology and its potential impact.

One way to think about TSN, according to Todd Walter, Chief Marketing Manager for National Instruments and the AVnu Alliance Industrial Segment Chair, is to compare it to the layers of wireless technology where 802.11 is the IEEE layer that defines the silicon and some of the lower level protocols.

If designers attempt to implement to that specification, the odds are that they will not end up with devices that can interoperate and work together because there is another layer that needs to address which pieces of the standard will be used, how it will be used, along with plug fests and conformance testing to verify operation. That has been the function of the Wi-Fi alliance, and AVnu shares a similar charter for TSN. But the goal is to build on time-sensitive networking capabilities.

Al Presher

Contents

Industrial Ethernet Book

The next issue of Industrial Ethernet Book will be published in **March/April 2016**
Deadline for editorial: February 19, 2016 **Deadline for artwork:** March 11, 2016

Product & Sources Listing

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

Update your own products

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

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

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

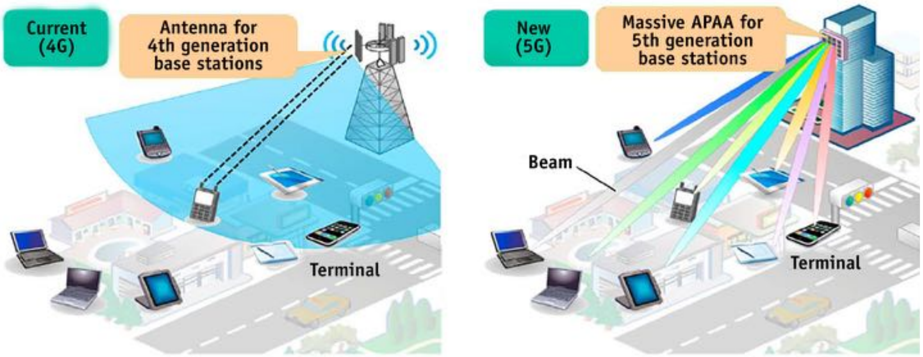
Published by IEB MEDIA
IEB Media, Bahnhofstrasse 12, 86938 Schondorf am Ammersee, Germany
ISSN 1470-5745

Multibeam multiplexing 5G targets 20Gbps throughput

New 5G technology will enable faster, higher-quality connections by combining tens of active phased-array antennas with massive antenna elements and new precoding technology for parallel transmission of data.

MITSUBISHI ELECTRIC has developed new multibeam multiplexing radio communication technology for base stations of envisioned fifth-generation (5G) mobile communication systems by combining tens of active phased-array antennas with massive antenna elements (massive APAAs) and a new precoding technology for parallel transmission of data streams by transmitters. The wideband communication technology will enable high-speed communication in high-frequency bands expected to be used for 5G systems.

The new multibeam multiplexing technology will achieve transmission speeds of 20Gbps, or around 60 times faster than current 4G mobile base stations that use multi-input multi-output (MIMO) technology.


Current (4G)
Antenna for 4th generation base stations
Terminal
New (5G)
Massive APAA for 5th generation base stations
Beam
Terminal

SOURCE: MITSUBISHI

The massive APAA technology developed by Mitsubishi is already used commercially for satellites and other systems.

APAA technology

Massive MIMO technology that would facilitate the use of more than several hundred antenna elements is drawing attention as a way to compensate for propagation loss in the high-frequency bands (from 4GHz) that will be used for 5G. Fully digitized signal processing would require enormous digital circuitry and power consumption, so one of the practical solutions is a hybrid configuration that combines analog and digital processing.

The massive APAA technology developed by Mitsubishi Electric is used commercially for satellites and other systems. Mitsubishi developed its multibeam multiplexing technology by combining massive APAAs and precoding technology in transmitters that deliver increased transmission power to overcome propagation loss in high-frequency bands. With two-beam transmissions of current 4G mobile base stations, up to 16-beam transmissions can achieve up to 20Gbps to satisfy needs for higher data rates.

When mobile terminals are in proximity in a crowded environment, signals from base stations can interfere with each other. In conventional diagonalization precoding schemes, the transmission power of interfering signals is lowered to reduce interference, but this also results in decreased transmission speeds. Mitsubishi's solution is its new nonlinear multi-diagonalization precoding technology combining multi-diagonalization precoding, with inherent interference, and nonlinear operation, which removes interference through multi-diagonalization precoding. Since transmission power does not have to be lowered, the result is high-capacity communication at 20Gbps in crowded environments.Mitsubishi is engaged in efforts to commercially deploy ultra-high-speed communication exceeding 20Gbps to accommodate the increasing number of terminals in the IoT. In September 2015, Japan's Ministry of Internal Affairs and Communications entrusted Mitsubishi with a research project to realize 5G mobile communication systems that could achieve peak throughput of 20Gbps. A system demonstration is scheduled in 2018. Going forward, Mitsubishi will work toward realizing practical use of these technologies in commercial 5G systems after 2020.

Industry news from Mitsubishi

Cybersecurity volume and EtherNet/IP enhancements for 2016

ODVA HAS ANNOUNCED A MAJOR MILESTONE with the pending publication of a new volume in its specifications specifically dedicated to cybersecurity. This body of work will be released under the name of CIP Security that will be initially applicable to EtherNet/IP.

The initial release of CIP Security includes mechanisms to address spoofing of identity, tampering with data and disclosing of information. Mechanisms supported in the initial release of CIP Security include device authorization, integrity of message transport and confidentiality of messages.

To support these mechanisms, ODVA has adapted encryption standards from the Internet Engineering Task Force (IETF) for encryption based on Transport Layer Security (TLS), Data Transport Layer Security (DTLS) and authentication based on the X.509v3 standard for certificate handling.

EtherNet/IP Enhancements in 2016

ODVA also announced major areas of technical work it plans to undertake in 2016 that will benefit users of EtherNet/IP.

One area of focus will be the adaptation of certain emerging standards for Time-Sensitive Networking (TSN) to EtherNet/IP. In particular, ODVA will create enhancements to The EtherNet/IP Specification for frame preemption and stream reservation based on the standards being defined in the IEEE-802.1 projects.

ODVA's adaptation of TSN is an evolution of the EtherNet/IP technology, which relies on commercial-off-the-shelf (COTS) technologies for Ethernet and the Internet to solve applications in industrial automation.

The goal is for users of EtherNet/IP to be able to realize performance improvements in systems using EtherNet/IP by as much as two orders of magnitude by combining Time-Sensitive Networking with existing standards already included in The EtherNet/IP Specification, such as Quality of Service, Gigabit Ethernet and CIP Sync.

www.odva.org

Fieldbus Box
EtherCAT Box
Zinc die-cast box
Stainless steel box

ZigBee and EnOcean collaborate on energy harvesting wireless with ZigBee 3.0

Joint development of open, global specification for energy harvesting wireless communication technology will help meet growing demand for interoperable, self-powered IoT sensor solutions.

THE ZIGBEE ALLIANCE, a non-profit association of organizations creating open, global standards that define the Internet of Things (IoT) for use in consumer, commercial and industrial applications, has announced with the EnOcean Alliance, a leading consortium for battery-less, wireless smart buildings and smart homes, that the two organizations will cooperate on combining the benefits of EnOcean energy harvesting wireless solutions with ZigBee 3.0 for worldwide applications.

The cooperation connects the two alliances' advantages, synergies and track record of standards advancements to create an open, global specification that will extend energy harvesting wireless communication to a broader range of self-powered IoT sensor solutions. These solutions use the surrounding environment as their energy source, making battery-less connected devices a reality.

Energy harvesting & Zigbee 3.0

"We are very excited that the EnOcean Alliance is bringing its energy harvesting expertise and widely deployed device profiles into the ZigBee 3.0 ecosystem," said Tobin Richardson, President and CEO of the ZigBee Alliance.

"Our goal with ZigBee 3.0 is to provide a unifying IoT standard that simplifies product development while reducing industry fragmentation and unlocking new market growth opportunities. This agreement with the EnOcean Alliance is a first important step down that path. A jointly developed specification for the ZigBee 3.0 ecosystem will bring the promise of interoperable self-powered IoT solutions to more markets and applications, meeting growing demand for plug-and-play solutions that can deliver seamless, ultra-low-power battery-less communication."

"This is a major next step on the way to an interoperable IoT, from two industry-leading organizations combining their expertise and influence to help make this vision a reality," said Graham Martin, Chairman of the EnOcean Alliance. "The globally available 2.4 GHz frequency is the key to the consumer market. We look forward to working with the ZigBee Alliance, one of the most experienced organizations in this field, to define the technical specifications for worldwide energy harvesting wireless solutions based on this worldwide standard. This will give our members access to new regions and additional fields of applications to grow their business for self-powered innovations. It perfectly adds to the EnOcean Alliance's established market of smart buildings in the sub-1 GHz frequency, which will continue to be a major focus for us, bringing field-proven and interoperable energy harvesting solutions to new areas of use. This is a significant win for the complete wireless community."

"The ZigBee Alliance's board of directors and I are pleased to be entering into this relationship with the EnOcean Alliance," said John E. Osborne II, Chairman of the ZigBee Alliance board. "We expect this technology cooperation to deliver significant new benefits and opportunities for our members and their customers as we move closer to true interoperability for the IoT."

This technical cooperation agreement will build on the EnOcean Alliance's already strong position with more than 1,500 interoperable products available for home and commercial building automation, and expand it bringing energy harvesting wireless communication to applications in the IoT and consumer arenas.

It will also take advantage of the newly ratified ZigBee 3.0 standard, which enables battery-less devices to securely join networks across a variety of energy harvesting applications. As a result, the industry will have new opportunities for creating intelligently connected buildings and developing other solutions across a variety of applications. The collaboration is designed to provide a foundation to bring data to the IoT frameworks of other industry initiatives, in order to facilitate interoperable communication from the sensor to the cloud.

A Technical Task Force will define the technical specifications required to combine standardized EnOcean Equipment Profiles (EEPs) with the ZigBee 3.0 solution, which operates in the worldwide IEEE 802.15.4 2.4 GHz standard. The alliances plan to complete definition of this technical specification and share details of associated collaborative marketing and business activities in the second quarter of 2016.

ZigBee 3.0 is a single unified, open and complete wireless IoT product development solution. It extends all the way from the physical layer to the application network layer, and includes certification and branding for improved interoperability across a growing range of market segments.

News report by ***ZigBee and EnOcean Alliances.***

Rinspeed's "Etos" concept car – emissions monitoring in vehicles

RINSPEED'S ETOS CONCEPT CAR is being fitted with HARTING IIC MICA for independent emissions and status monitoring. This digital innovation aims to ensure a clean future by providing a variety of condition monitoring information to the driver.

Using the intelligent mini-industrial-computer MICA in the concept car illustrates how drive and engine data can be continually recorded and transmitted and then evaluated and processed by an independent, neutral body (Dekra). It also allows statements on the credibility of mileage status to be made.

"MICA can be quickly and easily integrated into a wide range of vehicles. Its installation in the Etos is an excellent example of this," remarked Dr. Jan Regtmeier, Director of Product Management at HARTING IT Software Development.

MICA technology is a modular platform comprising open hardware and software components which can be adapted quickly and cost-effectively to many industrial applications. It is well-suited for battery management in electric vehicles, energy management of machines and plants (online and remote-enabled), as well as other data capture and communication tasks.

The MICA will be on display at the Hannover Messe in April 2016.

IIC MICA is being installed in Rinspeed's "Etos" concept car for independent emissions and status monitoring.

Monitoring water disposal wells use WirelessHART transmitters

Wireless remote sensing of water disposal wells at a gas and oil field has saved Linn Energy $150,000 annually. Trended data not only provides insight into the condition of each water disposal well, but also avoids erroneous conclusions by relying on single daily measurements.

SOURCE: EMERSON

Installing wireless pressure and totalizing transmitters on water disposal wells helped monitor productivity, eliminate unnecessary cleanouts and realize significant savings.

LINN ENERGY OPERATES OIL AND GAS WELLS in several areas across the United States, and has grown from a handful of natural gas wells in 2003 to a top-20 independent U.S. energy and production enterprise with approximately 7.3 Tcfe of proven reserves in U.S. basins as of December 31, 2014.

In Bakersfield, CA, Linn Energy operates oil and gas wells, and also a steam flood field, where steam is injected to provide pressure to force oil and gas out of the well. Unlike with fracking, this process does not use very high pressure liquid to fracture rock formations. The water used in this process is treated and injected into an underground reservoir via water disposal wells.

These wells need to be cleaned periodically using a process called well-bore cleanout, but it's difficult to determine precisely when to do a cleanout. Installing wireless pressure and totalizing transmitters on 15 water disposal wells helped Linn Energy monitor productivity, eliminate unnecessary cleanouts, and save $150,000 the first year—with similar savings expected going forward. Significant savings were also realized because they were able to determine that fewer new water disposal wells were required.

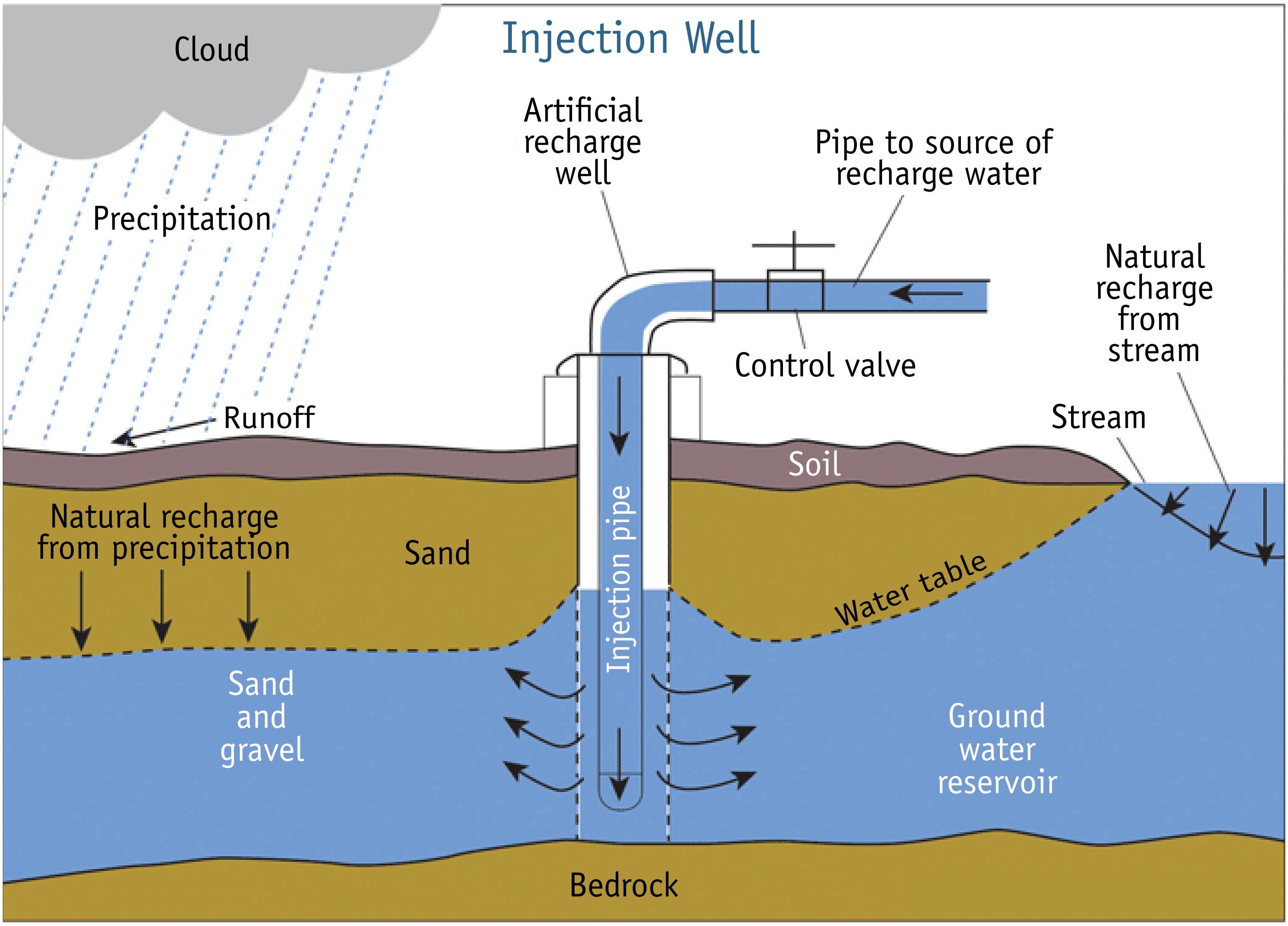
Monitoring water disposal wells

In the Bakersfield area, a separate underground reservoir is used to store treated wastewater from nearby production wells. Steam is used for injection into production wells to create a pressure that will push the gas and oil to the surface. Water comes to the surface with the oil and gas, is treated to meet EPA requirements, and then injected back into the underground reservoir via water disposal wells. When water is needed for steam injection, it is taken from the reservoir.

Water injection rates and totals are carefully monitored to meet EPA requirements, as well as to optimize water disposal well performance. Surface or injection pressure is also monitored to meet EPA and safety requirements, and to provide further insights.

This field has over 20 water disposal wells, each about 500 feet apart. Linn Energy's job is to maximize the productivity of existing wells by monitoring their performance, determining when they need to be cleaned out, and keeping them running to minimize the number of new wells that need to be drilled.

Not all wells are created equally as they vary in depth, total length of perforations and other parameters. Well performance is indicated by the volume of water injected per foot of perforations, a value Linn Energy wishes to maximize--because it's closely related to the total injected volume of water which indicates productivity of that well. Before the wireless installation, manual rounds were made daily to read local chart recorders indicating water flow into the well, and to read local gauges measuring surface pressure.



SOURCE: EMERSON

Injection wells return treated water to an underground reservoir.

However, these rounds were not sufficient to optimize cleaning or to determine when new water disposal wells needed to be drilled. Daily measurements fed into the efficiency model indicated that 10 new wells were required. But when a more rigorous study was done, using many more manual measurements daily, it was determined that only five new wells were required, saving nearly a million dollars.

It quickly became apparent that daily rounds were not supplying enough information for accurate analysis of water disposal well conditions. Well operation changes from hour to hour, so a single measurement at 8 a.m. can be quite different than a measurement made at 1 p.m. on the same day. A single daily measurement, therefore, does not necessarily represent what is happening in the field that day, and can lead to erroneous conclusions, such as the need to drill too many new wells.

Linn Energy's study showed they needed on-line monitoring and trending of key parameters. This would improve well modeling to optimize cleaning, measure well productivity more accurately, and determine the need for more wells. The study was quite expensive, and it isn't practical to conduct such studies on a regular basis. So, they analyzed its results very carefully, and concluded on-line monitoring was the best solution.

Because the water disposal wells are in remote areas, installing wired instrumentation was not economically feasible. It would cost too much to install power supplies, wiring and safety equipment at each site for wired transmitters, and then install cabling or a remote terminal unit to bring the information back to the central control system. Instead, Linn Energy installed battery-powered Rosemount transmitters.

SOURCE: EMERSON

High gain antennas are used when long distances are required for wireless transmissions.

Wireless to the wells

Linn Energy installed 15 Rosemount 3051S wireless pressure transmitters on existing manifolds to monitor the surface pressure, or injection pressure, of each water disposal well. These were installed in two hours each. They were factory configured for the application, including the Network ID and Join Key, so they were ready to go out of the box once the battery was connected at each transmitter.

One Emerson WirelessHART gateway was installed to receive the signals. Because of the distances involved for some of the wells, three high gain antennas were also installed. The field gateway communicates to the base station gateway, and the base station gateway is integrated to the Rockwell Automation control system via EtherNet/IP. The 3051S wireless transmitters began transmitting useful data to the control system within minutes after the transmitters and gateway were installed.

SOURCE: EMERSON

Wireless pressure and totalizing transmitters were installed on 15 water disposal wells.

Fifteen Wireless Totalizing Transmitters were installed shortly thereafter on existing turbine meters to measure injection rates and totalized values of injection water. These were installed on a Saturday morning in about four hours. Linn Energy had a hard deadline, and the two technicians were able to meet the deadline due to the simple installation requirements of wireless totalizing transmitters.

Emerson was on site to assist with the installation. Linn Energy took the Rosemount 705s out of the box and connected the lead wires from the turbine meter to the Rosemount 705 terminal block. They attached the Rosemount 705 direct mount threads to the threads of the turbine meter and powered the device. Within five minutes the Rockwell Automation control system was communicating with the wireless totalizer. Emerson assisted with 14 more wells, and total time for installation and startup was 10 minutes per well.

The wireless transmitters provide continuous data to the well performance model, which runs in a PC at their well field control. The data is trended and used to calculate the Injectivity Index, a key parameter for productivity. The index is a function of surface or injection pressure, injection rate, and the fixed number of perforations per foot. The wireless measurements give richer, more reliable data to optimize the model.

Results

Linn Energy's biggest benefit was optimizing the well-bore cleanout process. They can now trend the surface or injection pressure at each water disposal well to detect stoppage. This is much better than single daily measurements. Well-bore cleanout is expensive and time consuming, and they save $10,000 each time they avoid an unnecessary cleanout. Linn Energy has saved at least one cleanout a year for each of the 15 wells, totaling $150,000 in savings.

SOURCE: EMERSON

Wireless totalizers were connected to existing turbine flow meters in five minutes, and were communicating with the control system five minutes later.

Trended data gives much more insight into the condition of each water disposal well, and avoids erroneous conclusions that were too prevalent with single daily measurements. Equally important, Linn Energy can optimize future development and avoid unnecessary drilling of new water disposal wells, all without the need for expensive and time consuming studies.

The success has led to four more water disposal wells being monitored since the initial installation, with more planned as part of an expansion plan.

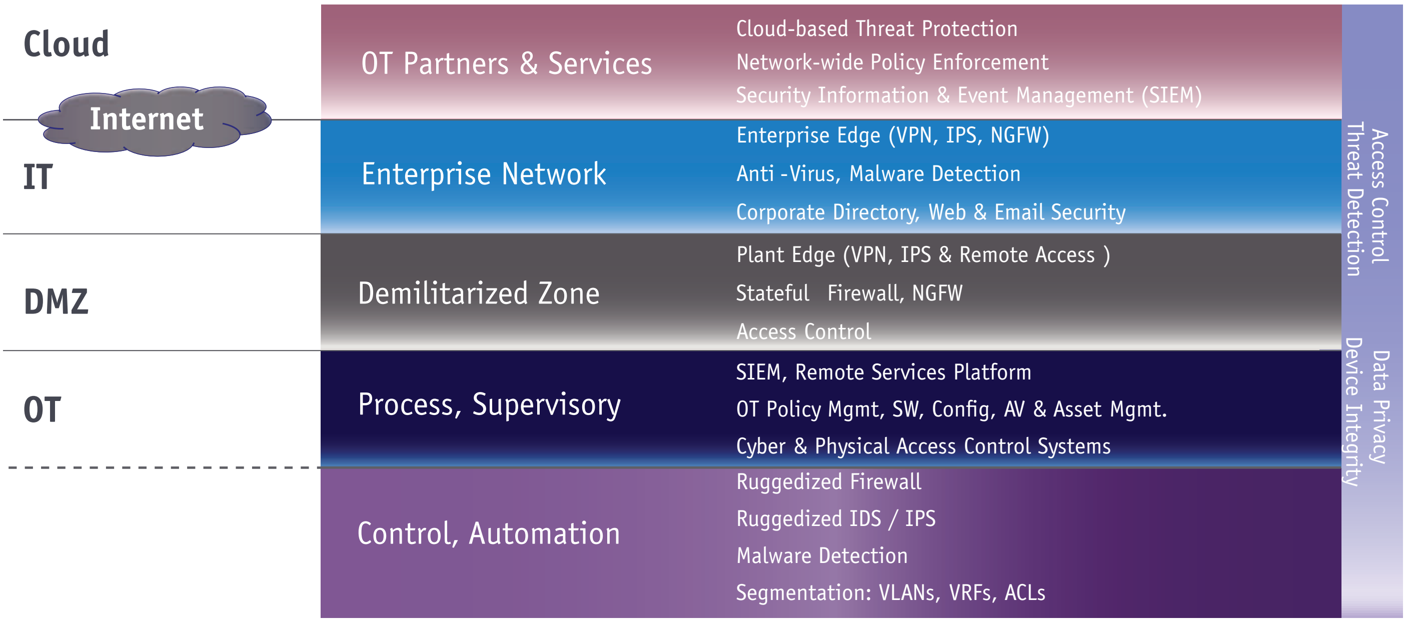
Wireless measurements eliminate the need to send personnel into the field on a daily basis, and give Linn Energy's a much better picture of what is going on at each water disposal well. This has enabled them to improve compliance reporting, improve operator productivity, optimize well-bore cleaning, improve well efficiency, and optimize future development.

Josh Hernandez works for ***Emerson Process Management.***

Cyber security model for manufacturing

A rise in threats to manufacturing systems is resulting in industry adoption of stronger security measures. ODVA specifically is working to develop a cybersecurity framework and design lifecycle focusing on the needs of industrial control systems.

IT/OT Converged Security Model



Cloud
Internet
IT
DMZ
OT

OT Partners & Services
Cloud-based Threat Protection
Network-wide Policy Enforcement
Security Information & Event Management (SIEM)

Enterprise Network
Enterprise Edge (VPN, IPS, NGFW)
Anti -Virus, Malware Detection
Corporate Directory, Web & Email Security

Demilitarized Zone
Plant Edge (VPN, IPS & Remote Access)
Stateful Firewall, NGFW
Access Control

Process, Supervisory
SIEM, Remote Services Platform
OT Policy Mgmt, SW, Config, AV & Asset Mgmt.
Cyber & Physical Access Control Systems

Control, Automation
Ruggedized Firewall
Ruggedized IDS / IPS
Malware Detection
Segmentation: VLANs, VRFs, ACLs

Access Control
Threat Detection
Data Privacy
Device Integrity

SOURCE: CISCO SYSTEMS

Manufacturing Systems Cybersecurity Model

INDUSTRIAL CONTROL SYSTEMS (ICS), and especially systems used in manufacturing, are becoming a primary Cybersecurity target. With the increased number of reported threats, industry is in the process of adopting security measures.

This article presents an Industrial Control System Cybersecurity framework and describes its mapping to manufacturing. In particular, we will put focus on how ODVA's effort fits into the larger framework and how it can continue to influence and strengthen on the ICS Cybersecurity framework.

The "ICS-Cert Year in Review" reports show a growing trend of reported incidents with the latest 2014 report demonstrating a growing trend in manufacturing where reported incidents went up from 38 incidents constituting 15% of the total reported ICS incidents in 2013 to 65 in 2014, constituting 27% of the reported incidents. With the growing trend in threats and reported incidents, the need to secure manufacturing deployments strengthens ODVA's initiative to provide security in the protocols and interfaces.

The National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) continue to address the security issues and of late are focused on Industrial Control Systems as they pertain to the nation's critical infrastructure. In particular, NIST currently has an active public working group focused on this topic in the Cyber Physical Security Working Group. It is a public forum (http://www.nist.gov/cps/cpspwg.cfm) with different focus groups where defining a reference architecture and cybersecurity are two of its main areas of focus. A general framework for an ICS Cybersecurity was also published on February 2014 enumerating the set of functions and activities required to achieve specific cybersecurity outcomes.

With ODVA's focus on defining the Industrial Automation standards for vendors and suppliers to interoperate, it is well aligned to address the Asset Management, Access Control, Data Security, Protective Technologies and general Communication categories. This focus is on outlining a cybersecurity framework and design lifecycle for specific categories.

Cybersecurity Model for ODVA

With the specific functions and categories as defined by NIST, we can map them into specific Cybersecurity features and functions and align them to the ICS Purdue model.

The Manufacturing Cybersecurity model maps the access control functions across the span of the entire deployment, from the Purdue Level 0 and Level 1 devices through the enterprise and cloud services in Level 5 (and above). Similarly, the Threat Detection mechanisms must accumulate the information for analysis across the entire infrastructure to enable the detection and protection mechanisms provided through IDS/IPS, SIEM and other vulnerability and malware assessment tools. These technologies rely on secure communications across every link and communication paths between all devices and applications. As these security services are now mapped into the common Industrial Automation and in particular, the Manufacturing Systems model, we can now focus on ODVA's alignment and proposed evolution in designing and defining the next generation technologies to address cybersecurity.

A Security Framework

To ensure the overall security and integrity of an Industrial Automation ecosystem, all devices whether they are a M2M device, a network device, a host or a data server must be secure. The requirements of building a trusted ecosystem implies that all devices, beyond securing its communications, must be robust and secure (e.g. trustworthy). To ensure such trustworthiness, different security components must be provided in the device. The components are summarized as follows:

Trusted Supply Chain: To build a trustworthy ecosystem, we must first ensure that all components of the ecosystem can be trusted; e.g. the supply chain must also be trusted. While this component is not in ODVA's scope to define fully, it merits mention as failure to consign trusted vendors, suppliers and processes for the componentry (whether it is for the Industrial Automation ecosystem or for the particular device being built) breaks the trustworthiness of the system. The ISO 28000 series provide a set of specifications for addressing and building a trusted/secure supply chain.

Root of Trust: A root of trust is a set of functions that are inherently trusted; these functions could be either hardware or software functions that perform measurements or verification of software, perform authentication and protect cryptographic keys. One such specification and implementation is the Trusted Protected Module (TPM) [7] defined by the Trusted Computing Group. Most systems offering root of trust implement hardware assisted components, such as a TPM as the hardware implementation offers best protection of the key storage and its supply chain can be better controlled. Without a root of trust, any outgoing information from the device could be deemed untrusted.

Trusted Operating System: A trusted operating system is one that provides a secure operating environment. Compliance or criteria for a "secure operating environment" have been defined by some organizations such as the ISO/IEC 15408. Some of the functions defined include providing memory and file protection, I/O device access controls, user authentication, access controls and be able to detect some attacks. A function to help provide one security level of assurance that the operating environment is trustworthy is secure boot. An untrusted operating system could allow malware and other attacks.

Secure Data storage: Beyond the protective measures to ensure the system software is protected, applications and data stored on the device must also be protected. This component's goal is to ensure that data stored on the device is only accessed by authorized users and processes as well as providing mechanisms to ensure the data cannot be infected, tampered or corrupted.

Secure Communications: communications involves providing the network services to facilitate communications with other devices securely. This function must provide the appropriate cryptographic tools to allow the communications to be secure, e.g. providing confidentiality, integrity and replay protection where appropriate. It is understood that not all communication needs confidentiality, but at minimum, communicating peers must be able to authenticate and ensure the information has not been forged, replayed or corrupted.

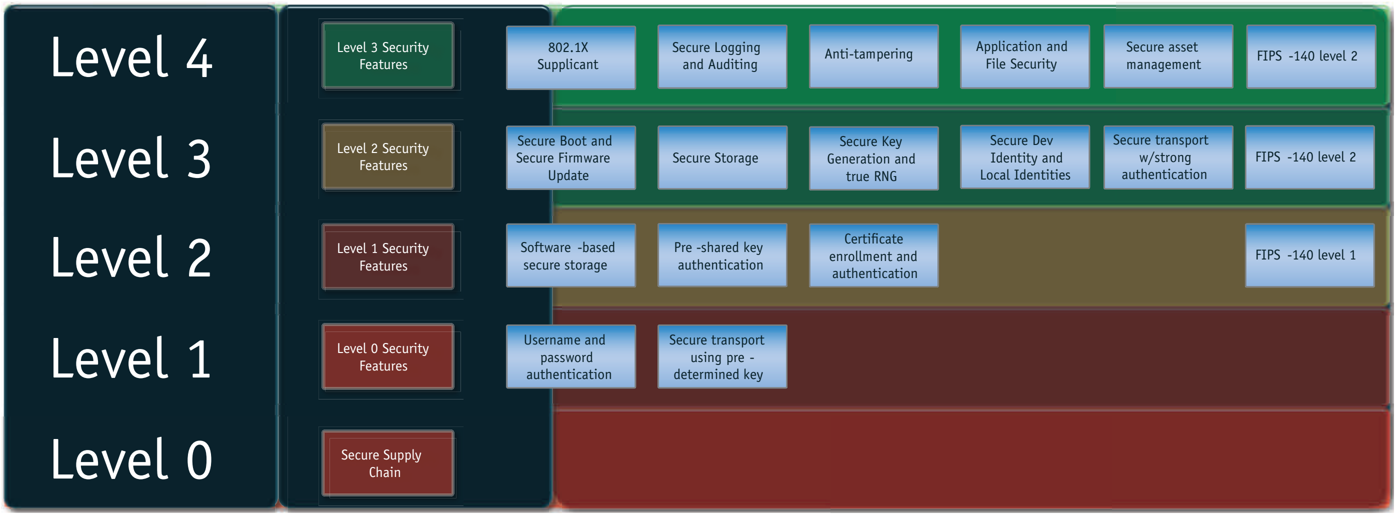
Software Integrity: Along with a trusted operating system, applications running on the device must be protected from tampering or infection. Software Integrity is the component that defines the functions, processes and tools that help in the detection and protection of software applications running on the device.

Secure Device Management: While each of the components described are functions that help secure a device, these functions and

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protectino Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communication
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

SOURCE: CISCO SYSTEMS

Critical Infrastructure Core Structure and Functions


Level 4
Level 3 Security Features
802.1X Supplicant
Secure Logging and Auditing
Anti-tampering
Application and File Security
Secure asset management
FIPS -140 level 2
Level 3
Level 2 Security Features
Secure Boot and Secure Firmware Update
Secure Storage
Secure Key Generation and true RNG
Secure Dev Identity and Local Identities
Secure transport w/strong authentication
FIPS -140 level 2
Level 2
Level 1 Security Features
Software -based secure storage
Pre -shared key authentication
Certificate enrollment and authentication
FIPS -140 level 1
Level 1
Level 0 Security Features
Username and password authentication
Secure transport using pre - determined key
Level 0
Secure Supply Chain

SOURCE: CISCO SYSTEMS

Implementing different Security levels of Trustworthy Device

modules must also be managed and managed securely. In particular, the device's security lifecycle must be carefully managed to ensure its identity, credentials and overall health remains secure.

Similarly, the configurations and software used to protect the device must also be securely managed. With trends shifting towards outsourcing management or facilitating device management at a larger scale through a cloud based computing system, it becomes more imperative that the management component includes secure communications between the device and the management system. Note that the device, as a whole, may also be managed by different software applications and as such, protective measures such as authentication and authorization of these management applications apply.

Implementing a Trustworthy Device

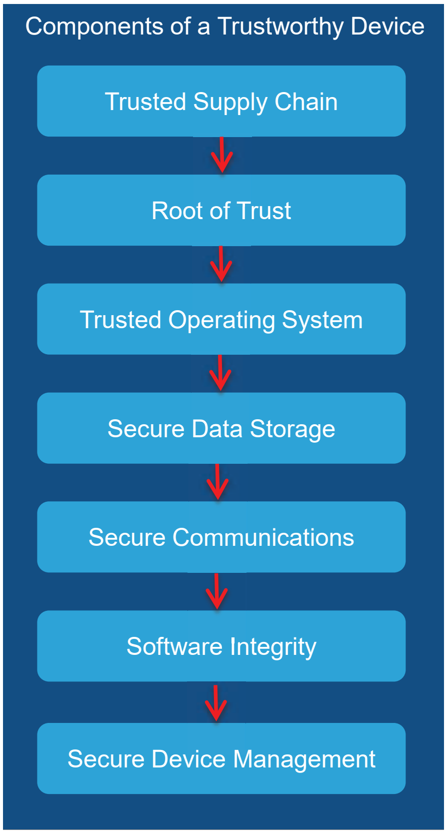
With a general framework and components defined to design a Trustworthy Device, different levels of security and trustworthiness can be achieved based on implementation. Thus, there are implementation considerations to determine what needs to be included to provide different levels of security.

As ODVA defines how to provide security, it is well poised to define both the protocols to allow products to be built and provide security at any of the levels defined while maintaining interoperability. Additionally, with the levels defined CIP secure specifications may also define best security practices based on these levels.

Different security levels can be achieved based on the type of functionality provided on the device spanning from no security (Level 0) to the "golden standard", e.g. Level 4. The list below provides a high-level overview for each level:

Level 0 – While at minimum, any component should follow a Trusted Supply chain process; this level offers no security. This level is not recommended for any industrial system.

Level 1 – Level 1 security devices have limited security functionalities, which are all software-based. It provides minimum functionality to secure protected (network) communications through the use of username/password techniques and minimal key management. It's suitable for low-cost connected devices that are not part of mission-critical operations. The security features include limited core security implementation in software (e.g. no key generation, no OS hardening, no software obfuscation) and software based cryptographic tools to establish secure communications



SOURCE: CISCO SYSTEMS

Trustworthy Device Components

Level 2 – For legacy devices, retrofitting hardware-based security technology is not practical; in which case, software-based security anchor technology can be leveraged. While it may not be as secure and trustworthy, with the right implementation, software-based anchor performs reasonably well and is a viable means to provide security when a hardware-based option is not feasible. Various Level 2 devices are available on the market today, including the smart home automation devices. The security features encompass:

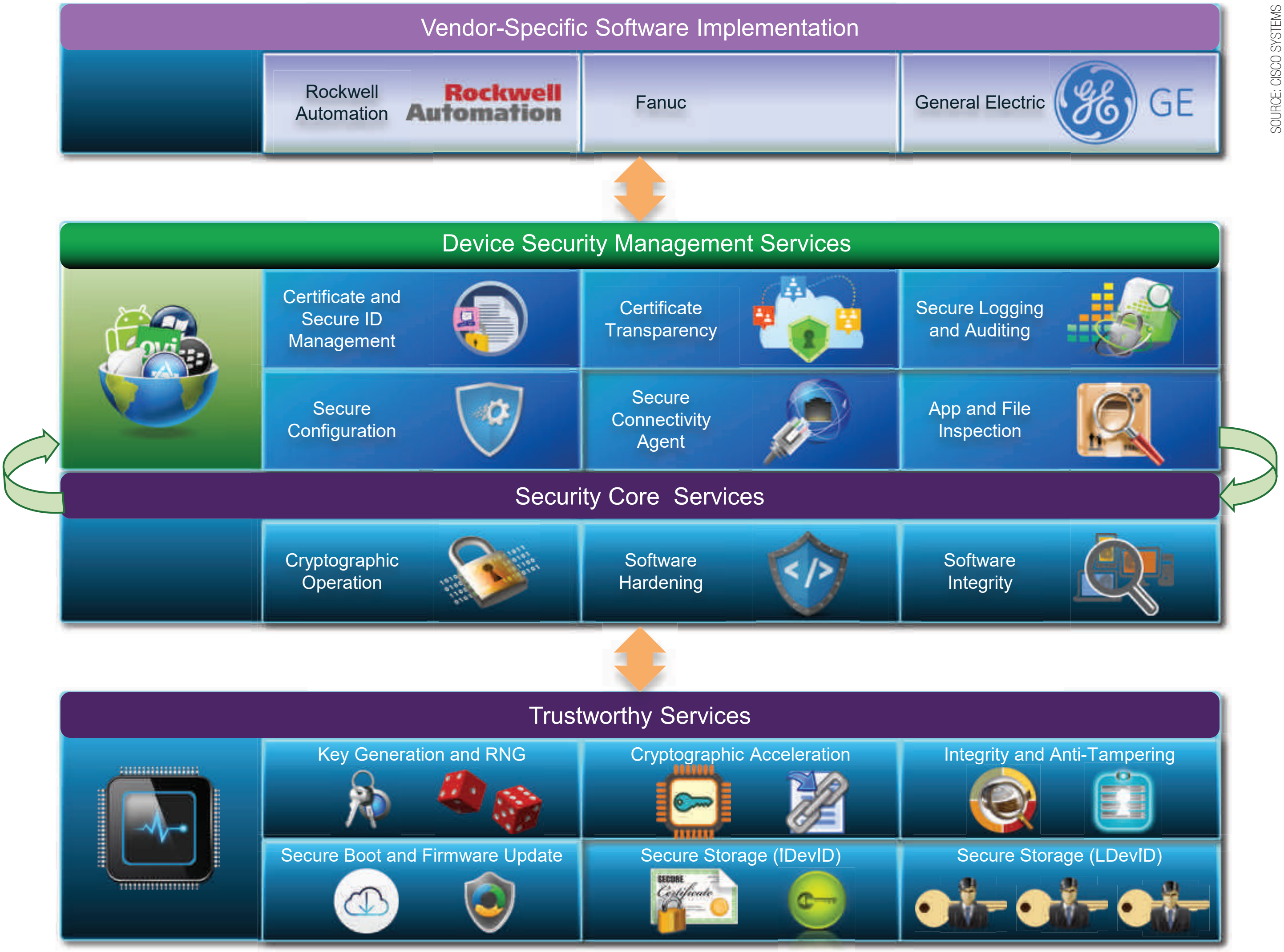
Level 3 – Similar to Level 2 but with the added hardware (vs. software) security anchor to enable a true root of trust. Recommended for adoption by all Industrial machines and devices are part of critical operations, for example, an industrial robot. The features encompass:

- Hardware security anchor (e.g. TPM or similar functional technology)
- All features as defined in Level 2

Level 4 – Best recommended practice for adoption by all Industrial management and control stations that need to manage operation and file manipulation. For example, any full-featured Industrial HMI System must support level 4 security. The security features encompass:

- Application and file security
- Secure device (lifecycle) management
- Anti-tampering protection of the "root of trust" component
- All features as defined in Level 3

Theoretically, vendors may choose to build a secure device in a number of different ways as long as it is bolstered by a security anchor (either hardware or software based) and meets all security requirements. However, as we all know that a poorly designed architecture or



SOURCE: CISCO SYSTEMS

Reference Architecture of Trustworthy Device. With a general framework and components defined, different levels of security and trustworthiness can be achieved.

implementation can introduce security holes and vulnerabilities into a system, regardless of the encryption key length or encryption algorithm strength. There needs to be a reference architecture that guides the design and implementation of such Trustworthy devices.

Another important note is to recognize that the protocols and interfaces designed, but include the agility and flexibility to allow for new cryptographic algorithms and key lengths to "future" proof when an algorithm has been proven to be weakened or compromised.

The reference architecture of enabling Trustworthy device and systems offers a layered design with each layer modularized to allow for each of the modules to be independently implemented and standard APIs defined between the layers.

Trustworthy Services: This is where the root-of-trust is established, identities and anchors stored and maintained. The security of all other layers hinges on the integrity of the security anchor. If the security anchor is compromised, the entire system can no longer be trusted. The set of trustworthy services can be implemented in either hardware or software, and includes following functionalities:

- Key Generation and RNG; while RNGs can be pseudo-random good sources of entropy are required to ensure randomness. NIST's recommendations [8] and approved methods should be used.
- Cryptographic Acceleration. At minimum, cryptographic algorithms must be supported, whether in pure software, firmware or fully accelerated in hardware.
- Integrity and Anti-Tampering. Integrity of at minimum, the operating system software and the trusted modules (and anti-tampering techniques against these modules) must be provided.
- Secure Boot and Secure Firmware Upgrade
- Secure Storage

Security Core Services: This software-based layer encapsulates functions provided by the trustworthy services and present them to the rest of the system via standard APIs. It may perform other security functions as well, for example, OS software hardening, and system-level software attestation.

Device Security Management Services: This layer embodies the set of security functions and features that are essential to secure software operations and the overall security health throughout a device's lifecycle. For example, this layer shall support some form of 802.1AR certificate enrollment (e.g. EST or SCEP) and certificate management functions, and bind the secure device identity to the certificate and private key.

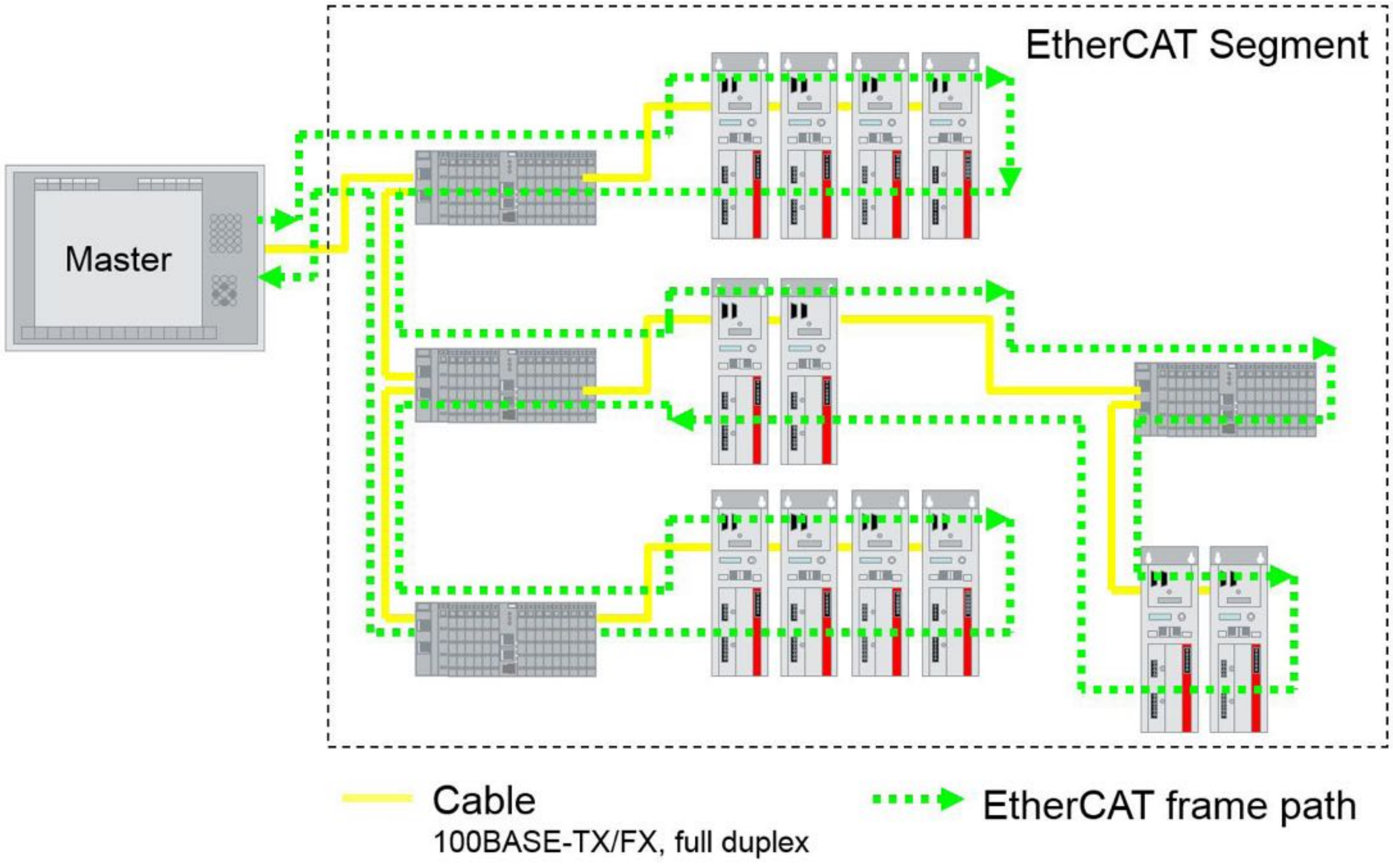
Typical services include:

- Certificate Enrollment and Secure ID Management
- Secure Connectivity Agent (e.g. 802.1X)
- Secure Logging and Auditing
- Application and File Inspection and Attestation

Nancy Cam-Winget is a Distinguished Engineer at ***Cisco Systems.*** *Xuechen Yang is Senior Engineering Director at* ***Solarwinds****.*

EtherCAT topology variations drive system performance

Network planning is a necessity but topology selection doesn't need to have a negative influence on the functionality or real-time operation of an EtherCAT network. Topology choices can be tailored to each plant, and usage of functions such as Hot Connect or cable redundancy.



SOURCE: ETG

System diagram illustrates how EtherCAT datagrams offer "on the fly" processing; read and write access operates only on a small part of the whole telegram.

INDUSTRIAL AUTOMATION SYSTEMS connect a wide variety of actuators and sensors, as well as one or more controllers via a range of communication systems, by means of executing efficient and flexible control tasks.

System dimensions and structure dictate the requirements of the necessary communication system topology. Using a systematic approach, topology variations and features are described from the user perspective, as well as from the view of the developer. This article provides basic background information and specific solutions, a system planning guide for end users and estimates implementation effort.

EtherCAT Functional Principle

As an Ethernet-based communication technology, EtherCAT provides an optimized foundation for the special requirements of modern automation technology. Standard Ethernet cables differ little in their usage, whether in the office world or in industrial applications. The EtherCAT industrial Ethernet solution is a master-slave system. An EtherCAT master, which controls the network and the communication, can be implemented in software on an industrial PC, requiring only a standard network card.

A special EtherCAT communication chip, the EtherCAT Slave Controller (ESC), provides the foundation for EtherCAT slave devices. In the ESC, the entirety of the process data communication is operated, as this guarantees unique transmission speed and reliability of communication, independent of the particular device and specific implementation. The process data are exchanged between EtherCAT and the application controller via common process data interfaces with a DPRAM.

The EtherCAT network configurator can detect the network topology by reading the port number and link status of every single device. The address space offers the possibility to address over 65,000 devices in one segment. The operation status of all devices is controlled in each cycle; device errors are detected synchronously, enabling the application program to react in real-time.

Processing on the fly

EtherCAT datagrams process while running through the system to offer "on the fly" processing; read and write access operates only on a small part of the whole telegram. The telegram travels immediately to the next EtherCAT device, rather than received, processed and then sent, as is common with other communication technologies.

EtherCAT operates in full-duplex mode, and telegrams are sent on a line pair in processing direction, moving from master to slave. The frames are processed by the EtherCAT device only in this direction, moving from device to device until the telegram traverses the entire system. The last device sends the telegram on the second line pair in forwarding direction back to the master. EtherCAT always builds a logical ring structure, independent of the chosen topology.

System time and synchronization

EtherCAT devices implement highly precise timing in hardware, or, more precisely, within the ESC. This precision timestamping lends its name to the synchronization mechanism of EtherCAT, the "Distributed Clocks" (DC).

Normally, the first DC device following the master provides a reference clock for all other devices. This comprises the balance of the different starting times of the clocks, including the one from the master, as well as the delay caused by cables and hardware.

With this uniquely generated time base, applications can be realized that need to insert or read data on several devices synchronously. Thanks to this mechanism, a time base with a delay of far under 1µs is achievable, enabling highly precise drive or measurement applications, for example.

EtherCAT also transmits on 100BASE-TX, 100BASE-FX and EBUS. EBUS uses LVDS transmission physics, provides internal device communication and can be implemented in a compact and cost-efficient manner. The 100BASE coding variants connect to the ESC via PHYs, with the MII (Media Independent Interfaces) serving as the interface.

Each ESC generates a new physical signal, facilitating constant, topology-independent signal quality. Additionally, an unlimited number of media changes are possible.

Topology possibilities with EtherCAT

Topologies can vary enormously with regard to complexity. These range from simple topologies such as line, tree, star or mixed variations, up to examples with segment or system-exceeding data and timestamp exchange.

Tree structure. The tree structure combines Daisy Chain topologies with tap lines/line topology. In pure form, these classic topologies combine arbitrarily and are fully supported by EtherCAT. EtherCAT devices differ regarding their port number. Devices with more than two ports (many ESC support up to four ports) can serve for the connection of tap lines.

Star topology. Star topology is realized with EtherCAT junctions. Much like the tree topology, this configuration enables continuity of service where a device failure or cable break does not lead to a disconnection of other devices. In addition, the logical ring remains with this topology, enabling corresponding real-time capabilities.

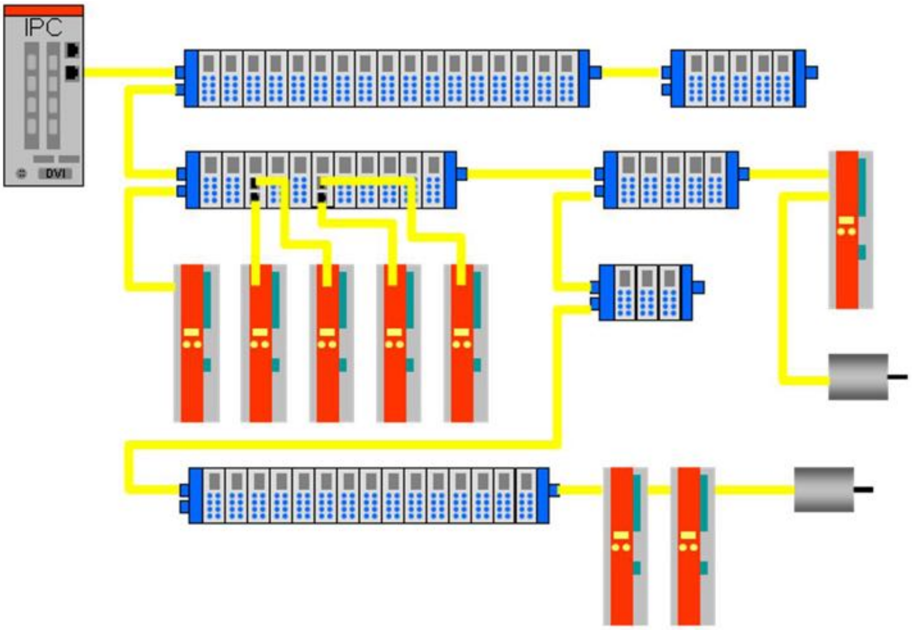
Hot Connect. Hot Connect allows coupling and uncoupling devices or segments during operation. This works especially well with an additional ID switch, as these are detected independently of their position within the network and thus can be connected to any free port. Thanks to the features of the EtherCAT Slave Controller (ESC), the disconnect process is detected very quickly. Ports can be switched off by the master, specifically before the device or segment is uncoupled.

Ring structure for cable redundancy. Implementation of ring topology enables cable redundancy. Therefore, the last device in the processing order connects directly to the master. To ensure suitability of connection, all devices must have at least one free MII port. Redundancy requires a second Ethernet port on the hardware side, as the master remains a software implementation.

Synchronizing several EtherCAT networks. Data exchange between two or more EtherCAT networks can be implemented simply, needing only switch ports or a bridge. Two switch ports from different segments can be connected to each other to enable data exchange. With a bridge device, networks can be synchronized in addition to the data exchange, creating a unique time base across system boundaries. This is especially interesting for test bed engineering or in modular machines with several controls. Additionally, EtherCAT provides further possibilities for master-to-master communication.

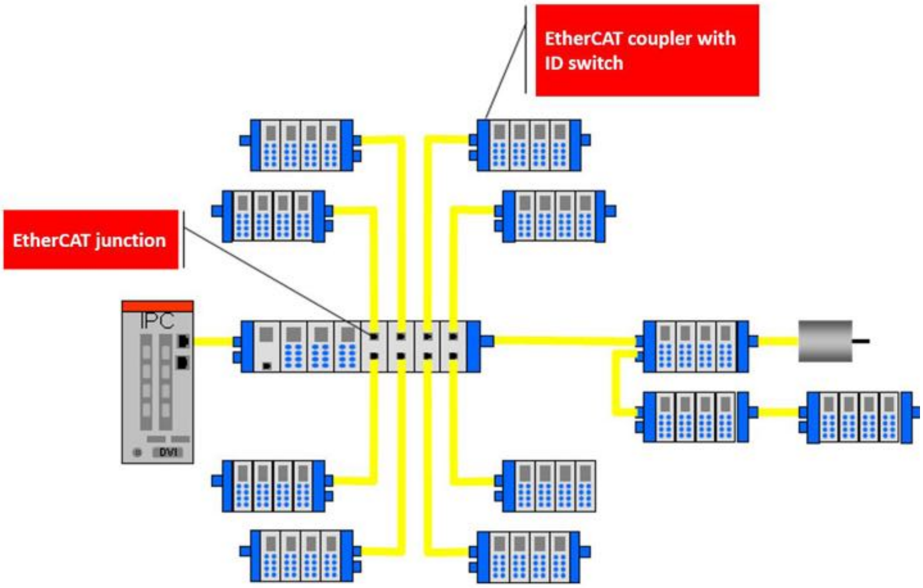
Master-to-Master Communication. Masters can be connected directly to standard switches and a second network card, or alternatively, via an EtherCAT switch port device to exchange data between one another, both cyclically as well as acyclically.

Slave-to-Slave Communication. When it comes to data exchange between different



SOURCE: ETG

A tree structure combines daisy chain topologies with tap lines/line topology.



SOURCE: ETG

Star topology offers real-time capabilities.

slaves, the master serves as a router. Data is read from one device, copied from the input process image to the output process image within the master and passed along to downstream devices. This can take place even within the same control cycle.

Highest-level communication requirements require use of the topology-independent version of the slave-to-slave communication. One device inserts data in the running through telegram, interpreted by the downstream devices as needed.

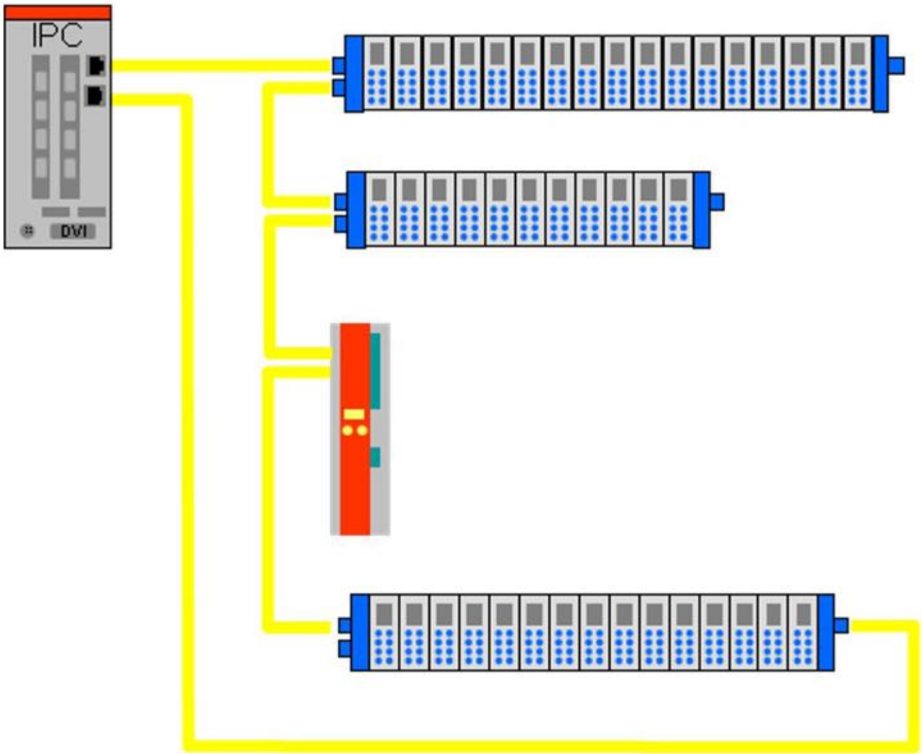
Planning aid for end users

The following section describes some of the most important topics for network planning. Since EtherCAT uses the full-duplex communication methodology, several telegrams can be sent after one another without having to wait for the return of the previous frames. Thus, cycle times may not be equal to the transit times. In practice, however, the transit time is often estimated as the minimum cycle time. This can be determined, regardless of all optimization possibilities and the symmetry of the input and output data, as follows:

$t_{Delay} = m \times t_{EBUS} + n \times t_{MII} + t_{PD} + 2 \times t_{Cable}$

(Refer to table on page 17 for more information.)

The delay caused by an EtherCAT device with two EBUS ports (e.g., modular I/Os) is determined by the hardware delay of the ESC, usually about 0.3µs.The delay caused by an EtherCAT device with two MII ports (e.g. a drive), and with two RJ45 Ethernet connectors, is determined by the hardware delay of the ESC and the two PHYs. This figure, depending on the PHY, is approximately 1.2µs.



SOURCE: ETG

Ring structure for cable redundancy

Choosing the topology

With EtherCAT, the selection of the topology has zero negative influence on the functionality, real-time operation or other features. This fact enables the topology to be tailored perfectly to the physical extension of the plant and the usage of special functionalities such as Hot Connect or cable redundancy.

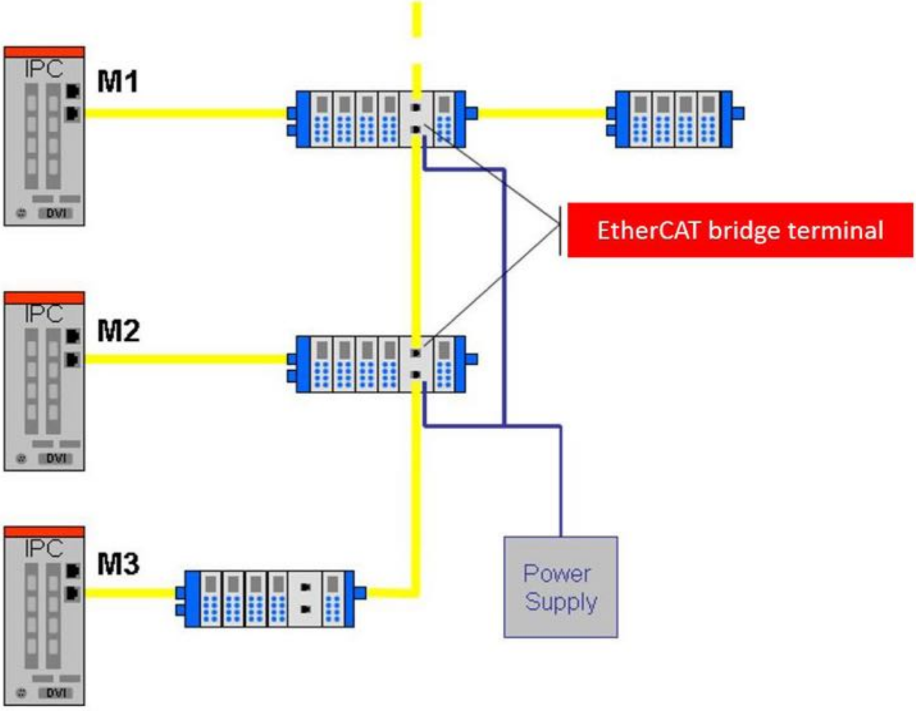
Using Hot Connect. Many applications require a change of the I/O configuration during operation. Examples include machining centers with tool change operations, sensor-equipped tool systems or printing machines where individual printing mechanisms can be switched off. The protocol structure of the EtherCAT system capably meets these demands: The Hot Connect function allows the connection and disconnection of network segments during operation, to reconfigure and react flexibly to changing extension levels.

Using Hot Swap. In the case of changing complex devices, the replacement device must be parameterized identically. This requires knowledge in dealing with special parameterization programs, as well as the parameters needing adjustment. Often, this knowledge is not available on-site. With EtherCAT, this problem can be avoided through the use of Hot Swap functionality. Here, the parameter data are saved within the master and recorded to the device automatically upon initialization.

Using Distributed Clocks. The functionality of the synchronization mechanism Distributed Clocks (DC) functions independently from the network structure. Devices with and without DCs can be arranged arbitrarily, as the synchronization of the clocks is performed automatically by the master, removing the need for user adjustments.

Implementation considerations

Looking at all the technological possibilities enabled by EtherCAT, the device manufacturer is mainly interested in determining the



SOURCE: ETG

Synchronizing several EtherCAT segments involved development effort. Some features are supported by the ESC automatically, while others require software and/or hardware extensions.

Choosing the port. The defining characteristics of an EtherCAT device are port number and type. To keep the flexibility of the topology, an EtherCAT device should have at least two ports to enable the coupling of further devices in the line. For non-modular devices, such as a drive, this means at least two MII ports and for modular devices, two EBUS ports can be used as well.

Devices with additional infrastructure capabilities such as a distribution terminal for star topology or a physics converter from 100BASE to EBUS and vice versa can also implement several different ports.

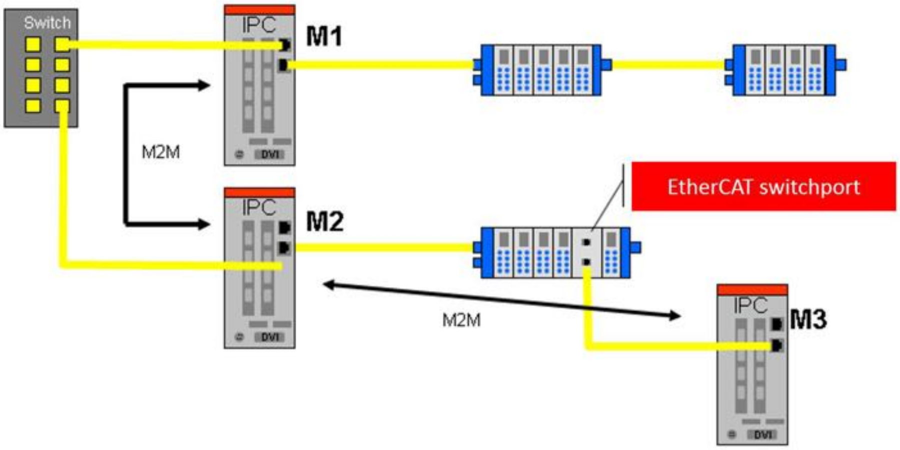
Hot Connect. Regarding Hot Connect, it is recommended to support a position-independent address in order to have the ability to connect and definitively identify a machine module on every free port within the network. This address must be available even after a voltage loss.

EtherCAT uses a second address for Hot Connect, called the Station Alias. Depending on the implementation, this address can be read from an ESC register or transmitted as process data.

In both cases, there has to be an adjustment option on the slave device which can be achieved via a DIP switch or an operating panel, for example. The non-volatile configuration memory of the ESC provides another source for the Station Alias, from which the address is loaded up into a register.

Delay	Description
m x t_{EBUS}	delay by m devices with 2 EBUS ports
n x t_{MII}	delay by n devices with 2 MII ports
t_{PD}	+ delay by process data length (outputs + inputs) at 100Mbit/s (neglecting that the process data length in the frame is halved at symmetric relation of I/O data per device + 26 byte overhead per Ethernet frame + 12 byte overhead/datagram
t_{Cable}	delay due to 100BASE-TX cable (~5ns/m)
t_P	delay in processing direction
t_F	delay in forwarding direction

SOURCE: ETG



SOURCE: ETG

Master-to-master communication

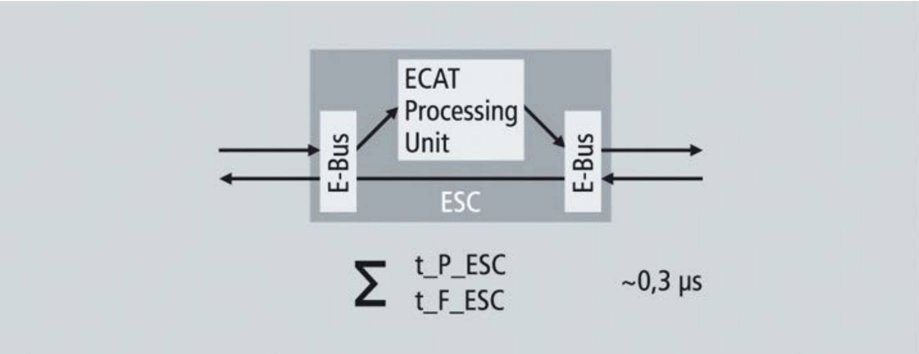
Hot Swap. In case of complex device replacement, such as a drive, a re-parameterization must usually be performed. To avoid this step, EtherCAT describes a method for backup, enabling the device manufacturer to sign important parameters. All signed parameters are loaded up into the new device automatically after replacement.

Within the slave, an extension of the firmware supports the backup mechanism. This includes the extension for marking the backup objects, the saving of the latter in a non-volatile memory and the inspection of the data validity.

Redundancy. The EtherCAT telegram travels through two network ports, as a function of cable redundancy. Normally, only the telegram in the processing direction is edited, while the second telegram in the forwarding direction runs through the network without being edited. To maintain redundancy, both telegrams run through a part of the network in processing and forwarding directions.

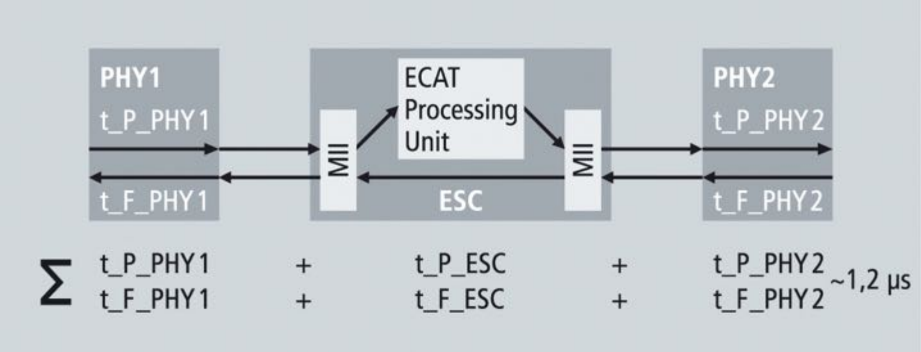
Within the slave, the redundancy concept requires no extension. The required functionality is based on existing mechanisms that are support by every ESC. On the master side, a software extension is necessary to evaluate both sent telegrams and generates a complete image of the communication for the master application.

Florian Essler works for the ***EtherCAT Technology Group*** *in Nuremburg, Germany.*



SOURCE: ETG

Delay of an EBUS device

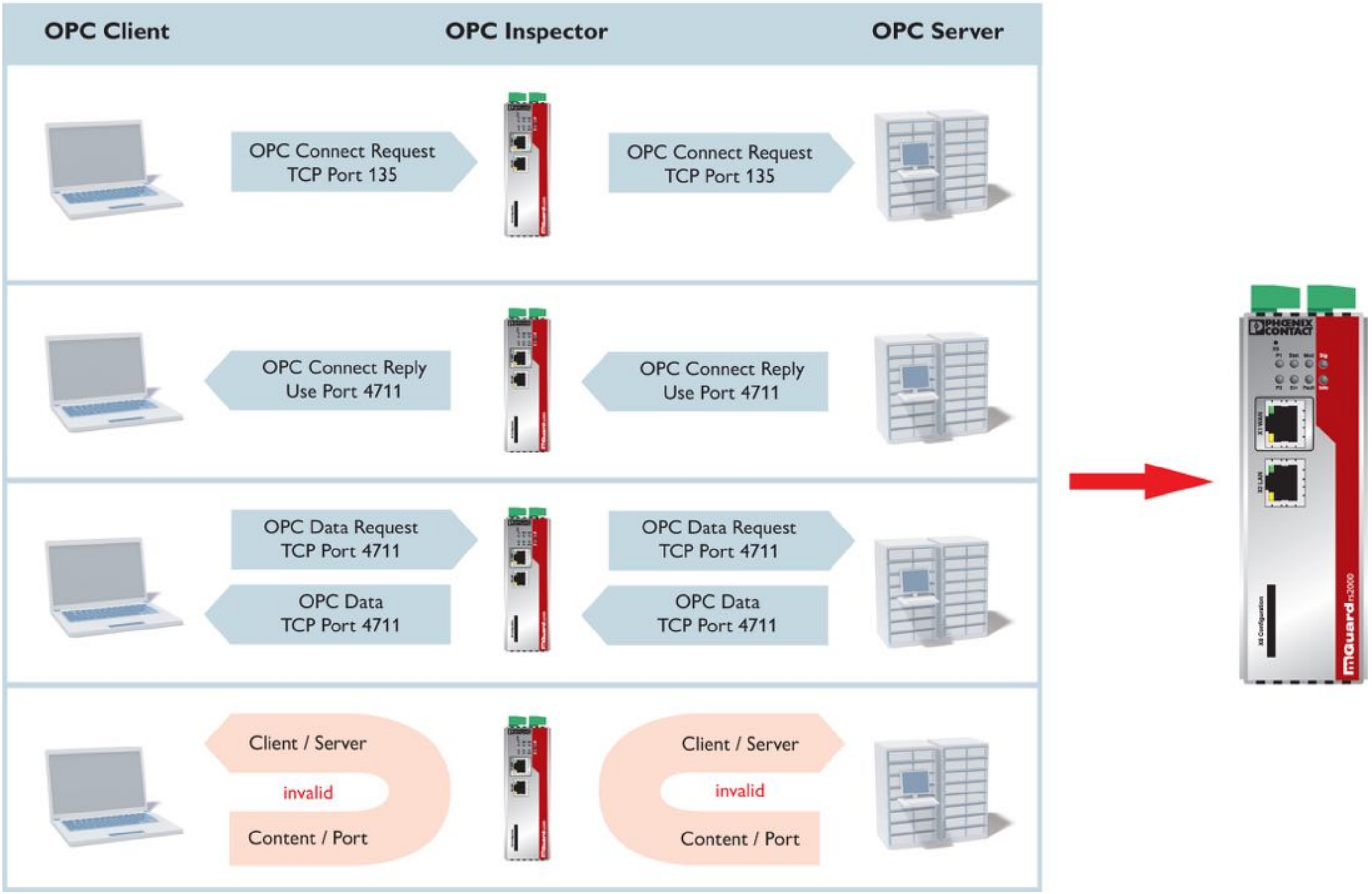


SOURCE: ETG

Delay of an MII device

Reliable firewall solutions protect OPC applications

Reliable, remote maintenance solutions for protecting OPC applications use a three-level security concept featuring a conditional firewall, demilitarized zone, and CIFS Integrity Monitoring (CIM). This allows administrators to build manageable security architectures for users while ensuring tamper-proof operation.



SOURCE: PHOENIX CONTACT

Schematic structure of OPC communication.

OPC CLASSIC (OLE for process control) is used in the manufacturing and process industry, as well as in many other industrial sectors. With more than 20,000 OPC products from over 3,500 manufacturers, the standard is among the most successful solutions for the interoperable exchange of data between applications by different providers.

Control systems and field devices equipped with an OPC interface are able to overcome the differences between various automation components. The solution also facilitates convenient, high-performance data transfer across the boundaries of individual systems. In this context, OPC offers a communication pathway for data collection, process visualization, and data management that can be used to transfer parameter sets, control sequences, programs, and production data.

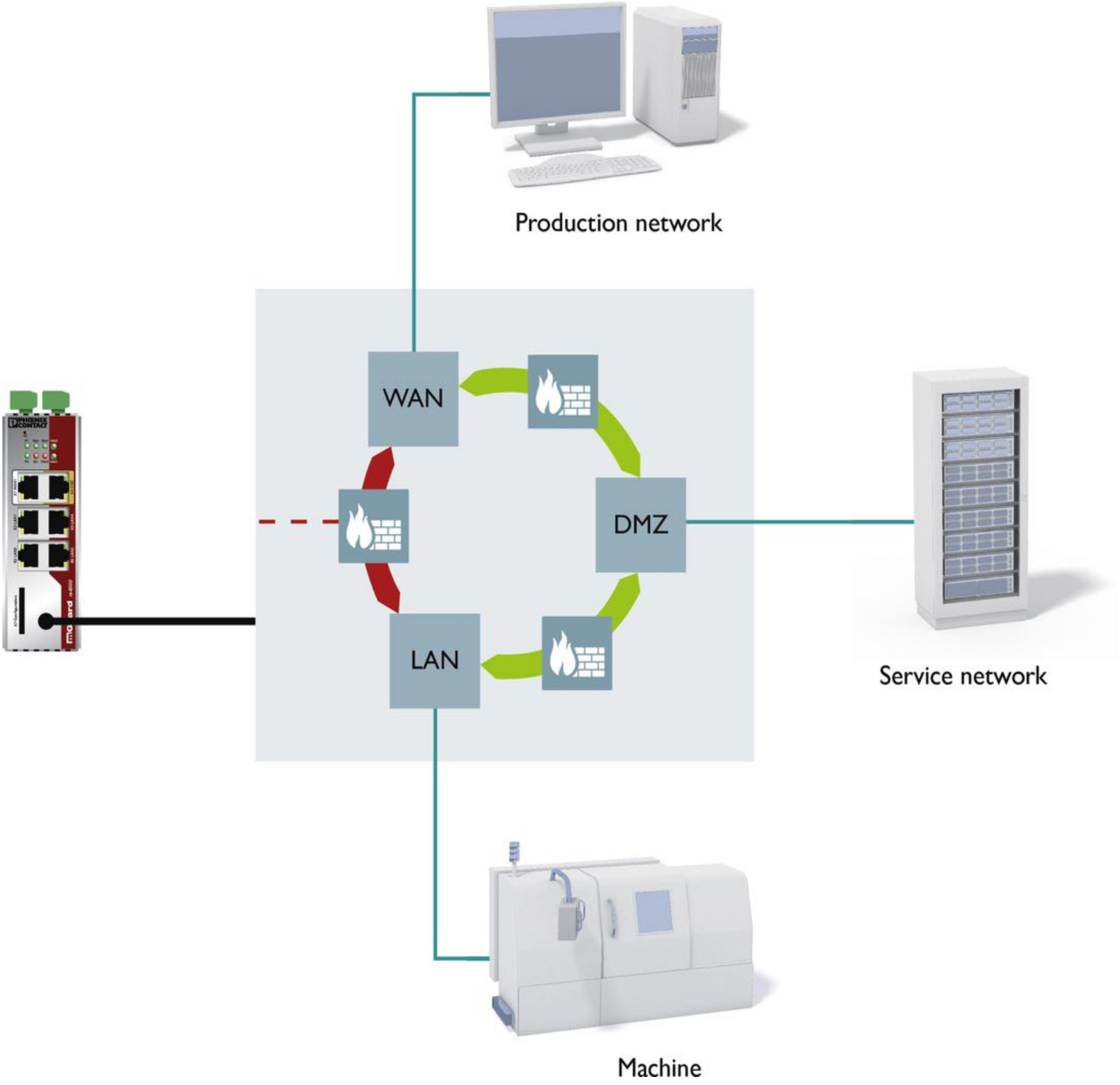
The COM/DCOM protocol from Microsoft serves to facilitate data exchange between the OPC server and the OPC client. However, the protocol was discontinued back in 2002 in favor of the .Net framework, while COM/DCOM is currently supported by all operating systems, a trend that is likely to continue in the future. Microsoft is not developing the technology any further, however. As a result, it has become outdated, particularly with regard to security threats.

Existing protection mechanisms

OPC servers function in an entirely transparent manner. Consequently, access to local communication data does not differ from access to remote data. Because automation projects are becoming increasingly complex and are no longer limited to individual machines or plants, OPC transmissions have proliferated to the same extent that plants have expanded.

The security settings available for the DCOM protocol exhibit a high degree of complexity. At the same time, incompatibilities emerge between devices by different manufacturers. For this reason, extensive access rights are required. On the one hand, these rights provide a basis for data exchange, but on the other, they erode existing protection mechanisms. As a result, it is not possible to implement a consistent and reliable security concept for security communication when using DCOM.

The situation becomes still more difficult when implementing OPC due to the fact that the standard requires numerous communication ports. The ports are used for authentication, initializing data transfers,



SOURCE: PHOENIX CONTACT

Conditional firewall for situation-based toggling; two different firewall settings are displayed.

and sending data, for example. Unlike HTTP (port 80) or FTP (port 21), they are undefined; instead, they are randomly assigned by OPC. If a port is unavailable, another is selected automatically. In light of the above, a firewall has to keep numerous ports open, which renders it ineffective in practice.

Advantages of NAT applications

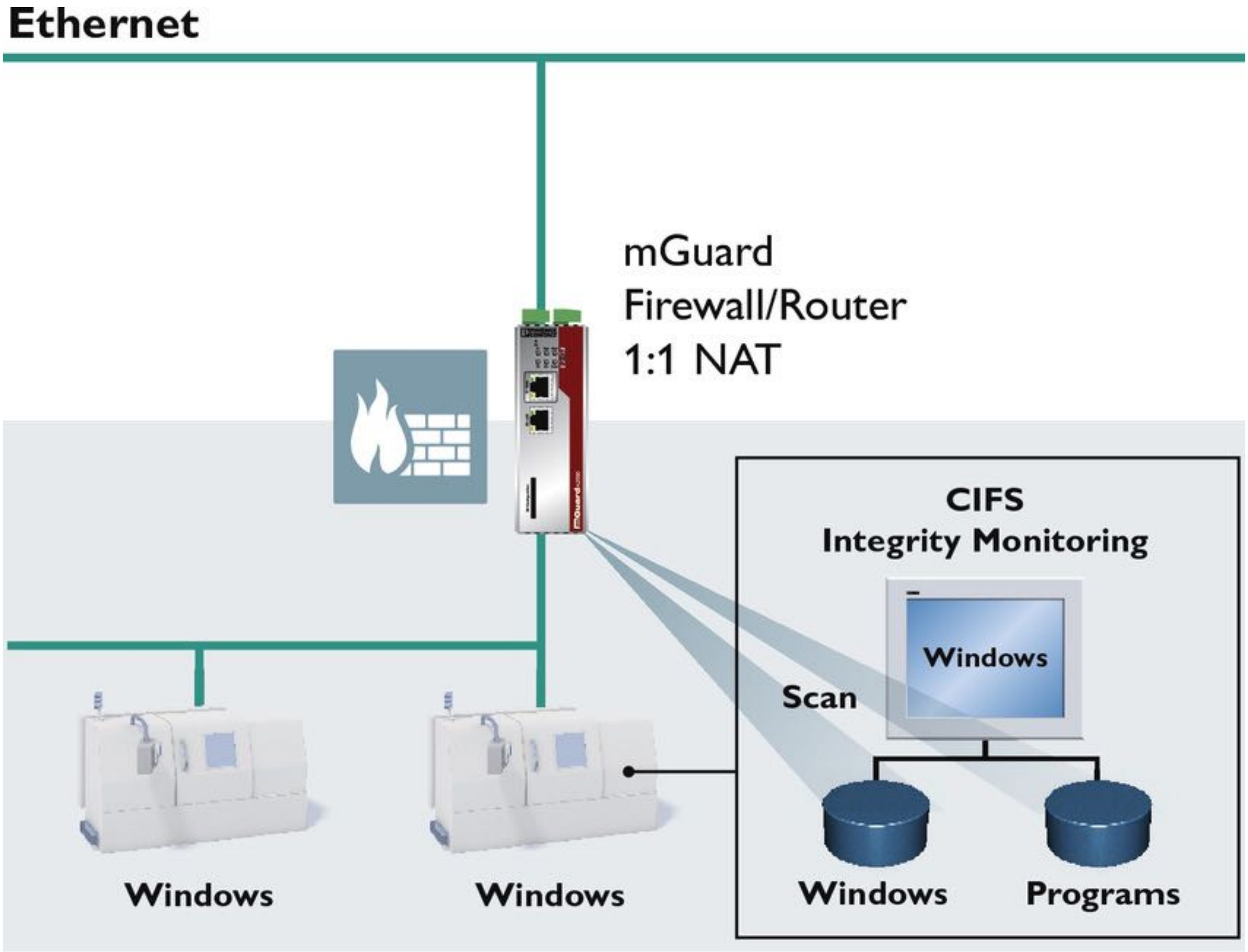
From a security standpoint, every open port constitutes a potential attack vector. Intruders and hackers search for these ports specifically, for example by using port scan, in order to penetrate the target system via the corresponding ports. Because industrial espionage and sabotage are constantly gaining ground, the security of OPC applications has become increasingly important. Furthermore, the potential benefits of an NAT application (Network Address Translation) can no longer be enjoyed if OPC is used in the application. The benefits of NAT or 1:1 NAT include:

- Reduced complexity due to a matching-part strategy for automation components.
- Reduced time and costs by avoiding individual configurations and the resulting expenditure for testing.
- Easier troubleshooting, as devices can be exchanged between different machines.
- Warranty is not invalidated when changes are made to the machine.
- Restrictive use of IP addresses.

The user cannot benefit from the advantages listed above because the ports used by OPC are specified in the header of a data telegram, as well as in the payload. When the NAT function changes a telegram header, the information in the header and payload becomes inconsistent and data transfer is interrupted.

Connection tracking function

The problems and security risks specified above can be resolved by using FL MGuard with the new OPC inspector. A deep packet inspection for OPC Classic analyzes the transmitted packet



SOURCE: PHOENIX CONTACT

The CIM principle (CIFS Integrity Monitoring) provides anti-virus protection suitable for the industrial environment.

and changes it as required. The configuration can be modified to specify that only OPC packets may be sent using OPC Classic port 135. The deep packet inspection reliably recognizes TCP ports that have been handled during the first connection opened between the participants.

In addition, the firewall opens the respective ports and releases them for OPC communication. If no OPC packets are dispatched via the ports in question within the configurable timeout, the ports are closed. Highly configurable firewall rules enable administrators to precisely define which clients can exchange data via OPC with which servers. This connection tracking function increases the security level considerably.

Decentralized protection of sections

Hackers use various approaches to access production plants. Stuxnet has shown, for example, that attacks are even possible within plants by means of compromised USB flash drives. This situation can be avoided by implementing the defense-in-depth concept, which is based on the ISA-99 standard.

The approach involves the segmentation of plant networks and the decentralized protection of individual segments. By deploying Security Appliance FL MGuard with OPC Inspector, it is now possible to implement the defense-in-depth concept in applications that use OPC Classic. For

High-access security in all application areas

The new generation of fanless industrial security routers offers reliable security and performance in a compact, rail-mountable metal enclosure. These devices have an SD card slot for easy device replacement as well as connections for inputs and outputs. Based on a hardened, embedded Linux operating system, the RS400x series features four coordinated security components:

- A bidirectional Stateful Inspection firewall with a conditional firewall.
- A DMZ port for another isolated network (variant).
- A highly secure VPN gateway.
- Optional protection against malware using CIFS Integrity Monitoring

RS200x-series devices have been designed for use as industrial VPN field routers, so they can be used directly on the machine or as central security components in distributed networks. They provide up to two parallel VPN tunnels, a simple two-click firewall, an integrated switch (variant), and flexible routing functions.

SOURCE: PHOENIX CONTACT

New security routers implement firewalls and CIM in parallel for maximum system protection.

individual segmenting of OPC-based networks, intelligent deep packet inspection by the FL MGuard OPC Inspector even allows the use of NAT processes such as masquerading and 1:1 NAT. This allows the user to profit from the aforementioned advantages offered by NAT processes.

Preconfigured firewall rules

Furthermore, the FL MGuard Security Appliances offer a conditional firewall that enables predefined toggling of firewall rules based on the situation. For the first time, this makes it possible for a firewall to switch between rules for various operating conditions by means of simple triggering events.

This function is useful because during production operation or maintenance and remote plant servicing it is necessary to allow or forbid certain connections. For example, it may be sensible to cut off all data traffic from or to the superordinate network when a control cabinet door is opened. This would simply and effectively isolate the service technician working locally on the system from the superordinate network. Another example would be allowing machine and system updates to be carried out only at suitable times, such as during regularly scheduled maintenance periods. At those times, an authorized person could use an accompanying key to switch the firewall over to allow access to the update server. This makes it unnecessary to change the configuration, thus saving time and money. At the same time, it also raises the security level, since spontaneous configuration changes are often prone to errors.

Recognizing malware

In the era of the Stuxnet worm, which is tailored to attack automation systems, dynamic monitoring of all Windows systems in the production environment significantly increases the level of security. That is why CIFS (Common Internet File System) Integrity Monitoring (CIM) provides anti-virus protection suitable for the industrial environment. The solution is available as an additional license for RS4004 devices in the FL MGuard product family. CIM, which works just like an anti-virus sensor but does not need to reload virus patterns, detects whether malware has infected a Windows system consisting of a control system, operator unit, and PC.

The use of firewalls and CIM in parallel provides maximum protection for systems previously thought unprotectable. This includes systems that use out-of-date operating systems and whose standard (software) settings were certified by the manufacturer or an official body, when a change would mean losing authorization from that body. Other systems cannot be equipped with a virus scanner in time-critical industrial applications or cannot download virus pattern updates because, for example, they lack a connection to the Internet.

*Ingo Hilgenkamp, Marketing Network Technology, **Phoenix Contact.***

600V Ethernet cables in industrial environments

Best practices for installation of 600V Ethernet cable in industrial environments begins with requirements of key regulatory groups, the National Electrical Code (NEC) and the Electrical Standard for Industrial Machinery (NFPA 79).

SOURCE: BELDEN

Industrial Ethernet cables must not only meet electrical safety standards, but also be crush resistant and resistant to electromagnetic and radio frequency interference.

COMMUNICATION AND NETWORK SYSTEMS, and especially Ethernet in the factories of the future, will no longer be separate from power and control systems. This trend is behind the growing need for all players – electrical engineers, control engineers and network engineers – to make electrical safety a consideration in network design and deployment.

As the lines blur between the use of Ethernet connectivity in office and industrial applications, many questions arise around best practices for installation of 600V Ethernet cable in manufacturing, mining, transportation and other industrial environments. Unlocking the mystery of when, where and what type of 600V Ethernet cable to install in an industrial setting must begin with an understanding of the standards or requirements of regulatory bodies for that media.

There are two main regulatory codes governing the design and implementation of connectivity media in industrial environments, both administered by the National Fire Protection Association: the National Electrical Code (NEC) and the Electrical Standard for Industrial Machinery (NFPA 79).

Which requirements to meet?

All systems used in industrial environments are required to meet the codes defined by the NEC, unless they fall under the scope of NFPA 79, which addresses the point of connection between the supply circuit conductors and the electrical equipment of machines. At the highest level, any field wiring installed and terminated at the manufacturing site is subject to the requirements of the NEC, while manufacturer supplied field wiring wholly inside OEM-supplied electrical or electronic equipment is subject to NFPA 79.

A few questions can be enormously helpful in determining which standard must be met:

- Is the wiring in question an integral component of a single machine, commencing at or beyond the point of connection of the supply circuit conductors? If yes, NFPA 79 may apply.
- Is the wiring in question an integral part of an industrial system, connecting component machines and supplied by the manufacturer, and properly supported and protected as an integral part of the system? If yes, then NFPA 79 may apply.
- Does the wiring leave the machine to connect to another machine or system? Is it not integral to the machine? If yes to either question, then NEC applies.
- Is the machinery in an area classified as hazardous? If yes, NEC would apply.

In any case other than those specific uses allowed under NFPA 79, NEC is likely to apply. Most importantly, when in doubt, the authority tasked with compliance is most likely to default to the broader requirements of the NEC.

Choosing the right rating

What rating should engineers use for Ethernet cables? There are several NEC standards to consider when designing communications

SOURCE: BELDEN

600V power cables provide an effective solution for demanding application environments.

networks in industrial environments:

- NEC Article 392 regulates cable tray installations, defining various wiring methods depending on cable type.
- NEC Article 336 dictates the wiring methods and allowed cable types for Ethernet cables in 600V environments.
- NEC Article 300(C) addresses wiring methods for conductors of different systems and governs the methods of determining the required ratings for the permitted cable types. Specifically, this article establishes the requirement that all conductors should have an insulation rating equal to at least the maximum circuit voltage applied to any conductor within the enclosure, cable, or raceway. This means that any cable installed in a cable tray including a 600V power cable must also be a 600V listed type under NEC.

In sum, only Type TC3 cables meet the standards defined in Articles 392, 336 and 300. The NEC does not recognize Appliance Wiring Material (AWM) cables outside of those that are manufacturer supplied components of equipment (excepted by NFPA 79 above), nor do Types PLTC, CM, CMG, CMR or CMP meet the standard for use in a 600V environment.

Beyond safety

First and foremost, the guiding principle in applying NFPA standards is safety. Also critical, especially when designing communications networks, are performance and reliability. When Ethernet cables were deployed in industrial environments using creative ways of routing cable, such as through conduits or as an attachment to pipes, the cables were out-of-the-way of equipment and other infrastructure.

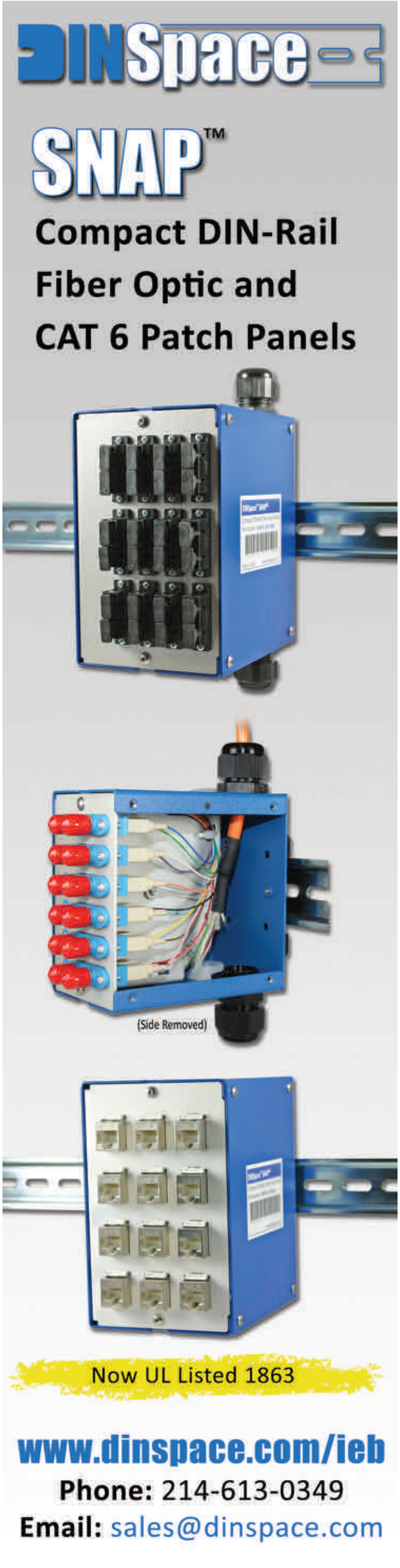
Now, cables must not only meet electrical safety standards, they must also be crush resistant and able to perform in environments subject to the presence of electromagnetic and radio frequency interference.

For enhanced reliability in industrial networks, 600V Ethernet cables should include:

- A thick thermoplastic jacket
- A foil and braid shield for high EMI/RFI immunity
- Oil and sunlight resistance
- Temperature tolerance from -40°C to 90°C
- Flame retardance as required by the NEC
- Technology that can eliminate gaps between conductor pairs

Cabling in industrial environments can be difficult to install and require extra protection and resilience. By starting with a grounded understanding of the electrical safety regulations and standards, network engineers and their colleagues in electrical and control engineering can design and deploy the cabling required for a communications network that both passes inspections and performs reliably in rugged conditions.

Peter Cox is director of global industrial projects at ***Belden****.*



Improving manufacturing power quality in the age of IoT

Real-time power quality monitoring is becoming the first building block of Smart Grids. Bringing monitoring data back to operational engineers in real time provides tools that can substantially improve power quality, make proactive decisions and reduce downtime.

THE INTERNET OF THINGS (IoT) and Industry 4.0 will impact many aspects of industry, and offer new and more efficient ways to solve old problems. One of those old problems is poor power quality in the manufacturing process. The continuous manufacturing process is made up of many different systems: PLCs, relays, power supplies, contactors, and motors. Though each component of the system accomplishes a different part of the overall task, they have something in common: they are all connected to facility power.

Poor power quality in manufacturing facilities causes equipment failures and directly results in costly downtime. According to Power Sensors Ltd. in Alameda, CA, the annual cost of power quality-related wastage in the U.S. is currently estimated at over $100 billion. How can we efficiently understand, identify, and resolve this costly problem?

What is Power Quality?

Power quality is the ability of a power distribution system to deliver power within the operating tolerances of the equipment using that power. From a PLC to a PC, chillers to VFDs, all systems must receive power within the manufacturer’s specifications in order to function as intended. For instance, on Opto 22 I/O systems, a SNAP PAC I/O processing unit must receive 5 VDC for the I/O to operate as intended. Power quality provides a level of performance and reliability that impacts both safety and economics in the organization.

A well-designed manufacturing system matches power system performance and load requirements to minimize problems. However, even an ideally designed system is susceptible to unforeseen and uncontrollable problems introduced by poor power quality.

Problems resulting from poor power quality can start off as a small disturbance in production. A PC may blue-screen during a manufacturing run. Or a PLC may trip an alarm and send a notification to an operator. These small interruptions in production, while certainly a nuisance to manufacturing operators, are often easily recoverable. But over time, disturbances can lead to overall system degradation. A microprocessor or memory control unit inside a device may become damaged, which can lead to unexpected behavior and often results in the system breaking down, as paths inside the microprocessor are degraded to the point that they’re no longer passing data or electricity.

SOURCE: OPTO 22

Key data such as load monitoring, energy usage, and power quality can be sent right to an authorized operator’s smartphone, tablet, or PC for analysis or action.

Common Power Quality Problems

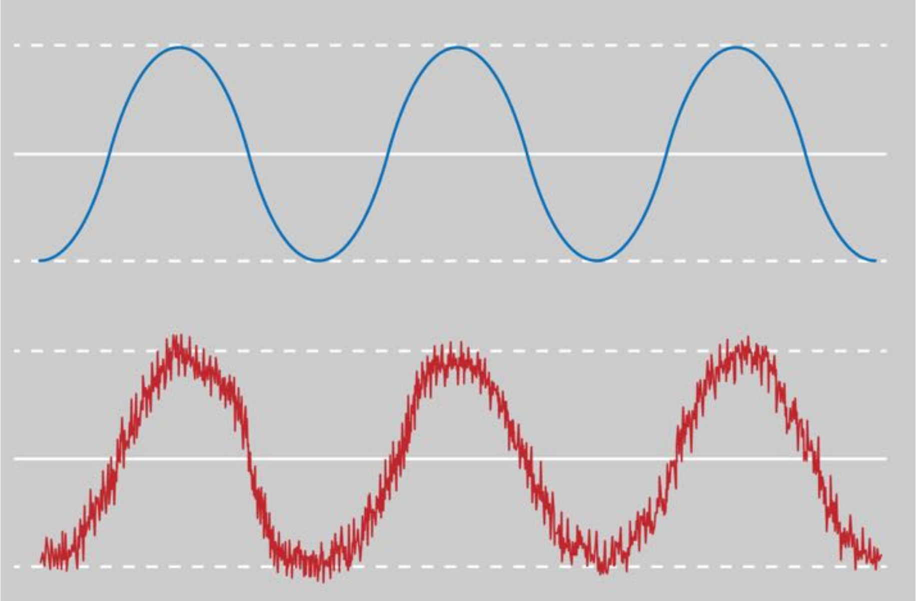
When you analyze the voltage and current sine waves applied to equipment from a power distribution system, the wave should be smooth, with no distortions, notches, or jagged points in the curve. Poor power quality comes in many forms: voltage dips or sags, voltage swells or surges, transients, and harmonics.

Voltage dips or sags are the most common and account for almost 80 percent of all power quality problems. A dip or sag occurs when the system voltage drops to 90 percent or less of nominal system voltage for a half-cycle to one minute. Some symptoms industrial engineers may encounter with voltage dips or sags include incandescent lights dimming (if the dip lasts more than three cycles), computers locking up, sporadic shutdown of sensitive electronic equipment such as Windows-based HMIs, relay control problems, and data loss.

Typically these problems are the result of sudden increases in current requirements in the plant, such as large motors starting up. To help pinpoint voltage dips and sags, the load should be monitored where the symptoms first occur and then traced further upstream until the source is located.

Voltage swells or surges occur only about half as often as dips but can cause much more damage. Voltage swells can occur slowly over time, breaking down system components and causing equipment failure. Sudden line-to-ground faults on a single-phase line may be the culprit. This type of fault can cause the voltage to swell suddenly on the two non-faulted phases. Large plant loads dropping offline or power capacitor switching can also cause voltage surges. For voltage swells, monitor voltage trends on feeders and branch circuits to equipment and watch for line-to-ground faults on a single-phase line. To reduce voltage swells and surges an uninterruptable power supply (UPS) and surge protector can be implemented.

Transient voltages, sometimes referred to as spikes, are substantial increases in voltage that occur for only microseconds. Typical causes of transients are lightning strikes, motor load switching, capacitor switching, and reenergizing systems after a power failure. In many cases the efficiency of equipment is affected when a transient occurs. Often times transient voltages cause degradation of integrated circuits within devices leading to device failure over time. In motors, transient voltages can cause higher running temperatures in the motor. Transients can also interrupt the normal timing of a motor resulting in micro-jogging which produces motor vibration, noise and excessive heat. In lighting systems transient voltages cause early failure in all types of lighting. A common indication of transient activity is the premature appearance of black rings at the end of fluorescent tubes. A UPS and surge



SOURCE: OPTO 22

Poor power quality comes in many forms: voltage dips or sags, voltage swells or surges, transients, and harmonics. More IoT connections will help record power data locally, or push it to the cloud for immediate or further analysis.

protector can also be used to prevent problems related to transient voltages.

Harmonics are currents and voltages where the frequency is typically an integer multiple of the fundamental frequency. These unwanted frequencies in the distribution system can cause a number of symptoms, including overheating neutral lines and transformers supplying the circuit. Harmonics can also cause electrical equipment attached to the circuit to report false alarms, and data loss may occur. Harmonics-related issues are often the cause of mysterious random problems in the factory or on the plant floor.

Power quality problems

Traditionally power quality problems were diagnosed and pinpointed using a power quality analysis tool or meter. There are many types of meters available on the market today that typically monitor parameters including current, voltage, phase relationship between waveforms, frequency, and many others.

One problem with traditional power analysis tools is that they are typically expensive. Also, the overall approach to solving power quality problems using this type of meter is to wait until a problem has occurred, connect the meter to the power lines, and wait for the problem to occur again. Obviously this is not the most efficient way to pinpoint and resolve a power quality problem, as waiting for another power quality event to take place may lead to additional equipment failure and increased production downtime.

IoT power monitoring

As more and more devices are connected to the Internet of Things, real-time data and analytics become more accessible in industrial applications. At the same time, the size and cost of power meters and the cost of enabling IoT have dropped significantly over the past decade. As a result, power quality analysis can be conducted in new and more efficient ways.

In the past, industrial engineers relied on one large and expensive power meter to troubleshoot after a problem had taken place. IoT has changed this approach. Today, smaller and lower-cost power meters are available, for example the PQube 3 power meter from Power Sensors Limited. These smaller, less expensive power sensors can be connected to an Ethernet network to provide real-time monitoring of power distribution. Rather than deploying a power quality meter after a problem occurs, these power meters allow industrial engineers to place many power sensors throughout their distribution system, providing more detail on each circuit.

The increasing availability and lower cost of IoT connections helps even more. Once meters are connected to an Ethernet network, they can record power data locally or push it up to the cloud for immediate and later analysis. Key data such as load monitoring, energy usage, and power quality can be sent right to an authorized operator's smartphone, tablet, or PC for analysis or action, using products like groov from Opto 22.

Real-time monitoring is the first building block of Smart Grids. Now we have the tools to transform electrical networks to make them fit and stable going forward. By bringing this monitoring data back to operational engineers in real time, we can substantially improve power quality, make decisions proactively rather than reactively, and reduce equipment failures and costly downtime.

Matt Newton is Director of Technical Marketing for ***Opto 22****.*

Advanced networking for power generation systems

There is a need for new networking technologies to meet the needs of the ever increasing complexity of industrial applications such as power generation. Power plants have a set of systems that must operate in harmony, and require a complex array of communications systems that need to support real-time control.

Power plants are not isolated control islands; they must exist within the broader context of the power grid. Wide area communications is essential to their operation. This drives complexity into the networks both outside the plant as well as inside the plant. Operators seek to optimize plant operations and manage multiple plants as an optimized fleet, equipment suppliers offer more cloud based services to assist their customers, this drives the market to higher levels of network complexity as well as the need for the networks to reach equipment deep within the plant as well as across plants.

AVnu Alliance is a trade group pulling together the industrial ecosystem to assure that new networking technologies will provide benefits to the industrial markets. This article explores how power generation applications can benefit from a simplification of networking architecture with the added functionality to support the IoT.

Introduction

Large power plants consist of a collection of control and protection systems that must operate in harmony. This requires a complex array of isolated communications systems to achieve the types of performance and reliability guarantees required to support real time control. A large plant can have six or more network levels in the hierarchy with multiple networks at each level.

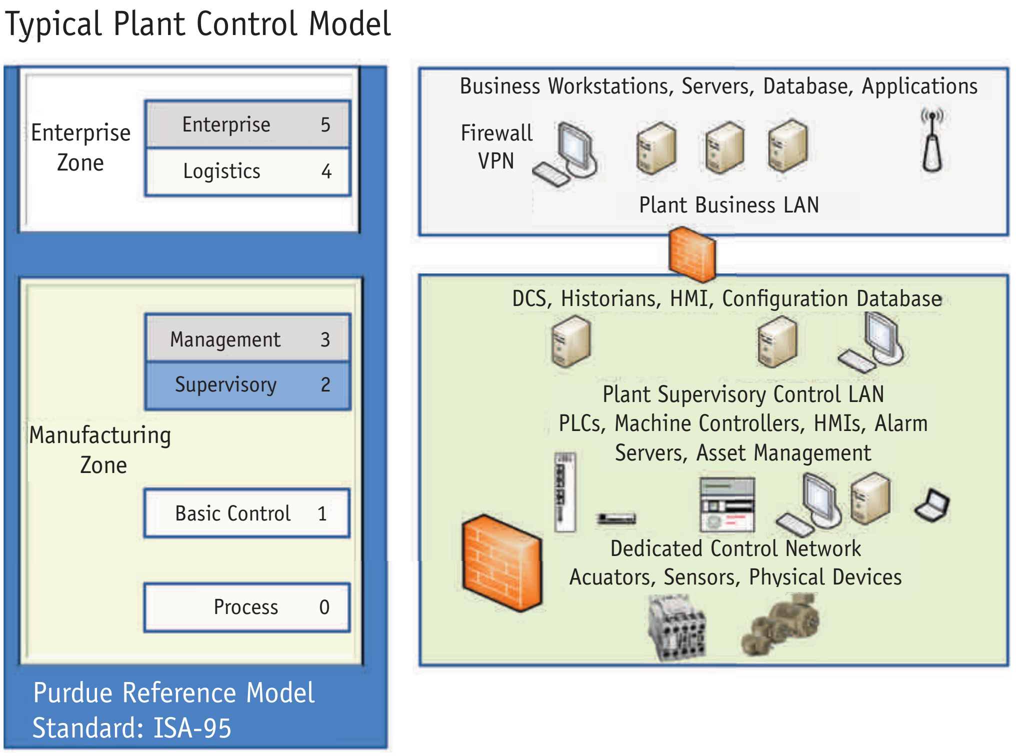
The illustration below shows just a small portion of the networks that can be within a power generation plant. Within each power plant there is:

- Business and operations center or back office.
- Supervisory control for the plant itself.
- Power generation unit control for each power island including control of auxiliary systems required to operate the machine.
- High speed control for the turbines and generators.
- Specialty I/O networks that handle unique sensors and actuators.
- Electrical protection and power distribution systems that protect the equipment and integrate power delivery with the grid.
- Machine maintenance and diagnostics.
- In addition, new applications are being added all the time.

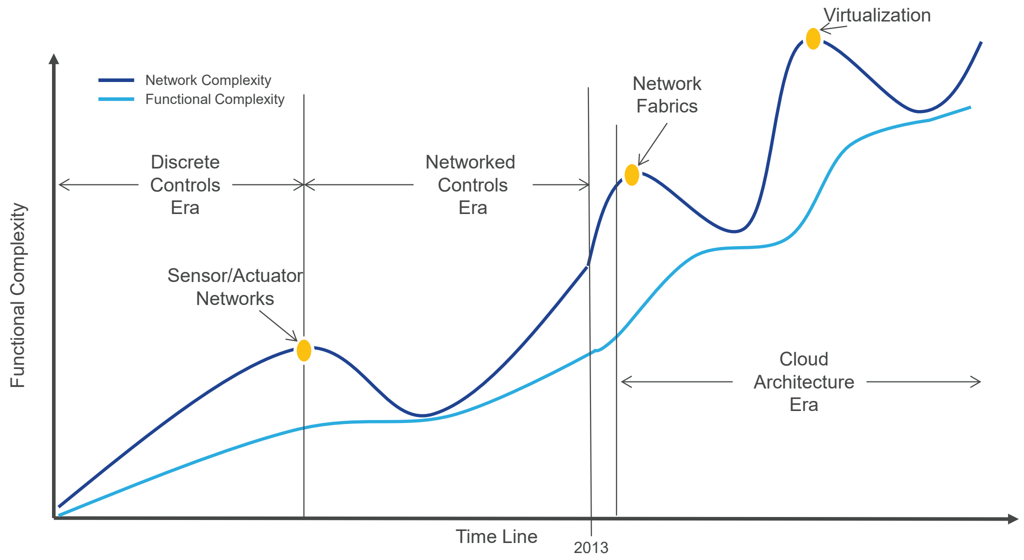
This makes for a very complex and dynamic network infrastructure where the maintenance needs are high and reliability is critical. What is described is a simple single cycle plant but in today's world many large plants are combined cycle meaning that not only is power being generated using gas turbines, but also steam turbines are used to recover the heat from the gas turbines to further increase the thermal efficiency of the plants. The system then grows in complexity adding more and more networks and applications. Lastly, consider the case where power generation is combined with another process application such as a petrochemical refinery or desalination plant and the system grows even larger. The number of networks to manage and the various skill levels required to maintain those network becomes very large.

Today network complexity is managed through application isolation, each application is given its own private network. In the cases where control is not critical, VLAN technology can be used to reduce the number of physical networks. Network architecture loosely follows the ISA95 reference model.This design methodology has worked well in the past but is now quickly nearing the end of its useful life. With the addition of new applications to support the ever expanding need for new cloud based services to support plant and equipment optimization and the increasing need for critical infrastructure security within the plant, current networking technologies don't scale well.

Today's operating plants have fewer and fewer maintenance engineers. It is not surprising to walk into a large operating power plant with multiple power islands and only find two operators and two maintenance engineers. The need to automate the equipment maintenance processes and provide the day to day optimization schemes is an area where modern plant operators are demanding more from their suppliers.


Typical Plant Control Model
Enterprise Zone
Enterprise 5
Logistics 4
Manufacturing Zone
Management 3
Supervisory 2
Basic Control 1
Process 0
Purdue Reference Model Standard: ISA-95
Business Workstations, Servers, Database, Applications
Firewall VPN
Plant Business LAN
DCS, Historians, HMI, Configuration Database
Plant Supervisory Control LAN
PLCs, Machine Controllers, HMIs, Alarm Servers, Asset Management
Dedicated Control Network
Acuators, Sensors, Physical Devices

ISA 95 Reference Model



SOURCE: GENERAL ELECTRIC

Control systems in all market sectors are perpetually increasing in functional complexity. But while communications complexity limits functional capabilities, advanced communications architectures are enabling advances in controls.

Attributes of a Control Network

In this new environment, control networks must be reliable and able to deliver information within a guaranteed amount of time under all loading conditions (guaranteed latency). They must be resilient and maintainable, able to survive one or more failures and operate as if a failure never occurred. They must be flexible and adapt to changes in plant configurations adding new applications, and they must be secure. In the age of the Industrial Internet reliance on physical security at the perimeter is not enough, the emerging cloud based services as well as global asset management require that there be connectivity everywhere and this places more stringent security requirements on the network.

It is rare today that a single supplier will provide all the equipment and applications within a plant. Interoperability and coexistence between applications operating on the same network is critical.

Combining critical control applications on a single network today and guaranteeing Quality of Service (QoS) can only be done by isolating traffic and substantial testing. Switched Ethernet can suffer from congestion losses if traffic flows are not controlled and the traffic itself is not engineered. Updates to standard Ethernet such as TSN provide mechanisms for mathematically provable latency and delivery guarantees without the need to do exhaustive testing. This can greatly reduce system requisition engineering and network testing and qualification time. Network hot standby redundancy is a feature which provides reliability and availability.

Traffic scheduling along with Virtual Local area Network (VLAN) technology provides traffic isolation on a fine grained basis. This allows the plant operator to add new applications at any to the network and be assured that currently running applications will not see any degradation in performance time as long as sufficient resources exist. He will also know beforehand if there is a chance that his network will become overloaded. If a new application needs specific QoS guarantees and they are not available the operator will be informed immediately and not find out later after the application fails on deployment.

Cloud Based Services & the Industrial Internet

Large scale Industrial Equipment Providers are now able to offer more plant and asset management and optimization services given the amount of computational power that exists within the cloud. To allow this to occur, the security barrier needs to extend much further down into the plant equipment than it has historically.

Virtualization at the controller level, hypervisors, and multicore processors provide the avenue for a whole new generation of control architectures which can be remotely managed in a secure way. Asset management in the power plant will be much more highly automated, product updates and upgrades will be faster and more transparent. TSN can provide the secure traffic isolation needed to allow cloud based services to communicate directly to the edge on the plant floor in this new generation of control platforms.

Cloud Based Services & the Industrial Internet

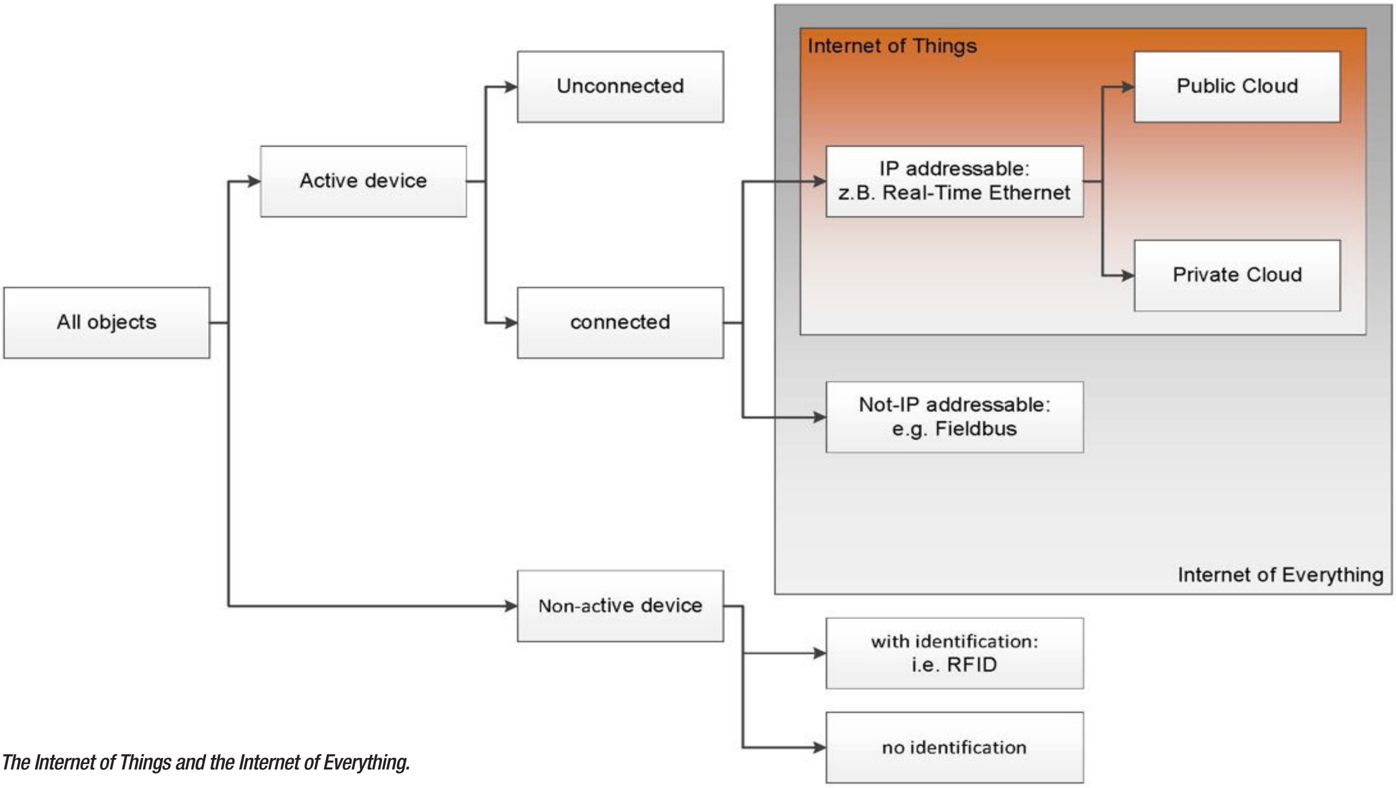
Many industrial application protocols have already been adapted to standard Ethernet. This does not mean they can coexist on the same network. For the network to enforce coexistence then all network devices must be compatible. This level of compatibility requires interoperability specifications and certification testing much as the WiFi alliance has done for 802.11 and all its variants.

Technology report by Dan Sexton, ***General Electric Research Labs.***

While others think about the IIoT
... we are already there.
embeddedworld2016
Hall 1, Stand 1-110
Networks and computers for a smarter industry.
• Powerful computers designed for your needs
• Secure and reliable networks – anywhere, anytime
• Vertical integration from SCADA to field device
Moxa in the middle.
www.moxa.com
MOXA
Reliable Networks Sincere Service

IoT & Industry 4.0 impact on traditional communications

The Internet of Things is considered to be a strategic focus for most companies but communications technology is changing and evolving. The key is development of cyber physical systems (CPS) that address both the challenges and opportunities that the IoT offers.



SOURCE: HILSCHER

The Internet of Things and the Internet of Everything.

THE INTERNET OF THINGS (IoT) originated in consumer markets where the added-value for producers and end-users was quickly seen as significant. In 2014, the potential in industrial markets was recognized and the term "Industrial Internet of Things" (IIoT) was coined. Industry began to have a significant influence on the design of IoT technologies and standardization. In North America, the Industrial Internet Consortium (IIC) became one of the main organizations defining how IoT fits into modern life.

The rise of IoT has also given substance to the idea of the "Internet of Everything" (IoE), in which not only connectable "things" are employed but many other elements too, even objects that are not (yet) equipped with their own intelligence or identification. The term "Industrial Internet" has also appeared, referring to the industrial use of the Internet. Terms like "big data", "the cloud" and "cloud applications" are also heard in the IoT context.

Real-time Ethernet systems and traditional fieldbus networks will continue to be used in the IoT context. Industrial Ethernet can be easily incorporated into IoT. However, fieldbuses cannot be connected directly with cloud technologies although they can be considered part of the Internet of Everything.

In industrial markets, particularly in Europe, Industry 4.0 has been a primary focus for industrial applications, with the optimization of production and sales being a key objective. Industry 4.0 is named for its historical relationship to the first industrial revolution.

The concepts on which IIoT and Industry 4.0 are based come from two domains: industrial manufacturing and information technology. For the purposes of this article, the "Internet of Things" is considered to be a comprehensive term covering IIoT, Industry 4.0 and Industrial Internet. "Industry 4.0" is used specifically whenever regional references to the European initiative are highlighted.

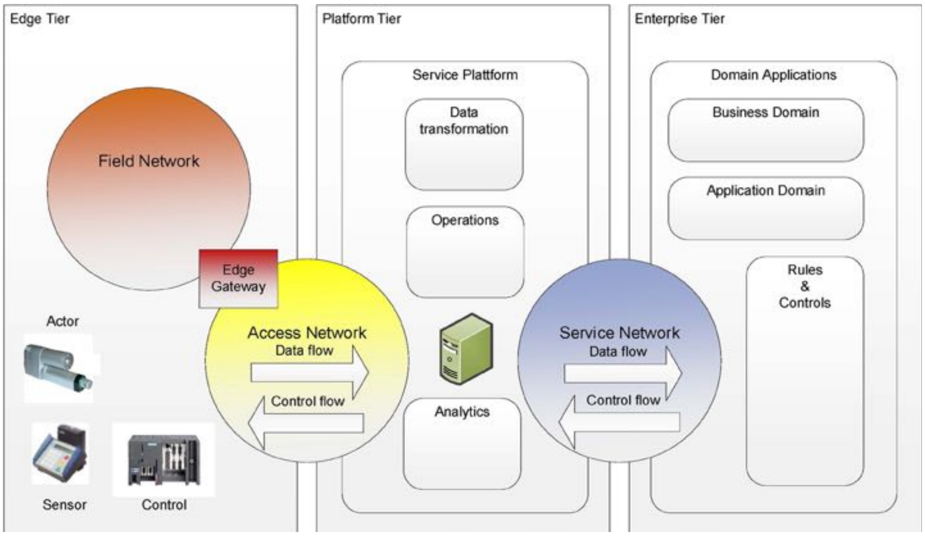
Perspective for the future

The resources being employed by industry in pursuing the IoT goal are impressive and too large to be ignored. Initiatives range from pure marketing programs, through prototyping applications (i.e. "test beds"), up to what are perceived to be "real" IoT products. Of course a question arises immediately: what is a "real" IoT product? One interpretation is that an IoT-enabled product fulfills or supports the following functionality:

- Self-organization
- Semantics
- Cyber-physical system
- Cloud-based applications

For most companies IoT is considered strategically critical. From a business perspective, new contract models in the field of capital goods have been developed. As an example, for the operation of aircraft engines a contract model based on usage and operating costs has been deployed. Prototype installations have shown tangible benefits.

Communications technology is changing and evolving. OPC UA, published in 2010 as IEC 62541, is being expanded to include a publish/subscribe mechanism to support de-centralized communications initiated at the field level. In the same context, real-time capability is being supported by the



SOURCE: HILSCHER

Communication in the layer model of the IIC reference architecture.

introduction of "Time Sensitive Networking" (TSN), a collection of new standards from the IEEE 802 groups based on streaming from the audio and video fields coupled with high-precision timing techniques from industry that move us towards a standardized real-time Ethernet concept.

Since return on investment (ROI) is not yet clear, cooperation is seen as necessary. The integration of suitable technologies into product lines requires cooperation starting with product development. Such cooperation is being continued into the marketing of products, opening up new customer segments and market areas. Competitive pressures play their part. There is global competition in the field of digitization at production and consumer level, and cooperation is needed in order for companies not to fall behind.

Of vital significance for communication technologies is the convergence of classic "information technology" and the production world we are familiar with.

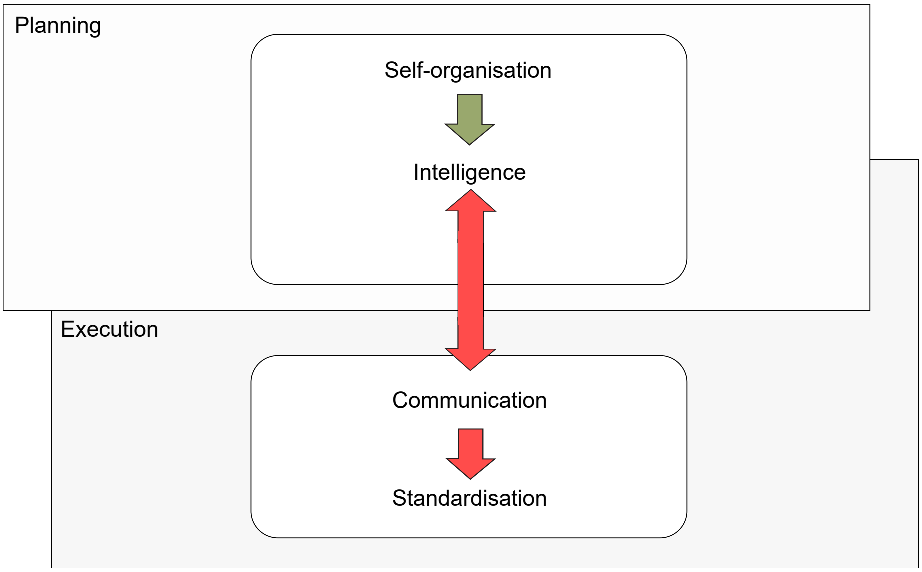
IoT in different countries

Germany: The Industry 4.0 initiative of the German Federal Government was recently relaunched as "Platform Industry 4.0". In addition to working groups addressing topics such as reference architectures, security and development and innovation, there are groups dealing with legal issues and the impact on employees. Conceptually, German activities follow the bottom-up approach used in earlier standardization activities. Work on concepts and the development of testbeds are the main focus. The German initiative also has a European context. Using EU funding, elements such as the 4-level architecture for data semantics and cyber-physical systems have been elaborated on. While the Industry 4.0 initiative is essentially an industrial manufacturing program, it is supplemented by initiatives focused on end users as well as new business opportunities.

North America: The Industrial Internet Consortium (IIC) has made a significant step towards a practical implementation of IoT in industrial applications with its recently-published reference architecture. The focus is now on the overall architecture of systems and components as well as on functional approaches. Applications in industrial environments are given emphasis. The IIC has taken the concept and defines it as follows: "The Industrial Internet is an Internet of machines, computers and people that permits intelligent industrial applications by using advanced data analysis in order to change the business process."

In the IIC document, the field network includes sensors, actuators, machines and control systems, and those components that enable access as "edge devices". The access layer provides access to the information at the control level. This is about the classic tasks of data management including production control as well as the analysis of information for optimizing the field level. The concept allows for edge gateways that handle the tasks of data selection and concentration, as well as the scalability of production systems from a communication point of view.

These can be implemented as a corporate network, as a private network inside the Internet, or even as 4G/5G networks. The access layer also allows the provision of information for the enterprise level where the classical domains of corporate management are located. The network structure is designed in triplicate for each access layer. The field network uses classic real-time Ethernet or fieldbus communication to link control systems, machinery, equipment and the sensors/actuators of production processes. The service network connects access layers at enterprise level with the control level. It can be implemented as a private network inside a corporate network or by using the Internet.



SOURCE: HILSCHER

Conceptual requirements of self-organization.

	Layer	Aim	Objects	Solutions
1	Technical	Technically secure data transfer	Signals	Protocols of data transfer
2	Syntactic	Processing of received data	Data	Standardized data exchange formats, e.g. XML
3	Semantic	Processing and interpretation of received data	Information	Common directories, data keys, ontologies
4	Organizational	Automatic linkage of processes among different systems	Processes (workflow)	Architectural models, standardized process elements

SOURCE: HILSCHER

Semantic four-layer model.

Japan: Several major companies have recently launched their "Industrial Value Chain Initiative". This new forum is intended as an alternative to the German Industry 4.0 initiative. The primary focus is on standardization as well as efforts to establish Japanese Industrial standards internationally. IVI is one of several IoT initiatives in Japan but involves market-leading corporations.

China: "Made in China 2025" is the Chinese government's 10-year plan to take their domestic manufacturing industries to the top. The Industry 4.0 initiative has received much attention in China and is considered as a next step for "Made in China 2025". The 10-year plan includes key sectors such as "new information technologies" and "high-end NC controllers and robots," a clear indication of the emphasis on industrial applications. Existing real-time Ethernet standards are already recognized as Chinese standards, but it remains to be seen to what extent a Chinese-driven communication standard will be developed as part of the 10-year plan.

IoT and Industry 4.0?

IoT is not about individual technologies; it involves the interaction of many technologies. A central tenet is the self-organization of production. The workpiece itself instructs individual work stations to carry out the required manufacturing steps, based on their own information and intelligence. Industry 4.0 even proposes the idea of "Batch Size 1".

Self-organization requires a much higher intelligence at field level in order to allow this level of production control, in turn requiring advanced communication capabilities that go far beyond simple data transfer.

There is interaction between local intelligence and functionality which communications needs to deliver. Intelligent algorithms only make sense if relevant information is available. In the future, information must not only contain data, it must also reflect the semantic content.

Data on the first layer (for example, a 32-bit value that was added to the workpiece in a previous step) are already represented by existing protocols. However, interpretation of that data takes place at the control level (e.g., "the 32-bit value represents 24°C"). For self-organization, additional semantic information such as the origin and location of the signal must be transmitted starting at level 1 (e.g., in the form of the surface temperature of the workpiece, with clear identification). Future extensions to include process information at Level 4 will be essential for implementing the idea of self-organization in production (e.g., "Do not apply any surface coating if the surface temperature is greater than 30°C").

ICPS is one innovation

A cyber-physical system (CPS) consists of an electromechanical (mechatronic) system with related software components that describe and control its essential features and characteristics, and are also able to communicate via a network. This means that a CPS represents a combination of communications, computing and control.

Interestingly, in this connection, there is the hint that the term "cyber" can be understood on the one hand as a word-forming element with the meaning of "referring to the virtual world of illusion generated by computers" (as in the term "cyberspace"), and on the other hand as an abbreviation of the English word "cybernetics", referring to the "science of control and regulation of processes".

The use of CPS in manufacturing automation raises some important questions that are important to consider:

- Does CPS change the requirements for industrial communication regarding form factors or real-time capability? Towards semantics as a basis for self-organization? Towards the general communication standard for CPS-based automation?

- How does CPS change the classic automation pyramid in particular due to the proportion of "processing"? Towards networked and decentralized structures? How critical are the security requirements for the introduction of CPS? Will safety become the most critical aspect for introduction?

A PROFIBUS description file (effectively a software component describing a device) can already be viewed in this sense. However, the CPS is characterized by the additional ability to communicate and by providing interfaces to a communication infrastructure.

CPSs are an important component of IoT because they open up new manufacturing possibilities by connecting embedded systems with the opportunities presented by global networks.

Cloud Technology

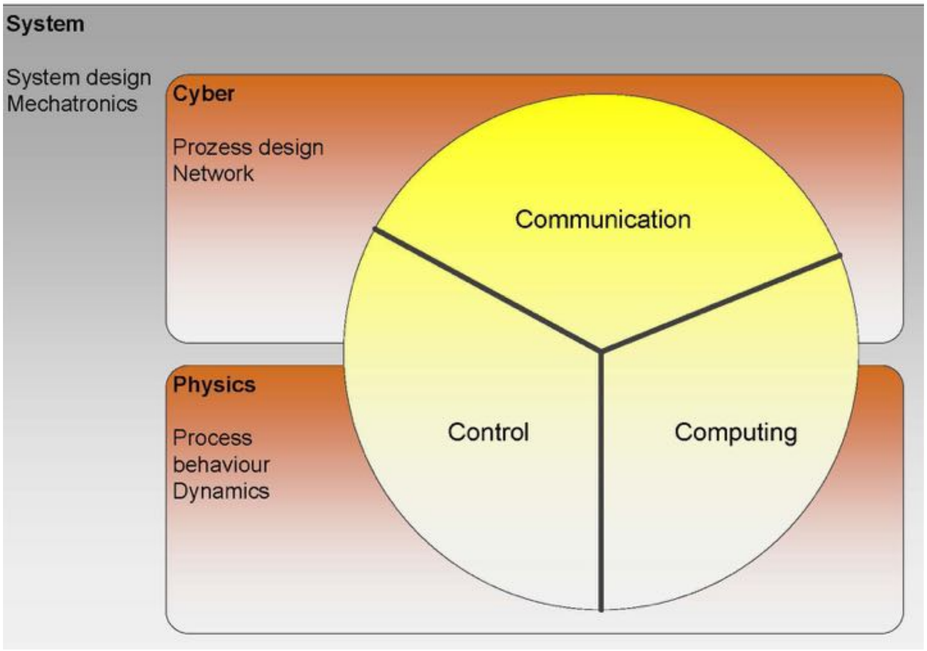
From a business perspective cloud computing can be seen as a business model that dynamically provides IT resources "as a service" and charges for its use using flexible payment models. Companies are able to use cloud computing to reduce long-term capital IT expenditures. From an industrial viewpoint, cloud technology can be used in the non-public realm without any Internet connection, or through a protected Internet connection. The major use cases will be applications that use "big data".

New communication technologies

TSN will see use in industrial communication because the OPC Foundation will support its real-time capability as part of OPC UA. In addition, the automotive industry is presently exploring the capabilities of TSN in connection with the use of Ethernet for on-board communications. These examples of the use of existing technologies in mainstream communications could continue. As part of the efforts of the IIC, standards in the field of server to server communication, or financial transactions with respect to their use in industrial applications, are also being tested.

The challenges of IoT

ROI is not really predictable. The up-front costs for products in development are initially higher because current technology needs to be enriched with additional functionality. This is not only about the implementation of new protocols but also about new requirements for the access layers at control and enterprise levels. System operators need to significantly expand their competence in fields such as engineering, and particularly maintenance. The actual benefits and added value of IoT will be determined by new business opportunities. Of interest are cloud-based applications that provide users with benefits such as increased availability through better maintenance.



SOURCE: HILSCHER

Communication as part of Cyber-Physical Systems.

Dependence between local intelligence and required information. The relationship between the required intelligence and necessary information will call for close cooperation between manufacturers of field devices and the communications providers. What information is needed by the intelligent device, and what kind of application is required to work with such information?

Systems and standards battles. Standardization has already proven to be a stumbling block in the implementation of Industry 4.0 related concepts. Currently, neither IIC nor Platform Industry 4.0 sees any reason to recommend or demand specific standards. In the field of cloud infrastructures there is a trend to proprietary positioning because that is where significant "value" is generated. The potential exists to experience a clash of cloud architectures comparable to battles between communication protocols.

Change of the automation pyramid. The consistent implementation of IoT concepts requires unbundling or simplifying automation structures. Interoperability between devices and systems from different manufacturers is both a requirement and a challenge.

The opportunities for IoT

Profitable application cases. In the U.S., Asia and Europe, applications in the field of predictive maintenance and condition monitoring are gaining popularity. Today, machine control systems are already equipped with technology to achieve savings in the field of maintenance, as well as reductions of repair costs for operators and suppliers.

Generating value in the cloud. The expansion of devices at the field level and the use of field network components and access components such as edge gateways only need additional investment – in other words, we are in a situation where the infrastructure serves as a door opener. Users will realize actual benefits through applications that are only possible in the cloud. CPS will be able to implement new and intelligent functions through cloud applications that share cloud-based data and field-level data.

Controlled migration. For users, gradual introduction is possible because CPS can be integrated into existing automation pyramids. Even existing field devices can be integrated provided they have a suitable communication interface. New business models are already in use as a development of XaaS ("X as-a-service") in the form of "pay per use" models.

Support of standards. Interoperability between systems and products is only made possible through common standards. An agreement on common communication standards is the opportunity to maximize the benefits of IoT at all levels of the semantic four-layer model. The advantage of the model is the fact that standardization can be carried out gradually, starting with the lowest level.

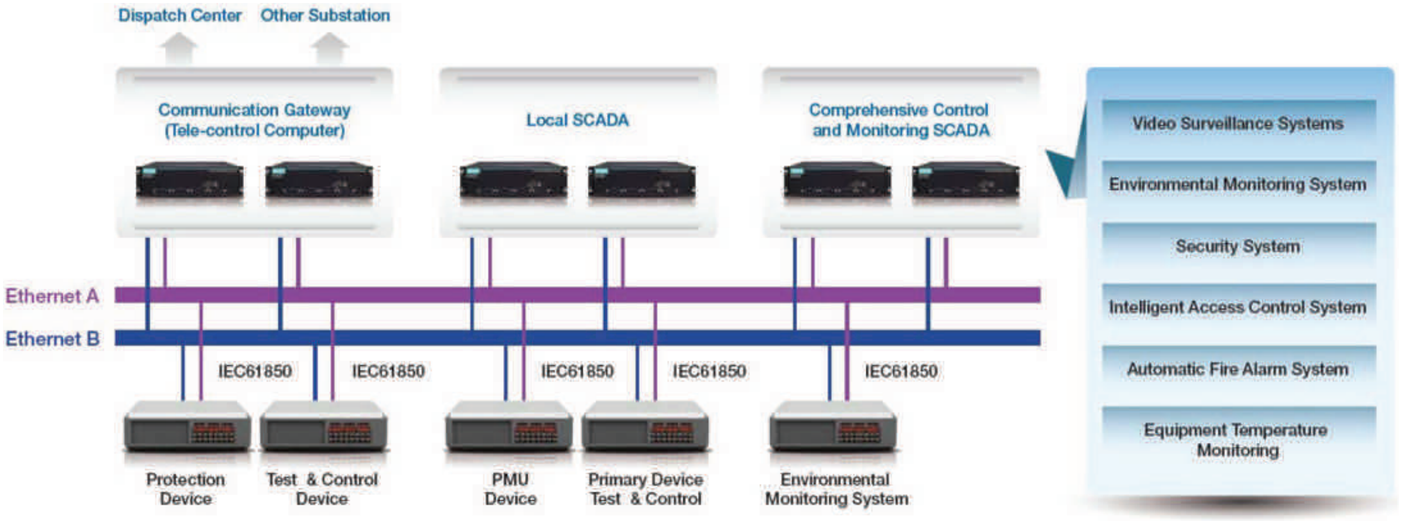
The outlook for IoT

The use of the Internet of Things has begun. Some successful business models have been developed and new strategies such as CPS are evolving. TSN and semantic models are approaching standardization for industrial use. In various countries, preventive maintenance and condition monitoring has proven to be a key application. Once continuous vertical integration is realized from the field level to the cloud, additional applications will be implemented on a broad scale.

Armin Pühringer, ***Hilscher Gesellschaft für System Automation mbH.***

System redundancy in power substation retrofits

Implementing system redundancy for retrofitting power substations can be achieved using either a decentralized approach or a centralized approach. But running multiple operating systems and multiple applications on the same physical server may reduce costs.


Dispatch Center
Other Substation
Communication Gateway (Tele-control Computer)
Local SCADA
Comprehensive Control and Monitoring SCADA
Video Surveillance Systems
Environmental Monitoring System
Security System
Intelligent Access Control System
Automatic Fire Alarm System
Equipment Temperature Monitoring
Ethernet A
Ethernet B
IEC61850
IEC61850
IEC61850
IEC61850
IEC61850
Protection Device
Test & Control Device
PMU Device
Primary Device Test & Control
Environmental Monitoring System

SOURCE: MOXA

A key trend with substation automation is to collect and integrate data from supervisory subsystems into a powerful and secure control system.

TO REDUCE POWER OUTAGES, power grids around the world are increasingly retrofitting legacy power substations to be intelligent and more highly automated. Due to the mission-critical nature of power substations, system redundancy is of the utmost importance to retrofit legacy substations.

System redundancy in power substation retrofitting applications can be deployed using either decentralized or centralized system architectures. In a decentralized architecture, network redundancy is ensured by multiple physical computers where each computer only runs a single operating system or application. In a centralized architecture, on the other hand, network redundancy is achieved by running multiple operating systems and multiple applications on the same physical server (i.e., server virtualization).

Although both decentralized and centralized architectures can be used effectively to provide retrofitted power substations with system redundancy, system integrators still need to be mindful of protecting against a number of control and management issues.

System redundancy Management

Since replacing existing legacy power substations with newly-built automated facilities is generally impractical and cost-prohibitive, most substation automation applications rely on retrofitting or upgrading legacy equipment and integrating the relevant subsystems.

Substation automation retrofitting generally focuses on deploying intelligent electronic devices (IED) to make primary equipment intelligent, or serve as secondary equipment in substation bus networking, by converting formerly analog condition monitoring data into digitalized data or protocols for transmission, storage, or further computations by a computer management system. Therefore, the trend of substation automation is to collect and integrate the data from all of these supervisory subsystems into a powerful and secure control system.

Due to the mission-critical nature of power substation applications, even light data loss may severely disable the substation if the management system were to malfunction, resulting in disaster. Therefore, focusing on management system redundancy is of the utmost importance when retrofitting legacy substations equipment and subsystems especially in remote and unmanned control, data acquisition and supervision.

Moreover, paying special attention to management-system redundancy when retrofitting for power substation automation can help system designers and engineers both minimize overall system downtime and allocate more technical resources to system diagnostics and troubleshooting.

Control and management

When retrofitting a power substation, system integrators need to overcome a number of control and management pain points.

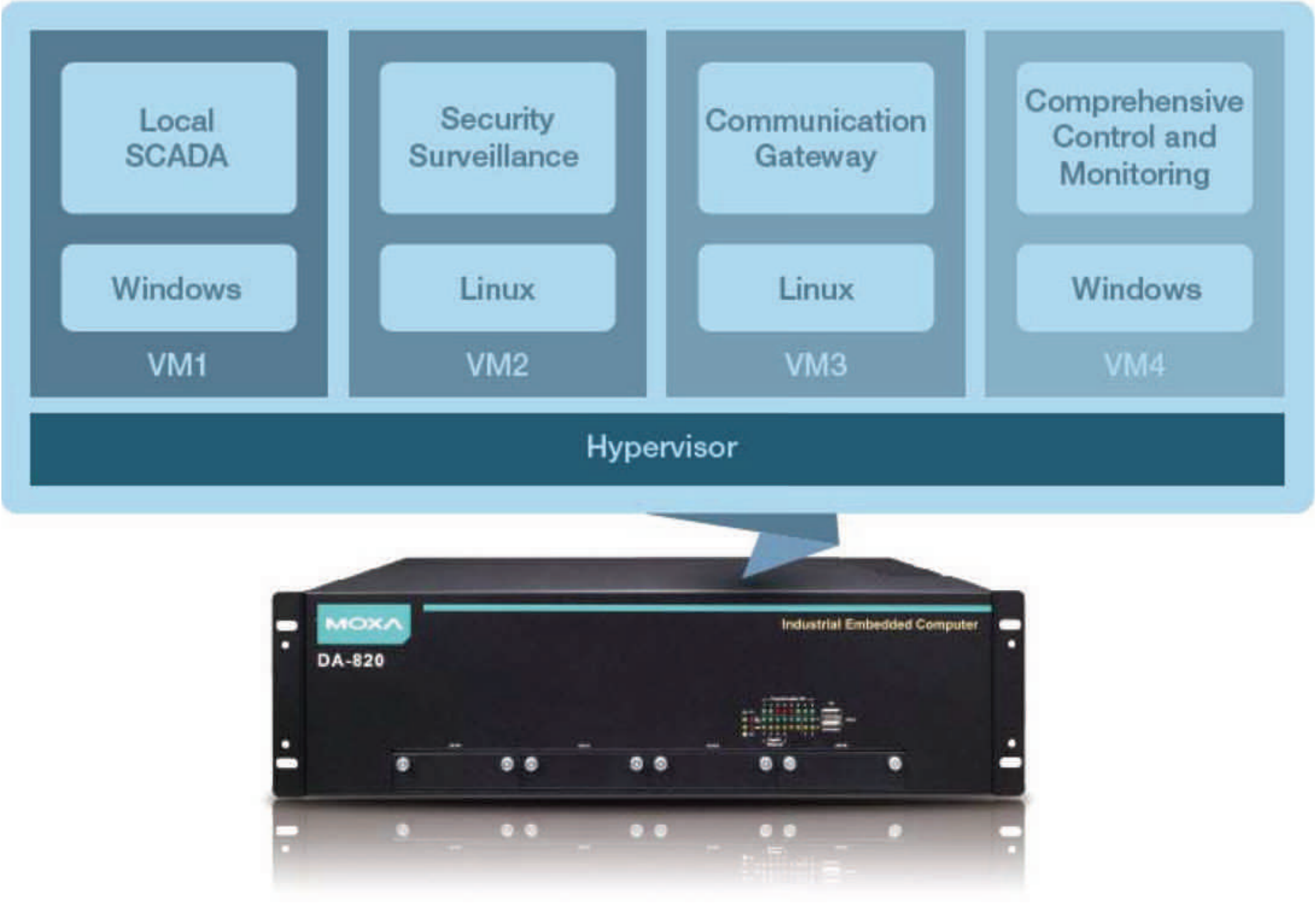
First, when an unstable application crashes on a system, system errors will not only affect the application crashed, but may also hang the entire system and affect other applications running on the same computer.

Second, control and management issues can also arise when migrating legacy operating systems and applications. For example, many legacy substation applications were originally designed for older OS versions by a third-party vendor who may no longer be providing support for the original application to the end-user.

Alternatively, the operating system itself may be too old (i.e., running on an outdated kernel). In both cases, simply upgrading the firmware may not be enough, or even feasible, to migrate these legacy software applications for use with the latest operating systems and hardware. Oftentimes, end-users may even need to commission a new application to be developed for the new OS.

Finally, system integrators also require a number of advanced features to maintain business continuity and increase uptime such as distributed resource scheduling, high availability, fault tolerance, and storage migration.

SOURCE: MOXA



Running multiple operating systems and multiple applications on the same physical server can reduce costs, while increasing the efficiency and utilization of existing x86 hardware.

Resolving management issues

Focusing on system redundancy in power substation retrofitting applications can resolve these system management issues by using either decentralized or centralized system management architectures.

Decentralization

In a decentralized management architecture, system redundancy is ensured by multiple physical computers where each computer only runs a single operating system and application. Since each computer on a decentralized system is only running a single application, an unstable application on any node represents a single point of failure in this multi-node network.

These are clear benefits to running a single operating system or a single application on the same physical server. But to deploy one physical machine for each application, this hardware-based approach will clearly incur additional equipment and maintenance overhead.

Moreover, a decentralized management architecture may not overcome the issues associated with migrating legacy operating systems and applications, due to the fact that new computer platforms usually do not support drivers for legacy operating systems.

Centralization

In a centralized management architecture, on the other hand, system management redundancy is achieved by running multiple operating systems and applications on the same physical server via virtualization technology (i.e., VMware). By running multiple operating systems and multiple applications on the same physical server, virtualization lets you reduce costs while increasing the efficiency and utilization of your existing x86 hardware.

First, instead of physically isolating applications on separate computers, server virtualization provides application isolation and removes application compatibility issues by consolidating many of these virtual machines across far fewer physical servers.

Second, integrated availability and fault tolerance protects all your virtualized applications. If a server or node ever fails, all the virtual machines (i.e., VMware) will automatically restart or continue on another machine, with no downtime or data loss. However, this virtual machine software feature is available only on the PC platform.

Finally, by virtualizing and encapsulating legacy applications, users can effectively extend the life of the legacy application, maintain system uptime, and finally replace aging and outdated equipment on the communications network with the latest hardware.

Conclusion

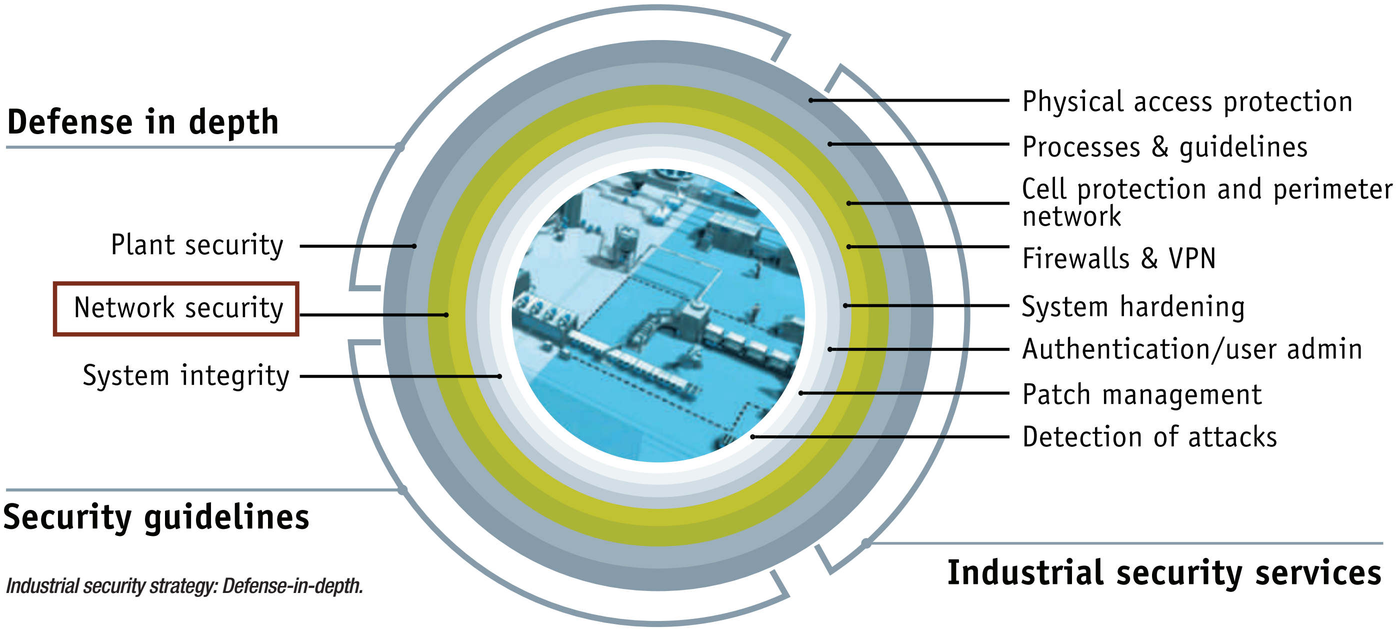
Upgrading legacy power substation equipment with IEDs and integrating the relevant subsystems is not a light-hearted task. Focusing on management-system redundancy in retrofitting power substations is the key to overcoming control and management issues.

Effective management-system redundancy can be achieved by employing either a decentralized or centralized approach to system redundancy. Although the choice between these two approaches to system redundancy are yours to make, note that running multiple operating systems and multiple applications on the same physical server will also allow you to reduce costs while increasing the efficiency and utilization of your existing x86 hardware.

Daniel Lai is a Product Manager for ***Moxa****.*

IT security priorities for industrial control systems

Defense-in-depth offers a multilayered approach to protecting industrial plants against attacks from the outside as well as the inside in several layers. The concept is based on the components of plant security, network security and system integrity according to recommendations from ISA 99 / IEC 62443.



SOURCE: SIEMENS

Industrial security strategy: Defense-in-depth.

ESTABLISHING IT SECURITY for automation systems is extremely important for industrial locations, since the automation and process control systems required are used in virtually all industrial sectors from energy generation and distribution, to water supply, traffic control systems and facility management. In order to protect people and plants, plant-specific measures are necessary using help provided by a staggered protection technology portfolio that reaches deep into each specific plant structure.

Due to the increasing networking of Ethernet connections down to the field level, industry is becoming more concerned with related security issues. Open communication and increased networking of production systems not only holds enormous opportunities, but equally big risks, whose potential damage to these networked systems must be identified.

The era of sealed off automation systems, based on proprietary protocols and inaccessible from the outside, is becoming a thing of the past. A connection of automation systems to the Internet or to existing office networks is a given, even though the requirements for automation networks differ greatly.

Automation network requirements

In the current "ICS Security Compendium" of the German Federal Office for Information Security (BSI), the different requirements for classic IT networks and automation networks are pointed out. It is intended to serve as basic guide for the operation of industrial plants with respect to safeguarding the production and processing systems, and addresses the needs of utility companies and water suppliers, providers of traffic control systems, and companies in the facility management sector.

A significant difference is the assessment of the risks concerning the different systems. While an attack on the IT infrastructure "only" affects the data integrity and at worst results in a loss of company data, a hacker attack on the processes and the automation environment can endanger people, destroy production capacities and uncontrollably damage the environment.

To comprehensively protect an industrial plant against attacks in terms of security, appropriately staggered and coordinated measures must be taken. It is not enough to implement a simple password-protected system access, since attacks from the outside can take place at several levels. For a comprehensive protection of industrial plants, Siemens AG has developed a defense-in-depth concept.

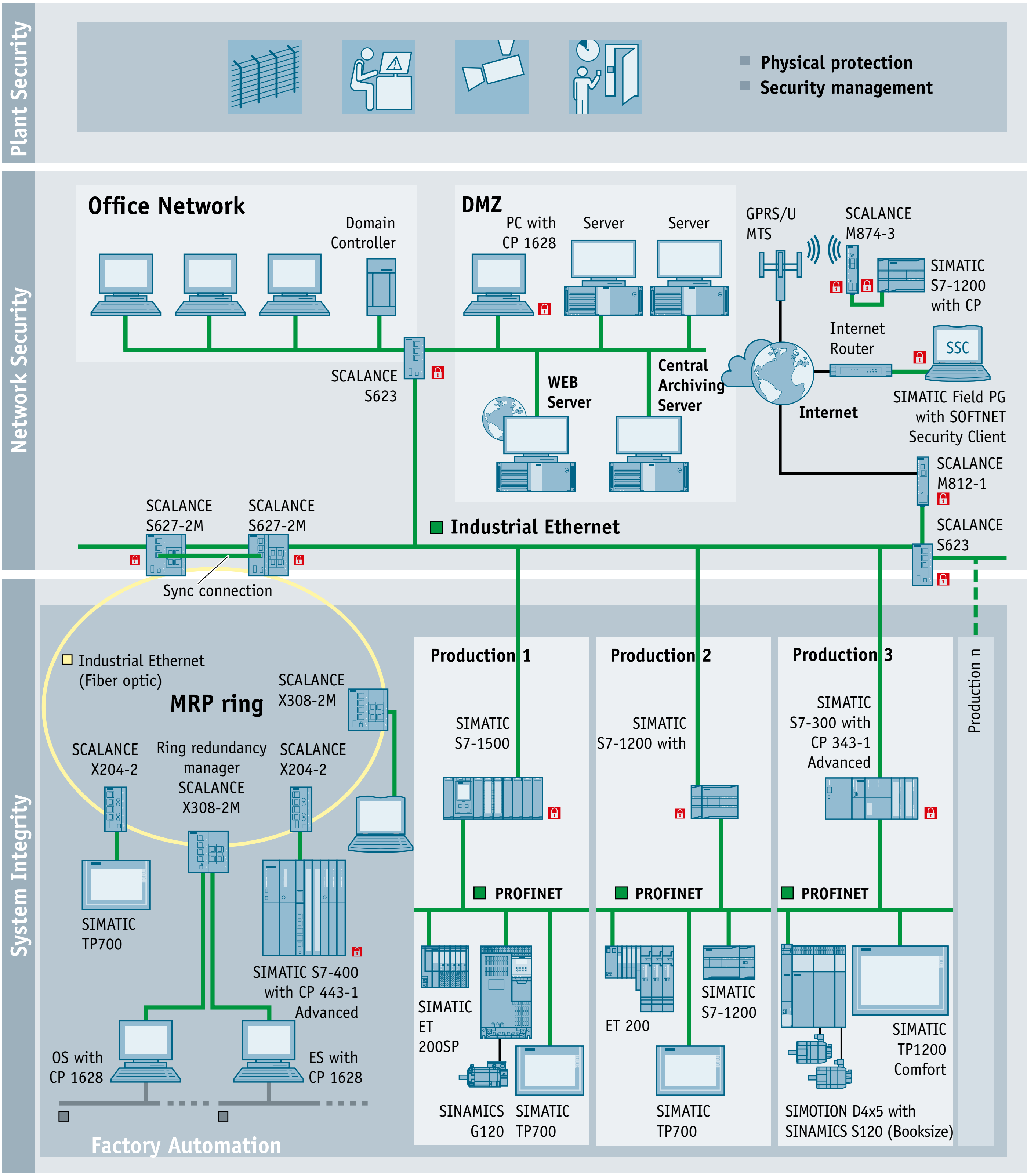
Complete protection goes deep

Defense-in-depth is a multilayered concept for industrial users that protects industrial plants against attacks from the outside as well as the inside in several layers. The concept is based on the components of plant security, network security and system integrity according to recommendations from ISA 99 / IEC 62443, the leading standard for security in industrial automation. While classic plant protection wards off physical access, network protection and system integrity protection prevent cyber-attacks and access by unauthorized operators or non-company personnel. The advantage is that an attacker has to overcome multiple security mechanisms, and that security requirements of the individual layers can be taken into consideration for each specific plant installation.

Success factor: network security

Network security means protection of automation networks against unauthorized (external as well as internal) access. This includes the monitoring of all interfaces, such as those between office and plant networks, or the monitoring of teleservice access to the Internet. This can be carried out by means of firewalls and, where necessary, the setup of a DMZ (demilitarized zone or security-relevant shielded zone).

The DMZ is designed to supply data to other networks, without granting direct access to the automation network. The security-relevant segmentation of the plant network into individually protected automation cells minimizes the risk and increases the



SOURCE: SIEMENS

Secure communication, network access protection and network segmentation with "security integrated" products.

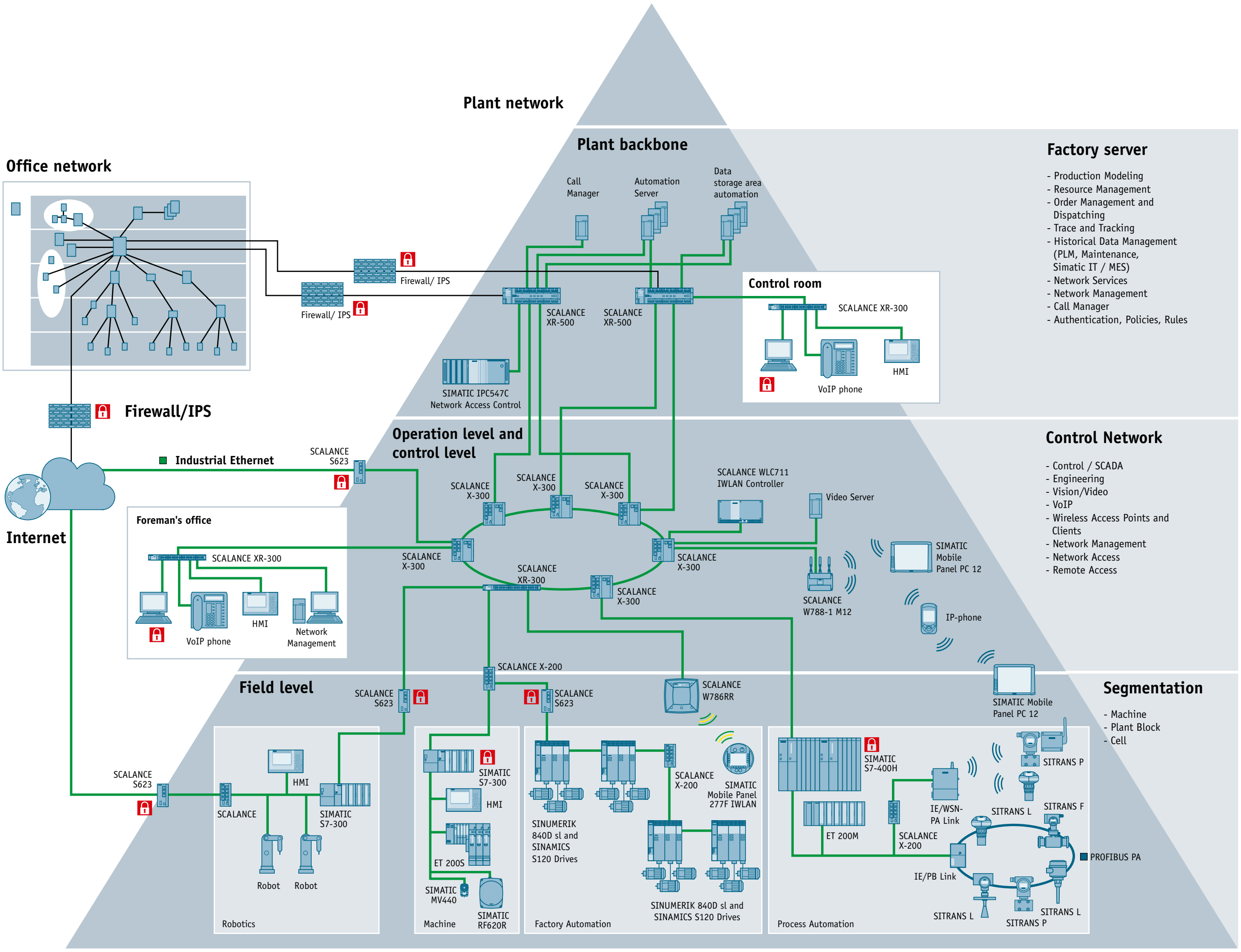
security. The segmentation into cells and the assignment of the devices follow the plant-specific communication and protection needs.

The data transmission between the cells is exclusively established via VPN connection (virtual private network), using encryption to protect against data espionage and manipulation, and all communication participants are securely authenticated.

With "Security Integrated" components from Siemens (e.g., the SCALANCE S security modules or security CPs for SIMATIC controllers), a cell protection concept can be easily implemented and communication can be secured.

Components for network security

For the implementation of these protection concepts, two means of security have proven themselves: the firewall and the VPN tunnel. A firewall is used for the content-related protection of the data traffic. Using filtering, suspicious/prohibited packets can be discarded and, where appropriate, network access can be blocked or granted packet-dependently. To secure the physical communication, a tunneling method is most often used. The firewall and VPN functions are supported by the



SOURCE: SIEMENS

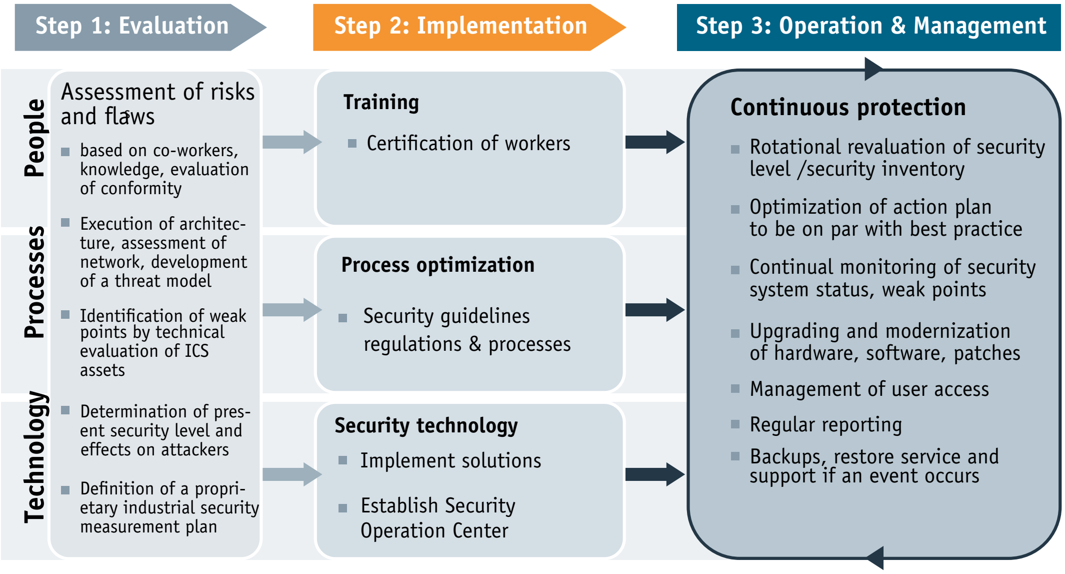
Secure industrial communication, systems example.

“Security Integrated” products and provide the user with protection down to the automation cell.

Application-specific plant security

To make it possible for almost all plant operators to effortlessly set up secure networks, Siemens is offering a wide range of “Security Integrated” products. A distinction is made between stand-alone modules, such as DSL modems/routers or cellular phone network routers, and communication processors, which directly integrate the security functionality into the controller world.

“Security Integrated” products are designed for harsh industrial use and offer proven protection for production plants. In addition to the security product offering, Siemens supports the user in the implementation of the defense-in-depth concept through Plant Security Services.



Step 1: Evaluation

Step 2: Implementation

Step 3: Operation & Management

People

Processes

Technology

Assessment of risks and flaws

- based on co-workers, knowledge, evaluation of conformity
- Execution of architecture, assessment of network, development of a threat model
- Identification of weak points by technical evaluation of ICS assets
- Determination of present security level and effects on attackers
- Definition of a proprietary industrial security measurement plan

Training

- Certification of workers

Process optimization

- Security guidelines regulations & processes

Security technology

- Implement solutions
- Establish Security Operation Center

Continuous protection

- Rotational revaluation of security level /security inventory
- Optimization of action plan to be on par with best practice
- Continual monitoring of security system status, weak points
- Upgrading and modernization of hardware, software, patches
- Management of user access
- Regular reporting
- Backups, restore service and support if an event occurs

Security process

Industrial security is not a purely technical subject, but must be consciously reinforced in the minds of all personnel. Security is a continuous process that must be taken into account at all times, and requirements of office IT differ from those of automation IT. It is critical to employ proven security products in automation. In the ideal case, component manufacturers will integrate required/necessary security functions directly into automation products as standard.

*Technology report by Robert Schwarz, **Siemens AG.***

EtherCAT servo drives

OSAI USA: OPENdrive OD700 servo-drives for brushless motors are EtherCAT servo-drives that integrate with the company's OPENcontrol family. They provide flexible and open CNC systems equipped with numerous fieldbus capabilities to handle complex operating challenges and strong customizations.

A key feature is automatic recognition of connected motors and configuration settings. This facilitates commissioning exclusively through the EtherCAT channel without modifying machine connections. ODM enables visualization and modification of characterization parameters of drives and motors in addition to drive analysis through diagnostic graphics.

ODM also enables drive functions such as digital filters for the compensation of mechanical imperfections and the actuation time of the brake motor to synchronize it with axis motions. A multi-track oscilloscope allows execution of detailed analysis of axes behavior for the best machine performance.

Dual-rate SFP media converter

EtherWAN Systems: The release of a new media converter model, EL2242, supports 10/100/1000BASE-T to 100/1000BASE dual rate SFP transmission with PoE compatibility.

Designed for industrial/harsh environments, the EL2242 supports wide operating temperature from -40°C to 75°C, high ESD/EMI protection and redundant terminal block power inputs. The EL2242 is housed with ruggedized aluminum enclosure supporting DIN-rail mounting. The LED indicators display power, alarm, link, data rate, PoE and LFPT status.

The EL2242's copper port is compliant to IEEE802.3at PoE/PSE standard, capable of the maximum power delivery of 30 watts via single UTP cable. The power can be utilized for PoE powered devices such as an IEEE802.3ac wireless AP or a PoE surveillance camera.

The EL2242's SFP fiber port supports 100BASE-FX or 1000BASE-X dual rate connectivity, reserving the possible migration to a Gigabit network. In additional to LFPT, the EL2242 provides relay alarm support, reporting an Ethernet link failure immediately to the on-site personnel to save maintenance time. Users may use EL2242's DIP switch for turning on/off LFPT and power alarm functions, as well as selecting 100BASE-FX or 1000BASE-X SFP transmission.

PoE+ Gigabit managed switches

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

Each unit is designed with eight 10/100/1000Tx Fast Ethernet ports that are IEEE 802.3at/af compliant (PoE+/PoE) with a PoE power output up to 30W per port and two dual rate 100/1000Tx SFP slots for fiber connections. This product series supports Jumbo Frames up to 9.6Kbytes, and it provides high EFT, surge (2,000VDC) and ESD (6,000VDC) protection.

In addition, all units have a dual power input design with a reverse polarity protection and a relay warning function to alert maintainers when any ports break or power failures occur. This makes it suitable for applications in a harsh environment requiring high reliability and distance extension capability.

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

Multiprotocol I/O modules

Belden: A new multiprotocol solution meets both EtherNet/IP and PROFINET specifications for the Industrial Internet of Things (IIoT), and detects both input and output data directly in the machine. This provides an all-in-one solution for robotics, machine handling, manufacturing, food and beverage, packaging and automotive applications.

The IO-Link Master, with class A and B ports, provides options for eight IO-link interfaces and 16 direct inputs (DI) or eight direct outputs (DO) for increased flexibility and functionality. L-coded M12 power ports with compact design and optimized arrangement simplify plant installation and give engineers more options for connecting additional Lumberg Automation LioN-Power products.

The new LioN-Power Active I/O modules meet application-specific regulations, including Underwriters Laboratories (UL) 61010-1 certification for safe implementation of electrical test and measurement equipment, and IP66 and IP67 ratings for protection against dust and immersion in water. The modules can be used with other Belden products, including the M12 power cordsets, 7/8"cordsets and the M8/M12 cordset portfolio, along with the mounting adaptor.

M12 panel feed-through

HARTING: The M12 panel feed-through with cable for Gigabit Ethernet has expanded the company's har-speed range of industrial connectors with an X-coded M12 panel feed-through that is supplied complete with a length of cable allowing it to be integrated directly into Gigabit Ethernet systems.

The new feed-through arrives at the customer fully assembled and ready to install, and can be put into operation immediately. The user benefits from significant time saving in the installation process, and does not have to worry about the connection of individual cables and connectors.

The cable supplied with the panel feed-through is available in various lengths, allowing for flexible installation to meet the available space and application requirements. It is suitable for both front and rear wall mounting, and is compatible with HARTING's M12 PushPull locking system. This allows plugging and unplugging of the connector in a matter of seconds, thus saving additional time in assembly.

The panel feed-through is designed to conform with IEC Standard 61076-2-109. It fulfils Cat.6A as well as Performance Class EA and thus corresponds with the current Gigabit Ethernet requirements for speed and bandwidth. The robustness and vibration resistance of the M12 panel feed-through also makes it suitable it for railway applications.

LTE Enabled industrial computer

Moxa: Devices located at the edge of Industrial IoT networks have already started using compact wireless-enabled industrial computing platforms to send pre-processed data to a control center through LTE, Wi-Fi, or other wireless protocols. Rugged wireless-enabled computers are often needed, since these "edge" environments may be subject to extreme temperatures.

Extreme temperatures can cause computing systems to crash or become unstable, which has led to the development of wide-temperature industrial computers. The fact that LTE generates more heat than other wireless options requires computer designers to use a housing with thermal properties that allow it to radiate away much of that heat. The thermal design of the new LTE-enabled V2201 wireless computers ensures reliable system operation in temperatures ranging from -40 to 70°C.

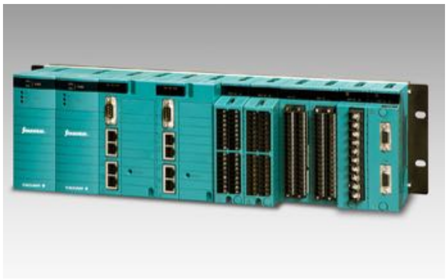
Direct Integration of PROFIBUS PA

Softing: A new pnGate PA is used to integrate PROFIBUS PA segments into control systems supporting PROFINET. The new gateway supports widely accepted device configuration, parameterization and condition monitoring tools like for example Siemens PDM, PROFINET Engineering Systems and Device Type Manager (DTM) frame applications. This significantly facilitates the change from PROFIBUS DP to PROFINET applications in the process industry.

In these applications, the pnGate PA serves as an interface on the infrastructure level between host systems and field devices and performs PROFINET Device- and PROFIBUS PA master tasks. In this way, there is no need for the use of additional equipment.

The gateway allows engineers to use familiar tools and makes the use of PROFINET controllers instead of PROFIBUS DP masters easier. For easy commissioning, the pnGate PA is compatible with the R. STAHL bus-Carrier Series 9419 and Power Supply 9412 products.

STARDOM network-based control



Yokogawa: The company has announced it will release an enhanced version of the STARDOM network-based control system in the spring of 2016 that includes a newly developed high-speed CPU module for the FCN autonomous controller. STARDOM will feature the new CPU module, improved environmental resistance, and an enhanced engineering tool. With this product, Yokogawa intends to expand the open network control system business.

STARDOM is a network-based production control system that consists of the FCN autonomous controller and the VDS or FAST/TOOLS SCADA software. Since introducing this system in 2001, Yokogawa has continued to enhance it by adding new functions to satisfy customers' needs. Combining the reliability of a distributed control system (DCS) with the versatility and economy of a programmable logic controller (PLC), STARDOM is widely used in medium-size manufacturing plants and in geographically distributed applications such as natural oil and gas wells. To date, more than 20,000 STARDOM systems have been delivered.

STARDOM's FCN autonomous controller will be capable of reliably controlling high-speed equipment such as compressors, large wind power generators, and other types of turbines, and will be able to operate in a wider range of climatic conditions. Moreover, it will include a function that aids engineers in the performance of installation, modification, and maintenance tasks.

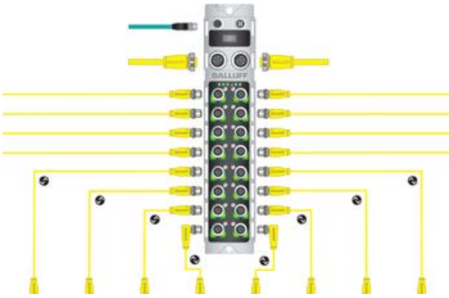
Powerful Ethernet switch

Siemens: The company has now added the Scalance XR526-8C to its portfolio of powerful Ethernet switches of the XR-500 product line. The device is compatible to a number of different network components and acts as a link between automation and office networks. Although it comes equipped with 24 Gigabit ports, two 10-Gigabit ports and integrated network sections, the switch has a low installation height of only 44 mm and thus saves space in the control cabinet.

Two additional SFP (Small Form-Factor Pluggable) slots for 10 Gbps ensure high device performance of up to 44 Gbps. High availability can be realized by the fan-free design and the redundant power supply. The partially modular switch for 19-inch racks supports Layer 3 switching via the Key-Plug and can be flexibly installed in high-performance plant networks. Users can integrate the switch into all standard network management systems (e.g. Sinema Server) and the TIA Portal for easy configuration and diagnostics.

Various different media can be connected to the Scalance XR526-8C using eight combo ports, plug-in transceivers and the link aggregation option. The switch is compatible to all Scalance X switches and all typical network devices in an office environment.

16 Port IO-Link PROFINET Master



Balluff: A new PROFINET powered 16 port IO-Link master is designed for scalability in distributed architectures while providing ease of use for I/O and smart sensors alike.

The 16-port IO-Link master can host up to 480 configurable I/O on a single PROFINET node when combined with Balluff's expandable IO-Link hubs. This enhances the controls architecture by promoting modularity and built-in scalability for the future.

Each of the 16 ports on the device can be configured as a 2-channel standard I/O port or used as an IO-Link port to connect smart sensors from hundreds of IO-Link device suppliers. It can also be used with Balluff I/O hubs to scale up the I/O counts. With IO-Link V1.1, this block offers added features such as up to 32bytes of data transfer per port and parameter server functionality for automatic re-configuration of sensors.

Wireless switchgear and networks

Steute: At field level, the sWave.NET wireless network facilitates variable communication between wireless switching devices and access points, which function in a similar manner to a router. They receive signals from wireless switching devices, bundle them and then transmit them, e.g. by Ethernet or Wi-Fi, to one or several application servers.

The access points are installed across the transmission range and communicate with the wireless switchgear. Approx. 100 wireless switches can be administered per access point. If more sensors are required within the range of an sWave.NET access point, additional access points can be registered. When a switching device sends out a signal, the order of the access points it reaches is fixed. If transmission fails at the first access point, the second is addressed, and so on. This guarantees very high transmission reliability.

The corresponding application server contains a database which collects all information at field level before transferring it, either directly or via middleware, to the customer IT platform, if required also via Web services to multiple-site IT systems.

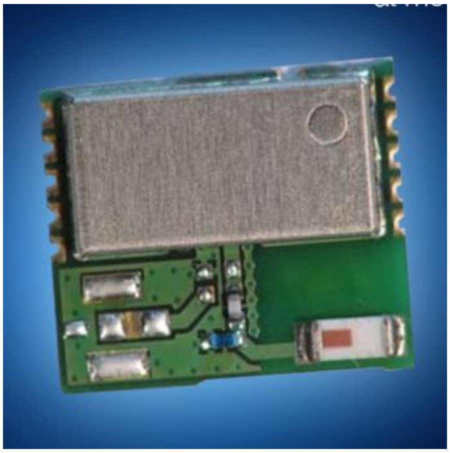
Powerful Smart module

Fujitsu: The company has announced a new, very small module with an integrated antenna based on Nordic Semiconductor Bluetooth Smart SoC, nRF52 Series.

The module has been designed to deal with a complexity of processes using very

little power, and offers an ultra-small size which is an important feature for small Smart wearables. The wireless module features a Cortex-M4F processor and 512kB flash + 64kB RAM. Features such as the on board NFC-tag and the on air compatibility with nRF51, nRF24L and nRF24AP series make the module a solution for various applications.

Bluetooth Smart Sensor/Hub

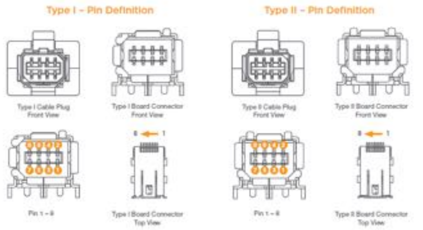


Mouser: The low-energy SPBTLE-RF module provides a complete radio frequency (RF) platform in a tiny form factor, integrating a 2.4 GHz RF radio, antenna, and high-frequency and low-power oscillators to optimize the time to market of the final applications.

The module is an easy-to-use Bluetooth Smart master/slave network processor module compliant with Bluetooth v4.1. It is designed around ST's BlueNRG-MS network processor and takes advantage of its enhanced features to create a complete RF platform in a small package. The BlueNRG-MS 2.4 GHz radio embeds a non-volatile flash memory which allows upgrading the stack when the device is deployed in the field. The SPBTLE-RF offers a certified (ETSI, FCC, IC) solution to simplify RF and wireless design, allowing engineers to concentrate on creating innovative applications.

The SPBTLE-RF module embeds the entire Bluetooth Smart stack and protocols. The external host application processor, where the application resides, is connected to the module through a standard SPI interface.

Ethernet pin-out recommendations


Type I – Pin Definition
Type II – Pin Definition
Type I Cable Plug Front View
Type I Board Connector Front View
Type II Cable Plug Front View
Type II Board Connector Front View
Pin 1 – 8
8
1
Type I Board Connector Top View
Pin 1 – 8
8
1
Type II Board Connector Top View

TE Connectivity: Newly released Ethernet pin-out recommendations for its range of Industrial Mini I/O connectors will ensure equipment interoperability, while meeting the needs of Ethernet users.

Industrial Mini I/O connectors give design engineers flexibility to use limited space on the PCB more effectively. Designed with two points of contact, this connector is built for the stringent demands of an industrial and high-vibration environment, enabling increased productivity through a more reliable connection.

Accidental unplugging of a network connection due to shock, vibration or pulling on cords causes expensive downtime in an industrial environment. To prevent this from happening, the Industrial Mini I/O connector offers a unique locking system with 100N of pull force.

With its piercing termination, the Industrial Mini I/O field-installable version decreases the time needed to terminate the wires through soldering. With an easy-to-use hand tool, field assembly in virtually any environment is now possible.TheMini I/O connector has two interface types (I and II). Both are standardized by IEC/PAS 61076-3-122 and help prevent cases of accidental mis-wiring. The connectors also support both 4-and 8-wire Industrial Ethernet at 10/100Mbps and 1Gbps.

Real-time Ethernet switch

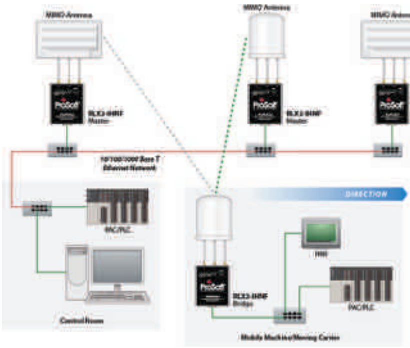
MEN Mikro: The F305 network controller with 3U CompactPCI supports four fast Ethernet channels and real-time Ethernet functionality. Especially developed for rail applications, the card is equipped with robust M12 connectors on the front, is working in an extended temperature range from -40 to +85°C and complies with the EN 50155 railway standard.

Four fast Ethernet channels can connect over distances up to 100 m. The card supports full-duplex or half-duplex for 10BASE-T and 100BASE-TX.The F305 is available with or without a real-time Ethernet controller and extended connectivity, making it flexibly scalable to system requirements.

The one-slot CompactPCI card comes with robust M12 connectors, conformal coating, operates in the extended temperature range and fulfills the requirements of the EN 50155 standard. The F305 also helps create an effective solution in demanding rail systems for rolling stock and wayside.

Due to its robust characteristics and real-time functionality the F305 plays a central role as a reliable network component in the MTCS Modular Train Control System from MEN.

Industrial hotspots



ProSoft Technology: A new family of Wi-Fi radios meet a wide range of application needs. The 802.11abgn radios are capable of RF data transmission rates of up to 300 Mbps, for I/O control and video streaming applications.

The EtherNet/IP object and Modbus Agent support enables the ability for EtherNet/IP and Modbus TCP controllers to read diagnostic information from the radios. This can help reduce down time when troubleshooting network issues.

A QoS feature allows for data prioritization. With QoS, users can set different data transmission requirements for each of their I/O Control devices or video streaming. Virtual Local Area Networks (VLAN) allow for network secure segmentation and the ability to deploy separate networks within the overall network.

Leveraging Big Data and IoT

OMRON: New NJ101-series Machine Automation Controllers connect to databases directly, and accelerate the ability to leverage Big Data and IoT at production sites.

The entry model NJ101-series with a simple hardware performance enables application functionalities and solutions of the Sysmac Automation Platform to be adopted in existing production equipment and general systems. It was released in April 2015 and has been adopted in existing production equipment and general systems at various production sites.

In addition to the functions of the NJ101-series, the new NJ101 Database Connection CPU Units are also equipped with a function to collect and utilize information at production sites. The units can be directly connected to a variety of databases including a Microsoft SQL Server without special software or middleware. Users are not required to have ICT-related programming knowledge to construct a system. The programming using ladder language, which is widely used at production sites, enables data utilization in manufacturing processes. The users can start big data utilization and IoT introduction in the manufacturing processes easily on a small scale for productivity enhancement, predictive maintenance, and constructing a quality traceability system by installing the Unit in existing equipment.

TwinCAT IoT

Windows Azure™
Amazon Web Services™
MQTT
AMQP
OPC UA
BECKHOFF
TwinCAT 3
I/O Signals,Fieldbus

Beckhoff: With the new TwinCAT IoT, the TwinCAT 3 provides a complete solution for fast and efficient realisation of IoT and Industry 4.0 concepts. TwinCAT IoT supports standardised protocols for cloud communication and for sending push notifications to smart devices. The extension of conventional control tasks, through applications such as Big Data, pattern recognition or condition and power monitoring in the cloud, results in production efficiency increases.

TwinCAT 3 IoT is fast and easy to configure. Together with an Embedded PC or Industrial PC as the IoT controller, the software provides a seamless connection between the Internet of Things (IoT) and the Internet of Services. Filtering, further processing and interpretation of the collected data via TwinCAT Analytics create genuine added value. Comprehensive analyses enable predictive maintenance, machine downtimes are reduced, and control solutions are optimised – for example, through the minimisation of cycle times or energy peaks.

SCADA Edge Industrial PC

GE-IP: New industrial PCs (IPC) will now come complete with the company's supervisory control and data acquisition (SCADA)/human machine interface (HMI) automation software preinstalled.

The new, integrated SCADA Edge IPC provides the intelligent processing power needed to sift through vast amounts of data to uncover actionable information that can be used to proactively manage today's machines and factories.

With the SCADA/HMI software preinstalled, GE is able to deliver streamlined, real-time visibility and control out of the box, improving decision-making, increasing operator effectiveness and reducing downtime in small- and medium-sized industrial applications through faster and smarter reactions at the plant floor level. The SCADA Edge IPC provides operators and engineers with the trusted technology and robust performance engine needed to precisely monitor and control every aspect of their environment, equipment and resources.

Secure cellular remote connectivity

Phoenix Contact: New TC mGuard devices leverage cellular networks, such as Verizon and AT&T, to provide secure remote communications wherever a wired connection is not possible. The TC mGuard meets the demand for remote maintenance and secure supervisory control and data acquisition (SCADA), two growing needs in today's connected industrial world.

For remote maintenance and support, the TC mGuard connects through Phoenix Contact's free mGuard Secure Cloud service. This gives original equipment manufacturers, machine builders, and system integrators access to service their equipment easily and avoid heavy travel expenses. The combination of cellular networks and a virtual private network (VPN) ensures a secure solution for remote maintenance and support.

Ethernet line extenders

Westermo: New Ethernet line extenders enhance network security and support larger bandwidth applications.

Westermo has released two additions to its range of Wolverine advanced industrial Ethernet line extenders. These rugged, reliable and compact devices are used to establish long-distance, high-speed remote connections between simple or complex Ethernet networks using existing copper cables, thereby reducing installation time and cost. The DDW-242 and DDW-242-485 include a range of features that deliver secure and resilient networking, even in extreme industrial environments, which makes them suitable for mission-critical applications.

The line extenders enable Ethernet networks to be connected over distances of up to 15km, at data rates up to 15.3 Mbit/s on a single twisted pair cable. Using two pairs bonded, the rate can be doubled to support applications requiring larger bandwidths. An integral switch allows two Ethernet devices to be attached, and a choice of either 232 or 485 serial port enables legacy equipment to be incorporated into the IP network.

To help improve cyber security the DDW-242 and DDW-242-485 include full layer 3 functionality and unique IP security provided by the Westermo WeOS operating system.

IP connections to serial devices

ORing: Fully compliant with Modbus/TCP, the IDS-342GT can act as a Modbus gateway to convert Modbus/TCP on Ethernet to serial Modbus RTU or ASCII. This offers a convenient and cost-effective solution to connect existing devices or controllers running Modbus serial protocols to an Ethernet network, allowing customers to integrate legacy, proprietary SCADA and HMI equipment into a modern Ethernet network.

With four RS-232/422/485 serial ports alongside two Gigabit Ethernet ports, the device server can convert serial signals to twisted-pair signals which can then be transmitted over the Internet. In addition, the device supports a baud rate up to 921.6kbps for fast data transmission. By making serial devices Internet ready, any serial devices such as card readers, measurement devices, or data acquisition terminals can operate as if they are locally attached.

Capable of transferring data simultaneously into five host PCs, the new device server assures all critical data is saved in different host PCs to avoid Ethernet downtime or host PC failure. In addition to versatile operation modes such as Virtual Com, Serial tunnel, TCP server, TCP client, and UDP modes, the administrator can also configure the device server remotely through the NAT router from different IP domains or via the Internet using the NAT Router Pass-Through features, DDNS, and PPPoE.

Connect CompactRIO to AS-i

National Instruments: With the new AS-i Master module, a CompactRIO chassis can connect to 32 nodes or 62 A/B nodes with extended addressing.Users can replace one-to-one connections between on/off devices, like sensors and actuators, with a network of sensors and actuators. These low level sensors can then be integrated with DeviceNet or PROFIBUS networks.

Key features include backwards compatibility with AS-i specification v2.1 and v2.0, the ability to connect up to 496 actuators/sensors with extended addressing and a way to connect sensors and actuators to higher level networks such as PROFIBUS or DeviceNet.

Industrial Ethernet PC connections

HMS Networks: The new IXXAT INpact merges the proven Anybus technology with years of IXXAT know-how in the PC interface card area. The result is an efficient PCIe card with multi-protocol support for numerous industrial Ethernet standards and a uniform protocol and card-spanning application programming interface.

Until now, it has been complicated to develop PC-based measurement, visualisation or service applications for several Industrial Ethernet standards since different interface cards and application programming interfaces had to be used for each protocol.

HMS now offers a PCIe card in standard and low-profile formats which supports all leading industrial Ethernet standards. Users can easily connect their PC-based slave application to EtherCAT, EtherNet/IP, Modbus TCP, PROFINET IRT/RT, Powerlink and standard TCP/IP by using the IXXAT INpact. Through the uniform driver concept, customers can switch between protocols quickly and without extensive programming and also profit from future protocol extensions and developments.

IoT network appliance

Lanner: The rising trend of IoT (Internet of Things) has triggered greater demands for reliability and serviceability in network security, cloud computing and data center operations.

To meet this challenging demand, Lanner has unveiled its first 6th generation Intel Core-based 1U network appliance NCA-4210, featuring 14nm microprocessor, the new LGA 1151 socket, DDR4 memory support and the I/O boosting, comprehensive Intel H110 and C236 series chipset, and flexible LAN configurations.

The NCA-4210 is powered by the new Intel 14nm micro-architecture CPU, the 6th generation Intel Core processor (codenamed Skylake-S), the successor of Broadwell. With the next generation 3-D tri-gate design, the adoption of the 6th generation Intel Core processor comes with the promise to enhance processor performance, while lowering the TDP.

A new socket type, LGA 1151, has also been released for the die-shrinking architecture. In terms of memory efficiency, NCA-4210 supports dual-channel DDR4 with frequency up to 2133MHz and capacity up to 32GB by 2 x 16GB DIMM. ECC is also supported (only available for C236 chipset).

Viva Las Vegas! Oddities from CES 2016

Las Vegas is mostly known for casinos, poker and slot machines, but once a year it becomes the high-tech capital of the world. At the Consumer Electronics Show (CES), hundreds of exhibitors show the latest, cutting-edge technologies. CES is getting bigger every year and 2016 was the largest CES in the event's 49-year history, wirh almost 2.5 million square feet of exhibit space

THE THEME OF CES 2016 was Smart everything. "Smart" meaning that the product includes one or more sensors, and is somehow connected to the Internet.

"20,000 new products debut at CES this year – and at least 75%, if not all of them have sensors," said Shawn DuBravac, chief economist of the Consumer Technology Association, which organises CES. Let's take a look at some of these smart new gadgets.

Internet Fridge

16 years ago, LG Electronics launched the world's first digital refrigerator, the "Internet Digital DIOS Refrigerator" R-S73CT. It was an unsuccessful product, just like all the other Internet fridges that followed.

Comes 2016 and the connected fridge still refuses to die. Manufacturer Samsung claims that it will "transform your kitchen with a revolutionary refrigerator featuring a Wi-Fi touchscreen". The US$5,000 four-door Family Hub Refrigerator comes in black stainless steel and has a big Gorilla Glass touchscreen panel that covers most of the upper right door. Thanks to a built-in proximity sensors, the screen switches on automatically when someone approaches it. We will see if the time is finally ripe for smart fridges.

www.samsung.com

PHOTO: SAMSUNG

Smarten up your kitchen

You don't have to invest several thousand dollars into a smart fridge to bring high-tech connectivity to your kitchen. British startup Smarter (who released a smart tea kettle last year) introduced several smart gadgets designed to work with your existing appliances.

One of these is the Smarter Fridge Cam, a connected camera that you'll keep in the fridge. It snaps a picture whenever the door is opened. While shopping at the grocery store you can pull out your phone to see what's in your fridge and what you are running low on.

The Smarter Mat performs a similar function. Using Smarter's app you tell the Mat what you're putting on top of it. Now the Mat will track its weight and let you check how much salt or ketchup is left while you're out shopping.

smarter.am

World's first smart bra

Like the connected kitchen, wearable electronics are having a hard time living up to the initial promise.

Still, manufacturers show that they are creative and introduced new IoT-enhanced apparel at CES. OMSignal, who already offer a collection of smart shirts, showed the OMbra, claimed to be "the world's first smart bra". Through a number of sensors it tracks different metrics like heart rate, breathing rate, calories burned, etc.

The data is recorded in a black box at the lower band of the sports bra, and wirelessly shared to OmSignal's mobile app. The app uses the data to calculate parameters like distance, pace, and fatigue levels during workouts.

PHOTO: OMSIGNAL

omsignal.com

What about smartwatches?

In 2015, smartwatches were one of the hottest topics at CES. A year later – and the Apple Watch not the smash hit it was expected to be – there was a noticable absence of wrist-sized technology.

The major exception was Fitbit, who unveiled the Blaze model. As you could expect from a company that is in the connected health and fitness market, the Fitbit Blaze is primarily a fitness watch.

PHOTO: FITBIT

It offers activity tracking, run logging (via your synced smartphone's GPS), and persistent heart-rate monitoring in a stylish package with interchangeable leather and stainless steel link bands. The Blaze comes without third-party app support, but it does feature a color touchscreen display and smart calls, texts, and calendar notifications.

Men's Health voted it one of the '10 most exciting products at CES 2016'.

www.fitbit.com

Leopold Ploner

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