November/December 2020

InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

75 1945 ISA 2020

Augmented reality for maintenance

Safety systems and cybersecurity

Cabinetless machine design

Servo motion control basics

Achieving multivendor interoperability with open systems

www.isa.org/intech

Wire you paying too much?

*Order your cut-to-length and bulk cable, or bulk wire today and save with AutomationDirect's affordable pricing - **No gimmicks. No hidden charges.***

22AWG Machine Tool Wire (MTW)

Starting at $18.00 (500 foot spools)

We just added 22AWG MTW wire to our already extensive selection of wire. Type MTW conductors are primarily used in control cabinets, in machine tool applications, and in appliance wiring applications. MTW wire is available in various gauges and colors in 500 foot spools; some gauges are available in 2500 foot reels.

- Gauges from 22AWG to 10AWG
- Bare copper conductors
- Color-coded Polyvinyl Chloride (PVC) jacket
- Striped version available for some colors / gauges
- Made in the USA

Affordable Cut-to-Length Cable with NO Hidden Fees

Don't be fooled by suppliers that add cutting charges, hidden fees, and inflated shipping costs that end up tripling the cost at checkout.

At AutomationDirect, we've got you covered with these advantages:

- UL certified re-spooling facility - ensures that our cut-to-length cables maintain the UL certifications
- Low price per foot - **Starting at 19¢ (Q7120-1)**
- Low minimum cut lengths
- Fast shipping (typically 2-day delivery), free on orders over $49*
- Easy online, phone or email* ordering
- 30-day money-back guarantee* (**yes, even custom cut cable**)

Types of cable available:

- Flexible Portable Cord
- RS-485 & RS-422/RS-232 Cable
- Flexible Control Cable
- Power Machine Tray Cable
- Variable Frequency Drive (VFD)
- Variable Frequency Drive (VFD) / Servo Cable with Signal Pair
- DLO, RHH, RHW-2 Heavy-Duty Flexible Power Cable
- Instrumentation Cable
- Continuous Flexing Tray Rated Control
- Continuous Flexing Control
- Continuous Flexing Motor Supply
- Continuous Flexing Industrial Ethernet Cable
- Continuous Flexing Profinet
- Continuous Flexing Profibus-DP
- Sensor/Actuator
- Control and Signal
- Multi-pair Thermocouple Extension Cable
- Quabbin DataMax Extreme Industrial Ethernet Cable

More Bulk Electrical Hook-up / Building Wire

We also have a large selection of quality THHN and TFFN electrical wire that meets all NFPA and NEC requirements, at unbeatable prices.

TFFN Fixture Wire

Starting at $33.50 (500 ft.)

- Sizes up to 18AWG and various color options
- 500 or 2,500 ft. reels

THHN General Purpose Building Wire

Starting at $48.50 (500 ft.)

- Sizes up to 14AWG and various color options
- 500 or 2,500 ft. reels

Order Online at AutomationDirect.com
BUY ONLINE
Available in the U.S. and Canada only

Huge Inventory for Fast Shipping

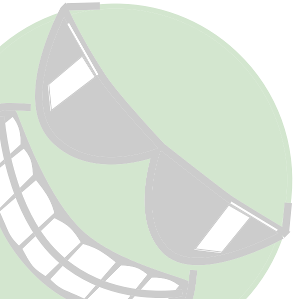
30-day Money-Back Guarantee
30 day

Bulk or Cut to Length shipped fast!

Research, price, buy at:

www.automationdirect.com/multi-conductor-cable

www.automationdirect.com/wire



Order Today, Ships Fast!

VOTED Best in SERVICE 15 YEARS

AUTOMATIONDIRECT.com

1-800-633-0405

the #1 value in automation

* See our Web site for details and restrictions.

We understand you need insightful process information to help you run your plant efficiently.
MEASURED VALUE
+ ADDED VALUE
You make confident decisions backed by process data and a complete portfolio of services and solutions to support you.

100%

of **Reference Standards traceable** to Nationally Recognized Standards.

Ensure compliance and increase process uptime with optimized services

- Lab and field accredited calibrations (A2LA) and verification capabilities for flow, pressure and temperature instruments
- Patented, industry-expert methods to optimize your calibration plan
- We are a leading manufacturer of process instrumentation – uniquely qualified to verify and calibrate
- Our global, harmonized calibration standards provide consistent service quality

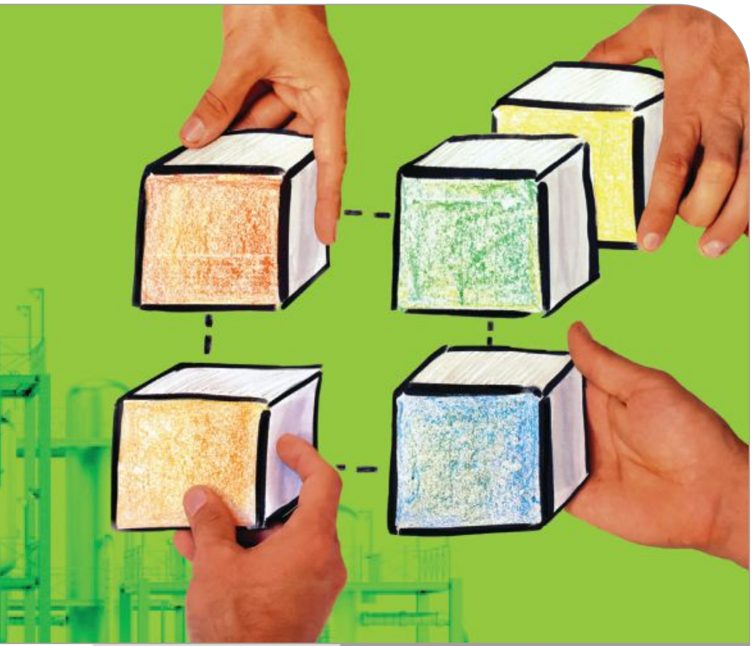
Do you want to learn more?
www.us.endress.com/calibration-usa

Endress+Hauser
People for Process Automation

November/December 2020 | Vol. 67, Issue 6

www.isa.org

InTech®



COVER STORY

CONTINUOUS AND BATCH PROCESSING

DISCRETE MANUFACTURING

CYBERSECURITY AND SAFETY

DEPARTMENTS

COLUMNS

RESOURCES

www.isa.org/InTech

InTech FOCUS — An InTech e-edition covering the fundamentals of automation

InTech plus ENEWSLETTER

InTech MAGAZINE

InTech Plus is ISA's online eNewsletter that connects automation professionals to all things automation. *InTech Plus* has technical content, educational training and videos, industry-related Q&A excerpts, and the latest and greatest on industry technology and news. *InTech Plus* focuses on a variety of topics, such as fundamentals of automation and control, certification, safety, cybersecurity, the Internet of Things, wireless devices, human-machine interface, pressure, level, temperature, and batch. All editorial content comes from a variety of sources, including ISA books, training course videos, and blogs and bits from ISA's cast of subject-matter experts. *InTech Plus* is powered by Automation.com, ISA's premier electronic publisher of automation content. Automation professionals can subscribe to *InTech Plus* at www.automation.com/subscribe.

InTech MAGAZINE

© 2020 InTech

ISSN 0192-303X

***InTech*, USPS # 0192-303X, is published bimonthly in Research Triangle Park, NC by the International Society of Automation (ISA), 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709. Vol. 67, Issue 6.**

Editorial and advertising offices are at 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709; phone 919-549-8411; fax 919-549-8288; email info@isa.org. *InTech* and the ISA logo are registered trademarks of ISA. *InTech* is indexed in Engineering Index Service and Applied Science & Technology Index and is microfilmed by NA Publishing, Inc., 4750 Venture Drive, Suite 400, P.O. Box 998, Ann Arbor, MI 48106.

Subscriptions: For ISA members, 8.65% of annual membership dues is the nondeductible portion allocated to the *InTech* subscription. Other subscribers: $175 in North America; $235 outside North America. Multi-year rates available on request. Single copy and back issues: $20 + shipping.

Opinions expressed or implied are those of persons or organizations contributing the information and are not to be construed as those of ISA Services Inc. or ISA.

Postmaster: Send Form 3579 to *InTech*, 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709. Periodicals postage paid at Durham and at additional mailing office.

Printed in the U.S.A.

Publications mail agreement: No. 40012611. Return undeliverable Canadian addresses to P.O. Box 503, RPO West Beaver Creek, Richmond Hill, Ontario, L48 4RG

For permission to make copies of articles beyond that permitted by Sections 107 and 108 of U.S. Copyright Law, contact Copyright Clearance Center at www.copyright.com. For permission to copy articles in quantity or for use in other publications, contact ISA. Articles published before 1980 may be copied for a per-copy fee of $2.50.

To order REPRINTS from *InTech*, contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

List Rentals: For information, contact ISA at info@isa.org or call 919-549-8411.

PRINTED WITH SOY INK

InTech magazine incorporates *Industrial Computing*® magazine.

InTech provides the most thought-provoking and authoritative coverage of automation technologies, applications, and strategies to enhance automation professionals' on-the-job success. Published by the industry's leading organization, ISA, *InTech* addresses the most critical issues facing the rapidly changing automation industry.

Cybersecurity standards hit their stride

By Renee Bassett, *InTech* Chief Editor

Like a racehorse streaking by, comfortable on the straightaway, the ISA/IEC 62443 series of standards are hitting their stride, finding their place among the essential building blocks of a secure industrial control system.

An ISA standards committee created the ANSI/ISA 62443 series of automation and control systems cybersecurity standards, which have since been adopted by the International Electrotechnical Commission as IEC 62443 and endorsed by the United Nations, by leveraging use cases from more than 20 different industry verticals. ISA/IEC 62443 approaches the cybersecurity challenge in a holistic way, bridging the gap between operations and information technology.

In July of last year, ISA/IEC 62443 gained its greatest champion in the form of the ISA Global Cybersecurity Alliance (ISAGCA). This group of what is now 40 member companies has come together to increase industrial cybersecurity awareness and readiness, in part by developing best practices for applying the ISA/IEC 62443 standards.

Through ISAGCA, industrial asset owners can sit down with automation and control systems vendors—regardless of industry segment or geography—to work together for the greater good. Eight companies were just announced as new members of this alliance, including UL, the global safety science leader; KPMG, one of the world's Big Four accounting and consulting firms; power management company Eaton; and others. They join initial founding members Claroty, Honeywell, Johnson Controls, Nozomi Networks, Rockwell Automation, Schneider Electric, and others.

Megan Samford, vice president and chief product security officer for energy management at Schneider Electric, is the recently appointed chairperson of the ISAGCA board. The new vice chairperson is Sharul Rashid, custodian engineer and group technical authority of instrumentation and control for PETRONAS, Malaysia's integrated oil and gas company. PETRONAS is the world's fourth-largest exporter of liquid natural gas, and Rashid has more than 30 years of experience leading teams handling instrumentation and control issues in refineries, gas liquefaction and petrochemical plants, and gas pipeline transmission operations.

Said Rashid, "I am honored to work with my colleagues around the world to advance critical cybersecurity initiatives. Together, we will work to increase awareness and expertise, [and] develop best-practice tools to help companies successfully navigate the life cycle of cybersecurity protection."

Samford said Schneider Electric is also "deeply committed to collaborating across industry to help our customers and all end users." She is personally excited to work with the diversity of ISAGCA membership, and she's also looking forward to seeing "community-identified needs and focused initiatives, like ICS4ICS, come to life through ISAGCA and its relationships with other nonprofits and governments from around the world."

Incident Command System for Industrial Control Systems, or ICS4ICS, is an effort under ISAGCA that seeks to establish an operational incident response organization by the first quarter of 2021. The initiative includes a common language for responding to cyberincidents, as well as the development of avenues for mutual assistance between organizations.

ISAGCA is clearly "driving alignment and clarity across public and private sectors," said its managing director Andre Ristaino. A diverse group of member companies working together on a standards-based, end-to-end approach can help safeguard industry against sophisticated cyberattacks. If ISA/IEC 62443 is the horse and ISAGCA is the jockey, the rest of us are in for a beautiful run.

Do you agree? Talk to me via email at rbassett@isa.org. ■

ISA *INTECH* STAFF

CHIEF EDITOR
Renee Bassett
rbassett@isa.org

CONTRIBUTING EDITOR
Bill Lydon
blydon@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Lisa Starck
lstarck@isa.org

GRAPHIC DESIGNER
Bonnie Walker
bwalker@isa.org

ISA PRESIDENT
Eric Cosman

PUBLICATIONS VICE PRESIDENT
Vitor S. Finkel, CAP

Industrial IoT efforts get new support in North America

In partnership with leading manufacturers and technology firms, MindSphere World has announced the formation of its newest chapter in North America. MindSphere World is a global community of companies and research institutions jointly shaping the future of the Industrial Internet of Things (IIoT).

Founded in 2018 by Siemens along with 18 partner companies, the organization was designed to expand Siemens' MindSphere, an IIoT-as-a-service solution. It has since expanded into a broad IIoT community that focuses on the development of business models, proposals on requirements, and recommendations to create uniform rules for the use of data.

Founding board of directors members for the new North American chapter include representatives from Deloitte, Fiat Chrysler Automobiles (FCA), IBM, Siemens, and Valiant TMS. Further founding member companies—BEET, Edge2Web, Pure Precision, Gleason Corp, GROB Systems, Hardinge, MAYA HTT, Patti Engineering, TÜV SÜD, the University of Georgia, the University of South Carolina, and Wunderlich Malec Engineering—form "a powerful initial ecosystem of North American manufacturing interests," said spokesman Michael Bowne.

As localized manufacturing efforts in the U.S., Canada, and Mexico continue to grow, companies are struggling with how to start their digital journey and how to use digital tools most effectively. MindSphere World aims to create "a platform to help accelerate the adoption of Industrial IoT and drive the digital transformation of manufacturing in the region."

Part of that struggle includes the lack of standards and best practices. Steve Burris, with the Powertrain Controls Center of Competency for Fiat Chrysler Automobiles, said FCA is "known for our technological strength, and [we] know that IoT is the next frontier of productivity, quality, and innovation. We believe that MindSphere World will help us to identify and implement standards and best practices more effectively."

MindSphere World's mission is to create an environment in which thought leaders, research institutes, and manufacturers representing all sizes and markets can come together. The plan is to provide the manufacturing industry "a mechanism within an ecosystem" to determine typical IoT business models and how to leverage them, identify industry-specific use cases, share best practices, and develop and implement more efficient digital solutions. ■

NEMA names new board of governors

The National Electrical Manufacturers Association (NEMA) announced that Annette Clayton, chief executive officer and president, North America, for Schneider Electric, was elected chair of the NEMA board of governors. Clayton joined Schneider Electric in 2011 after serving as vice president of global operations at Dell for five years. Before that, Clayton spent 23 years at General Motors in various roles.

In her remarks at the virtual NEMA annual meeting, Clayton said, "We have faced many new challenges this year, and we saw accelerated demand for a digital world. It's clear there is a need for new electrical infrastructure that is intelligent and supportive of renewable and sustainable environments."

"It's time to move NEMA beyond efficiency," Clayton added. "Together, we can move to a holistic energy system that is connected, cybersecure, renewable, sustainable, and intelligent."

In addition to Clayton, the NEMA board of governors elected a slate of officers: vice chair Richard Stinson, Southwire Company; treasurer Jack Nehlig, Phoenix Contact; and immediate past-chair Raj Batra, Siemens USA. The members also elected four individuals to fill vacancies on the board of governors: Bryan Mulligan of Applied Information, Inc; Michael Plaster of ABB; Richard K. Reece of Acuity Brands, Inc.; and Anders Sjoelin of S&C Electric Company.

NEMA president and CEO Kevin J. Cosgriff said Clayton's experience "will be especially important to incorporating the economic and other lessons of 2020 as we plot a course to enhance further the lives of citizens, the health of our businesses, and the well-being of our country in the years ahead." ■

Cyberattackers turning to encrypted attacks during pandemic

Cloud-security vendor Zscaler, Inc. released its *2020 State of Encrypted Attacks* report, which compiles new threat research published by the Zscaler ThreatLabZ team. The research reveals the emerging techniques and affected industries behind a 260 percent spike in attacks using encrypted channels to bypass legacy security controls.

COVID-19 is driving a ransomware surge, with Zscaler researchers witnessing a fivefold increase in ransomware attacks over encrypted traffic beginning in March. Phishing attacks rose in 2020, with the manufacturing sector being the most targeted (38.6 percent) followed by services (13.8 percent) and healthcare (10.9 percent). As one of the most commonly used attacks over SSL, phishing attempts reached more than 193 million instances during the first nine months of 2020, according to the report.

The research revealed the top industries under attack by SSL-based threats were: healthcare at 1.6 billion (25.5 percent), finance and insurance at 1.2 billion (18.3 percent), manufacturing at 1.1 billion (17.4 percent), government at 952 million (14.3 percent), and services at 730 million (13.8 percent).

The report provides guidance on how information technology and security leaders can protect their enterprises from the rising trend of encrypted threats, based on insight sourced from over 6.6 billion encrypted threats across the Zscaler cloud from January through September 2020. ■

U.S. DOE Smart Manufacturing Institute announces new project call

The U.S. Department of Energy's (DOE's) Clean Energy Smart Manufacturing Innovation Institute (CESMII) announced up to $4 million in new funding to improve energy-intensive manufacturing processes and strengthen the U.S. manufacturing sector. Founded in 2016, in partnership with DOE's Office of Energy Efficiency and Renewable Energy, CESMII accelerates smart manufacturing adoption through the integration of advanced sensors, data analytics, platforms, and controls to improve energy productivity and efficiency in manufacturing.

CESMII seeks research and development projects that can apply smart manufacturing solutions to real-world manufacturing process and operation challenges for improved energy productivity, performance, quality, and efficiency. For this request for proposals, CESMII anticipates making awards with periods of performance of up to six months. Industry partners must provide at least 50 percent of the total project funding. Projects may range from $50,000 to $200,000 (federal + cost share).

Learn more about the application deadlines, areas of emphasis, and submission requirements at www.cesmii.org.

"Smart manufacturing technologies have potential application and impact across the entire manufacturing sector. Creating innovations in new, integrated, systematic processes with a highly skilled smart manufacturing workforce and vibrant supply chain is vital to a global transformation of the manufacturing industry," said deputy assistant secretary for energy efficiency Alex Fitzsimmons. "DOE's investments in smart manufacturing allow the American manufacturing sector to become more productive, more energy-efficient, and more competitive on a global scale." ■

Industrial Internet Consortium releases COVID-19 response journal

The 15th edition of the *Journal of Innovation (JoI)* from the Industrial Internet Consortium (IIC) is focused on "IoT enabling fast response to COVID and other pandemics." This edition shows how IoT will play a crucial role in helping IT organizations adjust to the "new normal" being ushered in by the novel coronavirus, from working at home to social distancing.

"The impact on global business has been unprecedented, as millions of workers have moved their offices to their homes," said Edy Liongosari, cochair of the IIC Thought Leadership Task Group and chief research scientist for Accenture Labs. "In this edition of the *JoI*, IIC members discuss how IoT can help companies protect themselves and others now and [in the] aftermath of the pandemic." Guidance includes:

- "IoT-Enabled Global Process Validation System with Advanced Process Control (APC) Capabilities for Global Production Rollout of COVID-19 Vaccines," by Ramya Mopidevi of SAS Institute, which describes IoT processes for ensuring high manufacturing quality and accelerating production at the same time.
- "Physical Distancing and Crowd Density Monitoring Using Computer Vision," by several authors from SAS Institute, including Saurabh Mishra, Hamza Ghadyali, Kedar Prabhud, Varunraj Valsaraj, Hardi Desai, and Ravi Shankar Subramanian. The article provides an analysis of physical distance compliance in everyday spaces using video, deep learning, and streaming analytics.
- "COVID-19 Can Create Opportunity for IoT in the Caribbean: A Necessary Digital Transformation," by Jason Robert Rameshwar, The University of the West Indies, presents results of a survey that explores the potential of smart devices during the pandemic. ■

CO2 gas sensor technology breaks out

Due to the close link of indoor CO2 concentration and aerosol density, using CO2 gas sensors to monitor the indoor environment can be an efficient method to control the COVID-19 outbreak. According to industry research firm IDTechEx, the German government is among the first to invest in this technology, installing CO2 gas sensors in schools to indicate when the air in the room is unhealthily stale. The Federation of European Heating, Ventilation and Air Conditioning Associations (REHVA) has also published guidance for schools to install a CO2 monitoring system with traffic light indication.

The IDTechEx report "Environmental Gas Sensors 2020–2030," benchmarks the performance, cost, and manufacturing maturity for various gas sensing technologies. While electrochemical gas sensors and metal oxide semiconductor gas sensors are cheaper and smaller, says the report, NDIR gas sensors are more reliable and sensitive for CO2 monitoring.

Infineon launched new CO2 environmental sensors based on photoacoustic technology. This new product is believed to perform at a similar level as NDIR gas sensors at a significantly lower cost. Photoacoustic-based CO2 gas sensors are also provided by Sensirion. Both companies report increasing demand for such CO2 gas sensors for HVAC systems and indoor air quality applications.

This new trend will boost the potential market for CO2 gas sensors. IDTechEx predicts that more than 50K gas sensors will be installed in Germany alone in 2021 and the demand for CO2 gas sensors globally will exceed 1 million units if other European countries and the U.S. government decide to follow the same path. ■

Letter to the editor: Don't forget Bill Biles

In your recent *InTech* article, you called Pat Kennedy the "father of plant historians." No doubt Pat indeed brought to market in 1985 by far the most popular and widespread, essentially *the* de facto historian, in the industrial marketplace. But to my knowledge, Pat was not the first to introduce a historian with a compression algorithm to minimize data storage. That honor should go to Bill Biles of W.R. Biles & Associates, who introduced the (later named) AIM System before Pat's PI. Biles & Associates was formed in 1970 before both Oil Systems and DMC, where Charlie Cutler was also ex-Shell and a colleague of Bill's. I learned this when I worked for Biles from 1995–1997. Biles & Associates struggled to transition from VAX VMS to Microsoft Windows, something that Pat successfully did with PI. As a result, SimSci (now AVEVA) acquired them in October of 1997. The AIM system has long since disappeared. Unfortunately, few people are left to know the origins of Biles & Associates, as Bill passed not long after the SimSci acquisition, and we lost Charlie earlier this year.

Joseph O. "Joe" Perino
Research Analyst
LNS Research, Cambridge, Mass.

The Plant Floor in Your Pocket

Get an overview of your process at a glance.
Control your SCADA with a swipe.

See the live demo now.
Scan this QR code with your phone
or visit demo.ia.io/tech

Using IIoT technology to improve reliability and safety

By Marcelo Carugo

ABOUT THE AUTHOR

Marcelo Carugo works with downstream manufacturers globally to create a path to operational excellence and digital transformation. He joined Emerson in 1998 and has more than 30 years of experience in the chemical and refining process control industries both domestically and internationally.

Digital transformation is a strategy for using digital technologies, such as the Industrial Internet of Things (IIoT), to improve performance. While the process industries have used digital technologies for decades, the introduction of the Internet and other advanced communications methods, such as improved internal intranets, have eased implementation. This has helped to extend the same types of improvements seen in core manufacturing production processes into other operational areas, like reliability and safety.

Many of these IIoT applications, whether powered by the Internet or internal intranets, have become more relevant as employees increasingly work from remote locations, requiring enhanced collaboration among widely dispersed personnel. An example is the remote monitoring of valves, along with collaborating for maintenance and repair, to improve reliability. Remote monitoring starts with data collection, enabled by digital valve controllers, which provide extensive information for use by asset management, distributed control, and other host systems.

These controllers communicate to host systems using the HART protocol, WirelessHART with the addition of an adapter module, or a digital fieldbus. Host systems send data to remote experts via the Internet or internal intranets for analysis to provide actionable insights, which can call for valve maintenance or repair.

In the past, local technicians would have had to perform many of these activities on their own, because communication with experts was limited to email, phone, and text. But now, remote assistance services empower local technicians by giving them mobile device connectivity via the Internet, so they can securely share their field of view through augmented reality software in real time.

The software automatically identifies the specific valve installation, along with its maintenance history and repair instructions. Step-by-step instructions are overlaid in the user's field of view to support installation, calibration, or repair actions.

Real-time video communication enables users to resolve issues faster and minimizes instruction errors, while eliminating travel time and the cost of getting experts to the work site. In addition, companies can expand their in-house knowledge base and staff skill sets through on-the-job troubleshooting guidance and recommendations to remediate issues, up to and including oversight of the final repair.

Another digital technology widely deployed to improve safety and efficiency is radio frequency identification (RFID). Many valves are located in hazardous and hard to reach areas, with damaged or missing ID plates common. Technicians must often perform research to identify these valves, decreasing productivity.

> Once software automatically identifies a specific valve installation, step-by-step instructions overlaid in the user's field of view can support installation, calibration, or repair actions.

A better approach utilizes RFID technology to identify, track, and manage valve assets in a safer, more efficient, and more accurate manner. An RFID tag is installed on each valve, either before it is placed in service or during a safe period of operation, enabling automation of otherwise time consuming, error prone, and sometimes dangerous methods for identifying valves. An RFID reader is used to scan the tag, and the associated valve information is sent to an asset management system via the Internet or company intranet. This approach accurately enables more proactive maintenance—along with improved asset management and operational efficiency—by determining asset identity with a scan, and then using this detailed information.

These examples show how IIoT technologies can drive digital transformation to extend improvements beyond basic automation to provide enhanced reliability and safety, with other applications limited only by the end user's imagination and needs. ■

Achieving multivendor interoperability with open systems

ExxonMobil collaboration helps create a converged IT/OT industrial control system based on open standards

By Bill Lydon

A big step toward achieving multivendor interoperability with open systems was demonstrated by CPLANE.ai and collaborator ExxonMobil this year: It proved that deploying and integrating general computing and Internet of Things (IoT) technology using open standards as part of the industrial control system (ICS) provides great benefits. This foundational work will allow deep integration of intelligent processing, driven by machine learning, to achieve more efficient, adaptable, and reliable next-generation systems.

The pilot project used open computer industry standards to demonstrate the automation of provisioning, initiation, and life-cycle management of open-architecture, multivendor industrial control systems. The pilot leveraged a number of standards, including the Open Process Automation™ Standard (O-PAS), OPC-UA, DMTF Redfish, IEC 61499, and OASIS TOSCA (Topology and Orchestration Specification for Cloud Applications).

This pilot proved using orchestration to deploy and integrate general computing, IoT, and process automation, using open standards as part of the ICS, optimizes and simplifies the management of multivendor systems while improving security and reliability.

FAST FORWARD

- Open, multivendor system orchestration is critical for accelerating the innovation and adoption of converged IT/OT systems.
- A pilot project validates open, multivendor systems life-cycle management.
- Open computer industry standards efficiently deliver multivendor ICS life-cycle management.

Pilot overview

The pilot consisted of a heterogeneous mix of information and operational technologies (IT/OT) simulating a chemical processing plant. The system started with industrial IT compute devices (replacing legacy distributed control systems and programmable logic controllers) connected to an Ethernet network. The compute devices were also connected to specific industrial I/O networks (based upon the design of the plant). The CPLANE.ai industrial orchestrator was used to fully install and configure all process control software and control logic to bring the simulated plant to an operational state. This took approximately 10 minutes, compared to an estimated 50–100 person-hours by conventional methods.

Key findings of the project were:

- Multivendor, open process automation can be integrated into a holistic system using open system orchestration technology.
- Open standards, such as the O-PAS, make interoperability significantly easier to manage and more reliable to implement.
- An integrated, hybrid architecture of IT/OT digital assets can be managed in one framework.
- System orchestration is critical for accelerating innovation and adopting converged IT/OT systems, particularly in an open, multivendor, and interoperable control system.

Don Bartusiak, chief engineer for process control at ExxonMobil Research and Engineering said, “CPLANE.ai exceeded our expectations on what is possible in demonstrating the management of a converged IT/OT industrial control system. System orchestration is growing in visibility and importance within the Open Process Automation Forum, and many of the findings of this pilot will help us shape the evolution of our standards.”

Goals of the orchestration pilot

This pilot was conceived and executed in the context of rapid changes in industrial automation. Large industrial manufacturers like Merck, DuPont, Shell, BASF, Georgia Pacific, and Exxon-

Mobil are making new demands on traditional process automation vendors for solutions that unify information technologies and operational technologies into a single system of management and control. They want these converged IT/OT systems to be open, interoperable, and inherently secure. Global standards bodies, such as the Open Process Automation Forum, OPC Foundation, and NAMUR, are developing the standards for these open systems. The specific purposes and goals of the pilot were to:

- reduce the complexity and effort of deploying an ICS by orders of magnitude compared to conventional methods
- perform a full ICS deployment with little to no IT expertise
- conform as much as possible to open standards and practices as defined by the O-PAS
- demonstrate the automated provisioning and initiation of a multivendor, converged IT/OT control system from a pre-software-installation state to a fully operational and ready state—the “startup phase”
- demonstrate a significant reduction in the complexity and effort required to perform this “startup phase” of both IT and OT systems compared to existing, manual software installation processes
- perform this “startup phase” with little or no IT expertise from the perspective of the system operator
- prove that an orchestration platform can provide hands-off deployment of a converged IT/OT system that conforms to the open, multivendor specifications outlined in the O-PAS
- prove that DMTF Redfish can reliably provide physical system metadata to facilitate correct deployment of OT software applications
- specifically demonstrate the use of cloud technologies and standards like OASIS TOSCA for orchestration

Life-cycle system management

Managing an automation system over its life cycle is a significant investment that includes adding field controllers and I/O points, updating and upgrading software and firmware, adding features, and reconfiguring control. Today users are faced with using separate tools from each distributed control system (DCS) and programable logic controller (PLC) vendor they have in their operations, which requires unique support, training, and software maintenance agreements. For greater efficiency and responsiveness, the computer, communications, and IT world have been using open orchestration tools and techniques so a single operator, or even no operator, can manage huge and complex digital infrastructures.

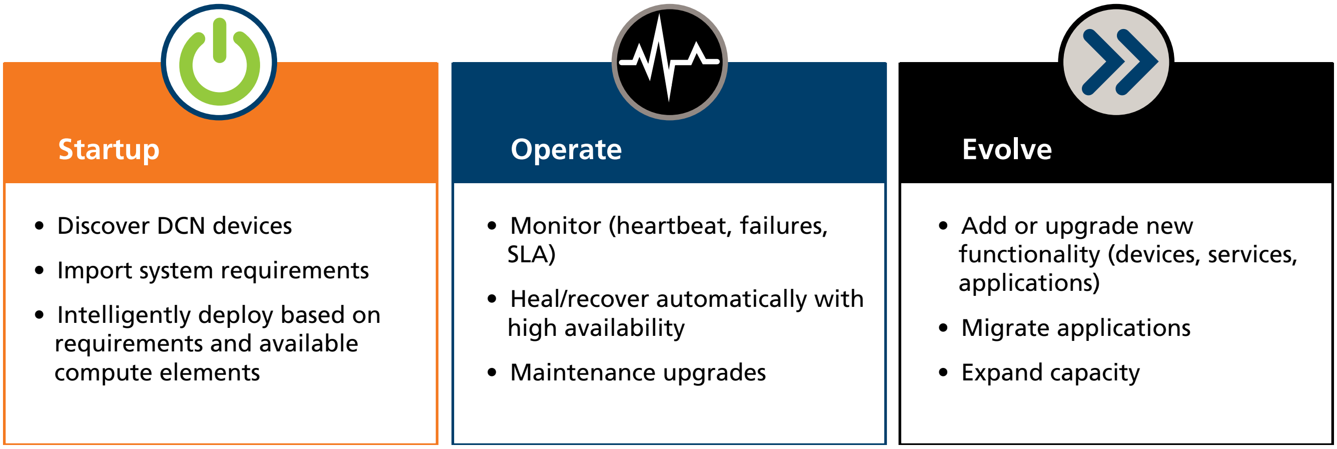
Industrial orchestration manages all compute elements, software stacks, control applications, networks, and containers as a single, integrated system. As next-generation industrial control systems transition to a rapidly maturing and increasingly complex digital technology stack, system orchestration customized for industrial systems is important for creating a system from open components from multiple vendors.

Steve Bitar, an automation leader at ExxonMobil Research and Engineering, said “this was an ambitious project from the beginning. And the results have really given us a vision for how complex open industrial control systems can be managed and automated.”

In this pilot, the CPLANE.ai orchestration platform was deployed to solve the complex digital life-cycle problems of managing large edge computing, distributed clouds, and Industrial IoT environments. It was customized to meet the needs of industrial systems. CPLANE.ai has been actively involved in the Open Process Automation Forum over the past three years and is an important contributor to the Open Process Automation Standard.

Pilot plant description

The pilot plant for the demonstration simulated a chemical mixing and heating process involving several plant assets: a reactor batch processor, a heat exchanger, product storage tanks, and a water chiller. The pilot infrastructure consisted of 14 individual compute devices that represented 13 distributed control nodes (DCNs) and a single advanced computing platform



Startup

- Discover DCN devices
- Import system requirements
- Intelligently deploy based on requirements and available compute elements

Operate

- Monitor (heartbeat, failures, SLA)
- Heal/recover automatically with high availability
- Maintenance upgrades

Evolve

- Add or upgrade new functionality (devices, services, applications)
- Migrate applications
- Expand capacity

Figure 1. Three phases of the plant life cycle are managed by system orchestration. This pilot focused on the startup phase, because it provides foundational capabilities required for the Operate and Evolve phases.

(ACP). The DCNs ran the control loops for the industrial process while the ACP hosted the human-machine interface (HMI) application and the IEC 61499 engineering design tool. The compute devices were a combination of different microprocessors (Intel X86 and ARM), with different configurations of RAM and storage, from different manufacturers. These devices were also divided between two locations, with approximately half in New York and the other half in California, to represent a truly distributed topology.

The compute devices were connected on the northbound side to an Ethernet network, while the southbound side was connected to a (simulated) Fieldbus network with simulated sensors and actuators. The two operational sites (Calif. and N.Y.) were connected through a VPN connection via a third site, the CPLANE.ai datacenter in California. The entire digital infrastructure was managed from a single location in California.

The pilot demonstration

The goal of the pilot was to use automation (via the CPLANE.ai industrial orchestrator) to correctly install all the software necessary to deploy the control system of a simulated chemical plant. The CPLANE.ai orchestrator should complete this "startup phase" operation in approximately 10 minutes. Manual installation of a similar system often takes a team of two or three engineers several days or a week.

1. **The initial state** of the control system:
   - Sensors and actuators (simulated) were connected via an I/O bus or directly to the DCNs.
   - IEC 61499 function blocks were already created and compiled for the process in the engineering design tool.
   - All DCN and ACP devices were connected to an Ethernet network for both the control and data planes.
   - All DCN and ACP devices were powered on and preloaded with Linux and DMTF Redfish client (simulated in this demonstration with CPLANE.ai client software).
   - The CPLANE.ai orchestrator and the process automation system were running on the same control network on a dedicated X86-based device running Linux.
   - The IEC 61499 engineering design tool was connected to the CPLANE.ai orchestrator.
2. **The demonstration** began with the HMI running, but showing that it was not receiving sensor data, nor did it have knowledge of the digital infrastructure underlying the control system.
3. **In the first step** of the three-step deployment process, the operator initiated discovery of the digital infrastructure with a single mouse click in the CPLANE.ai orchestrator. The orchestrator then polled all the digital devices on the control network, registering each device into the orchestrator's information model database. Additional details of each digital device were ingested into the orchestrator's information model using the DMTF Redfish protocol and other standard IT discovery protocols. This discover process takes approximately 90 seconds.
4. **The orchestrator** then built a digital topology model of the physical infrastructure including in-depth data describing the physical infrastructure and its state. This topology model will be used to make intelligent decisions on exactly where each software element of the control system will be installed. Now, the orchestrator effectively has a "digital twin" of the control system's digital infrastructure in its memory.
5. **The orchestrator** could then display all of the digital infrastructure of the control system including rich detail for every connected device. Examples of details in the information model are:
   - microprocessor type and manufacturer
   - device manufacturer and model number
   - available device RAM and storage
   - utilized and available CPUs
   - device IP address
   - network zone
   - OS type and version
6. **The second step** of the three-step deployment process was to "program" the CPLANE.ai orchestrator with all of the requirements for the control system's "digital life cycle." This "programming" step was performed by uploading one or more OASIS TOSCA documents that contained all the system requirements in a structured, reusable data format (YML). Examples of the requirements in an OASIS TOSCA2 document are:
   - device requirements for software applications (e.g., microprocessor type, available RAM, OS type and version)
   - policies that govern system life cycle (e.g., software applications that are prerequisites for other software applications, high-availability requirements, security zone requirements, affiliations with specific I/O locations)
7. **The orchestrator** was now programmed with the "system engineering knowledge" in its memory. Using sophisticated algorithms, it could make intelligent decisions about which application should be installed on which device. And, equally as important, the orchestrator understood exactly which steps must be taken in the correct order to install all of the software for the entire system in an automated and deterministic manner.
8. **A converged IT/OT system** like a modern, open process automation system can only be effectively and efficiently managed within a holistic framework. The orchestration platform merged all the requirements, policies, procedures, workflows, and state management into a single fabric. This single management fabric could now act in multiple dimensions (detailed below) with a deep understanding of dependencies and interdependencies of the entire digital infrastructure including:
   - supervisory applications (HMI, historian)
   - process control applications
   - compute layer (OS, Docker, virtual machines)
   - network security
   - networking

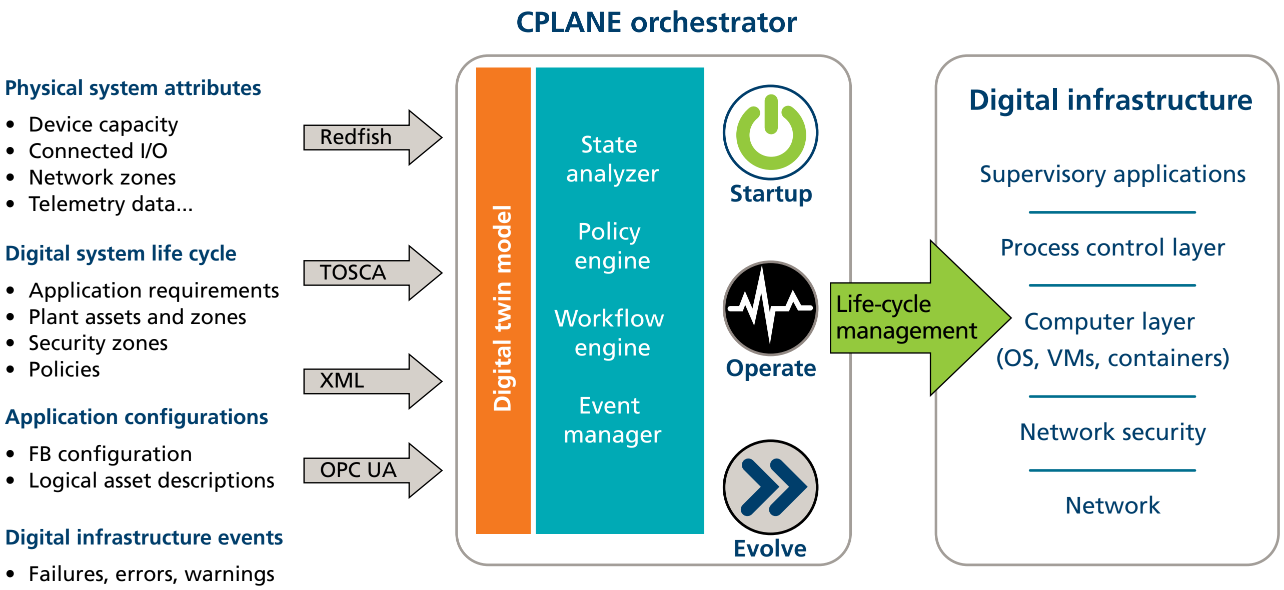


Figure 2. The CPLANE.ai orchestrator receives input from multiple sources and manages multiple layers of infrastructure as a single fabric.

9. **The final step** was to activate the orchestrator to deploy the ICS software. The operator simply pushed the "deploy" button, and the provisioning and installation operations commenced.

10. **The orchestrator,** in parallel, performed the following actions on all of the DCNs and ACP nodes of the system:

- examined the current state of each device as well as the entire system
- calculated the final desired state of each device and the whole system
- evaluated the policy constraints (the "rules") of each device (networking, security, prerequisites, etc.)
- calculated all the steps necessary to deploy the entire system without violating any of the constraints. This calculation then programed a workflow engine to execute each step both in sequence and in parallel where permitted.

The workflow engine (internal to the orchestrator) took actions such as:

- called premade scripts (like Ansible and Python) to direct installation routines
- dynamically created custom scripts where needed to instantiate a change in state of a device
- cleaned up devices to allow for new software installations.

Simultaneously, the orchestrator monitored the digital infrastructure for events that signaled successful actions taken or unexpected errors that required the orchestrator to take action or perhaps notify the operator.

11. **Some of the actions** performed on the system by the orchestrator include the deployment of:

- the OPC-UA client and server instance on 12 DCNs
- the OPC-UA discovery services (LDS) on a single DCN
- Docker containers on 12 DCNs that will host the engineering run time
- the engineering run time on 12 DCNs (in their respective Docker containers).

Also, the orchestrator directed the IEC 61499 engineering design tool to install function blocks on specific DCNs once the engineering run-time environment was ready.

12. **This deployment process** took approximately five minutes to perform. The end result was a fully deployed control system.

13. **Switching back** to the HMI, the first thing that was noticeable was that there were values in the sensor displays showing that OPC-UA had been installed correctly, was connected to the right I/O, and was successfully sending data to the HMI.

14. **Using the HMI,** the (simulated) chemical process was started. Each DCN successfully executed its function block code to make the chemical process operate as expected.

15. **This whole "startup phase"** operation took approximately 10 minutes from the initial state as described above to a fully operational state where the HMI could initiate control functions.

Engineering principles applied to pilot demonstration

System startup (the "startup phase") is not the end goal of using system orchestration. The primary goal is to maintain continuous plant operations during change, failure, or upgrade as specified by digital life-cycle policies. The "startup phase," demonstrated in this pilot, lays the foundation for future phases to demonstrate continuous plant operations.

Automated management of complex digital systems has been done before. Converged IT/OT control systems must follow the success of other industries' successful management of large, complex systems. Orchestration has been widely adopted to manage the life cycle of global telecommunications networks, automate the world's largest cloud data centers, and to accelerate the deployment and maintenance of software applications for every large business.

Do not just "make it work." To avoid costly dead ends, choose a standards-based framework that is designed for industrial automation, rather than the currently "hot" technology.

Key lessons from the pilot

1. "Systemness" for open systems is achievable using system orchestration. Multivendor, open process automation can be integrated into a holistic system using the technologies and techniques of orchestration.
2. Open standards make interoperability significantly easier to manage and more reliable to implement. These open standards will continue to evolve as technologies evolve, which will help to future proof your investment.
3. Integration with current OT solutions requires cooperation and collaboration from vendors but is achievable with spectacular results. Shift thinking from IT and OT to an integrated hybrid architecture of IT/OT digital assets managed in one cohesive framework.
4. System orchestration is critical for accelerating innovation and adoption of converged IT/OT systems.

CPLANE.ai is now conducting demonstrations of its digital infrastructure test bed with partners and members of OPAF. In the future, the company will apply the lessons from this pilot project to other OPAF-related test beds and pilots globally. Certainly, this pilot project illustrated a way to leverage open standards for life-cycle management of industrial control systems.

For a whitepaper describing the methods and results of the pilot, see www.cplane.ai/industrial_orchestration/whitepaper. ■

ABOUT THE AUTHOR

Bill Lydon, *InTech* contributing editor, brings more than 10 years of writing and editing expertise, plus more than 25 years of experience designing and applying technology in the automation and controls industry. Lydon started his career as a designer of computer-based machine tool controls; in other positions, he applied PLCs and process control technology. In addition to working at various large companies (e.g., Sundstrand, Johnson Controls, and Wago), Lydon served a two-year stint on a five-person task group, where he designed controls, automation systems, and software for chiller and boiler plant optimization.

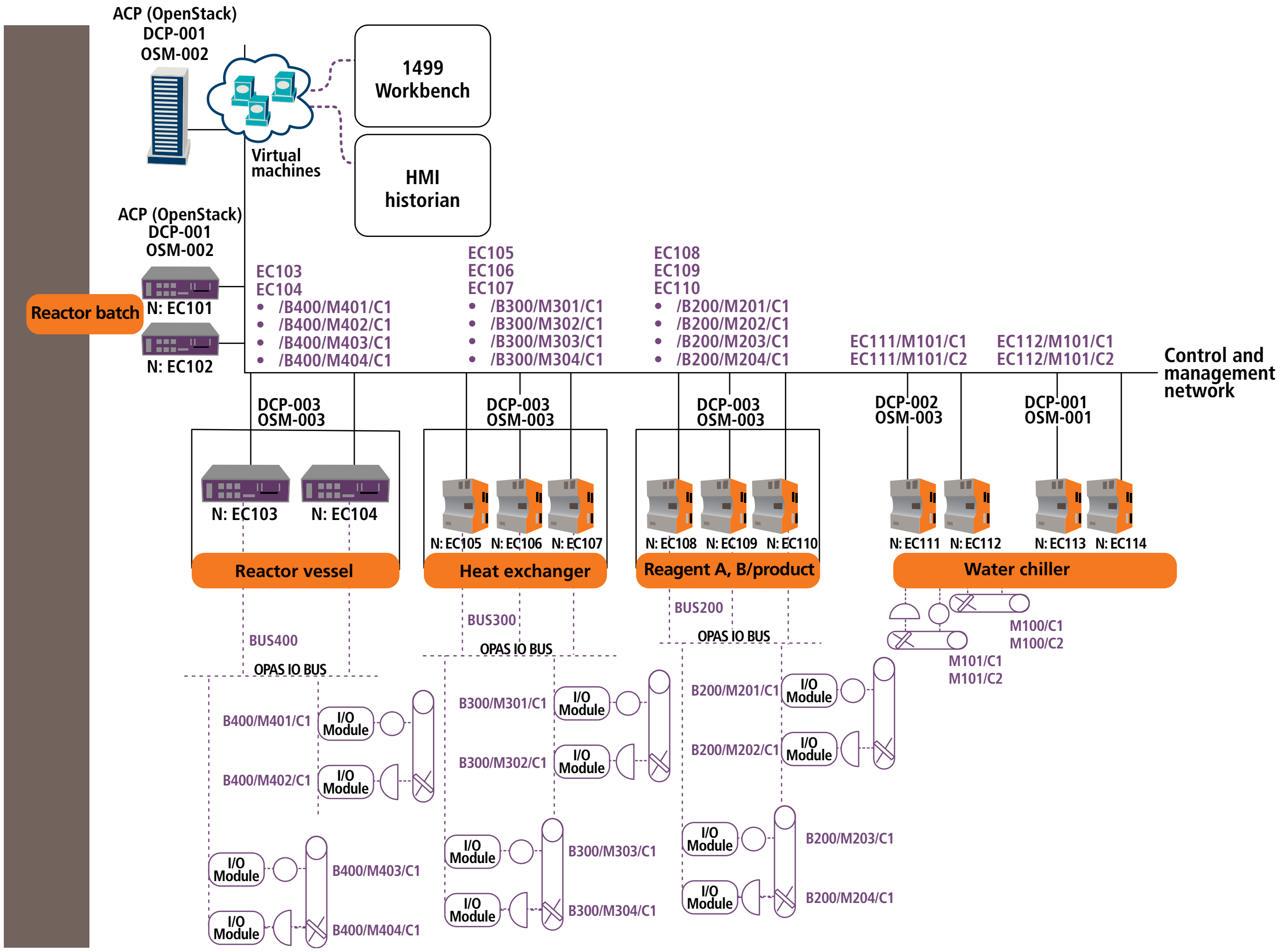


Figure 3. The topology of the pilot infrastructure.

Augmented reality supports fundamental maintenance shift

By Vincent Higgins

Augmented reality (AR) has the potential to dramatically enhance productivity and training in maintenance. It is, though, just part of a more fundamental shift. Its supporting technologies will have a greater impact.

In some sectors, such as refining and chemicals, maintenance costs constitute the largest operational expense after feedstock. Between 2015 and 2019, oil and gas companies involved in exploration and production spent an average of $80 billion a year on maintenance. Across the process industries, it is a major expense.

In the short term, it is hard to say whether the current challenging times will increase or reduce this. Requirements for employees to physically distance and work from home, along with plummeting demand, have seen many maintenance activities postponed. When sites miss weather windows or scheduled downtime, some tasks will be pushed into the next year or beyond.

Dramatically enhance maintenance productivity and training

Long term, though, two things should be noted. First, essential work must be done and has continued. Safety and regulatory requirements mean plants cannot postpone maintenance indefinitely. Second, the delays to scheduled maintenance carry risks, potentially increasing wear on parts and equipment or letting problems develop. In some cases, at least, plants are storing up problems for the future. Finally, operational expenses are, in most cases, being set against a decline in revenues.

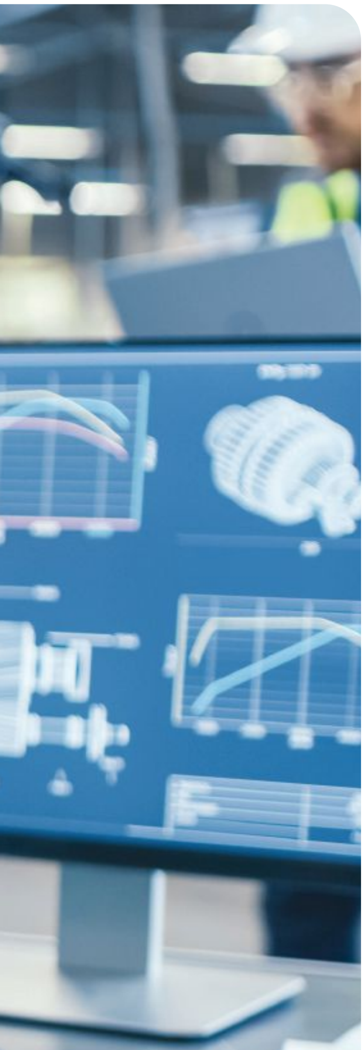
Controlling maintenance costs, therefore, remains a consistent challenge. And a range of technologies will play an increasing role in meeting it.

Changing of the guard

In fact, despite present challenges, many of the current issues for businesses when it comes to maintenance are long standing. Today's uncertainty has only made them worse. For instance, physical distancing and travel restrictions have in many cases led to reductions in on-site staff, the use of skeleton crews, and increased reliance on remote working and collaboration. But this was an existing trend across a range of industries.

On the one hand, that is driven by the pressure to cut costs and do more with less. Reducing overheads has usually meant efforts to reduce on-site headcounts. It is also informed by another imperative, however: the need to address skills gaps and an aging workforce.

In the energy industry, more than 70 percent of the workforce is over 50 years old. The generation of baby boomers is retiring, taking decades of experience with them. Consultant Accenture Strategy estimated in 2015 that baby boomers accounted for nearly 19 percent of the oil and gas workforce. By 2025 that figure is expected to be just 7 percent.



Companies can enhance productivity and training using AR/VR technology.
Source: Honeywell

FAST FORWARD

- Skills gaps, cost pressures, and ongoing technological challenges are testing traditional maintenance approaches.
- Augmented reality brings significant benefits as both a training and productivity tool to help meet this challenge.
- To realize the full potential, businesses need to look to the technologies behind AR for a new approach to maintenance.

In their place come the millennials, already the largest generation in the general workforce. Businesses face a number of related challenges:

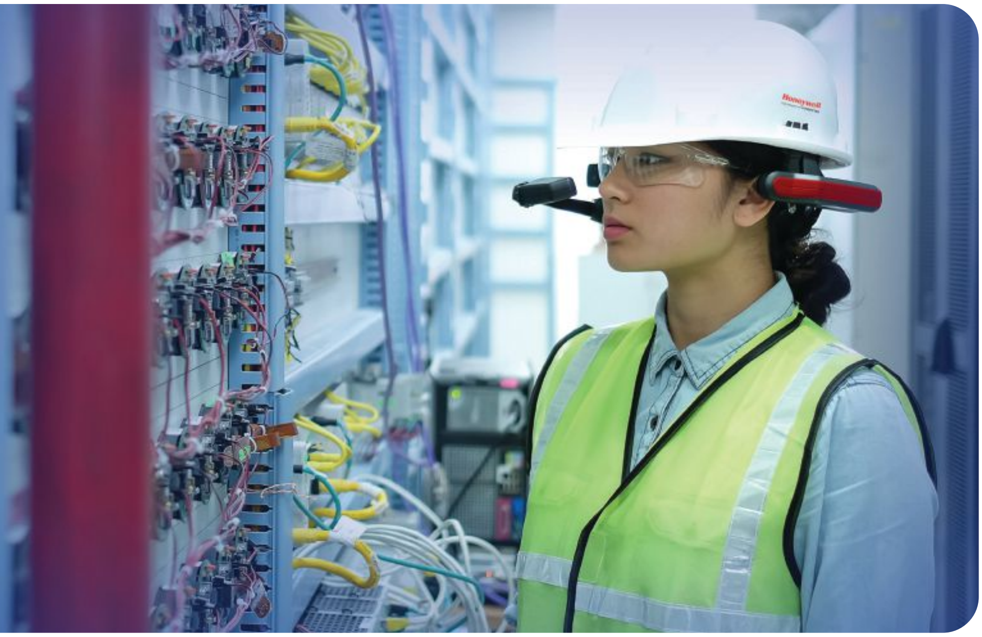
- Capturing the knowledge of the retiring workforce and harnessing the remaining expertise of their more experienced workers.
- Passing this knowledge and experience on to millennials, who as a generation prefer experiential learning to traditional classroom-based methods.
- Doing so quickly in the face of increasing staff turnover. Many millennials do not stay in jobs for long. Reducing the time to achieve competency maximizes their period of productive work.

Companies must do all this while promoting the quality of their maintenance, both to foster site safety and to protect against the massive costs of unplanned downtime. Research by the Abnormal Situations Management Consortium shows that individuals directly cause up to 40 percent of abnormal situation losses due to three key contributors: insufficient knowledge, operator oversights, and maintenance work mistakes.

A better reality for teaching

Augmented reality (AR) is starting to become a critical technology in avoiding these losses and meeting the challenges posed by both the current unprecedented times and longer-term trends. The technology has the benefit of being familiar to much of the generation currently entering the workforce. Basic AR technology using smartphone cameras and displays to superimpose graphics and information on the real world has been widely used for games such as Pokémon GO, downloaded over 1 billion times. Combined with smart glasses and wearable computers, AR is also a powerful industrial maintenance technology.

The applications are manifold, and AR has capabilities as both a training and productivity tool. For training, AR functions as a less immersive, but potentially more versatile solution



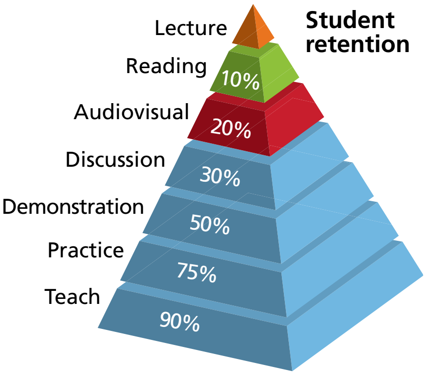
Hands-free, wearable devices allow industrial workers to more safely, reliably, and efficiently accomplish their tasks in the plant or the field.

than virtual reality (VR). A VR headset places workers in a fully immersive virtual world, recreating a realistic plant environment, for example. AR, though, can still simulate equipment and project its image using the headset, making it suitable for situations where workers need to retain an awareness of their physical environment. Workers could potentially even use it to learn or rehearse tasks while in the field.

In both cases, the benefits of AR and VR to learning are well demonstrated. The learning pyramid shows that students retain seven or eight times the information from practicing a task compared to reading about it or hearing a lecture. AR and VR offer tools to allow maintenance workers to practice critical, complex, or infrequent jobs in a realistic but safe environment. In practical industrial applications, this has been shown to slash standard times to achieve competency for field workers from six months to two.

The technology is also more flexible than traditional approaches. Rather than requiring trainers to be on site or bringing employees to a central training location, training can be deployed and managed remotely. Experts can view, guide, and assess the activity of trainees using the tool regardless of where they are based. Users can also access training on demand, both for initial training or to refresh or practice new tasks as required. Experienced workers can practice a job in the morning using AR and complete it in the afternoon—arriving in the field fully prepared.

Learning pyramid



Audiovisual tools help students retain more, and practice leads to 75 percent retention rates.

Just as simulation has become essential in the process industries for operator training, AR and VR have the potential to transform the way maintenance workers learn.

Using your head, freeing your hands

VR is primarily a training tool for maintenance; however, AR is also a powerful productivity solution. By combining a heads-up display, wearable computer, and voice recognition, the approach unlocks a wide range of functions and applications:

- Providing information on demand. Giving maintenance workers hands-free access to process information, equipment diagnostics, instructions, and manuals, AR can enhance situational awareness, accelerate troubleshooting, and reduce repair times.
- Video-on-demand can show workers how to complete every day or complex maintenance tasks, providing users with step-by-step guides they can access in the field.
- Front-facing cameras and cellular connectivity can share the field worker's view with remote experts to offer guidance or instruction, helping prevent errors and accelerate work.
- Tracking, monitoring, and logging maintenance work to monitor asset performance, inform training, and capture accurate maintenance metrics, such as mean time to repair (MTTR) and mean time between failures (MTBF).

With solutions built on top of standard mobile operating systems, businesses can develop bespoke applications, making the tool almost infinitely adaptable.

Providing hands-free access to contextual information, guidance, advice, and tutorials on demand and in the field, AR supports existing maintenance staff. They work more confidently, more correctly, and more quickly. It also enables businesses to send trainees safely into the field sooner, comfortable that they can receive instruction and guidance as required. It will empower a new generation of maintenance staff to learn as they work and work as they learn.

AR is not only a tool to provide access to guidance and expertise; it is also the ideal tool to capture it. Experienced workers using such headsets can capture and catalogue tasks as they complete them on their round, recording the steps taken to complete them successfully.

Although augmented reality is an undeniably powerful technology, it is important to be realistic about its limitations. Crucially, we should note that AR headsets are of little value without a range of supporting technologies.

Most obviously, workflow software is the platform on which the AR runs, and it largely decides the effectiveness. It is responsible for the ease and accuracy with which maintenance steps can be captured and shared. And its ability to access and display relevant contextual information will have a significant influence on AR's value as a tool.

More broadly, all this is also supported by the availability of data and the ability to turn it into actionable intelligence, which relies on two further technologies: the Industrial Internet of things (IIoT) and data analysis. The IIoT and the ubiquity of affordable sensors and transmitters is the foundation of smart maintenance. Cloud-based analysis—able to turn this into intelligence, trends, and reports—can provide the supporting walls.

This information gives AR users in the field essential contextual and diagnostic information that can reduce safety risks, prevent errors, and accelerate repair times. But these technologies have much greater potential.

Transformative technologies

Viewed critically, traditional approaches to maintenance assume either failure or waste. In the first case, run to failure strategies can be effective for easily and cheaply replaceable devices or assets, particularly where redundancy is built in. They are inappropriate for significant or critical equipment, however, and in any case where failure risks costly replacement, safety incidents, or considerable disruption to the process.

For this equipment, businesses employ some form of periodic maintenance, whether according to a standard schedule or adjusted to take a risk-based approach. Maintenance metrics such as MTBF may feed into these, as may MTTR. The first indicates the likely life of the asset, while the latter partly determines the disruption, overall cost, and therefore, risk involved in a failure. In both cases, though, a level of inefficiency is accepted. Maintenance is undertaken and parts replaced in the absence of any faults.

IIoT and analysis software can provide powerful insights for maintenance workers using AR, providing contextual information, improving situation awareness, and directing them to the likely cause of problems quicker. But it can have an even more significant effect in informing maintenance schedules and empowering genuinely condition-based programs of work.

The data from connected devices can detect early signs of impending problems and help determine the work necessary to correct them. It improves how the work is completed by feeding into AR platforms. More importantly, however, it informs when, where, and what maintenance is assigned to eliminate unnecessary work while reducing the risk of equipment failures.

When businesses realize the full potential of the technology, maintenance workers will arrive on site with the right knowledge, tools, and support to get the job done quickly and efficiently. But more importantly, they will be working in the right place and at the right time to have the most significant impact on the operation's performance. ■

ABOUT THE AUTHOR

Vincent Higgins is general manager for Honeywell's Digital Transformation/Workforce Competency business, Honeywell Process Solutions, part of Honeywell's digital transformation offering. Before working at Honeywell, he was the CEO of a technology company that provides advanced digital solutions to industrial customers. Higgins also led a leadership consulting firm, assisting senior executives in organizational effectiveness. He is author of the book *Social Influence and Genius, A Leadership Journey – A Better Future for your Business and the World*. In the book, Higgins develops a model for organizational and leadership development.

IIoT and analysis software can provide powerful insights for maintenance workers using AR, providing contextual information and improving situation awareness.

RESOURCES

Coronavirus creates repair headache for oil and gas industry
https://uk.reuters.com/article/us-health-coronavirus-oil-maintenance-an-idUKKBN22V0LT

The "Great Crew Change"
https://www.ogj.com/home/article/17294840/the-great-crew-change

Millennials are the largest generation in the U.S. labor force
www.pewresearch.org/fact-tank/2018/04/11/millennials-largest-generation-us-labor-force

Engaging the millennial learner
www.apa.org/monitor/2010/03/undergraduates.aspx

The 2016 Deloitte Millennial Survey
www2.deloitte.com/global/en/pages/about-deloitte/articles/gx-millennials-one-foot-out-the-door.html

Is the future of machine design cabinetless?

Packaging machine builder Syntegon has standardized using panel PCs with custom push-button extensions, along with control panels, to minimize enclosures and support its HMI 4.0 program.
Source: Beckhoff

Smaller devices incorporating distributed intelligence enable space savings

By Matt Prellwitz
and
Sree Swarna Gutta

From the Industrial Revolution and Moore's Law to Industry 4.0 and lot size 1, industrial technology has always aimed to make production faster, smarter, and as compact as possible. Machines continue to get smaller and more efficient through innovations in controllers, industrial networking, and motion control. Manufacturers across industries benefit from purposeful implementation of new automation technologies, experiencing greater throughput, higher quality, and more space for additional systems in the factory. However, one large piece of the machine continues to take up substantial space on production floors: the electrical cabinet.

The idea of cabinetless machine design, although not entirely new, has been gaining significant acceptance. Whether for new designs, redesigns, or retrofits, the concept requires highly durable industrial components that can mount directly to the machine and withstand harsh production environments. This includes everything from motion control systems and I/O terminals to even the machine controller. Several real-world examples will highlight how to approach the idea, what results others have already achieved, and what barriers still exist. First, it is important to understand the goals behind the trend toward cabinetless machines.

Benefits of cabinetless design

Increasing available space on the factory floor is a main driver of cabinetless design. If companies could eliminate the square footage needed for electrical cabinets, they could use that space to add more machines. This is a win-win for the manufacturer and for the machine builder original equipment manufacturer or integrator. It generates additional business opportunities for both—having more products and lines means more machines and systems to build and install. As such, the room taken up by the supply-cabinet-sized metal box wastes profits for everyone involved.

Eliminating the cabinet, however, should not make implementation more complicated and time consuming than the traditional approach. Simplification is another goal of cabinetless design. With machine-mountable components, engineers should have the power to create more modular designs and to reduce cables and installation effort. Beyond eliminating electrical cabinet requirements, this removes potential points of failure, minimizes the risk of incorrect wiring through the use of standard connectors, enhances troubleshooting capabilities, and cuts costs. Shrinking cabinet requirements also reduces transportation costs when delivering machines to the end user facility.

Another factor is the push for more functional distributed devices. Installing smart components across a machine or line also allows for faster decision making and data acquisition. This could include secondary controllers, programmable safety devices, and servomotors with integrated drives that include safety logic and Internet of Things (IoT) gateways, among many other technologies. The key to this is ensuring that the machine does not grow in size just because it grows in functionality. Fortunately, many new component and cabling options make this goal achievable.

Smart components in a small footprint

Designing or retrofitting a machine to shrink or eliminate the electrical cabinet requires rethinking most of the major components. IP67 and IP69K field-mounted distributed I/O terminals allow communication and diagnostics directly on the machine. They provide more functionality than simple data input and output, such as programmable safety, compact motion control, and condition monitoring. For example, terminals with built-in accelerometers can measure machine vibration to benchmark machine health and schedule maintenance. The compact box modules come in industrial-hardened plastic, stainless steel, and zinc die cast form factors with many cabling and connector options to suit specific application requirements.

FAST FORWARD

- Simplification is an important goal of cabinetless design.
- With machine-mountable components, engineers can create modular designs and reduce cables and installation cost.
- Cabinetless installation removes potential points of failure through the use of standard connectors.

One cable automation (OCA): Combining power and communication in a single cable greatly reduces the amount of space required on the machine and the number of cable runs back to the controller. The open EtherCAT P (EtherCAT + Power) standard, for example, provides these capabilities for various field devices and motion control components. In addition, it has robust diagnostics.

Motors and drives: Traditionally, motors are ruggedized for the field, while a metal cabinet protects the more sensitive drives, and they remain separate. The cabinetless concept handles this using servomotors with integrated drives, which come in many different sizes and can be distributed across the machine. These distributed servo systems not only ensure that both the motor and drive are hardened for tough production environments, but also reduce space requirements and spread intelligence, such as onboard safety logic (e.g., SS1, STO), throughout the machine. In certain product families, multiple integrated motor-amplifier components link to a main IP65 supply module that communicates with a single cable back to a single servo drive or machine controller.

IP67 and IP69K field-mounted distributed I/O terminals have power and communication in one cable, reducing the amount of cabinet space required on the machine and the number of cables runs back to the controller.

Hardened components, such as Beckhoff's Distributed Servo System that can connect five servomotors with integrated drives via a distribution module, enable cabinetless machine designs.

Machine controllers: Programmable logic controllers (PLCs), programmable automation controllers (PACs), and industrial PCs (IPCs) are some of the last components that engineers would imagine installing outside a protective enclosure. They require a safe environment, free from any possible collisions, and they may have fans, buttons, interfaces, and other openings where water, dust, and other contaminants could enter. A new generation of machine controllers—including both IPCs and panel PCs—addresses these problem areas head on. Passive cooling, new connector types, and robust housings enable IP65/67-rated IPCs that withstand shocks and extreme temperatures. They easily connect to I/O and motion systems spread across the machine.

Power supplies: Literally taking the electricity out of the electrical cabinet, some manufacturers now offer power supplies that can be mounted in the field. These can supply power for a broad range of needs, from controllers to motors and beyond. However, as a relatively new development, field-mounted power supplies do not yet have the proven track record that other components do, so the engineering community may be slower to adopt this innovation. In addition, safe power delivery is one of the more problematic aspects cabinetless design, especially in motion-intensive applications, and these issues will come into the discussion shortly.

Of course, this list is not exhaustive, and as components become more functional and spread out, the lines will blur somewhat. Consider, for example, a recent range of compact drive components that combines the servomotor, output stage, and multiple fieldbus connections in a space-saving design. With standstill torques from 0.5 to 1.1 Nm, this component family meets many motion control requirements, reduces the number of standard I/O modules needed, and can monitor motor parameters (e.g., overvoltage, undervoltage, overcurrent, or motor load).

Small additions can create big opportunities to shrink or eliminate control cabinets. The cabinetless concept has implications for nearly every industry. However, intralogistics and packaging stand to benefit immediately, maybe more so than others.

Cabinetless design in intralogistics

Automation for material handling in fulfillment in distribution centers (DCs) was growing steadily before the COVID-19 pandemic, and has accelerated as a result of it. Automated guided vehicles and autonomous shuttle systems already incorporate IPCs, I/O, and motion control directly into the machine. However, more traditional DC technologies have not adopted these capabilities as quickly. Long runs of conveyors and sorters that stretch across the warehouse floor suffer from fieldbus shortcomings, including the inability to use line topology, the lack of diagnostics, and limits in physical distance. This causes issues with high-speed merges and sortation system drops, leading to expensive order returns in the highly competitive e-commerce market.

Greater use of cabinetless concepts and EtherCAT solved these issues for intralogistics equipment supplier EuroSort. When installing a large split tray sortation system and other systems at the Gap Inc. distribution center in Fishkill, N.Y., EuroSort implemented field-mounted EtherCAT I/O and one-cable technologies. Along with shorter scan times, EuroSort reduced wiring and panel requirements, simplified commissioning, and distributed intelligence, including functional safety,

EuroSort used elements of cabinetless design in the distribution center redesign for Gap, Inc., which optimized space, performance, and cost.

across the DC. Considering the equipment footprint reductions and higher system performance, tangible benefits of the new EuroSort split tray sorters have already piled up for Gap Inc., as well as other companies.

"Achieving 100 percent faster scan times and increasing overall accuracy of PC- and EtherCAT-based sorters have been huge advantages," says Greg Meyer, VP of sales and marketing at EuroSort. "Once Gap Inc. began using the new EuroSort split tray sorters in a new fulfillment center, order fulfillment accuracy went up 2 percent compared to the technology it replaced. These improvements avoided what otherwise would have been thousands of costly returns for the retailer."

Cabinetless design in packaging

The packaging industry continues to create new ways to maximize throughput and minimize downtime for changeovers, for example with linear transport systems and other motion control advances. However, machine footprint remains a significant barrier for consumer packaged goods (CPG) manufacturers and contract packagers. These businesses need to produce more products in varying quantities and with greater customization, down to lot size 1. Cabinetless design helps make this possible.

To make this happen, Syntegon (formerly Bosch Packaging) uses pole-mounted IP65 panel PCs in roughly 40 percent of its applications; pole-mounted control panels make up another 40 percent; and built-in, cabinet-mounted control panels make up the last 20 percent. This visualization program, which the packaging machine company calls HMI 4.0, brings machine control directly to the multitouch operator interface with custom push-button extensions. The panel PCs also allow for greater Industrial Internet of Things capabilities, which was another major factor in Syntegon's standardization decision.

A particularly apt example is one new tray and carton former, which uses a panel PC for control and operator interface. Machine-mounted EtherCAT box I/O modules spread data acquisition and other functionality across the machine. Most importantly, the distributed servo system provides coordinated, multi-axis motion with a single distribution module powering multiple servomotors with integrated drives. The machine handles up to 240 cartons per minute with versatility for multiple carton types, while only requiring a very small, attached cabinet for fusing—which brings us to the main sticking point.

Reasons to be cautious: Power and plant environments

The main barrier to cabinetless machine concepts is and will continue to be power. Dust, dirt, moisture, and other hazards may make it difficult to install IPCs, I/O, motors that require regen capabilities, and other components in the field, but it is possible—or will be in the near future. However, the outlook is not as bright for electrical supply and fusing components.

First, these products are not typically hardened for installation out in the open. Also, for machine manufacturers hoping to build standard products, it is much easier to meet the National Electric Code (NEC), in addition to other global and local standards, if the electrical components are in a separate cabinet. Often an isolation transformer is needed, as well as an additional safety circuit branch for machines drawing power above 20 A. That is, most machines. In these cases, the electrical cabinet reassures both the original equipment manufacturer and end user that the machine can be installed and pass inspection with no issues. The optimistic response is that eventually these components can also integrate directly into the machine. However, some are quite large and generate substantial heat, making it unfeasible and potentially unsafe to incorporate them.

In fabrication, for instance, large CNC plasma, laser, and waterjet cutters require significant power. The supplies can range from 8 kW for an average fiber laser cutter to more than 60 kW and 300 A for many plasma cutters. These units are large on their own, and they require large fuses as well. Some components could still move outside the cabinet, helping to reduce the footprint, simplify implementation, and distribute intelligence. However, fabrication applications often have other difficulties, such as abrasive material used in water jets, metal shavings, large moving objects, and arcs that must be protected.

Due to these factors, the electrical cabinet will not go away completely, so engineers in these fields may view designing automated loading or other systems to reduce space requirements on the fab shop floor as a better use of time. However, that does not negate the benefits of cabinetless design in many other applications.

Minimize cabinets whenever and wherever possible

Despite current difficulties in certain machines and industries, cabinetless design is the future. As automation continues to spread, companies need to install more machines to do more tasks in less space. The space freed up by eliminating electrical cabinets will allow them to invest in new product lines rather than new real estate. Like Industry 4.0 concepts, we are beginning to see applications from early adopters of cabinet-free technology. But as more engineers embrace this new paradigm in machine design, vendors will produce more components to support that vision.

Currently, machine builders can already implement many machine-mounted devices. From controllers and control panels to I/O and motion systems, a range of powerful automation devices already have the protection rating and capabilities to shrink electrical cabinets significantly for now, until enclosures become obsolete. ■

ABOUT THE AUTHORS

Matt Prellwitz (m.prellwitz@beckhoff.com) is the drive technology product manager for Beckhoff Automation in Savage, Minn. Over his 15 years of experience in the field of automation, he has held multiple application engineering and product specialist roles, focusing largely on motion control.

Sree Swarna Gutta (s.potluri@beckhoff.com) is the I/O product manager for Beckhoff Automation. She earned a master's degree in electrical engineering from Cleveland State University and has worked in the industry for 12 years, focusing largely on EtherCAT-based technologies.

The impact of safety instrumented system isolation on current and future plant operations

'Isolation' is a challenge to creating a secure ICS architecture

By Uduak J. Daniels and Nidhal Jamal

Advanced persistent threat (APT) attacks are on the rise against critical infrastructure. APT attackers use continuous, sophisticated, and secretive hacking techniques to gain access to a system and remain inside for a prolonged period of time—with potentially devastating consequences. The resilience and response to these incidents by asset owners have been commendable, reducing the potential impacts on safety, integrity, and reliability. Industry has responded to the most recent cyberattacks targeting safety instrumented systems (SISs) by recommending and legislating changes to the architecture of SIS networks and their interactions with other systems.

These new design requirements may mitigate the exposure of safety systems to APTs, but they also introduce design and integration challenges. These challenges will require significant innovation and thought leadership for those asset owners, automation suppliers, and integrators willing to proactively address them. In addition, regulatory mandates are driving the accelerated adoption of some form of partial or full SIS system isolation, leaving many asset owners scrambling to include these requirements within procurement language, with clarity and within ongoing projects. This article will define the threat scenarios and industry response options, and provide an approach for addressing requirements.

FAST FORWARD

- Advanced persistent threat (APT) attacks are on the rise against critical infrastructure.
- Most of the controls identified to reduce the likelihood of ATPs are straightforward, except SIS segmentation.
- Until the term "isolation" is defined and understood, asset owners may misinterpret their compliance with regulatory mandates.

History of SIS cybersecurity efforts

Safety instrumented systems shut down an industrial process to a safe state in the event of unreliable system or process functionality. This definition, although simplistic, is concise and makes it explicit to the nonindustrial observer that the term "safety" is the primary emphasis.

Asset owners and system integrators employ various design approaches to connect their plant's distributed control systems (DCSs) with the SIS. The traditional approach relies on the principles of segregation for both communication infrastructures and control strategies. The past decade has seen a trend toward integrating DCS and SIS designs for various reasons, including lower cost, ease of use, and benefits achieved from exchanging information between the DCS and SIS (https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html).

Until the 1980s, the codes of practice for designing and using trip and alarm systems were set down by major chemical and petrochemical companies. These codes established most of the ground rules used today. Over the past three decades, the International Electrotechnical Commission (IEC) and ISA can be credited with providing global leadership around the issues facing SIS by releasing standards. The current ones are ISA/IEC 61511-2018 and the technical report ISA-TR84.00.09-2017.

Evolving ICS-targeted cyberattacks

The journey to SIS isolation began in 1998 when the newly published ISA/IEC 61511 standard recommended the separation of management systems

(figure 1). As is typical across most industry verticals, however, cyberincidents tend to drive regulatory mandates; so, it is interesting to note that the introduction of the majority of SIS cyber-related regulation followed the Triton attack in 2017. Such an incident-driven approach to improved security, although beneficial, could itself be improved. Stakeholders will need a more proactive and forth-right approach to stay ahead of the ever-burgeoning industrial control system (ICS) cyberthreats.

A list of the ICS cybersecurity incidents that have affected and changed the industry are shown in table 1. In 2000, the Maroochy Water cyberattack caused the release of thousands of gallons of untreated sewage. The Triton/Trisis/HatMan malware attack in 2017 was the first-ever publicly known malware on a very short list of ICS-specific malware designed to target safety instrumented systems. From an architecture perspective, and not focusing on the other security vulnerabilities, the Triton attackers took advantage of a lack of clearly defined standards mandating network boundary segmentation and enforcement. The industry has since focused on the "Trisis" attribution, since this was the first publicly disclosed SIS cyberattack.

Industry response to Triton

Vendors, asset owners, cybersecurity first responders, and legislators have all provided various guidelines, best practices, advisories, and directives to reduce the exposure to threat actors targeting safety instrumented systems. Some of these guidelines include:

- Safety systems must always be deployed on isolated networks.

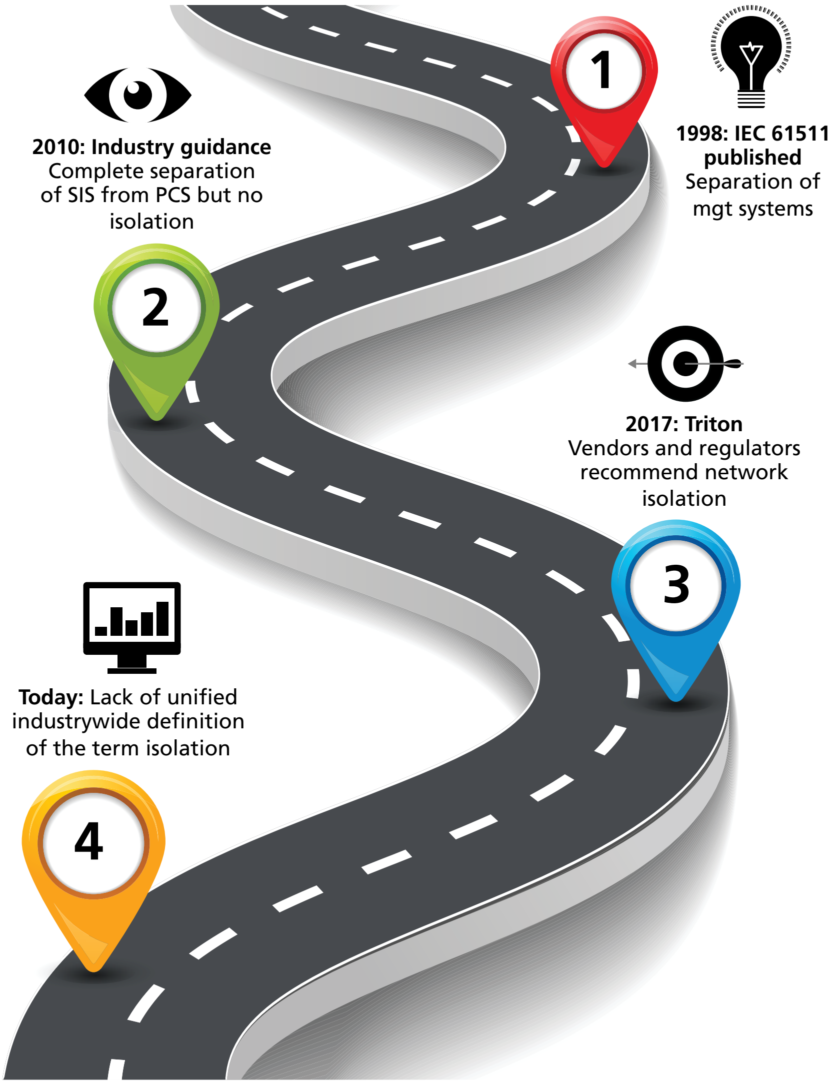

1
1998: IEC 61511 published
Separation of mgt systems
2
2010: Industry guidance
Complete separation of SIS from PCS but no isolation
3
2017: Triton
Vendors and regulators recommend network isolation
4
Today: Lack of unified industrywide definition of the term isolation

Figure 1. The journey to SIS isolation

- All engineering workstations should be secured and never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network, such as CDs, USB drives, and DVDs, should be scanned before use in the engineering workstations, or in any node connected to this network.
- Laptops and PCs should always be properly verified to be virus and malware free, before connecting to the safety network or any safety controller.

Most of the controls identified to reduce the likelihood of this type of attack are straightforward, *except* the segmentation of the safety instrumented system network. We have analyzed the various phrases used by the industry to represent this control objective, and found the following variations:

- Safety systems must always be deployed on isolated networks (automation vendor).
- Networks used for industrial control systems should always be segregated from enterprise and/or public networks (automation vendor).
- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network (government security agency).
- Isolate safety instrumental systems (national regulation).

Depending on the industry stakeholder, this control objective and the various verbiage used to represent its intent present various interpretations.

Security architecture risk

Asset owners who focus on breach statistics as the main driver to address the murky waters of SIS security architecture clearly demonstrate a high risk tolerance. Threat models, which identify and prioritize potential threats specific to plant operations, need to be developed with a focus on the SIS architecture. Typically, asset owners with a mature risk program may have already mapped out these models during the risk framing and assessment phases.

ICS cybersecurity breach headlines and regulatory mandates will not replace a mature and well-thought-out risk management program with verified capabilities.

Safety system architectures and challenges

Separation versus isolation? The term "separation" has been used in the automation industry to mean the restriction of management functionality from the process control network to the SIS network. Separation will not impact information flows—such as combining the sequence of events (SOE) for SIS and process control systems (PCSs) for rapid trip response—but isolation will. Ease of operational comparison of SIS and PCS instrumentation measurements is challenging when systems are isolated.

In this section we attempt to define the commonly represented SIS and PCS network connections currently found across various asset owner facilities. The architecture design categories include isolated, interfaced, integrated: restricted, and integrated: open. This representation is high level and attempts to show the various system interactions.

In the isolated architectural approach, the PCS and SIS systems are completely segregated from each other. There is no interaction between the two systems. Asset owners use dedicated human-machine interfaces (HMIs) for PCS and SIS. This is a truly isolated implementation, both physically and logically (figure 2).

Pros:

- Simpler hardening and lockdown: Since the SIS is completely isolated from the PCS, it should be a lot simpler to harden and lock down the systems, without worry of dependencies or architectural complexity.
- Less concern with SIS from consequences of changes or modifications that occur on the PCS.
- Confidence that SIS will act predictably if the PCS was compromised.

Cons:

- External media dependency: Users eventually will require external access to the system for tasks, e.g., extracting event records for sequence of event analysis, bypasses, overrides, proof test records, or performing configuration changes and applying security

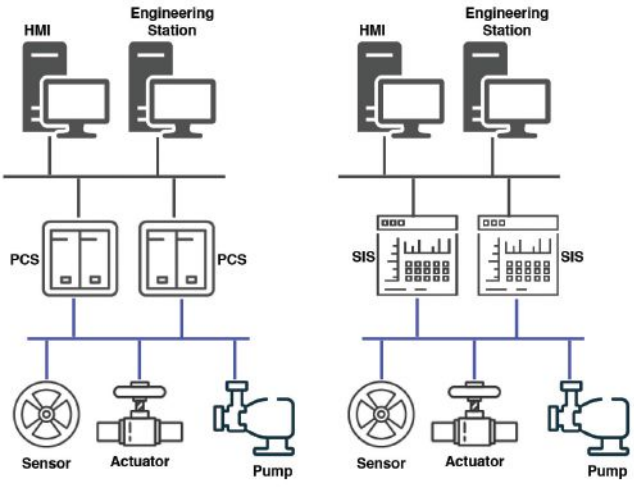


Figure 2. Isolated architecture

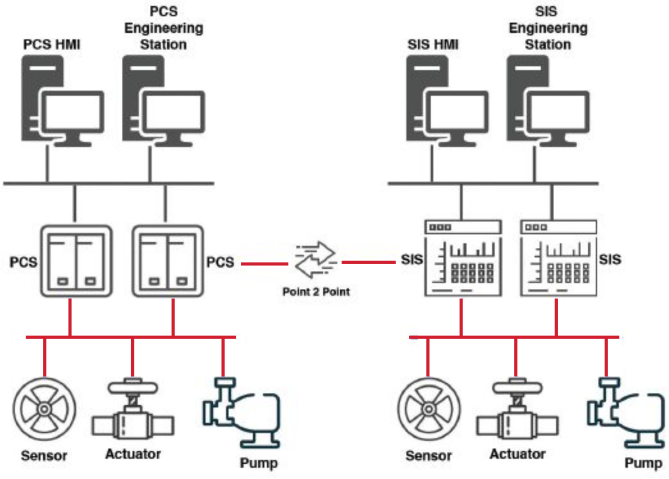


Figure 3. Interfaced architecture

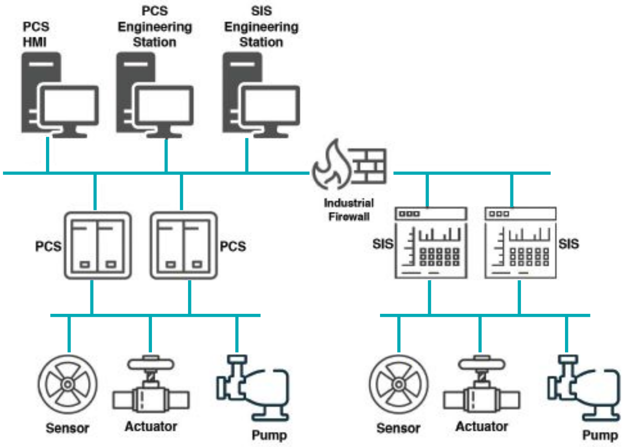


Figure 4. Integrated: restricted architecture

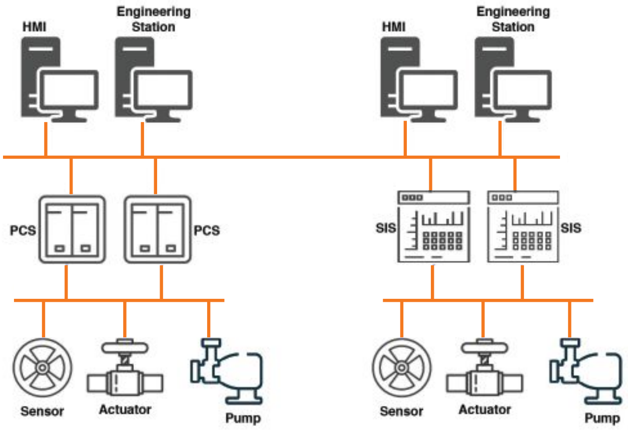


Figure 5. Integrated: open architecture

updates. USB drives, which are often used to implement these updates, are not easy to protect.

- Proper system hardening mandates leave asset owners managing two separate sets of defense-in-depth architectures. This creates a high potential for more work hours, longer downtimes, and additional areas where oversights might leave holes in the protection layers.
- Increased operational load: With full segregation, the console operator will now have to monitor/utilize a SIS-dedicated HMI, in addition to the PCS HMIs. This is more problematic when operators must divide their attention when it comes to alarm reaction.
- Promotes the tendency to ignore or downplay cybersecurity hygiene on SIS over time, due to their isolation.

In interfaced architecture, PCSs and SISs interface with each other using point-to-point interfaces, where individual PCS controllers connect to individual SIS controllers. Through these interfaces, the SIS sends information, such as trip events, pre-alarm triggers, bypasses, and SIS instrumentation values. It can also receive interlock reset requests and bypass requests (figure 3).

Pros:

- Optimizing HMI utilization, where the PCS HMI will be used to view some SIS information. This includes generic SIS alarms and events, SIS instrumentation readings, and override commands as transferred from the PCS to the SIS.
- Simplified troubleshooting during process events with unified views. Users do not need to check the SIS immediately, as summarized SIS events and instrument information are passed to the PCS.

Cons:

- Increased engineering complexity and cost due to dependency on point-to-point connections. Careful design considerations need to be taken to ensure this connection is capable of handling the data exchange from performance, safety, and security perspectives.
- Inability to get complete information from the SIS unless the SIS stations are accessed directly, as the point-to-point connection shares limited information by design. This forces technicians and engineers to access the SIS systems for diagnostic information and a detailed sequence of events. This may cause delays in identifying root causes of troubles.

In the integrated: restricted architecture, both the PCS and the SIS are fully integrated (figure 4). Measures are added to restrict and control access between the PCS and SIS.

Pros:

- The PCS HMIs (and in some circumstances, the combined engineering stations) have full visibility to the SIS information, including the integrated/combined sequence of events and diagnostic data.
- Implementing an integrated SIS/PCS architecture is less complicated and likely costs significantly less, as vendors typically provide unified development environments with built-in feature integration.

Cons:

- Implemented network restriction measures between PCS and SIS may not be fully effective, depending on the PCS/SIS technology used. Some protocols used may be proprietary, “closed spec,” or encrypted, increasing the difficulty to implement deep packet inspection technologies.
- More effort is required to secure this architecture due to the increased potential attack surface with direct access to the SIS.
- Such measures (e.g., firewalls) may also be compromised, introducing some exposure.

The integrated: open architecture approach has both the SIS and PCS fully integrated, with no segregation or restrictions (figure 5).

Pros:

- Simple to manage because it is centralized.
- It may be possible to use the same instrument resource management system to manage both SIS and PCS instruments.
- The PCS HMIs (and in some circumstances, the combined engineering stations) have full visibility to the SIS information, including the integrated/combined sequence of events and diagnostic data.
- Implementing an integrated SIS/PCS

architecture is less complicated, and likely costs significantly less, as vendors typically provide unified development environments with built-in feature integration.

Cons:

- It is challenging to provide adequate protection profiles, and there is significant exposure with major consequences.
- The system is not in compliance to regulatory and organizational policies and standards, such as NCA ECC-1 2018 and IEC 61511-2017.

Industry challenges

Until the term "isolation" is explicitly defined and clearly understood, asset owners may misinterpret their compliance to regulatory mandates with the potential for fines, and in extreme cases, a suspension of operational licenses. In addition, asset owners may have a false sense of security, assuming that their exposure to cyberthreats has been mitigated by a secure design architecture for their SIS, when in reality it is lacking.

Some might disagree with the conclusion that the term "isolation" is ambiguous and argue there is an agreed-upon common definition used by the automation industry. Systems can be physically or logically isolated and would meet the literal meaning of the word. Others have said that the "black channel" principle—which is the exchange of safety-related data and diagnostic information using the existing network connections—meets the "isolation" control objective.

We believe the automation industry and especially asset owners should consider the amount and magnitude of cybersecurity incidents as a key decision driver, as there will not be a reduction in their occurrence. In addition, the development and conformance efforts of industry consortiums such as ISA, through the development of standards and focused reports, will play a central role.

Asset owners should place significant effort during the procurement and design stages on a secure architecture, especially considering the long life cycles of ICS components and systems. Whatever is built will likely stay unchanged for many years. ■

ABOUT THE AUTHORS

Uduak J. Daniels has more than 20 years of experience, 15 of which are in cybersecurity, and is currently an ICS cybersecurity specialist with Saudi Aramco (SA). He has participated in various information and operational technology and infrastructure cybersecurity assessments, consultancy, designs, and deployments. He is an ISA member, vice chair of the SA ICS cybersecurity standards committee, and a technical member representative for SA at ISCI ISASecure. Daniels has a BS in computer science and is a Certified Information Systems Security Professional and Certified Information Security Manger.

Nidhal Jamal has 18 years of experience in OT, covering manufacturing operations management, MESs, control systems, and OT cybersecurity. He has participated in multiple cybersecurity initiatives comprising security architecture, incident response and security design, assessments, and reviews. He is currently the head of system control technical support at Petro Rabigh. He has a BE in computer engineering from Vanderbilt University and is a certified Global Industrial Cyber Security Professional.

Table 1. ICS Cyberincident timeline

Year	Type	Name	Description
2000	Attack	Maroochy Water	A cyberattack caused the release of more than 265,000 gallons of untreated sewage.
2010	Malware	Stuxnet	The world's first publicly known digital weapon.
2010	Malware	Night Dragon	Attackers used sophisticated malware to target global oil, energy, and petrochemical companies.
2011	Malware	Duqu/Flame/Gauss	Advanced and complex malware used to get specific organizations, including ICS manufacturers.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identified an active series of cyberintrusions targeting the natural gas pipeline sector.
2014	Attack	German Steel Mill	A steel mill in Germany experienced a cyberattack resulting in massive damage to the system.
2014	Malware	Black Energy	Malware that targeted human-machine interfaces in ICSs
2014	Campaign	Dragonfly/Energetic Bear No. 1	Ongoing cyber-espionage campaign primarily targeting the energy sector.
2015	Attack	Ukraine Power Grid Attack No. 1	The first known successful cyberattack on a country's power grid.
2016	Attack	Kemuri Water Company	Attackers gained access to hundreds of the programmable logic circuits (PLCs) used to manipulate control applications and altered water treatment chemicals.
2016	Attack	Ukraine Power Grid Attack No. 2	Cyberattackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.
2017	Malware	CRASHOVERRIDE	The malware used to cause the Ukraine power outage was finally identified.
2017	Attack	Triton/Trisis/HatMan	Industrial safety systems in the Middle East targeted by sophisticated malware.

Source: Kevin E. Hemsley, Dr. Ronald E. Fisher, *History of Industrial Control System Cyber Incidents,* INL, (https://www.osti.gov/servlets/purl/1505628), December 2018.

Figure 1. Motion applications like filling and labelling can take advantage of the ability of servo drives to accurately control the speed and position of many axes. Source: Emerson

Servo motion control basics

By Charlie Emerson

Servo motion controllers and motors provide excellent automation integration, accuracy, performance, and reliability

Any basic industrial automation system, such as those used on original equipment manufacturer (OEM) machinery, must have at least three fundamental capabilities:

- monitoring
- computing
- controlling

Monitoring takes the form of sensors and intelligent devices connected to a digital processor. These monitored values are used for computing and then controlling some sort of real-world action.

Many automation systems rely on one or more methods of controlling equipment by commanding physical motion, and this motion can be commanded in many ways. The specific phrase "motion control" in the context of automated equipment is most often understood to mean positively controlling the physical position of certain mechanical elements on or about a machine. Following are some of the automation basics involving motion control.

From here to there

Equipment motion control can involve one or more types, mechanisms, and geometries. Here are a few concepts:

- linear motion, such as a material handling pusher on top of a conveyor, may be simply extend/retract
- rotary motion, such as the conveyor drive itself, may be simply running at a commanded speed

or stopped

- positional motion, for both linear and rotary motion, some applications call for commanding the equipment to a given location using a specified acceleration/velocity/deceleration profile.

Every degree of linear or rotary motion on a machine is called an axis. Each axis may operate independently, or many axes may need to be closely coordinated. Think of a robotic arm with four rotary axis joints and one linear gripper axis—all these motions need to occur in concert for the robot to successfully grip a target payload.

Even with the motion type determined, there are other considerations:

- whether the motion is fixed or varying speed
- required accuracy of distance/positioning, velocity, and acceleration/deceleration
- force requirements
- duty cycle (how often the motion will be performed)
- reliability and durability
- available energy source
- the supervisory automation platform, such as the programmable logic controller (PLC) make, model, and communications protocols
- initial, operating, and maintenance costs.

For most cases, when designers think of motion control requiring precision, the discussion leads toward servomotors.

Servomotor basics

Servomotors are basically a high-performance type of electrical motor. They must be paired with a drive, which is also known as a motion controller. As a system, servos convert electricity into precisely controlled motion (figure 1).

A rotational servomotor could be used to directly drive a conveyor at a continuous or variable speed, for example, or it could move a conveyor forward and backward to a position. A servo can also be fitted directly to a rotational joint or via a gear reduction assembly to provide greater torque. Another common scenario for a typical servomotor system is incorporating it with another mechanism, such as a rack-and-pinion slide or a screw-drive, to achieve precise linear motion.

Servo drives

The servo drive itself is a relatively intelligent device that interprets signal commands from a supervisory controller, and then interacts with the servomotor to create the desired operation with extremely accurate repeatability. This interaction is closed loop, as the drive constantly monitors the position and velocity of the motor and reacts accordingly.

In the past, servo drives relied on specialized communications media and protocols to provide the necessary responsiveness between automation systems and drives. Today's servo drives generally use industrial Ethernet communication protocols for this purpose, which must be selected to deliver deterministic communications speeds fast enough for the application. Some popular protocols are:

- CC-Link
- EtherCAT
- POWERLINK
- EtherNet/IP
- SERCOS
- PROFINET

Even when servo operation is commanded by a PLC, the servo motion details are effectively programmed in the servo drive. Each motion encompasses many parameters for defining velocity, acceleration, and other performance characteristics. Servo drives may also communicate with each other to achieve very closely coordinated multi-axis control, which may be required in demanding applications.

It is certainly possible to specify servomotors, motion controllers, and automation platforms from separate vendors and integrate them all together. On the other hand, sometimes it is more practical to create a system using products from a portfolio offered by a single vendor. A single source can have coordinated products with integrated development environments to provide easier integration, as well as one-call support.

Because servo systems are often used with PLCs, some PLC vendors create motion solutions—installed natively into a PLC backplane in some instances—to provide the highest degree of integration. This can ensure superior communication and precision, especially important when there are large numbers of servos and many related axes (figure 2).

Many applications, such as printing presses and web control, may require dozens of coordinated axes and demand scalable servo solutions to maintain performance and ease of use.

Advanced features

The features listed below make development easier, protect mechanical equipment, and/or provide Internet of Things (IoT) capabilities.

Camming refers to an equipment configuration that has one main axis, with many other secondary axes operated in coordination with it. Some types of motion control equipment—such as for printing, filling, and labelling—use this type of configuration. Often this equipment must be capable of mechanically and electrically reconfiguring to run multiple operations or different-sized products. Some motion controllers can change camming profiles—which define the relationship between main and other

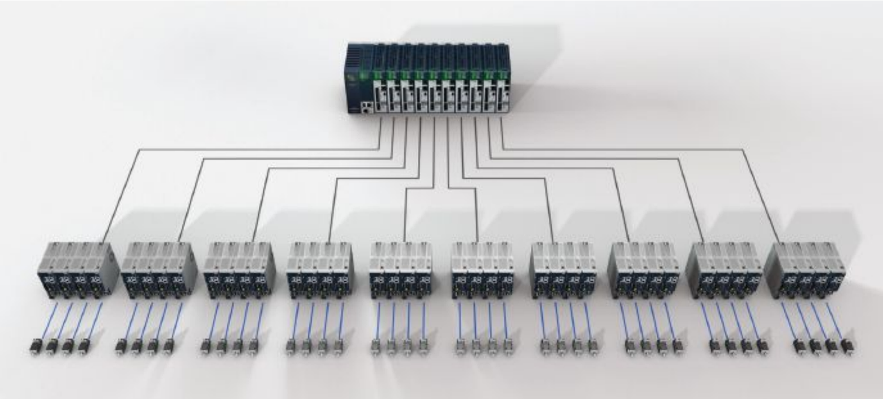


Figure 2. Emerson's PACMotion family is an example of a servo system that uses controllers installed in the PLC backplane to provide tight integration. They can reliably scale up to as many as 40 axes without performance degradation.

axes—on the fly, so users can make faster product changeovers and increase machine utilization.

Motion enhancements may be onboard features built into a servo controller above and beyond what users directly program. Some servo controllers contain patented technology for considering position, velocity, and acceleration to eliminate motion jerk in response to user commands, effectively smoothing out transitions for faster positioning, and for preventing handled products from slipping or tumbling.

Analytics are becoming more relevant for users integrating any sort of intelligent equipment. Because servo drives use microprocessors, they are already positioned to perform high-level computational and communication operations. This means they can supply extensive operational and diagnostic data to PLCs and to higher-level supervisory systems, in support of analytics. Analysis of this data helps users identify optimal operation and predict problems, which can be proactively addressed.

Design, installation, and operation

Servo systems can be demanding for designers to specify compared with other technologies. Even once the mechanical considerations are addressed, the following are needed:

- power distribution to all motion controllers
- power and control wiring for the motion controller, the servo motor, and associated automation system
- environmental protection for the motion controller
- software integration of the motion controller with the automation system.

The electrical aspects of installation may require permitting and installation by trained electricians. Once installed, technicians and engineers must commission basic drive operation and advanced motion control automation. Selecting a system from a single supplier can simplify and speed up all of these tasks (figure 3).

Despite these hurdles, once a servo motion system is successfully placed into service, end users can expect a long and reliable functional life with high operating and energy efficiencies. Servo systems can be difficult to troubleshoot, but their digital controls usually have extensive diagnostic information, which can inform the efforts of maintenance technicians.

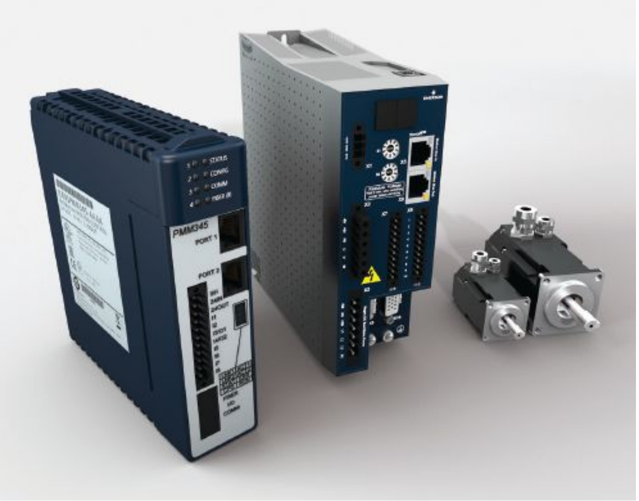


Figure 3. Servo systems from a single supplier can provide top motion control performance and simplified integration with automation systems.

Source: Emerson

Servos in motion

A common application for servo motion is a blister pack machine used on a pharmaceutical packaging line. Drug tablets are precisely arranged onto a tray, so they can be placed into formed blister pouches. Then a foil lid is rolled on and sealed and labeled, and the card is perforated and cut to size. This entire process must be precisely coordinated at high speed, typically producing more than 100 blister packs per minute. Using an integrated motion control system enables fast data communication between the automated product handling and multiple motion axes involved, simplifying coordination.

Another application is a cartoner, which manipulates flat carton stock using vacuum and other mechanisms to form a product packaging box. Formed cartons are moved along a conveyor where product is inserted at pick-and-place stations, and flaps are closed and sealed. Throughout this process, high precision, repeatability, and variable acceleration profiles are needed, so that products are not damaged and cartons are formed to properly secure the product. Servos deliver the coordinated control to achieve this.

High-performance motion control

Performing automated motion for OEM machinery and other processing equipment is a fundamental need that can be met with the use of many technologies. The term motion control is most often associated with the use of electrical servo drives—commonly called motion controllers—and associated servomotors to operate the equipment.

Servos are connected directly or via mechanisms, so they can drive equipment in a rotational or linear motion. They can be more complicated and expensive to design, procure, install, and commission than less capable systems, but once in service they are reliable and efficient. More importantly, servos bring the high level of accuracy and performance required by many applications.

Because there is commonly a high level of integration between servo systems and PLC-based automation systems and users are looking for more IoT data, it is important to consider the communications and interoperability aspects when specifying servo motion controllers and motors. Careful up-front design will provide easier integration and years of optimized control, while minimizing expenses. ■

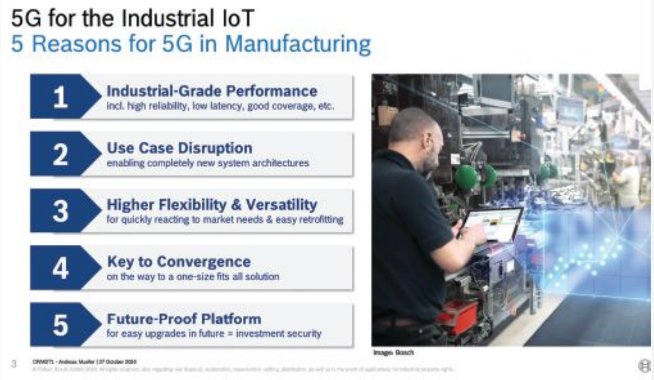
ABOUT THE AUTHOR

Charlie Emerson is the director of industry marketing for Emerson's machine automation solutions business. He has responsibility for defining the business's industry vertical growth strategy and solving industry-specific challenges using the industrial automation and controls portfolio.

IIoT & Smart Manufacturing Conference debuts virtually

ISA's virtual events program debuted its IIoT & Smart Manufacturing Conference on 27 October 2020. Speakers at this eight-session virtual event presented advances in connectivity, automation, and security in the context of hybrid manufacturing. The keynote speeches focused on the significance of 5G in the manufacturing and automation sectors. Speakers included Adrian Scrase, CTO for the European Telecommunications Standard Institute; Andrew Alleman, chief architect for network solutions, next generations, and standards, at Intel Corporation; and Andreas Mueller, PhD, head of communication and network technology for Bosch Corporate Research.

Other sessions during the day covered industrial wireless systems and advancements in automation cyber-physical security, practical machine learning and artificial intelligence applications, smartly connecting manufacturing systems, how smart manufacturing is safe manufacturing, and more. For more information, visit https://tinyurl.com/ISAevents-IIotSM. ■



5G for the Industrial IoT

5 Reasons for 5G in Manufacturing

1 **Industrial-Grade Performance** incl. high reliability, low latency, good coverage, etc.

2 **Use Case Disruption** enabling completely new system architectures

3 **Higher Flexibility & Versatility** for quickly reacting to market needs & easy retrofitting

4 **Key to Convergence** on the way to a one-size fits all solution

5 **Future-Proof Platform** for easy upgrades in future = investment security

Image: Bosch

3 CRWST1 - Andreas Mueller | 27 October 2020

Leader members living la vida lockdown

Hurricanes, the coronavirus pandemic, and more has caused many to create alternate activities for time-honored traditions in 2020. This year's Annual Leader Conference—scheduled to be held in Puerto Rico—was no exception. But ISA leaders and staff rose to the (virtual) occasion.

On 22 October 2020, during two separate but equally festive Zoom calls, leader members around the globe were able to enjoy "Living La Vida Lockdown." Attendees in tropical attire grabbed a cocktail and followed along as volunteers demonstrated cooking and beverage-making skills. "Quarantiki Time" was hosted by mixologists "Surfside" Steve Mustard and "Beach Bum" Bill Furlow. Others demonstrated how to cook tostones, a crispy fried plantain appetizer, and mofongo, a sweet and savory dish that is rich with centuries of Puerto Rican history.

According to ISA director of governance and membership Andrea Hopkins Holovach, a good time was had by all. ■

What is IIoT? What is an Industry 4.0 HMI?

During this year of digital transformation, the Smart Manufacturing and IIoT Division (SMIIOT) has been busy populating the ISA Interchange blog with a slew of useful content answering fundamental questions about automation. Two examples:

What is an HMI? "Human-machine interfaces, more commonly known as HMIs, have been used since a personal computer arrived on the plant floor. Most people think of them as the screens used in a production environment. In a broader sense, they are a form of user interface (UI) between people and machines. So the better question to ask is, 'What does an HMI look like in the age of Industry 4.0?' "

What is IIoT? "We first must define IoT. The Internet of Things (IoT) is a network of intelligent devices, computers, mobiles, and applications that are connected to the Internet. IoT collects a large amount of data, stores and processes it in the cloud, and shares it with the end user. The Industrial Internet of Things (IIoT) is a subset of IoT that specifically refers to industrial automation." Find out about the division's other activities at https://isa.org/smiiot. ■

STEM diversity and inclusion: Blacks in technology

Individuals and organizations are working for equal representation in STEM all over the world. To find out more, the ISA Interchange blog asked Greg Greenlee, the chairman and founder of Blacks in Technology (BIT), to discuss his group's work and mission.

Greenlee says he founded Blacks in Technology to "provide a space for Black people in tech to (a) connect and engage with one another; (b) learn from one another; (c) support one another in our tech careers, endeavors, and journeys; (d) create a sense of community amongst Black people in tech; (e) provide positive images to others in or aspiring to be in tech or just the tech-curious."

A main goal for the organization is to ensure Black people are not being underrepresented. "Black people make up 13 percent of the population in the United States but only 2 percent in the tech field. This is well-known," says Greenlee. "We are a long way off from equal representation, but we would like for the numbers to be reflected equally in tech. It would make it better because diversity of thought has always made things better throughout history."

The organization is looking to not only help provide educational resources to enhance the careers of Black people already working in technology, but also to provide "visibility, a network, a safe space, and a community that can help broaden the reach of technology in our community and also help to show that this field is a great option for us to be in," he said. BIT does that by partnering with organizations and companies to provide training and organizing events—in person and now virtual.

The annual tech conference called BITCon "pays talented and knowledgeable Black people in tech to come in and showcase their expertise to a huge audience. It's a true tech conference where techies, engineers, and others come to bond with one another, build relationships, support one another, and elevate one another," says Greenlea. "We had to cancel this year due to COVID, but we hope to be back in 2021." Find out more at https://tinyurl.com/ISAinterchange-BIT. ■

Improving ISA governance and strategy

Outgoing ISA president Eric Cosman spoke to ISA members about the executive board's decision to conduct a review of ISA governance structures and processes, the Society's first use of online voting for the meeting of the Council of Society Delegates, and other changes and accomplishments during this turbulent year in a blog post on ISA Interchange.

"It continues to be a very strange and unusual year, presenting new and unusual challenges for many of us," said Cosman. "Whether in our personal or professional lives, we have all had to show resilience and adaptability in the face of these circumstances. We have found new ways to work, communicate, and collaborate as we adapt to what the pundits euphemistically describe using the cliché of a 'new normal.' I have long believed that the traits most important for long-term success include willingness to accept change and openness to learning. Of course, the same holds true for our Society."

Cosman noted that the ability to learn from others and respond to changing circumstances is a significant challenge for any organization. And ISA is meeting this challenge.

The Society's first use of online voting by the the Council of Society Delegates resulted in the approval of a new set of bylaws for ISA. "With these changes, we now have a solid basis for the further improvements of our governance policies and procedures that will allow us to be more responsive to changing circumstances," said Cosman.

ISA has also been making progress on a strategic plan that is based on the values of professionalism, diversity and inclusion, excellence, collaboration, and integrity. By definition, strategies are focused on the long term, and "we will need the ideas, contributions, and experience of all members to achieve our objectives," Cosman said. "We all have a role to play in identifying and making the changes required to ensure our long-term success as a society, and to live up to our aspiration of being the home of automation."

Amid these changes, ISA continues to provide products and services for its members and customers. "We are responding to the changing needs in the industries that we serve and the availability of new technology and solutions," said Cosman. "An example of this is the formation of the Smart Manufacturing and IIoT Division, with the goals of providing clarity around these subjects, developing technical content and standardized approaches to solve critical problems, and providing a forum for networking and collaboration. This new division already has more than 1,000 members and recently held a very successful virtual event." ■

Professional Development

ISA Certified Automation Professional (CAP) program

CAP question

The function of PID parameters is best described as

A. placing the system in a safe condition during process upsets.
B. optimizing a control loop.
C. ensuring that specified components are properly calibrated.
D. ensuring that specified components are properly installed.

CAP answer

The answer is *B*, "optimizing a control loop." The parameters of a proportional, integral, derivative (PID) loop are typically called the "tuning parameters," which include the gain, integral time, and derivative time. The purpose of these parameters is to provide a fast, robust response to swings in the process as well as to maintain a consistent response to normal process sensor noise. These parameters are adjusted through the tuning process and "good control" response, such as quarter-wave dampening, to provide optimal control.

The parameters of a PID control loop do not factor into the physical installation or calibration of the loop. These are handled via other processes and procedures. The PID loop does not evaluate or drive a process to a safe state upon a process upset, but can be directed by other programming to change mode, set point, or output.

Reference: Sands, Nicholas P. & Verhappen, Ian, *A Guide to the Automation Body of Knowledge, Third Edition*, ISA Press, 2019.

ISA Certified Control Systems Technician (CCST) program

CCST question

From the list given below, select the group that is the U.S. representative to the International Electrotechnical Commission (IEC):

A. ISA
B. ANSI
C. ASTM
D. AIChE

CCST answer

The correct answer is *A*, "ANSI." The American National Standard Institute (ANSI), through an internal committee called the U.S. National Committee of the International Electrotechnical Commission (USNC/IEC), acts as the nation's representative to the IEC. The USNC serves as the focal point for U.S. interests in international electrotechnical standards, certification, and other related matters.

Reference: Goettsche, L. D. (Editor), *Maintenance of Instruments and Systems, Second Edition*, ISA, 2005.

New CAPs and CCSTs

Below is a list of individuals who have recently passed either ISA's Certified Automation Professional (CAP) exam, or one of the three levels of Certified Control Systems Technician (CCST) exam. For more about either program, visit www.isa.org/training-and-certifications/isa-certification.

Certified Control System Technicians

Name	Company	Location
Level 1		
Thom Wolfsen	None	U.S.
Matthew Coyle	None	U.S.
Andrew Costello	None	U.S.
Lorenzo Lanzi	None	U.S.
Brian Keel	None	U.S.
Kelvin Ware	None	U.S.
Reese Horton	None	U.S.
Douglas Ringgold	None	U.S.
Jeffrey Daniels	None	U.S.
Mark Keller	None	U.S.
Thomas Connolly	None	U.S.
Shawn Hardesty	None	U.S.
Frank Muscato	None	U.S.
Nicholas Hines	None	U.S.
Ronald Campbell	None	U.S.
Patrick Kendall	None	U.S.
David Myers	None	U.S.
Jeffrey Grovom	None	U.S.
Justin Davis	None	U.S.
Level 2		
Thomas Massey	None	U.S.
Brandon Cooper	None	U.S.
Angel Hernandez		U.S.
Henry Ng	None	U.S.
Reza Gholamrezaei	None	U.S.
Ryan Raiford	None	U.S.
James Marshall	None	U.S.
Clinton Thompson	None	U.S.
Norman Bates	None	U.S.
Brandon Karas	None	U.S.
Steve Gerovac	None	U.S.
Level 3		
Daniel Mos	None	Canada
Jason Misenhimer	None	U.S.
Micah Dudley	None	U.S.

Certified Automation Professionals

Name	Company	Location
Robert Albright	None	U.S.
Syed Muhammad Bilal Haider	None	Australia
John Melott	None	U.S.
Jeremy Wells	None	U.S.
Riaan Schoeman	None	U.S.
Vikram Baliga	None	U.K.
Rangit Kondattu	None	Norway
Jorge Jimenez	None	U.S.
Jacob Lindsay	None	U.S.
Muhanna Al Rahbi	None	Oman

New ISA standard provides auditable approach to assessing cybersecurity risk

The widely used ISA/IEC 62443 Industrial Automation and Control Systems (IACS) Security standards, developed primarily by the ISA99 standards development committee with simultaneous review and adoption by the International Electrotechnical Commission (IEC), provide a flexible framework to address and mitigate current and future IACS security vulnerabilities. The ISA99 committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

A new standard in the series is based on the understanding that each organization that owns and operates an IACS has its own tolerance for risk—and that each IACS represents a unique risk depending on the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. The new standard, ISA/IEC 62443-3-2: Security Risk Assessment for System Design, defines a comprehensive set of engineering measures to guide organizations through the essential process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels.

The new standard can be effectively applied across all industry and critical infrastructure sectors that depend on secure IACS operations. Moreover, it provides much-needed guidance to all key stakeholder categories, including asset owners, system integrators, product suppliers, service providers, and compliance authorities.

"Currently, there is wide degree of variability in how industry defines and conducts IACS risk assessments," says John Cusimano of aeSolutions, who led the ISA99 subgroup that wrote the standard. "ISA/IEC 62443-3-2 establishes fundamental requirements for an IACS risk assessment without being overly prescriptive. The result is a standard that will bring uniformity across industry while still allowing IACS owners and operators to apply any methodology that is compliant with the standard."

The new standard is the latest in a series of notable milestones in the ongoing development and growing global application of the ISA/IEC 62443 series. This included a decision by the United Nations Economic Commission for Europe to integrate the widely used standards into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe. It also included completion of several key additional standards, including:

- ISA/IEC 62443-4-1, Product Security Development Life-Cycle Requirements, which specifies process requirements for the secure development of products used in an IACS and defines a secure development life cycle for developing and maintaining secure products.
- ISA/IEC 62443-4-2, Technical Security Requirements for IACS Components, which provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications.

Other standards in the ISA/IEC 62443 series cover terminology, concepts, and models; establishing an IACS security program; patch management; and system security requirements and security levels. All may be accessed at www.isa.org/findstandards.

For more information on ISA99 and the ISA/IEC 62443 series of standards, contact Eliana Brazda, ISA Standards, ebrazda@isa.org. ■

ISA Standards & Practices board update

As the governing body of ISA Standards, the S&P Board, like all ISA committees, has been operating in a strictly virtual mode this year and will likely continue to do so until a possible face-to-face meeting at the ISA Annual Leaders Conference, planned for October 2021 in Puerto Rico.

Among its activities, the S&P Board has four ongoing teams working on key goals related to ISA's overall strategic plan as follows:

- SP1: Committee Effectiveness (leader: Nicholas Sands) – Developing job descriptions for new leadership positions in ISA standards committees, including membership, marketing, social media, and editing, to establish and clarify these roles for committees to fill as desired, and to create bigger pools of committee leaders for succession.
- SP2: Board Effectiveness (leader: Eric Cosman) – Developing a job description for S&P Board members who serve as managing directors of ISA committees.
- SP3: Portfolio Management (leader: Dennis Zetterberg) – Focusing on how to best assess the viability of older existing ISA standards, recommended practices, and technical reports.
- SP4: Stakeholder Engagement (leader: Chris Monchinski) – Assessing how ISA sections and divisions are starting to use the new ISA Connect tool to engage their respective members, for possible applicability to ISA standards committees.

Chris Monchinski of Automated Control Concepts is completing a two-year term as vice president of ISA's Standards & Practices Department. Dennis Zetterberg of Chevron will begin a two-year term as vice president on 1 January 2021. David Lee of Emerson will serve as vice president-elect. ■

Have an idea for an ISA standard, book, training course, conference topic, or other product or service? Send it to: crobinson@isa.org.

ad index

InTech advertisers are pleased to provide additional information about their products and services. To obtain further information, please contact the advertiser using the contact information contained in their ads or the web address shown here.

Advertiser	Page #
ARC Advisory Group www.arcweb.com	**40**
Automation Direct www.automationdirect.com	**Cover 2**
Endress + Hauser www.us.endress.com	**3**
Inductive Automation www.inductiveautomation.com	**bellyband, 11**
ISA Global Cybersecurity Alliance www.isa.org/isagca	**Cover 3**
Moore Industries www.miinet.com	**6**
ProComSol, Ltd. www.procomsol.com	**10**
Opto22 www.opto22.com	**Cover 4**
Tadiran www.tadiranbat.com	**13**

Contact *InTech* today:

Richard T. Simpson
Advertising Sales Representative
Advertising, Classifieds Section
Phone: +1 919-414-7395
Email: rsimpson@automation.com

Chris Nelson
Advertising Sales Representative
Phone: +1 612-508-8593
Email: chris@automation.com

Chris Hayworth
Advertising Materials Coordinator
Phone: +1 919-990-9435
Email: chayworth@ISA.org

View the *InTech* media planner at
https://tinyurl.com/ISA-InTechMediaKit

Reprints

Foster Reprints will work with you to create a customized reprint package, including hard copy reprints, eprints, and mobile-friendly products.

Contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

datafile

Datafiles list useful literature on products and services that are available from manufacturers in the instrumentation and process-control industry. To receive free copies of this literature, please contact each manufacturer via their provided contact information.

USB HART MODEM

The **HM-USB-ISO** USB HART modem meets industry standards for USB and HART connectivity. The small size, light weight, and durability of the HM-USB-ISO make it ideal for portable use. Operating power is derived from the USB connection. An easily installed Virtual Serial Port driver allows use in any Windows-based application.

It is the lowest cost USB Modem certified by the FieldComm Group to meet the HART communication specifications.

ProComSol, Ltd, *Process Communications Solutions*
Tel. 216.221.1550; Fax 216.221.1554
sales@procomsol.com; www.procomsol.com
Toll Free 877.221.1551

System Integration, Executive Search, and More

Promote your services to 43,000+ ISA members. *InTech* Classified ads are a simple and cost-effective way to reach active and interested automation professionals. **Contact:** Richard Simpson, +1 919-414-7395, rsimpson@automation.com

Sample of Jobs Available at Jobs.isa.org

See more at Jobs.isa.org, where you can search for available jobs or advertise positions available within your company. ISA Members post resumes at no charge.

Senior manufacturing engineer

Carrier: This engineer, working with the engineering manager, will support a manufacturing/assembly operation at the Athens, Ga., facility. Duties include establishing clear processes, procedures, and technology implementation; engaging with product engineering during the design cycle to ensure the design for manufacturability and tooling; applying working knowledge of product design and assembly to the manufacturing process; participating in brainstorming meetings and cross-departmental meetings; achieving product profitability goals; performing time studies and line balancing; and recommending methods to improve operator effectiveness in safety, quality, and productivity. The position requires a demonstrated ability to deliver to schedule, effective written and verbal communication skills, experience using continuous improvement methodologies, five or more years of experience in a manufacturing environment . . . see more at Jobs.isa.org.

Cybersecurity analyst intern

Dell Technologies: In this one-to-three month internship, the successful candidate will have the opportunity to share insights from recent coursework in the implementation of security and resiliency programs. The analyst intern will come to understand the company's overall business strategy and objectives and will help devise effective and efficient ways to implement security programs. Requirements include progress toward attaining a BS in computer science, risk management, information systems, or a related field; the ability to operate collaboratively and effectively in a fast-paced team environment with shifting priorities; basic-to-intermediate understanding of cybersecurity concepts; solid written and spoken communication skills . . . see more at Jobs.isa.org.

Electrical engineer

Lincoln Electric: The company, headquartered in Cleveland, Ohio, seeks engineers to conduct applied research into new areas of welding consumable design and new welding processes. The engineer will work in R&D on the design, specification, and documentation of components, assemblies, and products such as inverters, engine welders, and plasma cutters; serve as a hardware engineer for major development projects or multiple simultaneous projects; and work closely with software engineers, designing with systemwide perspective. Basic requirements are a BS in electrical engineering, five or more years of experience in a research or product development environment, knowledge of project management and process improvement methods, and a broad knowledge of principles, practices, and procedures to the completion of a variety of difficult assignments and changing priorities . . . see more at Jobs.isa.org.

Automation technician

FactoryFix: The technician, located in St. Paul, Minn., will support the manufacturing environment to ensure equipment and processes are operating at high efficiencies; troubleshoot and maintain custom electromechanical equipment, automated work cells, vision systems, and multi-axis robotics; create and debug PLC programs with varying levels of complexity; initiate an complete technical activities leading to improved production processes; and program and operate robotic cells. A high school diploma, knowledge of PLC programming, self-motivation to adapt to changes and juggle multiple competing tasks, and the ability to exercise strong judgment in analyzing and solving problems is required . . . see more at Jobs.isa.org.

Industry 4.0 and digitalization, sharpen your saw

By Bill Lydon

ABOUT THE AUTHOR

Bill Lydon (blydon@isa.org) is an *InTech* contributing editor with more than 25 years of industry experience. He regularly provides news reports, observations, and insights here and on Automation.com.

Modernizing manufacturing is vitally important, and knowledgeable automation professionals are instrumental for companies to be successful and profitable. Automation professionals need continuous learning to keep up to date on the latest ideas, concepts, and developments, including Industry 4.0 and digitalization.

Stephen Covey, author of *The 7 Habits of Highly Effective People*, puts constant learning in perspective with a story about man walking through a forest who came across a frustrated lumberjack trying to cut down a tree. He was swearing and cursing as he labored in vain. "What's the problem?" The man asked. "My saw's blunt and won't cut the tree properly." The man asked, "Why don't you just sharpen it?" "Because then I would have to stop sawing," said the lumberjack. "But if you sharpened your saw, you could cut more efficiently and effectively than before." "But I don't have time to stop!" replied the lumberjack.

ISA is providing members the opportunity to learn and keep up to date via its Smart Manufacturing and IIoT (SMIIoT) Division.

The moral of the story is we need to keep developing our minds by continually learning to become more effective: "sharpen the saw." This is more important than ever with the dramatic changes in technology and concepts, including Industry 4.0, digitalization, Internet of Things (IoT), Industrial Internet of Things (IIoT), cloud computing, wireless communications, and sensor technology advancements providing new industrial automation possibilities to improve, optimize, and digitize production.

ISA is providing members the opportunity to learn and keep up to date via its Smart Manufacturing and IIoT (SMIIoT) Division. It is the newest and fastest growing division of ISA and is aimed at helping members gain knowledge and learn from industry experts and peers professionally and technically. The primary goals of SMIIoT are to provide clarity around these ever-evolving spaces, develop useful technical content, develop standardized approaches to solve critical problems, and provide a forum for professional networking and collaboration.

Smart Manufacturing and IIoT Division technical committees

The goal of these committees is to advance technical competence in focus areas:

- Industrial Internet of Things
- cloud technologies
- artificial intelligence (AI) and machine learning (ML)
- communication and networking (Industrial Internet)
- cybersecurity
- cyber-physical systems
- digital twin and simulation
- virtualization technologies (virtual reality [VR] and augmented reality [AR])

Smart Manufacturing and IIoT Division activities

- create and collect technical resources for members (e.g., articles, white papers, case studies, tools)
- publish quarterly newsletter for awareness of SMIIoT division activities and industry news
- host technical webinars
- support Smart Manufacturing and IIoT Conference
- collaborate with ISA districts and sections to promote and disseminate relevant information
- expand volunteering opportunities for further collaboration and networking
- develop a network of smart manufacturing and IIoT partner organizations as resources to members

You can take advantage of this opportunity to "sharpen the saw," to become a valuable contributor to your company's success and advance your professional career building a better world through automation, by becoming a member of ISA. Members can find out more about the Smart Manufacturing and IIoT Division by visiting the Communities section of ISAConnect. Others can visit www.isa.org/smiiot. ■

ISA GLOBAL CYBERSECURITY ALLIANCE™

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

Honeywell · Johnson Controls · Rockwell Automation · PAS

Life Is On Schneider Electric · NOZOMI NETWORKS · MOCANA

CLAROTY Clarity for OT Networks · WALLIX CYBERSECURITY SIMPLIFIED · xage SECURITY · senhasegura by MT4

BAYSHORE · radiflow Secure your Assets · 威努特 WINICSSEC · INL Idaho National Laboratory

DRAGOS · exida · munio security · tenable

DIGITALIMMUNITY™ STAY PRODUCTIVE, STAY SECURE · TiSafe · aE Solutions™ · tripwire

1898 & Co. · ACET SOLUTIONS · WisePlant® Smart, Safe & Secure · MSi Mission Secure, Inc.

CYBEROWL · Deloitte. · EATON Powering Business Worldwide · Nova Systems

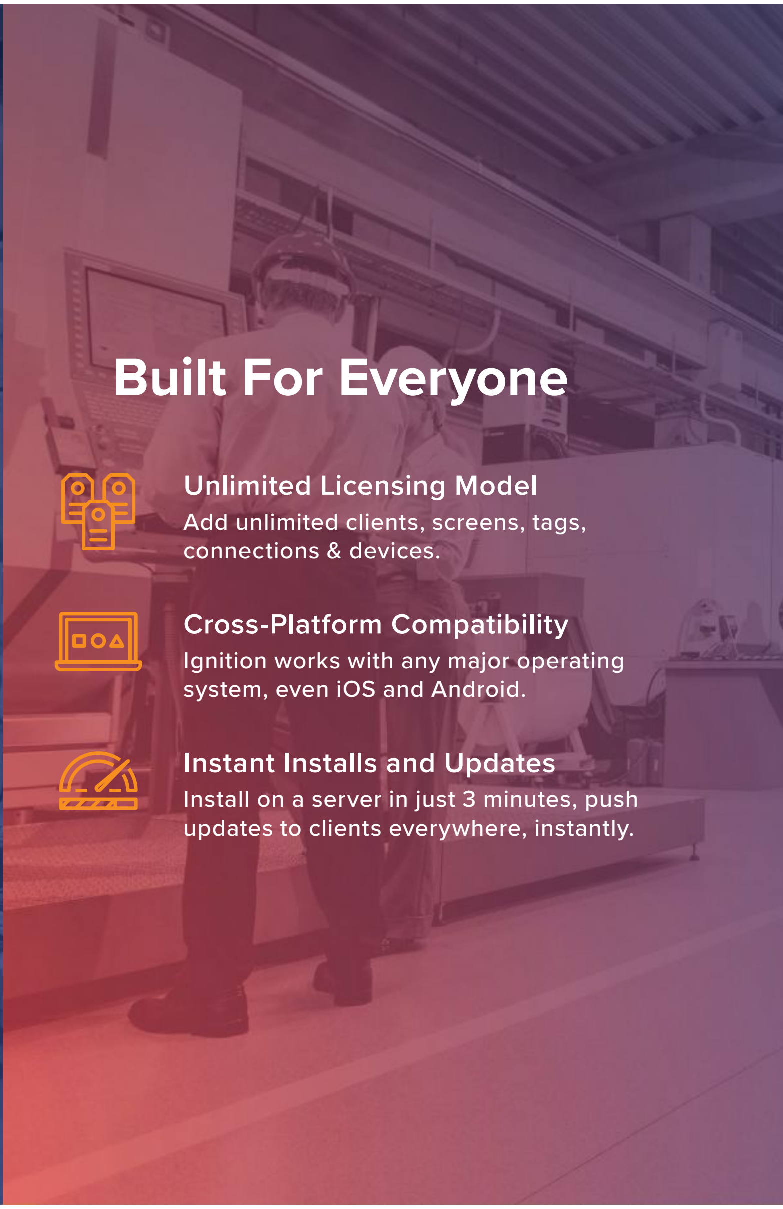
KPMG · ConsoleWorks Cybersecurity Operations Platform · PETRONAS · SURGE ENGINEERING

International Society of Automation

Setting the Standard for Automation™

Ignition 8.1
by inductive automation
Built For The Plant Floor
Build Mobile-Responsive HTML5 Applications
That Run Natively on Any Screen

Try Ignition 8.1 For Free Today at
www.***inductiveautomation***.com



Built For Everyone

Unlimited Licensing Model

Add unlimited clients, screens, tags, connections & devices.

Cross-Platform Compatibility

Ignition works with any major operating system, even iOS and Android.

Instant Installs and Updates

Install on a server in just 3 minutes, push updates to clients everywhere, instantly.