May/June 2020

InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

75 1945 ISA 2020

Analytics and regulatory control

Robotics

IIoT device connectivity

HMI and SCADA

Flow and level spotlight

Cybersecurity risk is the great equalizer

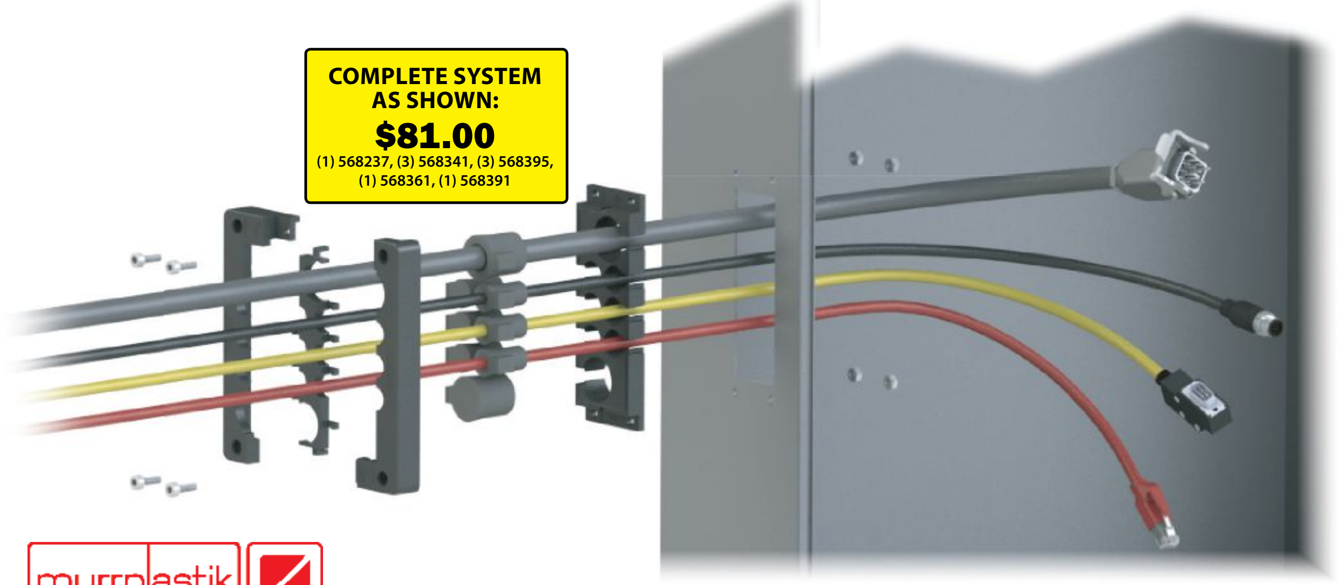
Awareness of challenges and collaboration on solutions can secure critical resources

www.isa.org/intech

Guaranteed Strain Relief...

for your cables and your budget

COMPLETE SYSTEM AS SHOWN:
$81.00
(1) 568237, (3) 568341, (3) 568395, (1) 568361, (1) 568391



Murrplastik KDL/D Series Cable Entry System

The new Murrplastik KDL/D cable entry system provides an easy and efficient method to install cables through an enclosure and other bulkhead surfaces without having to disassemble or cut terminated cables. Easy, fast, and robust, this cable entry system provides a high degree of environmental protection and is available at everyday low prices you expect from AutomationDirect.

Features

- Uninterrupted cable guidance
- Easy assembly
- Integrated strain relief
- Fits standard cutout dimensions
- High protection class IP65
- 2-year warranty

Also Available

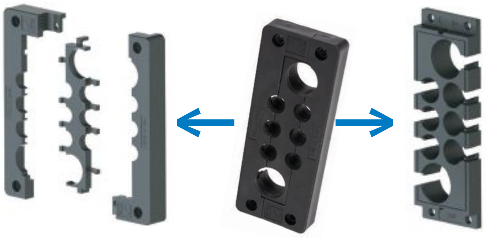
Top Quality Enclosures

Cut to Length Wire and Cables

Cable Glands

Split Frame *(Starting at $16.00)*

Consists of a frame and a grommet block that clamp together to provide a high-density cable entry point with an IP65 environmental rating.

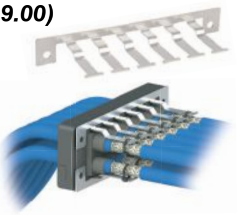


Grommets *(Starting at $6.00)*

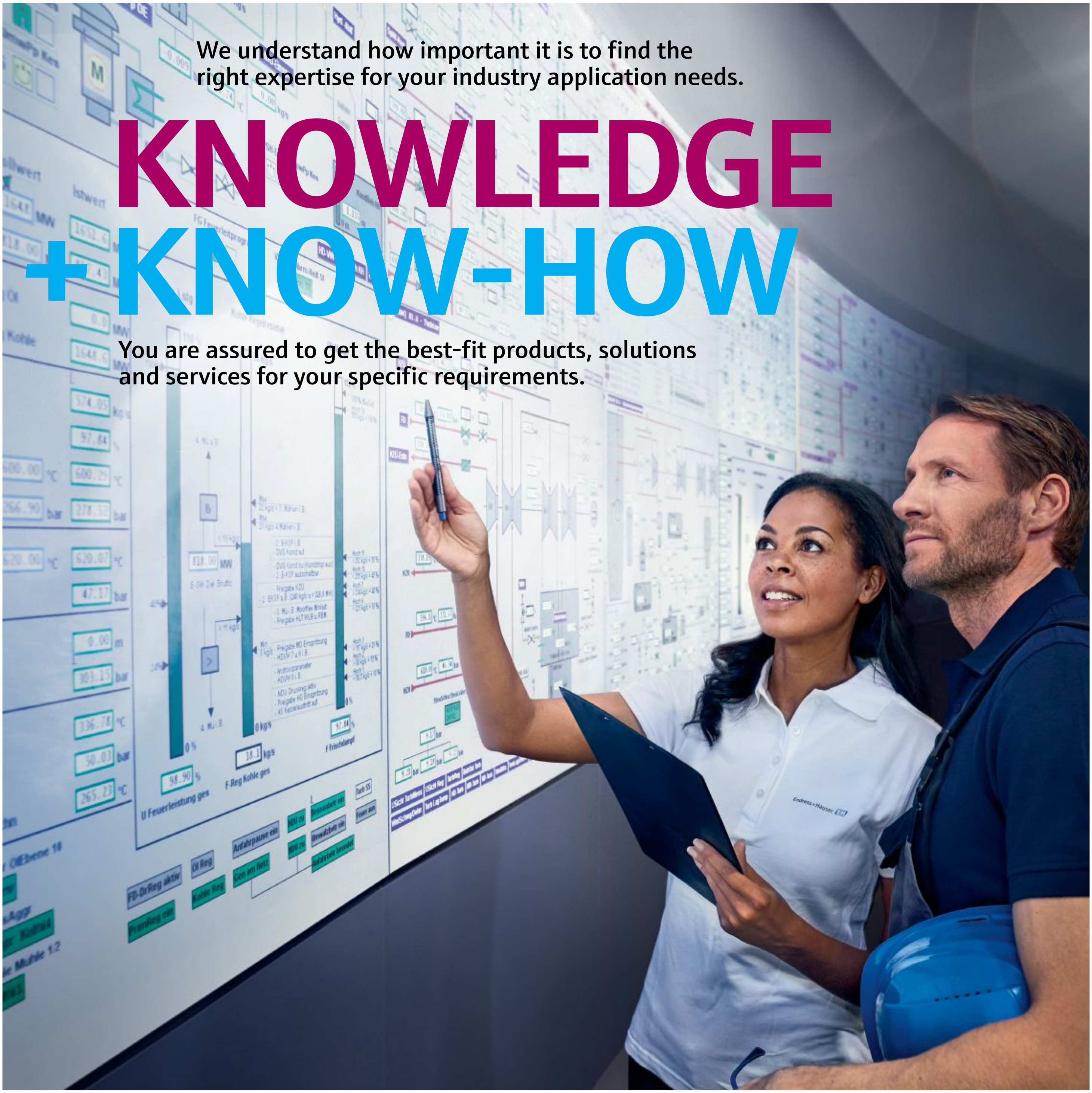
Grommets allow round cable entries and are available as single or multi-line grommets allowing easy entry for one or more cables.

Discharge Plate *(Starting at $29.00)*

The discharge plate provides a means to eliminate interference that can occur on cable shields.



Research, price, buy at: *www.automationdirect.com/cable-entry-systems*


We understand how important it is to find the right expertise for your industry application needs.
KNOWLEDGE
+KNOW-HOW
You are assured to get the best-fit products, solutions and services for your specific requirements.

May/June 2020 | Vol. 67, Issue 3

www.isa.org

InTech

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 3.**

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.

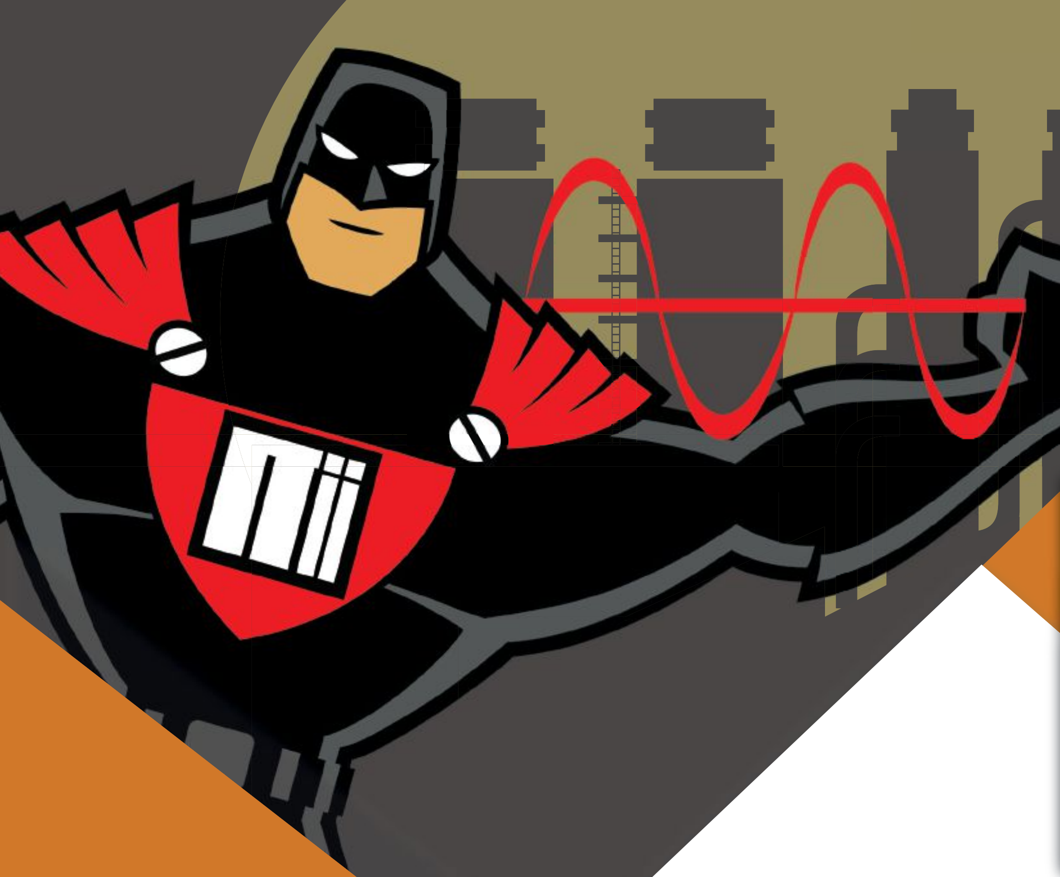
To order REPRINTS from *InTech*, contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

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.



Safe way to learn, connect, grow professionally

By Renee Bassett, *InTech* Chief Editor

More than eight weeks into the disruptive force that is the COVID-19 pandemic, I am saddened by the effect the novel coronavirus is having on hundreds of thousands of families, businesses, and individuals around the world. But I am also impressed by the quick switch to new business models and operating procedures that some are pulling off in order to: help each other, stay afloat financially, protect employees, or provide useful services in novel ways.

From beverage distilleries churning out hand sanitizer to auto manufacturers pivoting to produce ventilators and face shields, organizations are reinventing themselves at a record pace. Some versions of these "new normal" activities may stay in place for a very long time. Others will give way to new versions of today's experiments.

Preparing for a new normal is something that the staff and volunteers at the International Society of Automation are working on every day, and this issue of *InTech* contains snapshots of the times. We may not be on the front lines saving lives, manufacturing food, or keeping the proverbial lights on, but many of our members, customers, and volunteers work for and with organizations that are.

ISA already had a healthy set of webinars and online training in place before the pandemic, so we're no strangers to virtual work or the automation that can support it. But like many organizations, we're doubling down now. We've expanded our webinar offerings to deliver monthly online seminars in four broad categories: cybersecurity, IIoT & smart manufacturing, processing control & instrumentation, and digital transformation (see p. 8). We've instituted Zoom meetings to advance standards-making work (p. 53), and even joined in a virtual happy hour on 28 April 2020—ISA's 75th birthday (p. 51).

The most exciting news involves our plans for virtual conferences. I had expected to talk with many of you in person in April at our inaugural IIoT & Smart Manufacturing Conference live event, or in May at our planned CSIC Cybersecurity Standards Implementation Conference. However, not long after stay-at-home orders were issued and mass gatherings appeared risky, ISA management made the decision to bring the virtual conference experience to the automation industry.

Partnering with a company called vFairs, ISA will be providing half-day professional conferences complete with keynote speakers, expert presentations, booths filled with demos, and chat areas for conversations and Q&A. Virtual conferences are a safe, convenient alternative to in-person conferences, providing attendees with insight into key operational and business topics from the convenience of their desktop or mobile computer.

ISA's first Virtual Cybersecurity Standards Implementation Conference will be held 30 June 2020 from 10 a.m. – 3:45 p.m. ET. Find and register for any of ISA's webinars or virtual conferences at ISA.org/virtualevents. I hope to "see" you there. ■

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
Colleen Casper
ccasper@isa.org

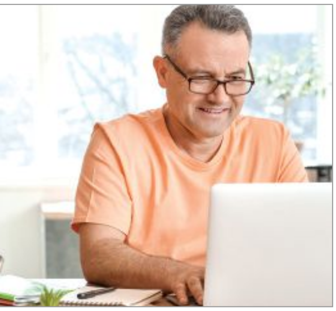
SENIOR GRAPHIC DESIGNER
Pam King
pking@isa.org

GRAPHIC DESIGNER
Lisa Starck
lstarck@isa.org

ISA PRESIDENT
Eric Cosman

PUBLICATIONS VICE PRESIDENT
Joao Miguel Bassa

New ISA virtual events include half-day online conferences



Not long after pandemic-related stay-at-home orders began being issued in the U.S., ISA leadership and staff realized that in-person events of all kinds were impossible in the short term and uncertain in the longer term. The slate of live events ISA was planning for 2020 had to be changed.

So the decision was made to cancel or move all ISA 2020 face-to-face conferences into virtual platforms. "The health and safety of ISA members and customers is most important," said ISA director Mary Ramsey, "and we will leverage digital and virtual platforms to deliver valuable content instead of holding in-person events."

The ISA Virtual Events Program encompasses webinars and virtual conference sessions on a series of essential topics, presented by ISA subject-matter experts and others. Webinars are hour-long online presentations with live questions and answers. Virtual conferences are multi-session, multi-"room" online events that have panel discussions with live Q&A, virtual exhibit booths, and attendee chat opportunities in addition to insightful presentations and user case study sessions. ISA virtual events are being created under one of four broad topic areas. These series include:

Cybersecurity

Explore the critical, dynamic world of automation cybersecurity with ISA's expert contributors. Learn about threats, emerging protection methods, industrial control system best practices, fundamentals of the ISA/IEC 62443 standards, and implementation tips for bringing a standards-based approach into your facility. The first virtual conference—"Cybersecurity Standards Implementation Conference"—is scheduled for 30 June at 10:00 a.m. – 3:45 p.m. ET. It focuses on cybersecurity gaps in industrial automation and control systems and ways to address threats using a standards-based cybersecurity program.

IIoT and smart manufacturing

Learn the latest trends and technologies driving the next generation of industrial operations, including the Industrial Internet of Things (IIoT), data analytics, edge computing, artificial intelligence, wireless communications, cloud and mobile computing, robotics, and simulations.

Process control and instrumentation

This series explores the fundamental technologies and topics essential to your plant's operations, including safety, quality, compliance, instrumentation, measurement, and maintenance. The Virtual Process Industry Conference is planned for November; the first on-demand webinar in the series is "Securing Industrial Environments with OT Endpoint Management."

Digital transformation

Get real-world examples of IT/OT convergence, business transformation, and operational excellence using digital tools and technologies through this series of virtual events. An ISA100 wireless condition monitoring webinar is planned, for example, as is a half-day conference dedicated to deep water automation for the oil and gas industry.

Within the Digital Transformation Series, a new webinar is available for on-demand viewing. "Using New Technology to Maintain Progress During a Pandemic" describes how immersive technology, such as smart glasses, may be a solution to organizations needing to move parts of their supply chain out of affected areas during the pandemic, or if workers need to be demobilized to minimize their threat of infection. Ken Nguyen, program manager for major capital projects with British Petroleum describes how BP has used smart glasses to support remote inspections and reviews. ■

Report: Most countries to surpass 2019 levels of manufacturing production by 2024

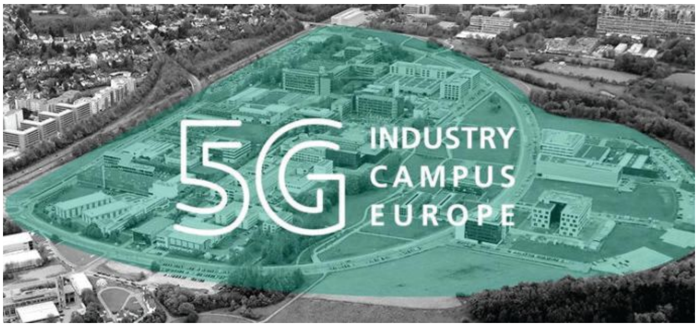
In the latest update to its Manufacturing Industry Output Tracker (MIO), Interact Analysis forecasts a steady but varied recovery for global manufacturing, notwithstanding the fact that some sectors have been hit harder than others during the COVID-19 crisis. Most countries will have surpassed 2019 levels of manufacturing output by 2024. Some as early as 2022, according to the report.

In January 2020, Interact Analysis predicted the start of a gradual short-term rise in global manufacturing output, after relatively lean years in 2018 and 2019. This was based on various historical measurements and forward-looking indicators. COVID-19 has completely changed that outlook.

Adrian Lloyd, CEO of Interact Analysis, says: "This MIO report update is informed by our analysts on the ground in countries across the world, and is a forensic analysis of the short- and long-term prospects of 16 key manufacturing sectors in 37 of the largest economies, as efforts are made to recover from the global shock of COVID-19."

There have been significant downturns in the past, notably in 2009, but this MIO update says that the crisis happened when basic market fundamentals for many economies were sound, so recovery, though slow, will be sustained. The report predicts a global pandemic-induced contraction of 7.6 percent in 2020—which is not as severe as the 8.6 percent contraction experienced in 2009. ■

5G-Industry Campus Europe opens in Germany



The 5G-Industry Campus Europe switched on its radio network in Germany in May to become what is called the largest 5G research network in Europe. In an area of almost 1 square kilometer, 19 antennas combine to create a bandwidth of 10 gigabits per second for a 5G network. In March, the 5G-Industry Campus Europe was awarded a first 5G license in the 3.7 to 3.8 Gigahertz range, and now the network is running. Germany's Federal Ministry of Transport and Digital Infrastructure is funding the ambitious project with around 6 million Euros.

The network is at the RWTH Aachen University campus, and it connects the Fraunhofer Institute for Production Technology IPT, the Laboratory for Machine Tools and Production Engineering WZL, the FIR (Institute for Industrial Management), and, in the future, other university departments with the new mobile radio standard. Additional partners for the development of the 5G infrastructure are the mobile network supplier Ericsson and the IT Center of the RWTH Aachen University.

Together, the partners at the 5G-Industry Campus Europe can research and test various applications of 5G in industrial use. The aim is to open up new fields of application for 5G mobile communication technology in production, ranging from 5G sensor technology for monitoring and controlling highly complex production processes to mobile robotics and logistics and cross-location production chains.

Another target of the Aachen scientists is to test modern edge-cloud systems for fast data processing in order to exploit 5G for fully networked and adaptive production.

Contact the consortium via the project website (www.5G-Industry-Campus.com). ■

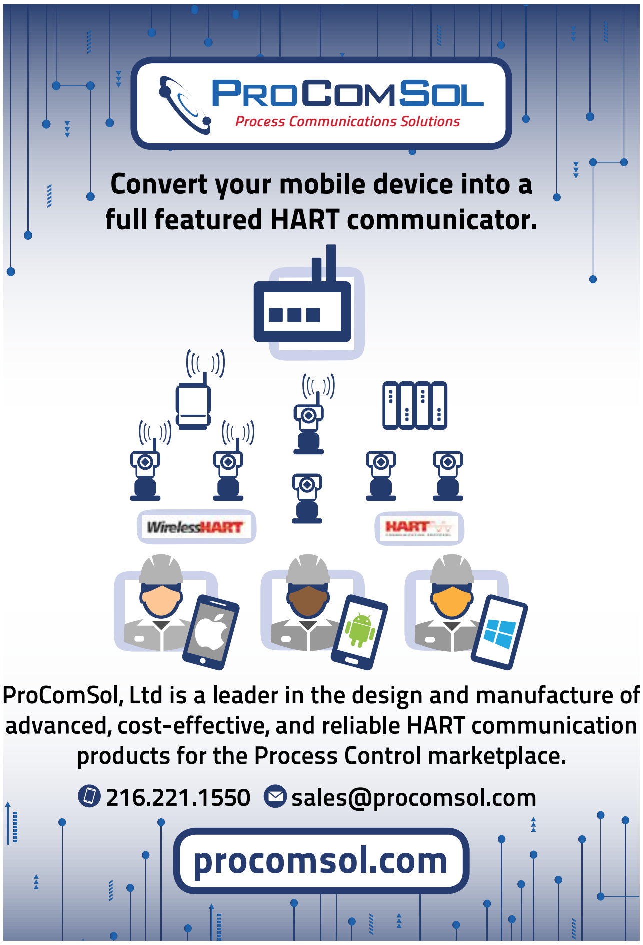
IDG Survey: Only 25 percent have completed IT modernization goals

Only one in four enterprises pursuing IT modernization initiatives have completed their initial objectives, yet even those in the earliest stages of the journey are reaping measurable benefits that are driving business transformation, according to a new IDG Research Services survey commissioned by Insight Enterprises' Cloud + Data Center Transformation solution area.

The survey, "The State of IT Modernization 2020," examined the maturity of efforts to optimize IT operating environments, cloud strategies, applications, and processes, including progress made, barriers encountered, and variations in initiatives at different phases. Respondents included 200 IT executives working in organizations with an average of 29,000 employees across a wide range of industries. Among the findings:

- Just 25 percent have achieved their initial IT modernization objectives, in part because of hurdles including competing priorities, outdated processes and tools, outdated infrastructure, lack of in-house expertise, insufficient budget, and operational limitations.
- The 26 percent of organizations in the beginning stages of modernization are seeing a measurable impact on business operations. This includes improved quality of service (65 percent), better customer experience/satisfaction (52 percent), cost savings (50 percent), uptime (44 percent), and creation of new revenue-generating products and services (42 percent).

Results are available at www.insightcdct.com/IT2020. ■



Automation helps honor pandemic-affected 2020 graduates

In the midst of the worst pandemic in a century, social gatherings are becoming a distant memory, and schools have either closed down or turned to online learning. While sporting events, conferences, family reunions, and other gatherings can be rescheduled, what of once-in-a-lifetime events like a graduation? Many seniors have been facing the end of their schooling without the ceremony they worked so hard to earn. To bring its graduates their special day of recognition while still maintaining social distancing standards, Arizona State's Thunderbird School of Global Management partnered with Double Robotics to provide a unique solution.

Looking a bit like rolling broomsticks with human faces, mobile telepresence robots served as student "avatars," rolling across the stage to receive their award from Dean Sanjeev Khagram. The tablet-computer "heads" of the two-wheeled robots used full two-way audio and video, so the graduates could experience the feeling of walking across stage and interacting with the dean, no matter where in the world they were. The entire 11 May ceremony was broadcast via YouTube so parents and friends could be part of the event.

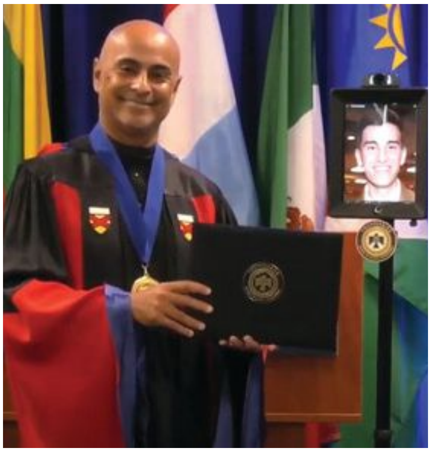
Explained Dean Khagram, "We teach our students how to maximize the benefits of the Fourth Industrial Revolution by embracing global ingenuity and innovation, so leveraging transformative technologies like mobile telepresence robots for an unprecedented commencement was a fitting final lesson for the Class of 2020."

Providing safety in the time of COVID-19 while still giving the students the recognition they deserve was the primary driver of this effort, said Khagram. "We'd love to be there to give [graduates] a hug or a high five. But if there is one thing the pandemic has shown more than ever . . . it's that the digital transformation is underway and accelerating," he said.

During his remarks, Khagram said those who can embrace new technologies and achieve a "digital global mindset" would become the leaders who take us into the increasingly digital world.

The ceremony consisted of some 140 graduates and four rented Double 3 robots. Although only the students who won special awards earned the treat of being able to maneuver the robots from behind the podium, each student sent in personal photos or videos that were loaded onto the robot screen. Therefore, each graduate received the treat of being able to see themselves in robot form.

It was fascinating to watch their robots maneuver across stage and around the podium so students could give their acceptance speeches. The Thunderbird support staff had time to get familiar with the robots and their usage, in order to run the ceremony, but it was evident that the graduate awardees were not as familiar with maneuvering the robots. Yet, their fascination with this innovative use of technology was evident throughout the ceremony.



"I want to thank ASU and Thunderbird for their innovative design to hold this ceremony for us, while keeping us all safe," expressed graduate and award-winner Juili Amit Kale. "I was able to receive my award and converse with Dr. Khagram with the help of robotics. Isn't that innovative?" ■

—*Cory Fogg, Automation.com*

In memoriam

Enrique Valer, senior vice president of the Iberian Zone of Schneider Electric, died 19 March in Spain. Valer was appointed general director of Schneider for the Iberian Zone in 2004, following more than 25 years in the electrical sector. Javier Pascual, managing director for Yokogawa Iberia, broke the news to Valer's professional colleagues and wrote this touching tribute:

"All of us have someone who gives some impact in our lives. I had a very good friend who unfortunately passed away on the 19th of March 2020. Our current worldwide health situation is dramatic. We are losing friends and relatives, but we can hardly say farewell to them. Even worse, it is difficult to pay homage to them.

"Enrique Valer was my friend. He was an excellent professional, and an excellent father. He has built a long list of friends and has raised, along with his wife, a brilliant and beautiful family. I feel honored by having been a friend of him, working and enjoying life together. A few years ago, he won a battle with leukemia. However, and very sadly, COVID-19 arrived and snatched away his life.

"A big man deserves a big recognition. For this reason, I [am] giving tribute to him, and waiting for better times in the near future in order to celebrate his life with a proper funerary ceremony."

Jean-Pascal Tricoire, chairman and CEO at Schneider Electric, said: "Very sad with the news. Enrique has been a great professional and companion, on top of being a good person. Many people will miss him, and many people can thank him. Our thoughts go to his family." ■

Autonomous disinfecting robots join the front lines of the coronavirus battle

By Per Juul Nielsen

As the global war against the coronavirus rages on, interest in safe, disinfecting technology that can kill the virus in hospitals is growing. Next-generation disinfecting robots created a few years ago for disinfecting hospital rooms using UV-C light have been gaining significant attention as a way to disinfect against coronavirus. In particular, the technology is enabling hospitals to protect patients, medical professionals, and frontline cleaning staff from infection while simultaneously bringing greater operational efficiency.

Using UV light is not a new idea. Since the 1870s it was known that ultraviolet light had an inhibiting effect on bacteria, and history shows that in 1895, Niels Ryberg Finsen used concentrated beams of ultraviolet light to treat patients with lupus vulgaris with some success. UV-C was also used to disinfect the municipal water supply of Marseille, France, in 1908, and Westinghouse developed the first commercial UV-C germicidal lamps during the 1930s to be used primarily in hospitals. After World War II, UV-C was used for sterilizing air in hospitals, kitchens, meat storage and processing plants, bakeries, breweries, dairies, beverage production, pharmaceutical plants, and animal labs. It became a major component in the control and eradication of tuberculosis, but the advent of antibiotics and vaccines meant that the technology was largely abandoned for decades.

The renaissance of UV-C light

Today, with the emergence of antibiotic-resistant bacteria and viruses that we cannot vaccinate against, this technology is seeing a renaissance. Scientific reports continue to underscore the benefits and importance of UV-C light in disinfecting. One study from September 2019 evaluating the effectiveness of improved cleaning interventions in hospitals reported that approximately 5–30 percent of surfaces remain potentially contaminated due to the inability of existing detergent formulations and disinfectants to kill certain kinds of bacteria.

Scientific reports continue to underscore the benefits and importance of UV-C light in disinfecting.

In recent years, hospitals have been using UV-C light to sanitize rooms to reduce hospital-acquired infections (HAIs) with a cluster of UV-C emitting lamps that can be wheeled into a room. The lamps disinfect the room in an hour or less, reaching surfaces that may be overlooked by cleaning staff. However, the drawback is that this early technology requires a human to enter the room (between cycles) and move the UV-C emitting lamp from one position to another, so all surfaces, in theory, receive the maximum dosage of radiation. This calls into question the effectiveness, and raises the possibility of some surfaces that are either "shadowed" or further from the lamp potentially remaining infected.

A UVD robot using UV-C light to disinfect while navigating a hospital room autonomously.

The shadow effect

To understand the shadow effect, one need only look as far as the sun, by far the Earth's most powerful source of UV-C radiation. The amount of UV-C generated by the sun every second is higher than all of the artificially generated UV-C in the history of UV-C disinfection combined. We all know that overexposure to the sun's UV light can result in a sunburn. However, this is impossible at night, when the Earth blocks the light from the part of the planet facing away from the sun.

Similar to shadows, another law of light that complicates the use of UV-C as a room disinfectant is intensity over distance, which can be easily calculated using the inverse square law. The inverse square law dictates that to reach the same level of UV-C intensity (or germicidal effect) achieved at 1-meter distance, it is necessary to radiate for nine times longer from a 3-meter distance and 16 times longer from a 4-meter distance. UV-C intensity at 1 meter is 100 percent; therefore, the light intensity at 2 meters will fall to 25 percent (a quarter). At 3 meters, the intensity drops further to 11 percent (a ninth), and at 4 meters, intensity is only 6.25 percent.

When applying the idea of shadows and distance to a hospital room scenario, one can apply this thinking to the effectiveness of UV-C light. In fact, according to Professor Valerie Edwards-Jones of Manchester

Continued on page 12

At the Hospital ABANO in the Veneto province in Northern Italy, the UVD robot disinfects a room used to scan patients for COVID-19.

Metropolitan University "shadowing effects," which reduce the UV-C intensity, and the distance from the contaminated surfaces can vary enormously, as she explained in her report, "UV-C Light and Coronavirus Statement."

99.99 percent disinfection rate

Unlike their stationary counterparts that cannot reach shadowed areas or move close to all surfaces in a room, a self-driving robot has the ability to autonomously reposition itself multiple times and to disinfect during repositioning. These are critical factors in achieving the highest possible level of disinfection to eliminate bacteria and other harmful microorganisms.

Hospitals around the globe are benefiting from reduced shadowing and consistent exposure to every section of a room, resulting in a 99.99 percent disinfection rate, including from coronavirus.

Further, a major advantage of using robotic technology over manual disinfection systems is traceability, as the robot will repeat the validated room disinfection precisely again and again. If it does not, it will deliver a fail report, producing a much higher level of accountability than stationary lights.

The development of autonomous disinfecting robots started in 2014, when a group of Danish hospitals demanded a more effective way of reducing infection rates in hospitals. Through a collaboration of bacteriologists, virologists, and hospital staff from hospitals and robot developers, designers, engineers, investors, and business people from Blue Ocean Robotics, UVD Robots deployed its first autonomous robot at the Odense University Hospital in Denmark in 2018.

These self-driving robots can now disinfect a hospital room in about 10–15 minutes. UV-C light is also known to kill airborne microbes, which is becoming increasingly of interest. UV-C light is not harmful to humans in small dosages, and the light emitted through door cracks, etc., is not a health concern.

Further, a UV-light disinfection system also does not require changes in a room's ventilation, and does not leave residue after treatment. There were no reports of damage to materials in the room during the use of UV-light disinfection systems.

A large volume of UVD Robots are currently in operation in close to 50 countries worldwide. They have now been deployed at hospitals in areas hard hit by the coronavirus, such as in Wuhan, China, and in Italy.

Operational efficiency

In U.S. hospitals alone, the Centers for Disease Control estimates that hospital acquired infections (HAIs) account for 1.7 million infections and 99,000 associated deaths each year. Further, according to research, patients who acquire infections from surgery spend, on average, an additional 6.5 days in the hospital, are five times more likely to be readmitted after discharge, and are twice as likely to die. Moreover, surgical patients who develop infections are 60 percent more likely to require admission to a hospital's intensive care unit. Surgical infections are believed to account for up to 10 billion dollars annually in healthcare expenditures.

For some perspective on how autonomous disinfecting robots can help, last December, just before the coronavirus outbreak, an autonomous robot disinfected an entire hospital theater suite of 17 rooms including corridors. The disinfection comprised 60 separate disinfection positions. It was completed in fewer than two hours and involved fewer than 10 minutes of manual labor, underscoring how state-of-the-art robotic technology can drastically increase the coverage of automated infection prevention procedures within a theater setting. For the first time in history, theater personnel can routinely disinfect between procedures, as well as carry out a daily yet thorough disinfection of the complete theater suite, in less than two hours using minimal labor resources. This drastically reduced associated labor costs without sacrificing efficiency.

Beyond the pandemic

As we move beyond the coronavirus pandemic, it is likely that we as a global society will emerge with a very different sense of the need for disinfection. We will demand greater protection against not only hospital-grade infections, but new infectious risks to health in other environments.

While the coronavirus is pulling the effectiveness of UV-C light into the spotlight, self-driving disinfecting robots were already being successfully deployed to fight HAIs well before. Looking ahead, prevention will likely become central to controlling and eliminating the spread of diseases like coronavirus. We will see this disinfecting technology moving back into environments like those where UV-C light was being used in the 19th century and into more places, including factories, food storage facilities, prisons, schools, supermarkets, and airports. ■

ABOUT THE AUTHOR

Per Juul Nielsen (pjn@uvd-robots.com) joined UVD Robots as CEO in 2017 following 10 years of executive management experience in hygiene solutions for the global healthcare market. He holds a BS in engineering and a BS in business administration. He is a graduate of the INSEAD General Management Program.

To autonomy and beyond!

By Tsuyoshi "Ted" Abe

We are facing a perfect storm created by a volatile, uncertain, complex, and ambiguous world. All industries are threatened by recession more than ever because of COVID-19. In the energy industry, this means digital transformation must be accelerated to change the game.

Plant assets and operations can be upgraded with learning and adaptive capabilities to provide automatic responses with minimal human interaction, freeing and empowering operators and other plant personnel to perform higher-level optimization tasks. This goal will be reached by undertaking a journey from industrial automation to industrial autonomy (IA2IA) to take us beyond Industry 4.0. While Industry 4.0 describes the high level of automation interconnectedness common in today's systems, IA2IA moves further by introducing autonomy capabilities.

We have been discussing different aspects of this IA2IA journey with customers for a couple of years now, and recently we have extended that discussion to other industry stakeholders and experts. A pharmaceutical firm executive observed that: "The benefits of autonomy are clear; you can make the process cost effective because right now a lot of human interaction is still needed, which is quite expensive."

The oil and gas industry has a particular need for autonomous operation. "You can bring less people offshore and bring more people onshore, essentially bringing them out of harm's way and into a proper office building where you will have all the control systems," points out a director at a market research firm.

As the second comment point out, autonomous operations free up personnel to innovate while improving safety. The need for autonomous operations is also becoming acute due to demographic shifts, as 71 percent of the energy industry workforce is now aged 50 or older, with similar numbers throughout the process manufacturing sector. Simply put, there will not be enough skilled or knowledgeable personnel to support current and future manufacturing needs. When routine, repetitive, physically demanding, and dangerous tasks can be performed autonomously, personnel can be redeployed on more mentally challenging tasks. A professor specializing in artificial intelligence stated: "The question is not whether the system will be autonomous. The question is what will the level of autonomous decision making be?"

Progress toward industrial autonomy appears to be inevitable, and it will be used for these twelve main benefits:

- increase efficiency by improving personal and process productivity
- improve availability by implementing predictive maintenance
- provide better cybersecurity by delivering solutions with built-in features
- improve safety through more intelligent application of relevant systems
- increase flexibility by making plant production more agile
- resolve supply-chain issues through better visibility upstream and downstream of production
- improve operator actions through increased situational awareness
- accelerate innovation by making better use of workforce creativity
- deliver smarter products and services to improve offerings and drive revenue
- implement a wider range of remote operations with minimal staffing
- establish fully unmanned and autonomous operation
- increase mobility by providing secure access to information from anywhere at anytime.

But we should keep in mind that even these benefits are just scratching the surface, because they will be achieved by applying autonomy to just a single asset, or perhaps to its direct value chain at best. This will certainly lead to benefits for the operator of the asset, but corporations now are expected to consider their operations from the point of view of planetary sustainability. That is why we must already start thinking about symbiotic autonomy, which delivers multi-win outcomes for a much wider range of stakeholders.

One example is the Kalundborg Symbiosi, a partnership between nine public and private companies in Kalundborg, Denmark. The partnership's lead project links these companies together such that the energy, water, and material residue from one company becomes a resource at another, benefiting both the environment and the economy (www.symbiosis.dk/en).

Yokogawa plans to take a leading role to make symbiotic autonomy a reality across the world. These types of projects point the way to the ultimate goal of the IA2IA maturity model, creating ecosystems where all benefit: people, companies, and the planet. As we like to say: "What's next for our planet? Let's make it smarter." ■

ABOUT THE AUTHOR

Dr. Tsuyoshi "Ted" Abe is the senior vice president of marketing for Yokogawa Electric Corporation. Dr. Abe spent 31 years at Intel Japan in a variety of technology, manufacturing, and marketing roles before joining Yokogawa in 2016 as senior vice president of Yokogawa's global marketing headquarters.

Power protection at the edge: How industrial batteries are evolving

By Shawn Hatton

Extending control to the edge has great potential for reducing operational costs and improving efficiency, but it brings a host of new challenges, including ensuring power availability to all devices. Uninterruptible power supplies (UPSs), which provide battery backup for operations, are essential for all critical processes, and these are now evolving to deliver continuity in the digital age, beginning with their core battery technology.

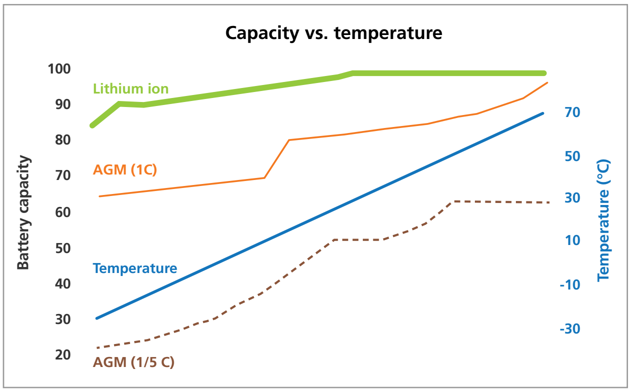
Conventional UPSs use lead-acid absorbent glass mat (AGM) batteries, which are antiquated and have severe shortcomings. AGM lead batteries are large and heavy, must be vented, and must be mounted upright. Advancements in battery chemistry have decreased battery cell size without compromising output or efficiency, but these models have been slow to replace AGM batteries in the industrial world. This is changing rapidly, however, as UPS manufacturers replace lead-acid AGM technology with lithium-ion technology.

Lithium-ion technology has numerous advantages for backing up critical industrial processes. It has superior useable capacity and extended cycle life over lead-acid batteries, which is required for mission-critical applications.

AGM batteries typically use only 30 to 50 percent of their rated capacity. Discharging them below this limit greatly reduces their life. The (AGM) lead-acid pack must be limited to 30 percent depth of discharge (DoD) to get cycle life comparable to a lithium-ion that is used at 75 percent DoD. Moreover, the AGM battery must be 2.5 times larger in capacity than the lithium-ion to get comparable life.

Li-ion batteries also have the following advantages over AGM batteries:

- Flexible deployment: Li-ion units are sealed and can be mounted in any orientation.
- Fast charging: Li-ion units charge 10 times faster.
- Extended life: Li-ion units have a 12 amp-hour capacity and a 10-year life at 40°C.
- Lower de-rate: Li-ion batteries can deliver 75 percent of their original capacity after 2000 charge cycles. AGM batteries are not suited for a continuous trickle-charge environment that is common in remote industrial installations. AGM batteries are dependent on a full depth of discharge to obtain the maximum amount of charge cycles.
- Improved capacity retention: Li-ion batteries operate across a wider temperature range with longer life. They maintain 100 percent of their load capacity between –10°C to +50°C versus 30 percent for AGM batteries (figure). Lead-acid batteries operate best at 25°C (77° F) and lose half of their life with every 8°C (15°F) rise in temperature. Even valve-regulated, lead-acid batteries, which are designed to maximize AGM efficiency, would last only 10 years at 25°C, five years at 33°C (95°F), and one year at 42°C (107°F). In hot regions, AGM-based UPSs typically need to be replaced every year.



Lead-acid batteries operate best at 25°C (77°F) and lose half of their life with every 8°C (15°F) rise in temperature. Li-ion batteries maintain most of their capacity regardless of temperature.

Lithium needs protection as well

Despite the performance advantages of lithium over lead-acid, the UPSs need protection as well. Batteries consist of multiple cells, depending on how much power is needed. Rather than stack cells and monitor, control, and contain that stack, advanced Li-ion battery safety requires every cell to be engineered as an independent system. This starts with galvanic isolation of charging circuits and dedicated circuit boards, sensors, electronics, and passives to monitor, control, and limit charging current, charging voltage, and discharge current. In this way, the battery pack becomes less vulnerable to the status of a single cell, and the charge and discharge of each cell is independently optimized for safety and performance. The cells should be encapsulated and protected by multiple layers, including compliance with NEMA 4x, FIPS 140, and ingress protection (IP) standards from an all-metal housing.

Completing the package

With Li-ion technology at their core, UPSs are evolving in many other ways to optimize reliability at the edge. This includes improvements in intelligence, integration, ruggedness, and cybersecurity.

Embedding secure microcontrollers with high memory capacity enables collection and analysis of operational data, which can be used to identify and prevent critical errors, optimize performance, integrate with other technologies, and enforce authentication and encryption to protect the end device from cybersecurity threats.

Armed with advanced Li-ion technology, UPSs stand ready to meet the challenges of the digital age. ■

ABOUT THE AUTHOR

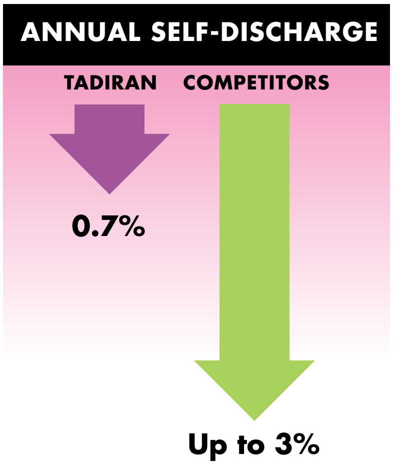
Shawn Hatton has 15 years of experience in electrical, instrumentation, and control system design. He is a senior field automation specialist at Bedrock Automation, makers of the Bedrock UPS, which encases Li-ion battery technology in an all-metal, anti-tamper enclosure.

IIoT devices run longer on Tadiran batteries.

PROVEN
40
YEAR
OPERATING
LIFE*

Remote wireless devices connected to the Industrial Internet of Things (IIoT) run on Tadiran bobbin-type $LiSOCl_2$ batteries.

Our batteries offer a winning combination: a patented hybrid layer capacitor (HLC) that delivers the high pulses required for two-way wireless communications; the widest temperature range of all; and the lowest self-discharge rate (0.7% per year), enabling our cells to last up to 4 times longer than the competition.



Looking to have your remote wireless device complete a 40-year marathon? Then team up with Tadiran batteries that last a lifetime.

TADIRAN
BATTERIES

Tadiran Batteries
2001 Marcus Ave.
Suite 125E
Lake Success,
NY 11042
1-800-537-1368
516-621-4980

www.tadiranbat.com

* Tadiran $LiSOCL_2$ batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.

Cybersecurity risk is the great equalizer

Awareness of challenges and collaboration on solutions can secure critical resources

By Eric C. Cosman

Protecting automation systems from cyberattacks—particularly those in critical infrastructure—has been an imperative for almost 20 years. Professional and trade associations have developed standards, practices, and guidelines. Government agencies and national laboratories in several countries have supplied frameworks, guidelines, and in some cases, regulations. Traditional automation companies have retooled their product and service offerings to focus more on security. Entirely new companies are offering technology and services to address perceived needs. In spite of all of this activity and investment, many experts and industry pundits say that we are still far from being able to ensure the security of these critical systems. What is holding us back?

There are as many answers to this question as there are specific circumstances. However, there are some common themes. Many asset owners find it difficult to define the business case for changing their security practices without evidence of specific and pressing risk. Others may struggle with selecting from what often appears to be a large, confusing, and perhaps conflicting collection of available guidance. Many small to midsized companies simply do not have the necessary staff or expertise to adequately address the need for a cybersecurity program.

Common or industry specific?

One of the more interesting topics of discussion is whether standards and guidance should be broad and general or tailored to specific industries. It has been hotly debated within the industrial cybersecurity community for several years. The assertion that industries are more similar than different, and that standards and practices should be developed to be applicable across industries has elicited a range of responses depending on the perspective of the individual. There is an interesting analogy here with the Kübler-Ross model, also known as the stages of grief, which describes a progression of emotional states associated with traumatic events (figure 1).

Stage	Typical response
Denial	Our needs and situation are different.
Anger (or frustration)	This "security speak" is too complicated. Just give me a checklist.
Bargaining	I can accept that the principles are the same, but they still need to be tailored to my situation.
Depression	There is no way that I can adequately understand, apply, or afford all of these requirements.
Acceptance	The requirements and guidance seem reasonable. Help me to apply them.

Figure 1. Responses to common standards and practices.

While this model may not be a perfect fit for the situation, it does supply a context and steps for moving the discussion beyond the question of the *suitability* of particular guidance and toward what is required to reduce cyberrisks. The aim must be to gain maximum value from the guidance and practical examples available, without discounting information simply because it comes from a different industry.

FAST FORWARD

- Cybersecurity risks are common across industries and regions.
- Effective response to this risk requires a multidisciplinary approach.
- Standards are essential but must be accompanied by practical guidance and examples.

Similar risks and consequences

There are certainly differences between industries, but the risks associated with potential cyberattacks or deficiencies are rather similar. Consider that risk is commonly defined as a function of threat, vulnerability, and consequence, combined with an estimate of likeliness of occurrence. To fully assess similarities across industries and companies, it is necessary to look at each of these factors.

Threats to industrial systems come in many forms, ranging from direct attacks to nonspecific attacks that capitalize on the nature of these systems and their availability or accessibility via the Internet. While many asset owners feel that they are not of a high enough profile to be the target of a directed attack, they can easily become collateral damage when malicious software is released on the Internet. Recent cases of ransomware attacks illustrate this very clearly. Those releasing this software may not have an individual target in mind but are simply looking for situations where vulnerabilities can be exploited to encrypt data and demand payment for its release.

The second major factor in calculating risk is vulnerability. It is here that we see the greatest level of commonality across applications. Virtually all industries that employ computer-based or automated systems use products from the same suppliers. In recent years, the number of major suppliers has decreased, with all using essentially the same commercial-off-the-shelf technology for components such as databases, operating systems, and network components. This has created a technology monoculture where the vulnerabilities inherent in automation solutions are common to all.

Vulnerability mitigation requires asset owners to update or patch their installed systems as quickly as possible. In cases where such patching is not practical or even possible, it is often necessary to employ compensating countermeasures or controls to mitigate the vulnerabilities. Examples include the use of various isolation methods, up to and including disconnecting such systems from networks. Products, such as industrial firewalls and unidirectional gateways, are now available for this purpose.

Perhaps the most important component of the threat calculation is the potential consequence of system compromise. These consequences may extend well beyond shutting down the automation system itself to loss of view or control of the process under control. In some cases, it is difficult or impossible to operate such a process safely without automation, leading to a dependence on automated safety systems to move it to a safe condition or shut it down in a safe manner. As recent events have shown, even the safety systems themselves may be susceptible to cyberattack.

Although the details of these consequences vary across industries, their nature is often similar, if not identical, ranging from loss of product or service to explosions or release of hazardous or noxious materials and equipment damage. Perhaps the most common grouping of industries based on potential consequences is what is known as critical infrastructure component sectors. In the U.S., this is defined as including sectors that are ". . . considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety, or any combination thereof."

Based on the above analysis it appears that the risks faced by different industries are more similar than some might perceive, which would in turn lead one to conclude that more cross-industry sharing may be beneficial.

Common challenges

There are other factors that have often limited the creation of effective cybersecurity programs for industrial systems. These also tend to be common across a wide range of industries.

Standards complexity. Industry standards are written using very precise structure and terminology to allow the creation of formal conformance specifications. The language can be viewed as arcane to those who are not experts in the subject matter. Unfortunately, this means that these documents may be seen as intimidating to almost incomprehensible by those trying to apply them in practical situations. This in turn affects the level of acceptance and adoption. It is clear that standards by themselves are not sufficient to promote adoption of proven and effective practices.

The aim must be to gain maximum value from the guidance and practical examples available, without discounting information simply because it comes from a different industry.

Lack of practical examples. While standards typically document what has already become accepted engineering practice, they also supply a starting point for the collection of case studies and use cases. Case studies describe the approach and results from a specific application; while use cases focus on a specific aspect of the topic. In both cases, it is important to identify and describe common principles and fundamental concepts that form the basis of an effective response, irrespective of the industry involved.

Unfortunately, practical and representative case studies are often hard to find. Asset owners may be reluctant to share what they consider proprietary or otherwise sensitive information, or they may simply lack the time and resources to prepare and publish such documents. The most common scenario is for suppliers to publish case studies that have much of the identifying information redacted, but these may be viewed as thinly veiled advertisements of specific products and solutions.

Need for work process guidance. There is a specific type of guidance for which there appears to be particularly high demand. Asset owners and others who wish to establish an effective cybersecurity program are very interested in understanding how their peers have integrated such programs into their normal work processes. There is ample evidence and experience that shows that a project approach to cybersecurity is not sustainable over the long term. Just as with safety, security must become an integral part of normal processes and procedures.

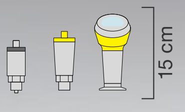
Multiple competencies. There is also the question of what skills or competencies are required to adequately address cybersecurity risks. Obvious needs include expertise in the management and protection of information, and of the systems and networks on which it resides. But this is not enough when dealing with automation systems. It is also necessary to have a thorough understanding of both the process under control, and the strategy and logic used to affect that control. This expertise is only available from automation and similar engineering disciplines. This combination of information, systems, and network security with engineering expertise is needed to fully address the problem.

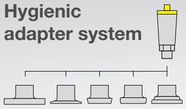
Little of what has been presented to this point is specific to an industry. The threat and vulnerability components of risk are largely the same for everyone, and while the detailed consequences may vary, the potential impact is very similar for sectors considered to be part of the critical infrastructure. The challenges faced by those trying to mount an effective response to cyberrisk are also largely the same. Moreover, most of these challenges can be more effectively addressed with increased sharing of practices and experiences.

Elements of the response

Given that there is so much commonality between industries, it seems clear that more collaboration would be helpful in addressing the need for improved cybersecurity of operations systems. To share an often overused phrase, "We're all in this together." Such collaboration should include several essential elements:

- Context: First, there must be a common context that can be used to position components of the response and establish relationships between them.
- Concepts and terminology: Effective collaboration and cooperation across industries and disciplines is only possible if there is a common set of concepts and terminology.


15 cm



Although this exists for functional elements in the automation industry and for the system elements in the networking and security disciplines, there are sometimes difficulties when these disciplines must work together. This situation is improving as each constituency becomes more familiar with the other.

- Comprehensive requirements: An effective response is only possible if there is a clear and unambiguous description of the desired future state. Typically, this comes in the form of a set of normative requirements and associated supplemental guidance. It is important that these requirements are constrained to defining *what* is to be done without making assumptions or assertions about *how* this is to be achieved.
- Recommended practices: Requirements—even when accompanied with supporting or explanatory rationale—are not enough, as they often use broad or generic terms in a form that allows for the definition of conformance criteria. Recommended practices take these requirements and restate them using terminology that is tailored more to the specific environment. Thus, there may be several practices based on a single standard, each addressing a specific scenario.
- Case studies and use cases: These are perhaps the most useful resources for system integrators and asset owners, because they describe what has and has not worked in previous situations.

In creating, vetting, and sharing the above resources it is essential to involve all relevant disciplines and stakeholders. Suppliers must work closely with system integrators, asset owners, and service providers to address all phases of the life cycle, from specification and development through implementation, operation, and support. It is also crucial to draw on the expertise from all relevant and affected disciplines. For example, risk assessments must include input from engineers and operations personnel who are familiar with the underlying processes and possible consequences of compromise.

Help is available

Much of the above already exists, albeit not from a single source. This can cause a lack of awareness and understanding on the part of those needing the information. More collaboration is necessary to put the pieces together and provide the full range of necessary guidance. There is also a need for increased awareness and understanding of what is readily available.

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) has been available for several years. Although developed in the U.S., it reflects contributions from other parts of the world and has become widely accepted as a general framework for characterizing an effective cybersecurity response.

NIST CSF core functions

It is now very common for suppliers of products and services to describe their offerings in terms of alignment to the core functions described in the NIST CSF. In addition, NIST has published an implementation guide for the Cybersecurity Framework Manufacturing Profile that is aligned with manufacturing sector goals and industry best practices.

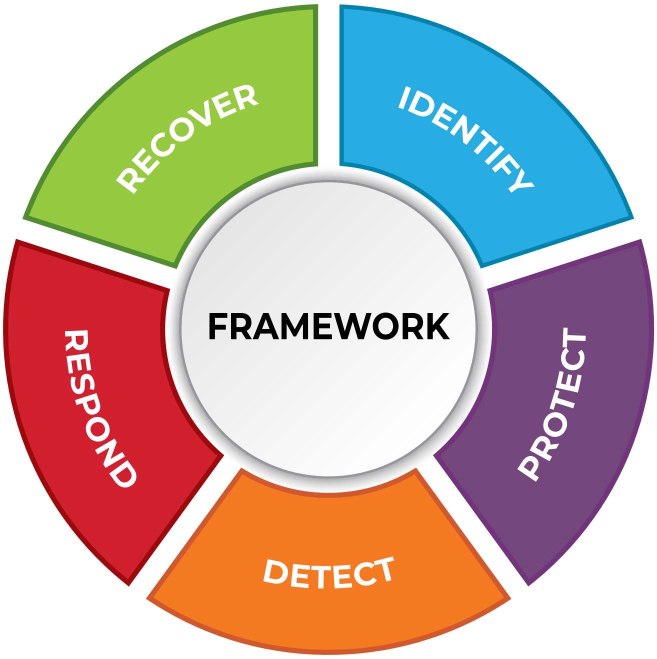
Several organizations have addressed industrial cybersecurity concepts, models, and terminology in various forms; ISA and IEC, however, have jointly developed what are arguably the most comprehensive set of standards in this area. The ISA/IEC 62443 standards are not industry-specific, but define their scope based on a combination of activity-, asset- and consequence-based criteria (figure 2).

The benefit of the ISA/IEC 62443 approach is that the standards are not tied or limited to a specific industry or sector. While originally developed with process industries in mind, they have since been successfully applied in industries such as rail transportation and

> **The benefit of the ISA/IEC 62443 approach is that the standards are not tied or limited to a specific industry or sector. While originally developed with process industries in mind, they have since been successfully applied in industries such as rail transportation and mining.**

Activity	Asset	Consequence
• predictable operation	• necessary to maintain the economic value of a process	• endangerment of public or employee safety
• process or personnel safety	• performs a function necessary for operation	• environmental protection
• process reliability or availability	• represents intellectual property	• loss of public confidence
• process efficiency	• necessary to operate and maintain process security	• violation of regulatory requirements
• process operability	• necessary to protect personnel, contractors, and visitors	• loss of proprietary or confidential information
• product quality	• necessary to protect the environment	• economic loss
• environmental protection	• necessary to protect the public	• impact on entity, local, state, or national security
• compliance with regulations	• needed for disaster recovery	

Figure 2. ISA/IEC 62443 scope criteria.



The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) has become widely accepted as a general framework for characterizing an effective cybersecurity response.

mining. The most common approach in developing these applications involves interpretation of the concepts and requirements in the context of the industry in question, and using this interpretation as the foundation of more focused recommended practices.

The practices developed thus far can serve as useful examples for those interested in developing similar guidance for other industries. As these practices are applied to specific situations, the results can be documented in the form of case studies.

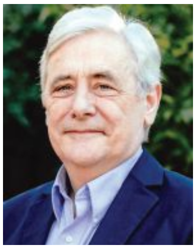
Industry also needs clear definitions of the skills and expertise required to staff cyberattack response programs. Several organizations have addressed this need through the use of competency models or similar tools. For example, ISA has worked with the U.S. Department of Labor to create competency models for both automation and cybersecurity. These are valuable resources for those trying to decide how to best staff their programs.

For the above to be successful, it is necessary to increase the general awareness of what resources are available and how they may be used. In 2019, ISA created the ISA Global Cybersecurity Alliance (ISA GCA) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. The Alliance brings end-user companies, automation and control systems providers, information technology infrastructure providers, services providers, system integrators, and other cybersecurity stakeholder organizations together to address common interests and advance the state of automation cybersecurity.

The intent of ISA GCA is to be the basis of the collaboration required to address cybersecurity challenges, irrespective of industry sector. Because cybersecurity is a cross-competency activity, ISA GCA also hopes to bridge the IT-OT gaps within manufacturing and process industry companies. End user members are welcome, and are encouraged to include people from multiple disciplines.

Cybersecurity risks are common across industries. An effective response to this risk must be multidisciplinary. Being aware of the challenges and collaborating on the solutions is the way to secure our critical resources today and into the future. ■

ABOUT THE AUTHOR



Eric C. Cosman (eric.cosman@gmail.com) is the founder and principal consultant with OIT Concepts LLC, providing consulting and advisory services with a focus on the management of IT solutions in operations and engineering. With more than 35 years of experience in the process industries, Cosman has contributed to various standards committees, focus groups, and advisory panels. Currently the society president of ISA, he has also served as the vice president of standards and practices and as an executive board member at ISA. He is an industry leader in the development of standards and practices for industrial control systems security. Cosman also co-authored the American Chemistry Council strategy for cybersecurity in the chemical industry and is a founding member and current co-chair of the ISA99 committee on industrial automation and control systems security. Visit him at www.linkedin.com/in/eccosman or on Twitter @OITConcepts.

View the online version at www.isa.org/intech/20200601.

RESOURCES

Kübler-Ross stages of grief
https://grief.com/the-five-stages-of-grief

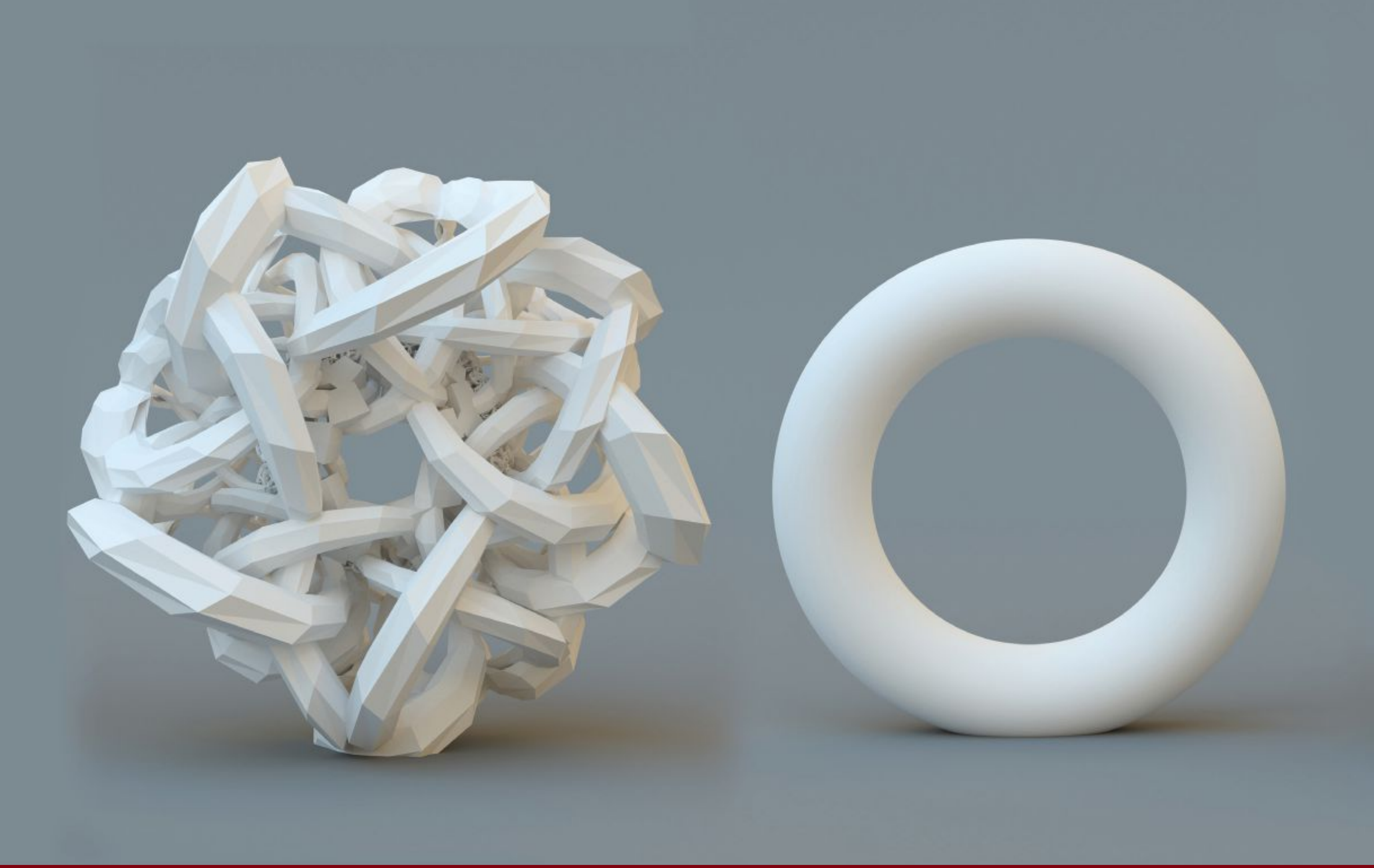
NIST Cybersecurity Framework
www.nist.gov/cyberframework

NIST Cybersecurity Framework Manufacturing Profile
www.nist.gov/news-events/news/2019/09/cybersecurity-framework-manufacturing-profile-low-impact-level-example

U.S. Labor Competency Model for Automation
www.careeronestop.org/competencymodel/competency-models/automation.aspx

U.S. Labor Competency Model for Cybersecurity
www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

ISA Global Cybersecurity Alliance
https://isaautomation.isa.org/cybersecurity-alliance



Simplifying the IIoT technology stack

By Josh Eastburn

Different industrial users have different IIoT goals, but they can all benefit from a simplified connectivity approach

The Industrial Internet of Things (IIoT) means different things to different people. End users from all sorts of industries and businesses incorporate IIoT elements to realize value in ways that suit their unique needs.

In the most general terms, implementing an IIoT strategy involves connecting sensors and automated systems located in challenging manufacturing and process locations to create a unified data network. This enables extensive remote monitoring and data acquisition, deeper operational analysis, and autonomous machine-to-machine interaction. Common goals for users are smarter operations, improved equipment effectiveness, and cost reduction. But whether the user is the operations or engineering group in a plant, an original equipment manufacturer (OEM) who builds manufacturing machinery, or perhaps a systems integrator (SI) tasked with tying it all together, everyone agrees that IIoT implementation should be easy and secure.

At the simplest level, IIoT implementation involves getting field data into cloud systems so it can be processed and shared among many users and applications. That data is most often the domain of operations technology (OT) personnel and systems, conventionally incorporating devices like programmable logic controllers (PLCs), human-machine interfaces (HMIs), and supervisory control and data acquisition (SCADA). While these OT systems can perform a certain amount of computing in the field, or transmit raw data over to the information technology (IT) side of the business for additional processing, they are not very good at either compared with modern options.

This article discusses how new options for industrial edge computing provide a simple and secure alternative approach to achieving different IIoT connectivity objectives. It presents the general architectural improvements that edge computing affords and explores their application in solving the specific challenges of the three user groups mentioned above: plant operations and engineering teams, OEMs, and SIs.

Who wants what?

While everyone is looking for solutions that are good, fast, and cheap, those three attributes rarely intersect. A better way to define the attributes of a robust and optimal IIoT solution is to examine the needs and goals of different end user groups.

Operational end users. End users at manufacturing businesses and production plants all need good data. There are operators who rely on visualization to run their plants on a daily basis, process engineers who want to optimize operations, plant engineers who will expand systems when necessary, and maintenance teams who troubleshoot and correct issues. A good IIoT implementation automatically delivers the right information to the right person at the right time.

FAST FORWARD

- End users, OEMs, and systems integrators are looking for IIoT solutions that have the remote connectivity and data access they need.
- The traditional technology stack suffers from complexity and a lack of security.
- Today's technology stack uses edge computing to make IIoT connectivity secure, scalable, and easy to implement.

Original equipment manufacturers. OEMs create the machinery and equipment operated by end users. They are experts in the equipment they build and automate, but once a machine ships it is not under their direct control on their own site; it could be anywhere in the world. To build better machines and improve support to existing clients, OEMs need IIoT solutions that enable remote connectivity and have the ability to gather performance data for troubleshooting and continuous improvement. The right IIoT implementation will connect them with a highly distributed fleet of equipment across disparate networks and security schemes.

Systems integrators. Of all the parties interested in using IIoT connectivity, SIs likely have the most automation specialists on board, with skill sets spanning platforms, technologies, and industries. Typically, however, they are also the service providers and subject-matter experts (SMEs) for a large customer base. They are tasked with the constant demand to win new business and provide long-term support for previous projects. Effective IIoT solutions will give them cost-effective and efficient ways to deliver systems to their customers, including proven security and multiple communication options for broad interoperability and remote access.

A design profile that satisfies the needs of all

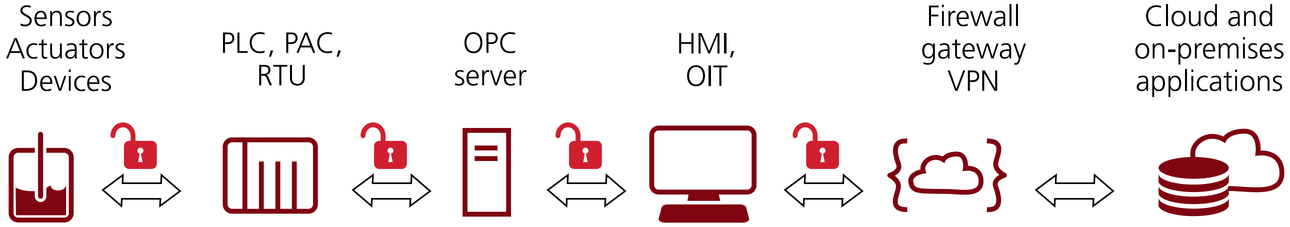


Figure 1. Traditional industrial communications architectures have demanded many layers of hardware and software, driving up cost and complexity and driving down performance.

these parties will include, to varying degrees:

- flexible scalability
- high interoperability
- embedded security
- good performance relative to cost
- low administration and high maintainability

The complexity and expense associated with the current OT solution set oftentimes keeps end users from fully realizing these goals. In the next section we will examine some of the inherent limitations of the conventional approach.

Traditional architectures have lots of layers

Lots of layers in a birthday cake, lasagna, or bean dip are usually considered a good thing, but it is exactly the opposite situation for industrial communication architectures. In these cases, more layers mean more devices, physical connections, configurations, programming, bottlenecks, and single points of failure. Yet traditional architectures have needed all these things to bring even one data point up to the cloud (figure 1).

A simple alarm contact or field sensor is most often wired into a PLC, which is programmed to accept the signal and perhaps scale it. More code is needed to get this signal into the HMI or SCADA system, with yet more code and networking required to transfer the signal to the cloud.

Once commissioned, these connections can be unreliable and difficult to troubleshoot. Additionally, the poll-and-response communications, manual data mapping, and lack of embedded data context make these connections cumbersome to configure and expand. Legacy products and older protocols offer little or no security and can become progressively more unwieldy as time progresses. Software updates to one link in the chain, for example a PC-based HMI or SCADA system, can negatively affect communications.

Some IIoT data connectivity goals can be achieved with traditional technologies, but only after applying great effort and settling for many caveats. The main barrier raised by conventional

Figure 2. Remote I/O devices incorporating edge computing functionality let users connect field I/O signals right to the cloud without extra layers of hardware, software, programming, or IT intervention.

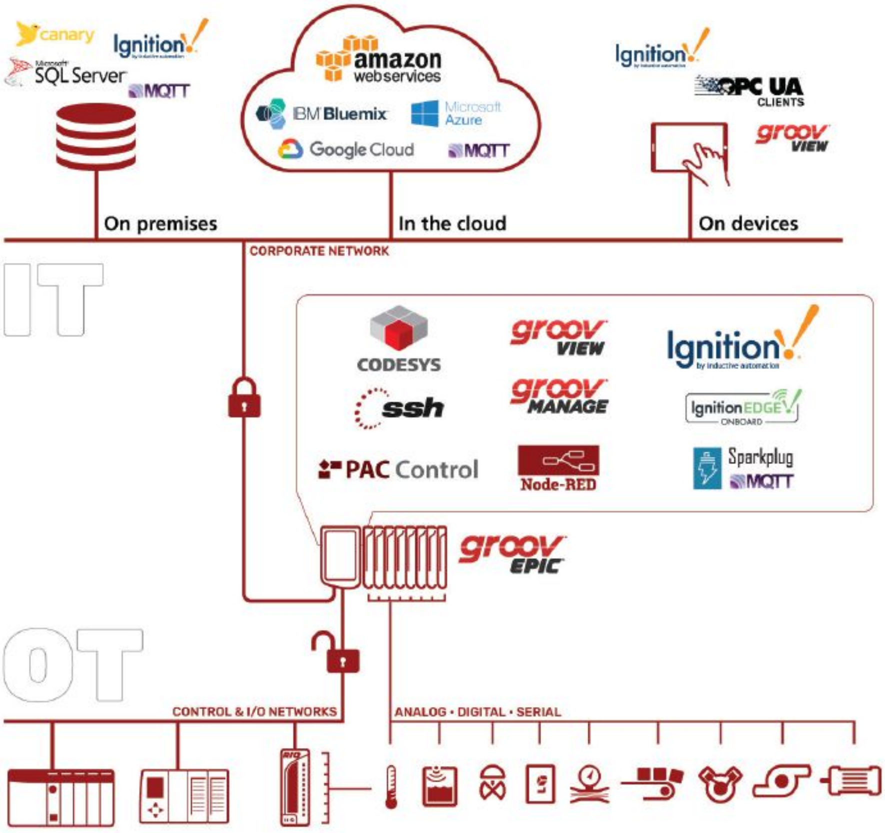


Figure 3. EPICs flatten the architecture, making it possible to connect legacy systems, classic I/O, and modern IIoT devices efficiently and securely to the cloud.

approaches is complexity, which leads to costly hardware, software, and labor for the initial design and sustaining operation. For early adopters trying to obtain data from the automation edge before the rise of the IIoT concept and its underlying technologies, it is clear how challenging the task could be.

Flatter architectures, newfound capabilities

Hardware, software, and communication technologies are progressing and harmonizing to make IIoT implementations practical for any type of end user and application. An important design technique underlying this evolution is called edge computing. It addresses some of the key challenges faced by end users by shifting the traditional communication hierarchy described previously toward a more distributed model.

Traditionally, OT hardware has used proprietary protocols and media with a relatively limited scope of operation. This fact has led to the previously described problems associated with complex, layered system architectures, which were required to facilitate data processing and transmission. In the edge computing model, however, the data demands of large networks are served by embedding more computing power in the field, where data is produced. Rather than requiring a deep technology stack to move data from limited field devices to powerful central computing resources, edge computing devices are capable of processing data directly at the source and then transmitting it wherever it needs to go.

Industrial edge computing hardware addresses the complexity and security concerns of end users by flattening the communication architecture and introducing up-to-date IT standards to the OT domain. For instance, a traditional wired sensor can be connected directly to a field-installed, remote edge I/O device, which will establish an encrypted, certified connection directly to the cloud and transmit the signal data securely through its own internal firewall (figure 2). This avoids the complexity of traditional systems, which would have required interposing PLCs, PCs, and security hardware.

For applications where users need control logic or more advanced computing in the field, they can use an edge programmable industrial controller (EPIC) for this purpose and still have the same connectivity experience. EPICs perform the same real-time control tasks as classic PLCs and PACs but also natively incorporate secure modern management and IIoT communication (figure 3). Because of their more powerful computing capability, they can also function as communication gateways for legacy PLCs and assimilate other automation functions, like HMI visualization or database hosting, further reducing the complexity of the control network.

Edge computing devices support wired Ethernet and Wi-Fi in various configurations, and typically include support for other IT standards like domain name system (DNS), dynamic host configuration protocol (DHCP), virtual

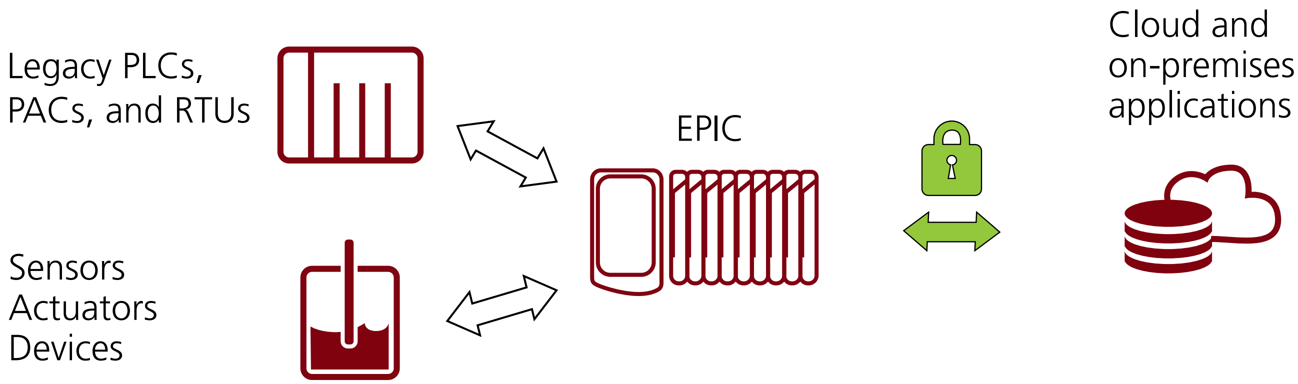

Legacy PLCs, PACs, and RTUs
Sensors
Actuators
Devices
EPIC
Cloud and on-premises applications

Figure 4. Industrial edge computing hardware, like the groov EPIC and groov RIO from Opto 22, creates a secure OT foundation for industrial IoT implementations.

private networking (VPN), and secure shell (SSH) access. These features make it easy to install, configure, and access devices locally or remotely in almost any infrastructure setting, but more importantly they help to close the skill gap between OT and IT. SMEs from both domains can work with a common set of tools to manage automation and business networks, reducing the cost of labor and maintenance, and allowing data to move seamlessly across the organization.

As opposed to PCs and other consumer- or enterprise-grade devices, however, industrial edge hardware is constructed to withstand the physical space constraints and environmental conditions found in the field (figure 4) with appropriate certifications for hazardous environments.

Unique software and communication developments also feature heavily in the portfolio of technologies for enabling IIoT capabilities. Edge computing devices allow these technologies to be embedded directly in the field, including support for OPC, an industry-standard method for connecting with heterogeneous devices, and MQTT (formerly MQ Telemetry Transport) with Sparkplug B, the popular and efficient IoT-specific communications protocol with extensions for mission-critical applications. Edge devices may also include support for IoT tools like Node-RED, an open-source IoT programming language, providing a low-code way for users to combine data from web services, devices, applications, and databases.

Combined, these edge computing hardware and software technologies support a flatter and simpler architecture, which delivers more functionality than classic layered architectures.

Simplified IIoT resonates with all end users

In contrast with traditional architectures, edge computing provides a completely scalable approach to digital transformation. For brownfield sites, operational users can install edge computing devices incrementally and in parallel with existing automation, giving them a migration path that avoids process interruptions. Engineers can expand the data network over time without large, upfront investments in infrastructure, making it easier to bring valuable data to users and applications.

Combined with embedded technologies like VPN and MQTT, edge computing also enables OEMs to offer new support options. Using an EPIC as the native control platform, they can perform routine checks, upgrades, and service calls by connecting directly to their controller online instead of in person. With embedded security, OEMs can also gather extensive operational data

on their installed base of equipment safely over the public Internet. Over the long haul, this data can be used to expose operating trends, so their equipment can be fine-tuned, or even receive beneficial design modifications.

SIs will find that industrial edge computing creates a reliable, cost-effective foundation for their IIoT projects that is applicable to all types of machines and processes. As with the other user groups mentioned, edge computing devices simplify remote support for SIs and facilitate integration with legacy control systems and devices. The combination of streamlined infrastructure, network-oriented security at the device and control level, and support for IIoT interoperability technologies like MQTT and OPC UA helps them deliver the kinds of functionality, visibility, and insights their clients want at a price that wins more business.

Simple and secure

Applying IIoT technologies to obtain valuable remote connectivity and data communications is attractive to operational end users, OEMs, and SIs. Each of these groups has certain needs specific to their role, and they all can benefit from simple and secure solutions.

The traditional hardware and software technology stack has made previous IIoT endeavors difficult due to legacy products, a multitude of layers, and a lack of security. Today's technology stack combines IT-friendly edge computing hardware and software to address these and other issues. By flattening the architecture and offering built-in security and communication options, end users of all types can easily deploy edge computing to achieve their goals. ■

ABOUT THE AUTHOR

Josh Eastburn is the director of technical marketing at Opto 22. After 12 years as an automation engineer working in the semiconductor, petrochemical, food and beverage, and life sciences industries, Eastburn now works with the engineers at Opto 22 to understand the needs of tomorrow's customers. He is a contributing writer at blog.opto22.com.

View the online version at www.isa.org/intech/20200604.

RESOURCES

"Combining IoT, Industry 4.0, and energy management suggests exciting future"
www.isa.org/intech/20180401

"Simplified remote access"
www.isa.org/intech/20180603

"Big data analytics need new solutions"
www.isa.org/intech/20170204

Analytics is changing our understanding of regulatory control

Aggregated PID data provides process manufacturers with new insights into control loop performance

By Dennis Nash

While process manufacturers have justified nearly 30 years of automation investments on the observations of one man, today's control loop performance monitoring technologies are providing new, data-driven insights into the state of regulatory control.

To no one's surprise, data facilitates more and more of today's manufacturing decisions. The data itself is abundant, its storage is low cost, and accessing it is increasingly easy. What is more, novel software tools and enhanced processing capabilities empower today's manufacturers to uncover opportunities for improvement that are invisible to the naked eye. An evolution within the manufacturing sector is unfolding as data analytics continues its progression from basic descriptive functions to predicting outcomes and prescribing corrective measures. All of these model-based capabilities are made possible with data.

In recent years, the manufacturing sector has focused on leveraging data to improve asset reliability, but greater attention is now being invested in process optimization. Whereas one emphasizes uptime as a primary financial lever, the other pursues the quality and throughput gains that result from tighter, more efficient control. In particular, advances in process analytics, such as control loop performance monitoring (CLPM), now simplify the procedures by which manufacturers proactively identify, isolate, and correct negative performance trends.

Recent aggregation of CLPM data confirms industrywide advances in control, and it suggests that new optimization opportunities are on the horizon. For process manufacturers, data analytics in general and CLPM in particular has the power to be a disruptive force for positive change.

Findings and shortcomings

Early insights into process control and optimization highlighted the need for better, more relatable data. In an article written in 1993, David Ender, president of Techmation Inc., asserted that more than 30 percent of proportional, inte-

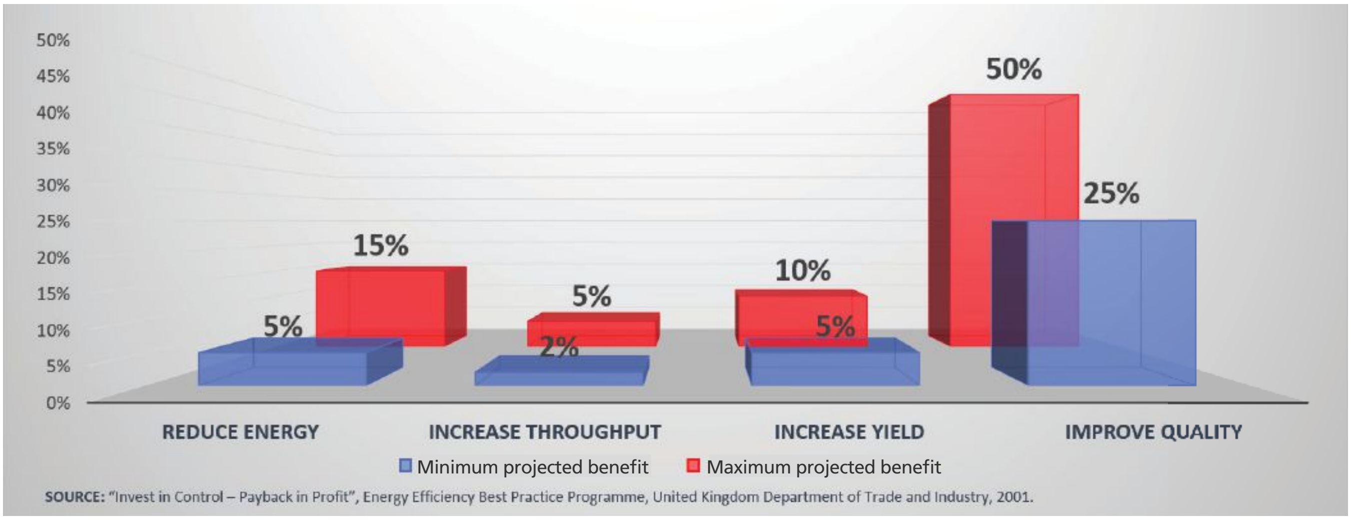
gral, derivative (PID) controllers at a typical production facility were operated manually rather than in their designated automatic mode. Also attributed to Ender and the article, 65 percent of a facility's regulatory controllers were either poorly tuned or even detuned as a means of concealing other control-related issues. As noted in "Process Control Performance: Not as Good as you Think," the Techmation executive's assertions were based on projects conducted at hundreds of production facilities. And while the observations pointed to widespread shortcomings in industrial process control, they also highlighted opportunities for improving both the production and the financial performance of facilities across the process industries.

Several years later the economic impact of poor control was given some much needed clarity. A 2001 report published by the U.K.'s Energy Efficiency Best Practice Programme directly linked gains in operational efficiency and energy consumption with improvements in control. More specifically, the 30 percent of control loops cited by Ender as being operated in manual mode were found to be a primary source of operational losses. The report entitled "Invest in Control – Payback in Profit" quantified the impact of poor control in meaningful terms. By failing to properly harness a production facility's PID controllers, manufacturers left considerable value on the table. The report sized those losses as follows: 2–5 percent in lost production throughput, 5–10 percent in lost

FAST FORWARD

- Observations from 1993 described widespread deficiencies in PID control loop performance and helped to spur three decades of both automation investment and product innovation.
- Control loop performance monitoring solutions equip process manufacturers with hard evidence, and they are clarifying the current state of regulatory control.
- The manufacturing industry lags behind others in the use of data analytics at a time when the meaning of world-class manufacturing may be redefined.

Benefits of PID controller tuning



SOURCE: "Invest in Control – Payback in Profit", Energy Efficiency Best Practice Programme, United Kingdom Department of Trade and Industry, 2001.

The U.K.'s "Invest in Control – Payback in Profits" report published in 2001 offered a much-needed assessment of the impact that poor regulatory control had on production performance. The report cited lost opportunities that manufacturers could recapture through better use of existing automation capabilities. Included were opportunities to increase throughput by 2–5 percent and yield by 5–15 percent.

production yield, and 5–15 percent in excess energy consumption, among other operational consequences.

At the time of publication, Ender's findings were compelling, but they were also anecdotal in nature. They predated availability of the historians currently used to capture and catalog voluminous amounts of process data. Similarly, the software tools needed to systematically analyze large numbers of control loops did not exist in 1993. Although the British government's report provided a means for quantifying the value of process improvement, the findings were nonetheless presented as generalized ranges. They lacked the segment-specific breakdown and unambiguous financial values favored by both plant and corporate management. In spite of these shortcomings, considerable progress has been achieved over the past three decades, and there is now data to prove it.

Growth of CLPM and process analytics

The ability to assess PID controller performance on a plantwide scale first became a reality at the start of the new millennium. The first CLPM products were introduced by a cadre of small and large automation firms known for their expertise in process control and PID tuning. The subsequent rise of CLPM solutions as a unique product category mirrored manufacturing's rapid adoption of sensing, storage, and processing technologies. Within a modern production facility, data is now seen as an essential resource in day-to-day operations. Following the rise of data, CLPM solutions are an increasingly well-established tool in manufacturing's process diagnostic and optimization toolbox. There is steady year-over-year growth in end-user inquiries and licensed deployments. CLPM is enabling more and more manufacturers to realize greater returns on their investments in data.

CLPM solutions consume a production facility's readily available process data. The data is either streamed live from a centralized control system or extracted on demand from a historian. With access to a PID controller's vital signs—set point, controller output, and manipulated variable—even basic CLPM solutions can calculate key performance indices (KPIs) capable of proactively identifying negative trends. More sophisticated solutions include advanced forensic capabilities used to isolate root causes and to formulate recommendations for issue-specific corrective actions. Select CLPM solutions recommend controller tuning adjustments by automating the identification and modeling of data associated with everyday output changes. Some allow access to the calculated values that can then be synthesized with data for analysis using other business intelligence tools, such as Microsoft Power BI, Tableau Software, and Looker.

Objective versus subjective KPIs

A key distinction sets several KPIs apart from the majority that are commonly included in CLPM solutions. That distinction is a function of the objectivity of the insights. Objective KPIs such as uptime, percent time in normal, and stiction offer information that is indisputable. Their values are concrete, uniformly understood, and not subject to interpretation. As examples, a process is either running or it is not, just as a controller is either in its designated "normal" mode or it is not. These KPIs output values that are normalized and that enable comparison with other loops.

In contrast, controller performance metrics such as output travel and output reversals offer insights that are subjective. Values calculated by these metrics are not normalized. Although valuable, the output from these KPIs requires interpretation; additional context is needed. Consider a control loop that has an output travel calculated at 10 full range movements per hour. For a valve, that would equate to 10 fully open to fully closed cycles per hour. Just as a designation of "good control" varies from process to process and even engineer to engineer, it is nearly impossible to state unequivocally that 10 represents too much controller effort without additional consideration of the associated process.

Whereas the binary nature of objective KPIs makes them ideal for analysis and comparative purposes, there remains potential value in the output of most every CLPM metric. Viewed in the context of a single facility, all of the KPI-based information equips management with a clearer understanding of the facility's capacity for improving production output and efficiency. When viewed through a broader lens, however, the aggregated KPI results from facilities around the globe and representing all industry segments have the potential to bring additional insights. The increasingly widespread deployment of CLPM solutions is making that possible. A more comprehensive understanding of regulatory control is afoot, as is the basis for establishing industrywide standards. Potential by-products are the ability to define "good control" and a new perspective on what constitutes world-class manufacturing.

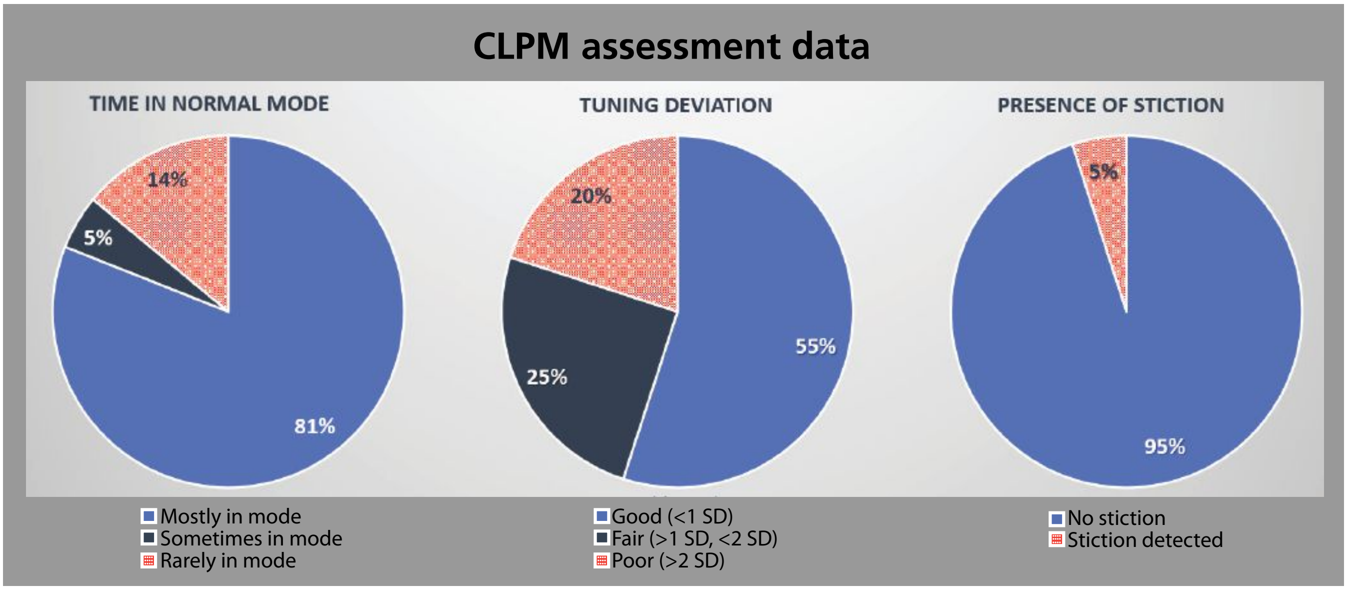
New technology, new findings

My company arrived late to market, first piloting its loop performance monitoring solution in 2009. Included in the company's evaluation initiative were numerous North American manufacturers representing the basic materials, chemicals, oil and gas, and power and utilities sectors of the process industries. Since then the system has been commercially licensed for use at production facilities in 25 countries, and it is used to actively monitor the performance of tens of thousands of PID control loops. Recently the company leveraged its community of customers to compile blinded data from a subset of those production facilities. It used the data from 116 different facilities to test the findings that were originally published nearly three decades ago and to launch an assessment of macro-level controller performance and process optimization trends.

Manual versus automatic mode

Ender's 1993 review of control loop performance noted that manufacturers operated a large share of their facility's PID controllers manually. Indeed, the report asserted that in excess of 30 percent of PID control loops were not operated in their designated or "normal" mode. At the time of publication this singular finding revealed to many manufacturers that they would not fully realize the return on investment from their investments in automation without additional changes. Findings culled from the CLPM assessment point to meaningful improvement in controller mode. Specifically, current data indicates that a significantly smaller 14 percent of controllers spend the majority of time operated in a non-normal mode, with another 5 percent occasionally operated in a non-normal mode.

It was well understood then as it is today that manual operation of control loops is undesirable. Statistica, a provider of aggregated data and market analysis, projects sizeable investments that target the further eradication of manual processes.



Control Station conducted a formal assessment using CLPM data collected from 116 production facilities. Compared to observations from 1993, results from the CLPM assessment suggest that process manufacturers have made significant improvements in PID control loop performance.

Specifically, Statistica forecasts global automation investments by process manufacturers that exceed $83 billion by 2021. What seems less appreciated than the financial resources being applied, however, is the underlying factors that continue to drive operator behavior. Operators tend to transition critical or dangerous loops from automatic to manual control when such loops function at or near a constraint. Similarly, significant changes to the rate of production without a corresponding adjustment in controller configuration routinely result in a shift away from the prescribed automatic mode. A common refrain from operators over the years is that they feel a greater sense of safety when they are in control.

The reduction in manual operation supported by the CLPM assessment is noteworthy, and it is not unreasonable to attribute the increased use of automatic control to general improvements in automation technologies. In particular, modern supervisory control platforms like distributed control systems are more robust than those from the ‘80s and ‘90s. Regulatory controllers are better too. They are more responsive than the programmable logic controllers from years past, which enables manufacturers to maintain tighter control. Similarly, today’s control room is often equipped with monitoring and diagnostic tools that bolster operator confidence by systematically alerting them to production issues and potential equipment failures. Investments by manufacturers are hitting the target.

Controller tuning

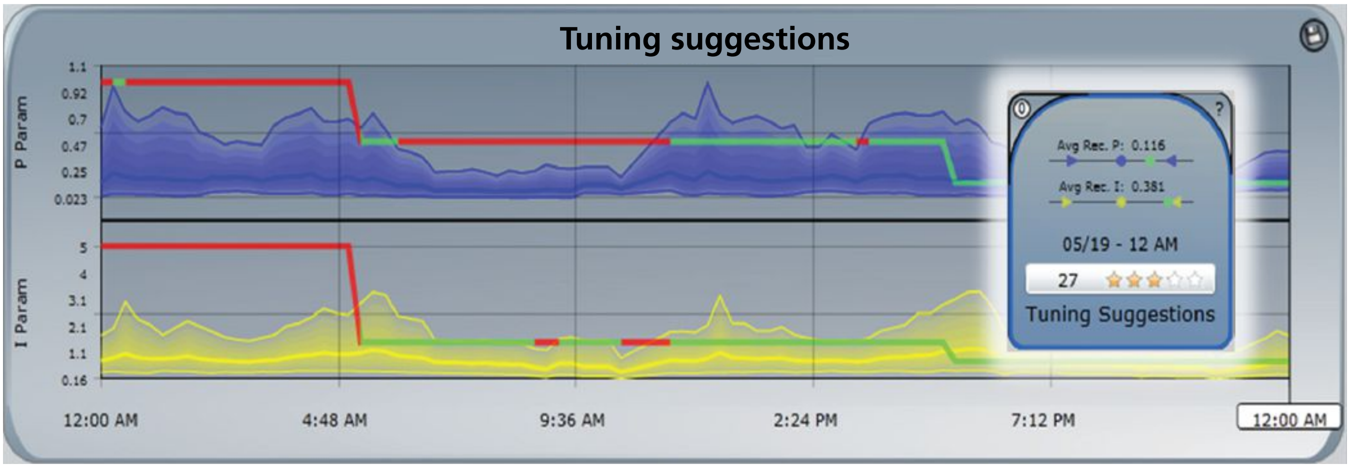
The improvement in controller mode mirrors gains that were also achieved in controller tuning. Whereas 65 percent of controllers in the ‘90s had apparently been found to be either poorly tuned or tuned in such a way as to mask other control-related issues, a greater share of today’s PIDs appear to be tuned appropriately. As a metric for analyzing the efficacy of a control loop’s existing tuning parameters, tuning deviation is an effective approach. By modeling a controller’s response to output changes, select CLPM solutions can determine a range of acceptable or recommended tuning values. The tuning deviation KPI quantifies the relationship between a controller’s existing tuning values and the recommended range based on a given controller’s objective. It is expressed in terms of standard deviations (SD). The CLPM assessment data found only 20 percent of controllers in need of tuning based on tuning deviation. Included in that calculation were controllers with a value in excess of 2 standard deviations of the recommended range. The data characterized an additional 25 percent of all PIDs as having “fair” controller tuning values based on SD values between 1 and 2.

To this day, the process of tuning PID controllers is commonly viewed as a “black art” even though controllers have been used commercially since first being introduced by Taylor Instrument Company in 1940. Most manual approaches involve subjective decision-making processes, and they produce results that can be wildly inconsistent. The current market for tuning software includes numerous products that are incapable of accurately modeling the noisy, oscillatory data that is typical of real-world applications.

Advances over the past few decades in PID tuning can be attributed to better education and to a few meaningful innovations. Among those innovations was the elimination of the steady-state requirement, which had forced practitioners to start and end each tuning session with data held at a steady state. Improvements in regulatory control strengthen a production facility’s foundation, and they enable manufacturers to realize the benefits promised by advanced supervisory and model-predictive solutions.

Valve stiction

As pivotal as Ender’s observations proved to be in terms of creating awareness and motivating action, they included only questionable input on the most common mechanical issues associated with poor PID controller performance. Data cited from a valve OEM was based on a statistically irrelevant set of 31 valves from a single system. Although hardly representative of the broader process



Select CLPM solutions use high-resolution data to automatically isolate process changes, model the associated dynamics, and calculate optimal PID tuning coefficients. The image from PlantESP’s TuneVue™ utility indicates when existing coefficients fail to satisfy the control objective (red) and how recommended coefficients would improve performance.

industries, the article shared that an excessive level of friction was present in 11 of the valves (35.5 percent). Static friction, or stiction, is widely cited as the leading mechanical issue faced by engineers. Stiction prevents a valve or other final control element from functioning properly. It generally results when a valve is packed too tightly such that the valve's stem cannot respond without the use of excessive force. Stiction is a problem that cannot be corrected with tuning. Analysis of CLPM data uncovered that only 5 percent of all loops exhibited an excessive amount of stiction (i.e., > 2 percent).

Stiction exhibits itself in the form of either saw-toothed or square-waved data when trended. Sharp changes in the value of a control loop's process variable correspond with the time at which the associated valve stem overcomes static friction in the valve. The stiction metrics available in most CLPM solutions evaluate changes in the process variable. More specifically, they take the size and frequency of changes into account as a means of determining the probability of stiction. Some CLPM solutions not only calculate the probability of stiction, they also quantify the amount of stiction that is present. Combined, the details of probability and amount are useful when prioritizing maintenance projects.

The initial CLPM assessment results are a starting point for understanding the state of regulatory control in the process industries. It shifts the discussion from a review of observations to a review of data-based evidence. If the original observations are to be believed, then the CLPM assessment points to significant progress.

Analytics and risk

Data analytics is used extensively by businesses to examine financial operations and to seek new opportunities for market growth. In its report published in January 2018, the global consulting and advisory services firm McKinsey & Company depicted the effect that analytics has had on business practices. The report cited the functions of sales and marketing and research and development across all industries as being fundamentally changed as a result of analytics. However, McKinsey's analysis showed the function of manufacturing as experiencing moderate to no change. With the exception of the basic materials and energy sectors, the process industries were found to be lagging in their use of data as a means of advancement.

The process industries lack objective guidelines for evaluating regulatory control performance.

Clearly, manufacturers utilize data analytics, and some use it extensively. A challenge facing many manufacturers is that not all data from the production floor is readily available for more intensive assessment. The separation of business and process networks is a well-known barrier to access. In a form of jest, corporate and plant engineers routinely refer to this separation of networks as the "DMZ." The result is that data scientists and others are unable to tap into the full extent of their company's available data resources. Though reasons for the separation are valid, such security measures have long been a hinderance to analytical initiatives.

Now over two years ago, the authors of the McKinsey report noted that manufacturing was in the midst of the most significant disruption in decades. Citing the Industrial Internet of Things, they wrote: "Competition is intensifying not just within industries but also between them." In a way the report offered a warning. Those who ignore the importance of data analytics and who fail to understand their relative position in the market will be at risk.

A case for disruption

Consistent with the views of McKinsey and other leading advisory firms, a fundamental benefit of CLPM data is the establishment of clear performance benchmarks. The process industries currently lack objective guidelines for evaluating regulatory control performance. And while guidelines for the manufacturing industry would provide an ideal starting point, there would be similar benefit to segmenting CLPM data and to instituting segment-specific benchmarks.

As with analytics, there is a wide berth between those industry sectors that rely heavily on automation and those that utilize little of it. Sectors such as oil and gas are known for their investment in automation technologies. The refinement of oil is such that incremental improvements in throughput and efficiency can result in outsized financial gains.

Although the value of benchmarking control loop performance is speculative, the role PID controllers play in regulating production is undeniably significant. It is conceivable that CLPM benchmarking could be used in highly impactful ways. It could shape decisions for responding to an ever-changing competitive landscape and for justifying the funding of additional automation investments. As manufacturers advance toward more optimal control, their expectations could certainly be expected to change. Similarly, CLPM benchmarks could guide decisions for transitioning from regulatory to supervisory control or from supervisory to more advanced, multivariable solutions.

A deeper understanding of controller performance truly has the potential to be disruptive. To that end Ender's original observations deserve credit for highlighting a combination of dysfunction and opportunity that seem obvious today. As in 1993 but now equipped with aggregated performance data, the question remains: How will we use this information? ■

ABOUT THE AUTHOR

Dennis Nash (dennis.nash@controlstation.com) is president of Control Station, Inc. Since joining in 2004, Nash has led the company's transformation from a vendor of educational tools to a global supplier of award-winning process analytics and optimization technologies. Nash received his undergraduate degree from the University of Notre Dame and his MBA from University of Connecticut.

View the online version at www.isa.org/intech/20200602.

Overcoming challenges to digital transformation

Modern technologies, properly applied, are helping organizations move ahead

By Travis Cox

Although there are certainly challenges to improving the Industrial Internet of Things (IIoT) and creating real digital transformation, today there are solid tools that can really help us. And some of this work is becoming easier than ever. For example, web browsers and cell phones are very easy to use—and both are enabling valuable projects in human-machine interface (HMI) and supervisory control and data acquisition (SCADA). Meanwhile, available development resources are making it faster and easier to build the solutions we need. And interoperability is on the rise. Overall, there are exciting opportunities for all of us.

We have already seen modern technologies helping factories go paperless—doing away with manual data entry, clipboards, whiteboards, and spreadsheets. Numerous industrial processes have been automated: recipes, reports, alarming, data collection, packaging, security management, and more. Entire enterprises now have the ability to access, visualize, and analyze data like never before—allowing them to make better decisions and stay competitive.

If you are not there yet, how do you get there? First, consider five key challenges that make digital transformation hard to achieve:

- difficulty collecting data at the edge of the network
- issues with turning data into real action
- the long, hard process of project development/deployment
- costs for solutions that scale
- complexities of working with big data in the cloud.

Meeting the challenges

What do we need to meet these challenges? A new architecture, one that starts with operations technology (OT) on the plant floor. Platforms upon which to easily build the ideal solutions. Modern, interoperable technologies. Edge computing and Message Queuing Telemetry Transport (MQTT). The new SCADA capabilities with tablets and phones. Hardware that comes with SCADA software embedded. New tools in the cloud. Unlimited licensing. And taking HMI and SCADA beyond their traditional roles. All these

together—or even some of them—can show us data we have never had before, and give us new ways to analyze that data.

Fortunately, it is easier than ever to remove technological and economic obstacles. There are plenty of examples of organizations doing just that while building their dream IIoT projects. Let's start with a new architecture—what it is and why we need it. Organizations see the promise of digital transformation: the ability to get their operational data into cloud information technology (IT) applications and do all kinds of analysis, business intelligence, and machine learning. But most organizations are trying to drive digital transformation from the top down. If you approach it in a way that does not work for the operator on the plant floor, it will not succeed. Digital transformation really must be implemented from the bottom up, with OT on board first.

You have to create a migration strategy that implements digital transformation but also meets all the OT requirements. It boils down to a single, crucial concept: an architecture change. We need to stop connecting devices to applications with protocols. Instead, we need to connect devices to infrastructure. By decoupling devices from applications, we get more access to data. At the same time, we must provide a superior OT solution that meets the needs of operators—a solution that is plug and play, reliable, and scalable. Organizations can start small with an OT-infrastructure plan that is inherently scalable. They need to learn more about the underlying complexities with OT, solve OT first, and then move to IT.

FAST FORWARD

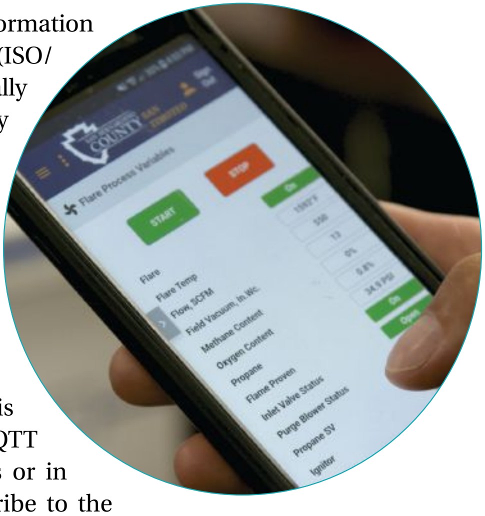
- Digitalization starts with a new operations technology on the plant floor that seamlessly integrates with IT and enterprise.
- It is easier than ever to remove technological and economic obstacles to digitalization and implement IIoT technology to openly and seamlessly share data throughout the enterprise.
- We need to stop connecting devices to applications with protocols and connect devices to infrastructure.

Leveraging the benefits of MQTT

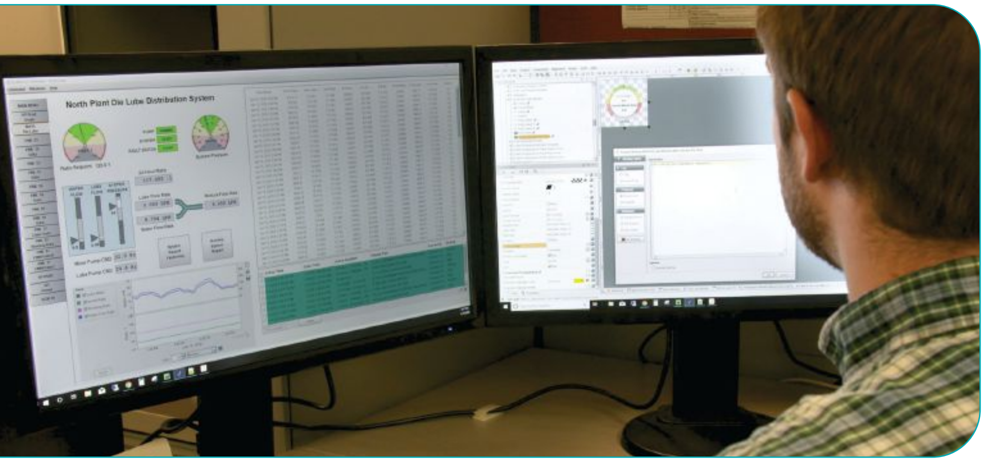
This new OT architecture uses MQTT, a lightweight publish/subscribe protocol that enables message-oriented middleware architectures. MQTT is an open OASIS (Organization for the Advancement of Structured Information Standards) and ISO standard (ISO/IEC 20922). The protocol usually runs over TCP/IP; however, any network protocol that provides ordered, lossless, bidirectional connections can support MQTT. It is meant for connections to remote locations that require a small code footprint or where the network bandwidth is limited.

With MQTT, device data is published by exception to a MQTT server, either on the premises or in the cloud. Applications subscribe to the MQTT server to get data; there is no need for applications to connect to the end devices themselves. MQTT has become the leading messaging protocol for IIoT, because it has several benefits:

- open standard/interoperable



Some SCADA systems can leverage mobile devices in new and powerful ways.



Edge computing and MQTT provide more data at a faster rate.

- decouples devices from applications
- reports by exception
- requires little bandwidth
- TLS (Transport Layer Security)
- remote-originated connection (outbound only, no inbound firewall rules)
- stateful awareness
- single source of truth with context (name, engineering units, low, high, etc.)
- auto-discovery of tags
- data buffering (store and forward)
- plug-and-play functionality.

As an organization acquires new sensors or upgrades equipment that supports MQTT, the SCADA system immediately gets access to that data without having to know about the end device. With this new architecture, data is openly shared throughout the enterprise.

To get to a new architecture, we also need edge computing and platforms for HMI, SCADA, and MESs. A platform is an environment or ecosystem that provides a foundation for creative problem solving. It enables innovation and allows a community of players to contribute—thus creating additional value around the platform. Platforms typically have:

- open access and interfaces
- cross-platform compatibility
- connectivity both in and out
- modular architecture (easy to build on and extend)
- scalability (easy to add more tags, devices, and clients to meet demands)
- extensibility (through software development kit, application programming interface).

No one system can provide everything. A good platform is so important, because it lets you build exactly what you need, when you need it. It is a foundation to solve immediate needs while also allowing for expansion and scalability with ease and affordability. Information technology has been using platforms for many years. Now it is time for the operational world to get on board with platforms.

Unlimited licensing is another key element. You cannot build your ideal SCADA systems if you have to pay more fees every time you expand. With unlimited licensing, a SCADA system is sold by the server, so you get an unlimited number of clients, tags, and connections for the cost of one license. This gives you the opportunity to create more projects with the scalability you need. It also allows you to put data in front of as many users as you want—operators, managers, IT people, your CEO, and even your customers.

Improved edge capabilities

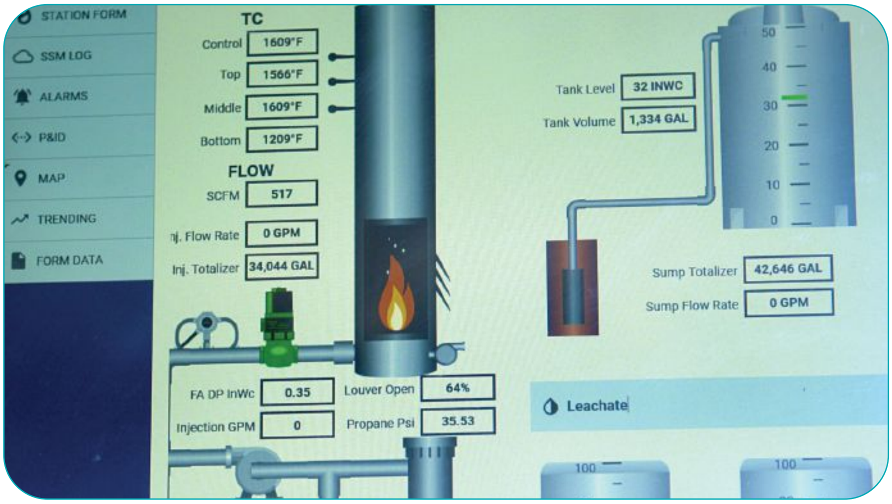
Capturing, processing, and visualizing critical data at the edge can be difficult and expensive. But with the right tools, organizations can extend data collection, visualization, and system management all the way to the edge of the network. Local HMIs on the edge have control, alarm notification, trending, and other tools. Software can give edge devices the ability to do more without needing to depend on the central server. Web services and powerful intelligence, such as analytics and machine learning, can be provided with edge-of-network devices. Field devices can be turned into lightweight edge gateways that publish data to an MQTT broker. There is more power and speed at the edge than ever before. Along with that, the edge can be managed centrally, including diagnostics, automatic backup and recovery, central licensing, and project and tag synchronization.

HMI and SCADA systems are becoming more powerful too. Organizations today want more access to industrial data; they want to integrate more systems; and they want solutions that solve real business challenges. Modern SCADA systems can help by leveraging the best of controls and IT technology. We are now seeing companies embrace modern industrial application platforms and technology, creating innovative industrial systems in all industries. New ways of utilizing SCADA include:

- combining data from, and integrating with, disparate systems
- running advanced logic engines and calculations
- getting data to more people
- leveraging the power within mobile devices.

SCADA has done an excellent job of communicating to programmable logic controllers (PLCs) and field devices. Traditional SCADA systems often have limitations on the brands of PLCs they can communicate with. It is important to be able to pull data from multiple disparate PLCs into a single platform for a "single pane of glass" for operators. Using modern standards, such as OPC UA, SCADA systems can seamlessly connect to these devices and other data sources, such as computerized maintenance management systems, enterprise resource planning (ERP), and MES. There is enormous benefit in connecting these systems together and adding more context to the operator's screen.

Also, people are running complex calculations with their SCADA systems. Or they are connecting ERP or other business systems with SCADA, so customers can communicate directly to the plant floor—increasing the quality, speed, and efficiency of the supply chain. Engineers are putting three-dimensional images and virtual reality into SCADA, providing a more complete picture. The list goes on and on, and we are seeing creative, new uses of these technologies all the time.



Control 1609°F
Top 1566°F
Middle 1609°F
Bottom 1209°F
SCFM 517
Inj. Flow Rate 0 GPM
Inj. Totalizer 34,044 GAL
Tank Level 32 INWC
Tank Volume 1,334 GAL
Sump Totalizer 42,646 GAL
Sump Flow Rate 0 GPM
FA DP InWc 0.35
Injection GPM 0
Louver Open 64%
Propane Psi 35.53

A new architecture should take a bottom-up approach, starting with operations on the plant floor.

More power in mobility

Data leads to prompt action more than ever now, with the increased use of smartphones and tablets. People can see data, make decisions, and control operations from a downtown sidewalk or anywhere else they happen to be. Smartphones and tablets are incredible pieces of technology. They have an amazing number of built-in sensors, such as GPS, camera, accelerometer, and Bluetooth.

Mobile applications for smartphones and tablets are entering the industrial space at an increasing rate—changing the way we acquire, view, store, analyze, and act on data and information. Pure-web HTML industrial applications are being built for any device. They can be mobile-responsive, automatically fitting screens of all sizes. Mobile-first applications are being built in native HTML5 and CSS (Cascading Style Sheets). They can run on any device with a web browser. With today's tools, you can create smart industrial applications using a mobile device's many sensors and other capabilities.

Another improvement in reducing development times is the use of free, community-built resources. Existing styles, views, templates, and more can be dropped into your project, saving time. Leveraging the work of others helps you get to the deployment phase more quickly.

Embedded software also helps save time. More and more device manufacturers are embedding SCADA software in their products. You can buy a device with the software you need already installed, configured, and licensed. It saves organizations time and money, and it provides the best hardware and software together. It is much easier for users to deploy, because the vendor has done most of the work for them. Many of the devices are IIoT-ready, with MQTT. As with other approaches mentioned above, this gets you closer to true digital transformation as efficiently as possible.

Get into the cloud

Today it is easier to leverage data with cloud platforms, machine learning, analytics, and artificial intelligence. New tools are using MQTT to get SCADA data directly into cloud infrastructures. Once it is there, the cloud offers many opportunities. It provides numerous databases, deep storage, and data lakes that make it easy and affordable to store all your data. The cloud provides instant availability, reliability, and scalability without the hassles of maintenance or local infrastructure.

Once the data is in a cloud platform, you can use tools to turn that data into information, slicing and dicing the data in various analytic tools. You can overlay data from multiple sites into a single dashboard. You can use machine learning algorithms and tools to tune processes, predict machine failures, do forecasting, and more. The many options with cloud computing can be a huge help in your journey toward digital transformation.

With all the modern technologies and methods available, development and deployment can be faster than ever. There will always be challenges, but we are now more prepared to meet them head on. With a "digital-first" mindset, we can think beyond the traditional SCADA systems, and focus harder on getting more data to more people throughout the enterprise. ■

ABOUT THE AUTHOR

Travis Cox is co-director of sales engineering at Inductive Automation. He has been with the company for 16 years, and has overseen numerous successful launches. Send questions or comments to jmeyers@inductiveautomation.com.

View the online version at www.isa.org/intech/20200605.

More data from the plant floor is helping managers make better decisions.

Business transformation through digitalization

FAST FORWARD

- Digitalization, Industry 4.0, and digital transformation are different concepts that can help companies strategically plan to upgrade their operations.
- Technology, culture (organizational and geographic), and processes are three important pillars of any digital transformation strategy.
- Massive industrial and corporate automation and data analytics can create new monetization possibilities, allowing companies to grow.

Technology, culture, and processes are all essential to success

By Victor Venâncio

Oil and gas businesses around the globe are undergoing a broad range of transformations these days, pushed by nations needing to meet the United Nations' 2030 Agenda for Sustainable Development, by the availability of new digital technologies, by the use of renewable energy, and by changes in consumer behaviors. Energy industry drivers of change known as the "four Ds"—digitalization, decentralization, democratization, and decarbonization—are boosting the adoption of new technologies and challenging the business models that the industry has been built upon. We are also globally experiencing a moment of major change accelerated by the effects of the COVID-19 pandemic, with transformation equally impacting organizations and individuals.

The digital transformation journey of any business is a period of organizational turbulence even in the best of global conditions. It is a time of information technology (IT) and operational technology (OT) convergence. It is when professionals with different skills should align their efforts toward overcoming challenges and delivering the elements of value that are important for clients and other stakeholders. The idea is understood differently depending on the department or a professional's background but, for industrial companies, transformation encompasses three pillars: technology, organizational and geographical culture, and processes.

These three pillars are always immersed in a huge amount of structured or unstructured data, originating from several sources internal and external to the company. That data is the "digital" portion of the transformation journey. And the purpose of the journey is to answer a series of questions.

Are organizations prepared to ensure the sustainability of their businesses with the agility and responsiveness required at this moment? Are they prepared to move fast enough to build a solid bridge between strategy and execution? Can they link the company's vision to the values that they will actually deliver to their clients?

Can leadership's primary focus change from return on investment (ROI) to customer value, or from operational costs and efficiency to agility and adaptability? What percentage of budget is allocated to business as usual (BAU) activities, and what percentage is actually allocated to initiatives that will leverage digital transformation strategies?

Some paradigms of traditional management must shift so that transformation can actually occur. And this is no easy task. This article discusses how the three pillars of digital transformation correlate with each other and highlights issues that organizations must be careful about. Examples are specific to the oil and gas (O&G) industry, but the discussion applies to many other market segments as well.

The technology pillar

Digitalization is a construct different from digital transformation, which in turn is different from what is known as Industry 4.0. Several sources mix up these terms and cause a fair amount of confusion among readers less acquainted with automation or digital technology roots.

Digitalization has been happening for some years and consists of converting analog signals generated by sensors into digital signals. It is also activities that used to be carried out manually in spreadsheets that are now carried out using computers. Basically, the same processes that existed before have become digital—and that is it.

Digitalization is one of the characteristics of Industry 3.0, and most companies are still in this era. Digitalization activities are growing exponentially because of lower sensor prices, easy cloud storage of data, the evolution of the electronics required to process the data, and the new and powerful hardware and software tools available.

Automation, whether industrial or corporate, is a crucial part of the strategies applied for digital transformation and the adoption of Industry 4.0 tools.

Digital transformation, on the other hand, fundamentally changes business models and activities, often with the use of Industry 4.0 technologies. Digital transformation challenges the cultural paradigms of organizations and promotes the use of cocreation networks (open innovation) as a way to leverage their sources of monetization or value creation. It develops new opportunities for companies and their employees, and also creates innovative products or services for society. Digital transformation occurs when its three pillars are being worked on simultaneously, following a well-defined corporate strategy.

Industry 4.0 is about adopting emerging technologies that, together or in isolation, offer better operational, business, or security performance to organizations. Among these technologies, the following stand out: robotic process automation (RPA), machine learning (ML), artificial intelligence (AI), cognitive intelligence, big data and analytics, system integration (OT and IT convergence), digital twin (simulations), 3D printing, Internet of Things and Industrial Internet of Things (IoT/IIoT), and cloud computing (enterprise resource planning [ERP], cloud), all supported by solid cybersecurity (OT and IT) governance.*

Automation, whether industrial or corporate, is a crucial part of the strategies applied for digital transformation and the adoption of Industry 4.0 tools. Massive automation is, in fact, the first step of the digital transformation journey.

Automating all repetitive processes has become almost mandatory for organizations, whether they are oil producers, freighters or drilling rigs, floating production storage and offloading (FPSO), or suppliers of equipment and services. The strategic use of data will offer new monetization possibilities, and therefore will allow companies to grow in an increasingly more competitive environment where new entrants from segments that have not operated in the energy industry before will challenge incumbents.

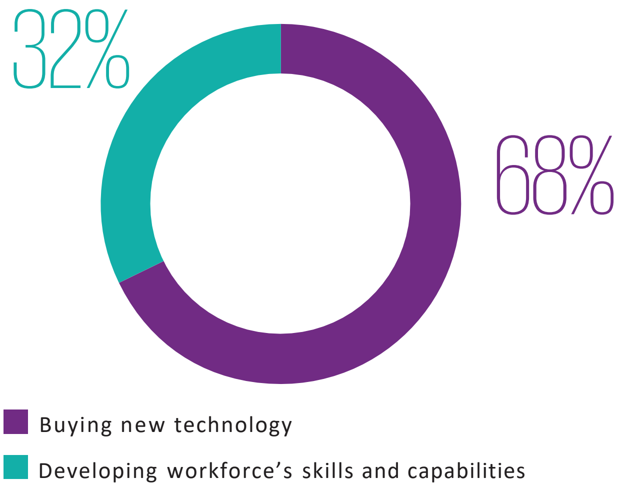
Brazil: A case study

Even with so many Industry 4.0 technologies available, Brazil's O&G industry still mostly belongs to the Industry 3.0 era. Initiatives to adopt Industry 4.0 tools are rare, and it is even more difficult to find companies that are doing digital transformation.

A few companies have launched initiatives to implement a digital transformation strategy, working on the three pillars simultaneously. But many times, companies adopt emerging technologies and plan to check later what type of value they can derive from them. This is the first mistake of organizations that focus only on the technology pillar of digital transformation. So how can companies make gains from the use of Industry 4.0 technologies and promote digital transformation?

The first step is to formulate a digital transformation strategy by relying on the collaboration of business and technology experts who have multidisciplinary knowledge about the industry. The choice of emerging technologies that will add value to the company should be based on corporate, business, and functional strategies. Support services to both internal and external clients should be implemented after processes (1) are well-defined and validated, (2) are aligned

Investing in new technology vs. workforce upskilling



Survey results show a potential imbalance between two important pillars of digital transformation: Companies have been found to invest more in new technologies than in training for employees.

Source: 2019 Global CEO Outlook, KPMG International

with the organizational culture and the mindset of company teams, and (3) comply with corporate governance, risk, and compliance rules.

An effective digital transformation strategy goes far beyond technology adoption and requires a multiskilled group dedicated to checking interactions and potential synergies between several departments. With such a comprehensive view, we will find the value created by adopting those technologies. In other words, a well-designed digital transformation strategy goes beyond which technology to adopt.

All company departments should be aligned around a corporate mindset that may help people to participate in the cocreation of the strategy and perform a real digital transformation. However, challenges to this alignment are posed by merging different departments, personal interests, desires, egos, cultural dimensions, and goals that are too often ruled by key performance indicators that clash with the common good.

Essential OT/IT convergence

The first step for a company starting its digital transformation journey—relying on a formulated strategy duly shared with everyone—is the adoption of OT and IT convergence. Industrial assets, through the automation systems already in place, are a major source of data. Industrial automation systems (sensors, programmable logic controllers, distributed control systems, supervisory control and data acquisition) process a huge amount of data that is restricted to these "factory floor" systems. This comprises what we know as OT.

Data from different corporate departments, such as finance, procurement, human resources, and tax, are concentrated in and confined to the ERP system, which generates reports and dashboards for department and C-level executives. In several organizations, data from the industrial area is still coming from Microsoft Excel spreadsheets fed manually into the ERP.

In both cases, the equipment already exists in companies, and data is processed separately in its corresponding OT and IT silos. In most cases, companies do not make strategic use of the data to create value for the organization and its clients. Value comes from more reliable information for C-level executives to use for decision making, and also from a better internal client (employee) or external client (customer) experience. OT/IT convergence means contextualizing and combining data in a data lake, so highly skilled professionals and data scientists, supported by experts in industry business, can create that value. This total integration creates a sustainable competitive advantage.

OT/IT convergence is the first step in joining the Industry 4.0 era and starting the journey for a true digital transformation. Up to this point, the transformation initiative does not require major hardware and software investments. It is about using existing assets in a strategic manner with higher medium- and long-term goals that include fast and significant gains at the very start of implementation. This provides financial support for setting up the other pillars of digital transformation.

To the extent that additional data is necessary in alignment with corporate strategy, the next step is the implementation of other emerging technologies used in an Industry 4.0 environment. The strategic goals of companies for how to carry out digital transformation will determine whether the implementation of these technologies makes sense.

The cultural pillar

Management literature says that culture is the set of values and beliefs shared among the members of an organization. However, this construct is discussed differently by anthropologists and sociologists, showing the complexity of the topic. Global companies should pay attention to organizational culture and also the culture of individual countries or geographic regions.

The quantity, scale, and price of the products produced by a company no longer guarantee its survival. The aggregate intangibles, or elements of value perceived by clients, have become of utmost importance for success. This ability to deliver elements of value depends on the speed and adaptability that companies manage to introduce in their decision-making processes. And that is a function of culture.

Flexibility, adaptability, agility—all are characteristics that organizations should develop in their cultures to create competitive advantages in this moment of transition. Organizational and country culture should be aligned with the digital transformation strategy, so that any strategy for adopting emerging technologies is actually used to create value for the organization. That is not always the case.

The results of KPMG's 2019 CEO Outlook Survey show a potential imbalance between these two important pillars of digital transformation. Companies have been found to invest more in new technologies than in training for their employees: 68 percent report investing in buying new technology, but only 32 percent say they are investing in developing their workforce's skills and capabilities.

Repetitive work performed by people is likely to be fully automated. Therefore, unskilled professionals may become jobless, causing a range of social problems. Although several jobs may be terminated, more skilled professionals will have new opportunities. However, the professional who carries out repetitive tasks usually is not the same professional who is prepared to seize the new opportunities—unless companies invest in upskilling.

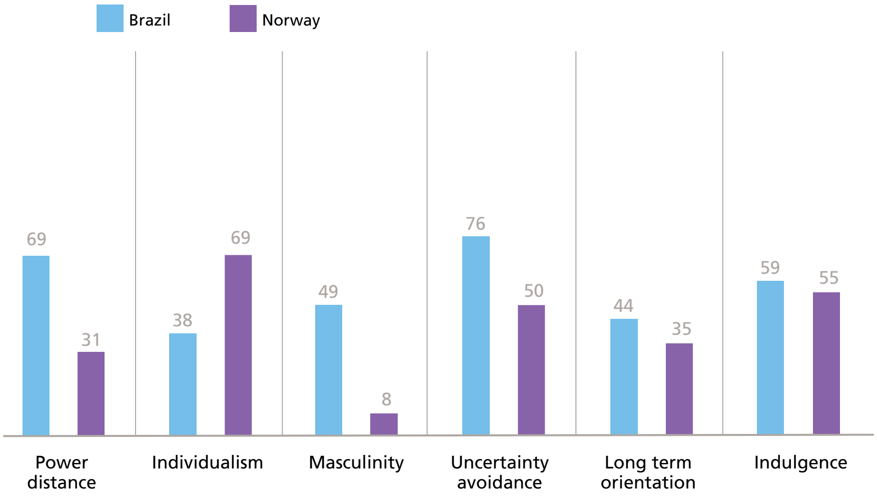
Because digital transformation will affect not only the organization but also the environment and the society where the company operates, many companies focus on environmental and social governance (ESG) strategies. However, the organizational culture, mindset, and training issues will have to be addressed, so that adopting emerging Industry 4.0 technologies and new processes has the effectiveness expected by executives.

Addressing cultural dimensions that affect the relationships between employees of a broad range of departments and hierarchical levels and incorporating these new technologies into the company's daily routines are key factors in ensuring the success of a digital transformation strategy. Human beings have a natural fear of the unknown. Many times, out of self-protection, they are against the adoption of an emerging technology, impairing the company's strategy.

Using Brazil as an example once again, a high power distance gap and low trust levels are part of its cultural dimensions, making it very different culturally from other countries, such as Norway. A Norwegian company that is trying to replicate the headquarters' digital transformation strategy in its Brazilian operations may have serious implementation problems if it does not address cultural and mindset issues properly. The cultural pillar may have a determinant impact on the digital transformation strategy as a whole.

In other words, no matter how easy the adoption of new technologies is, culture may slow or impair a successful implementation of a digital transformation strategy. Hence the need for a more comprehensive and broad view of what is beyond technology in digital transformation processes.

Comparison between the cultural dimensions of Brazil and those of Norway



Source: https://www.hofstede-insights.com/product/compare-countries

Oil and gas companies started to have a strong market presence at the end of the 19th century and have expanded their activities by acquiring tangible assets and fostering a robust operational performance culture. A digital transformation process requires a view of the company's intangible assets, which several industry professionals are not yet used to delivering. Without a constant effort to adapt organizational culture to the new era we are experiencing, with massive automation and digitalization, the whole digital transformation process will certainly be useless.

The processes pillar

Processes are another important pillar of a digital transformation strategy. If they are not well analyzed, defined, validated, and tested, emerging technologies will run inefficient processes in a more accurate and fast manner. That will be even worse for organizations, destroying value and generating financial losses. Both in the industrial and corporate areas, processes are crucial for the organization to positively perceive the results obtained from OT/IT convergence.

Lean Manufacturing methodologies support operational efficiency and allow constant improvements in production routines to eliminate or mitigate losses and waste reported in production processes. These methodologies are used in several industrial segments still today, even in the O&G industry. Well-structured processes both in the industrial and corporate areas help organizations to be more efficient and more competitive.

Working on the pillar of processes simultaneously with the pillars of culture (organizational and country) and technology will help the company implement

SMART MANUFACTURING AND IIOT

Article author Victor Venancio is the chair of ISA's newest technical division, Smart Manufacturing and IIoT (SMIIoT). ISA membership (www.isa.org/membership/join-isa) conveys a number of personal and professional benefits, including the opportunity to connect with other members through technical divisions. SMIIoT (www.isa.org/iiot-and-smart-manufacturing-division) focuses on the Industrial Internet of Things, cyber-physical systems, digital twins, advanced robotics and AGVs, cloud computing, additive manufacturing, artificial intelligence and machine learning, virtual and augmented reality systems, and much more.

the new tools. It will also send a message to employees that the company is working to facilitate their daily activities to allow them more time to understand the new technologies, acquire new skills, and have more free time for creativity to boost the company's businesses through entrepreneurial activities.

In conclusion, whatever your line of business within the O&G value chain, it will be affected by digital transformation. The company that does not have a clear digital transformation strategy and does not simultaneously address these three pillars is putting its own survival at risk.

New entrants using disruptive technologies or new business models are already having an impact on business in the O&G industry, and every company should be aware of the risks of not keeping abreast of the most recent developments. As a country, Brazil and several other nations have to be more agile in this shift from Industry 3.0 to Industry 4.0.

This situation is not different in the O&G industry specifically. Some governments have excellent initiatives to encourage the adoption of new Industry 4.0 technologies. This is good, but it is up to organizations to formulate their own strategies to act on the three pillars simultaneously in an orchestrated manner. If possible, organizations should use external knowledge sources in a collaborative manner by tapping the key skills of expert business and technology companies, startups, universities, and other institutions to help them undertake this journey. ■

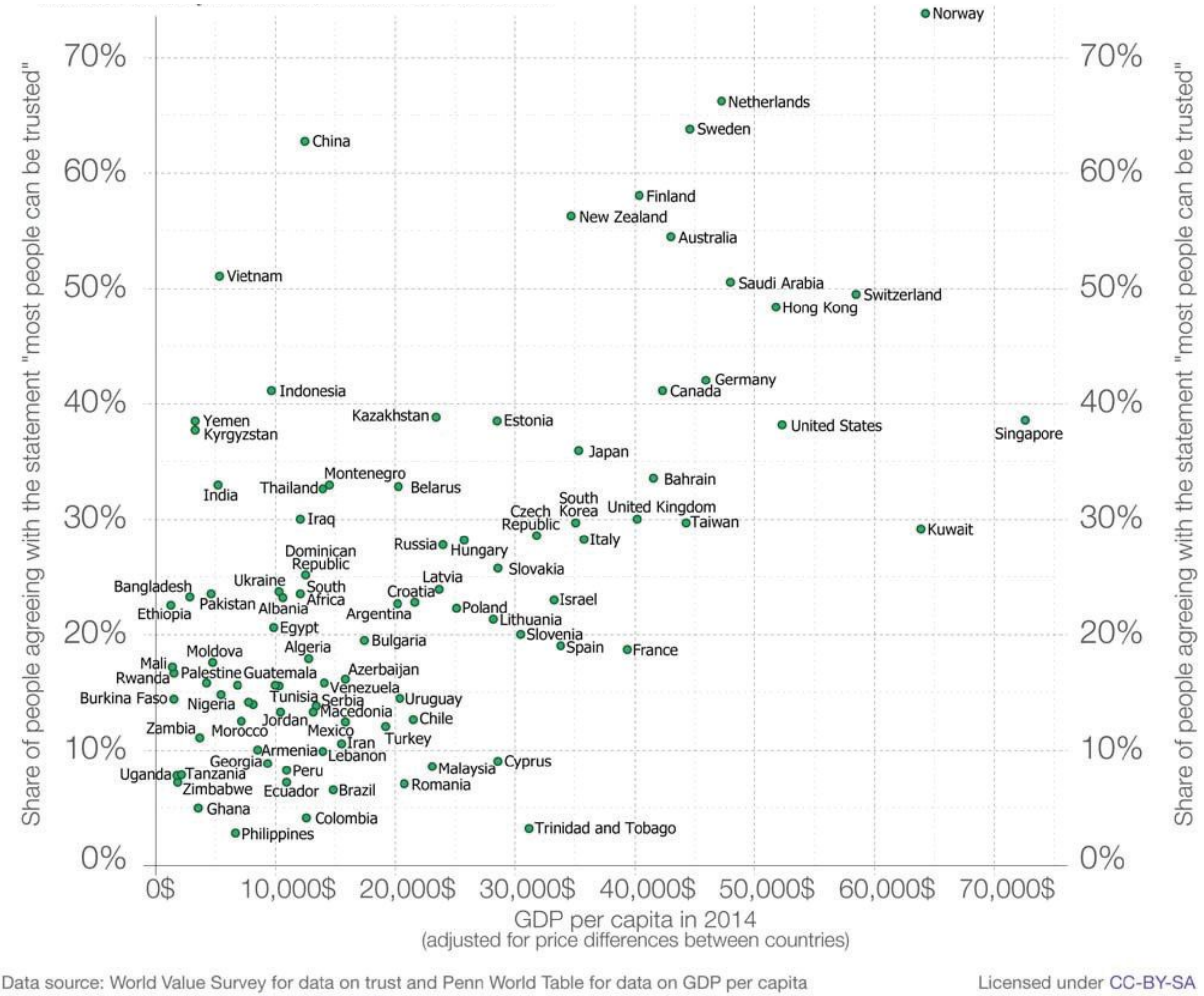
ABOUT THE AUTHOR

Victor Venâncio (victorvenancio@kpmg.com.br) is partner director for automation, Industry 4.0 & digital transformation for the Energy and Natural Resources group within KPMG Brazil. He has more than 25 years of experience in automation, instrumentation, and business for the oil and gas and energy industry. He is also ISA chair of ISA's newest technical division, Smart Manufacturing and IIOT, and strategic partnerships director for the ISA Rio de Janeiro chapter (Brazil). See his LinkedIn profile (www.linkedin.com/in/victorvenanciodias) for additional details.

View the online version at www.isa.org/intech/20200606.

Country by country: Trust vs. GDP per capita

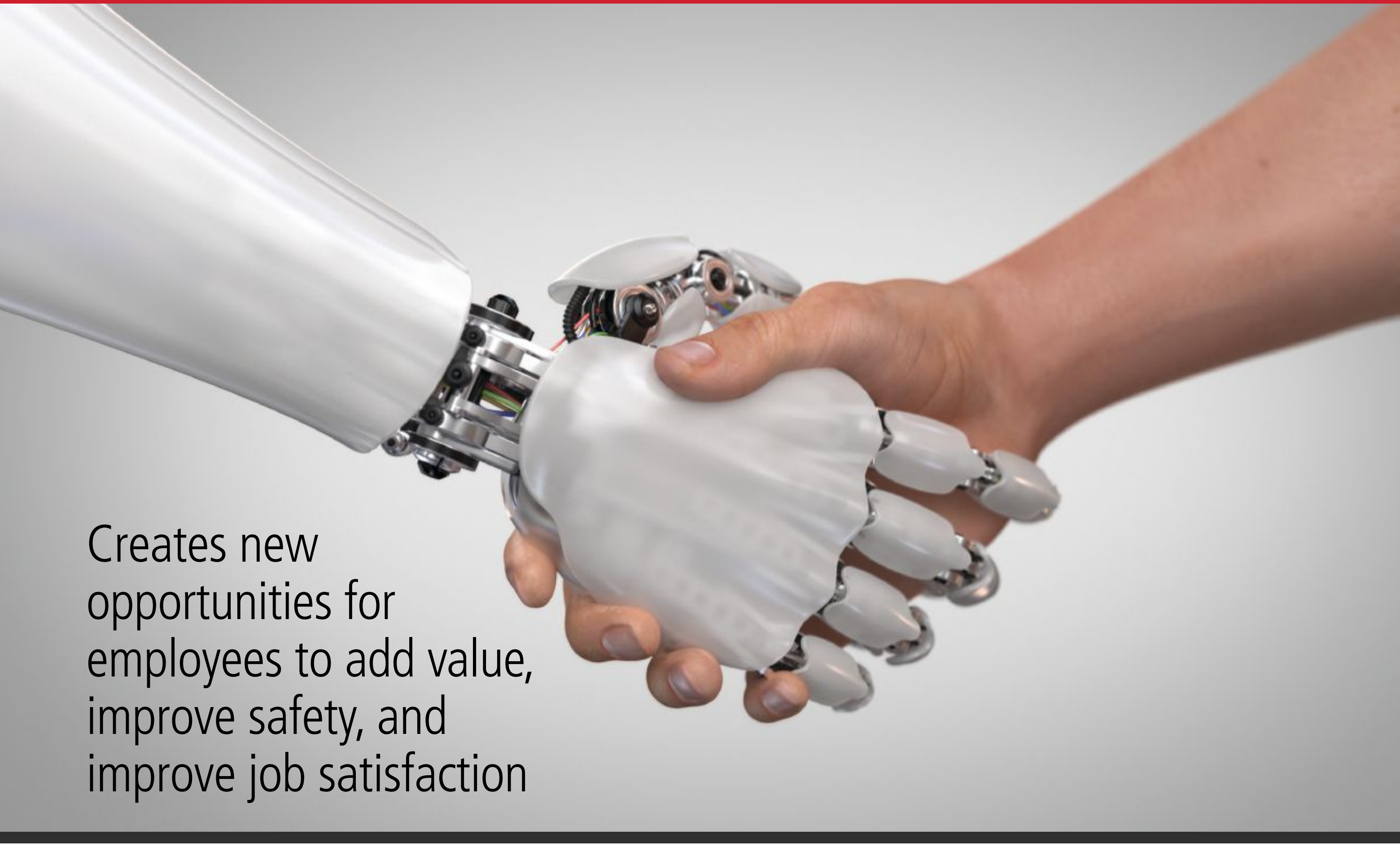
Shown is the share of people agreeing with the statement "most people can be trusted."
For each country the latest available data is shown.



Data source: World Value Survey for data on trust and Penn World Table for data on GDP per capita
This visualization is available at OurWorldinData.org. There you find the raw data and more visualizations on this topic.

Licensed under CC-BY-SA
by the author Max Roser.

Collaborative robots save production costs



Creates new opportunities for employees to add value, improve safety, and improve job satisfaction

By Joe Campbell

Jim Lee, Tool Gauge general manager, faces the stark realities of doing business in a global market. Even though the company is close to many of its customers in the Pacific Northwest, their customers can do business anywhere in the world, including in much lower-cost labor markets. It became clear to the company that the way to compete in a global market is more automation to improve efficiency and quality and to add more value. The company's fixed-price contracts can extend for five to seven years, without the ability to renegotiate even if labor costs increase. Tool Gauge needed to build in efficiencies and found cobots were the perfect solution.

In the past, Tool Gauge has been a bit trepidatious about using automation, because there is a huge capital investment for robots, so the challenge was to find solutions that required lower capital investment and improved return on investment (ROI). Additionally, the company was concerned about the cost and complexity of implementing traditional robots that require walling off portions of their manufacturing to put in automation cells with elaborate safety interlock systems.

The best use case

After learning about and analyzing new options, Tool Gauge installed two collaborative robots—or "cobots"—from Universal Robots to address repetitive, high-labor applications in both its metal and plastic parts departments. On the metal side, an easily damaged copper machined part was being produced and being fully attended by a highly skilled journeyman CNC machinist simply to pull parts off the CNC chute, and clean, rinse, dry, and box them. In the new configuration, the parts pass a proximity sensor that sends a signal to a cobot to pick them up. The cobot places parts in a rinse bath, then holds them up in front of a dryer and drops them into individual cardboard cells when dry. This frees up a highly skilled journeyman CNC machinist to do higher value-added work.

Tool Gauge used the palletizing wizard built into the system to configure the cobot to drop each part into an open cell in the box in a grid pattern without complex programming. Additionally, when it put the robot in place, there was a labor savings of $9,000 on the very first order.

Cobot doubles production while reducing labor by 75 percent

In the injection molding department, a cobot is used for an intricate plastic extrusion assembly, picking up end caps for a plastic panel, and moving them through a glue dispenser. After correctly dispensing the glue in the end cap, the robot places the part in an actuator on a table where the part is clamped. An operator then takes over, inspects the glue, and removes the part. This task previously required four operators to produce about 200 units per day. Now, the automated application requires one operator working with the cobot to produce four hundred units per day.

General manager Lee adds, "What I thought would be one of the most difficult assembly operations—using a robot to apply glue on a very complex surface—works very, very well." Beyond the labor savings, Lee also emphasizes the quality and consistency of the robotic bond, and the fact that it gives operators time to inspect the bond rather than just producing the part as quickly as possible.

Not only was it difficult for a human operator to dispense glue exactly the same way every time, potential injury was also a concern. This is because the area where the glue needs to be applied is incredibly narrow, so over time, operators were experiencing fatigue in their hands. The company has gained additional savings through a decrease in repetitive motion injuries. The robots have also enabled Tool Gauge to appeal to younger workers, providing a hiring advantage for recent graduates who want to work with exciting, interesting technologies.

Easy programming key for workers without robot experience

Tool Gauge manufacturing engineer Steve Ouzts had minimal robotic experience—just some time in college using a traditional, nonintuitive SCARA robot. The easy programming of the cobots experience was a huge benefit. "When switching to Universal Robots, the intuitive nature of the graphic user interface is what really drew me in," he says. "I really appreciate how all the terms in the software are in layman's terms. I can understand them a lot easier and know exactly how the code runs from start to finish, and I get very good positive feedback graphically of what my actions will cause the robot to do."

Another benefit of the cobots is how easy it is to connect digital and analog input signals to a control box. Ouzts found that using the proximity sensor was as easy as plugging the wires into one of the 12-volt digital inputs, selecting it from the I/O screen on the cobot teach pendant, and waiting for a signal from the sensor to tell the cobot when it is time to pick up a part.

Employees welcome cobot colleagues

One of the first reasons Tool Gauge looked at automation was to address serious labor shortages. The company was looking at the need to hire as many as 100 new employees, who simply were

FAST FORWARD

- Using collaborative robots is decreasing scrap, increasing efficiency, and improving product quality.
- Collaborative robots opened new opportunities for employees to add value, improve safety, and gain job satisfaction.
- Improving production using collaborative robots was highly effective with ROI under one year.

Tool Gauge installed two Universal Robot cobots and is already seeing success in incorporating automation into its pricing models. General Manager Jim Lee (left) says, "We expect this to be an integral part of every single thing that we produce. We will say, 'Where do we have labor now? Where can we eliminate repetitive-motion labor—the unskilled labor, the difficult-to-maintain labor—by using automation?' That will be factored into our price, and we expect to see even more success."

not available in the tight Pacific Northwest labor market. With cobots, the company cut that number in half, while being able to hire workers for jobs they desire.

ROI much faster than anticipated

In the aerospace industry, where product designs can remain unchanged for 20 or 30 years, expectations for a return on capital investment is longer than many other industries. Lee initially thought that a three- or a four-year return on the robot investment would be good. He was pleasantly surprised by the 50 percent ROI on the cobot investment within the first quarter of production on the first application, and with projected payback for both cobots of under a year. "We're very thrilled with that," he states.

The cobots' ability to be easily moved and reprogrammed for additional processes, with easy changes of end-of-arm tooling, lets Tool Gauge look at a wide range of tasks where cobot advantages can improve processes and output. For instance, traditional robots on injection molding machines could be replaced with cobots, and cobots could tend presses and other machining tasks, as well as final assembly. As easy as it is to move the cobots to new applications, the company is also looking forward to bringing in more robots to take on additional high-volume jobs, including one for riveting and assembly. ■

ABOUT THE AUTHOR

Joe Campbell (joca@universal-robots.com) is the head of strategic marketing and applications development for Universal Robots North America and has more than 35 years of experience in the robotics and factory automation industry. Before joining Universal, Campbell was vice president, sales and marketing, for Swiss-based gantry robot and track manufacturer Güdel. Campbell is a graduate of the University of Cincinnati. He is a regular speaker and lecturer at trade shows, industry events, and manufacturing symposiums, presenting the technology and economic benefits of robots and factory automation.

View the online version at www.isa.org/intech/20200603.

"It is hard to find employees here in the Pacific Northwest, because aerospace is such a large volume," says CEO of Tool Gauge, Debbie Lee. "We have a great opportunity here with bringing in the cobots, because we're now looking for a different type of employee than in the past. Before, we were hiring for machine operators, people that would just stand, swing a gate, and pull parts off the press. Now, with the robots coming in, we're looking for that type of employee that is going to be able to do the programming and set the robots up and work alongside the robots."

The cobots can be taught in "free drive mode" enabling the user to teach the cobot the desired trajectory simply by moving it through waypoints. "We believe the teach method for the Universal Robots is one of the biggest benefits by far," says Tool Gauge manufacturing engineer Steve Ouzts.

Coriolis flowmeter calibration

By Marc Buttler

When considering new technology, there are many data points to consider before making a substantial investment. One of the most important factors to consider when looking at upgrading flow measurement tools is the calibration and measurement traceability of that equipment.

The calibration of the meter is just as important to your confidence in the measurements as the design, skill, and quality of materials used in manufacturing it. The calibration-related capabilities, accreditation, and experience of the manufacturer will often influence whether you can accept the manufacturer's factory calibration, or if you need to seek a third-party calibration service provider at additional cost to achieve the measurement uncertainty and traceability you need to meet your goals and expectations. The best advice is to choose a manufacturer that has invested the necessary resources in building and maintaining the competence needed to provide superior calibrations along with their products.

Not all Coriolis flowmeters are created equal, and not all can meet the most exacting measurement standards. There are many industry applications where "good enough" is not an acceptable measurement. These types of applications, such as pharmaceutical production or custody transfer, for example, require a more precise measurement to satisfy stringent local and federal regulations. Even global standards can apply when a facility manufactures in one place but sells into another in our connected world.

Having a well-calibrated device affects the ultimate product a company produces as well. By producing a product within tight tolerances and unique specifications, a business builds a reputation for quality, but that can only be maintained if that business has the tools to do so. Before we delve deeper into calibration, let's first look at what makes a Coriolis flowmeter such a reliable and valuable tool to different industries.

Coriolis flowmeter basics

The first important element to note about a Coriolis flowmeter is the fact that it has no mechanical parts that can wear out, which increases the lifespan of a meter significantly. Another benefit of this, somewhat unique to Coriolis meters, is they do not need nearly as frequent recalibration as mechanical type meters. The measuring element has no cause to wear or change over time.

The operation of a Coriolis flowmeter is based on the principles of motion mechanics. As fluid moves through a vibrating tube, Coriolis force is generated as the fluid is forced to increase its angular momentum to move with the tube vibration as it approaches the point of peak-amplitude vibration. Conversely, angular momentum is lost when the fluid moves away from the point of peak amplitude as it approaches the exit point of the tube. The result is a twisting reaction of the flow tube during flowing conditions as it traverses each vibration cycle.

There are a few things to consider about calibration best practices before choosing a Coriolis flowmeter. Primarily those are the traceability of the reference standard that will be used for the meter calibration and the calibration procedures that apply to a specific meter model.

Measurement traceability

There are two essential elements to traceability:

- an unbroken chain of measurement comparisons, each to a higher standard, that eventually link back to national or internationally maintained reference standards
- a documented uncertainty calculation that includes the accumulated uncertainties of all the previous measurement comparison links in the chain.

It is essential to a facility that its most important tools for flow process control (i.e., Coriolis flowmeters) meet local, state, and federal regulations, as well as their own internal quality standards. Having a rigorous

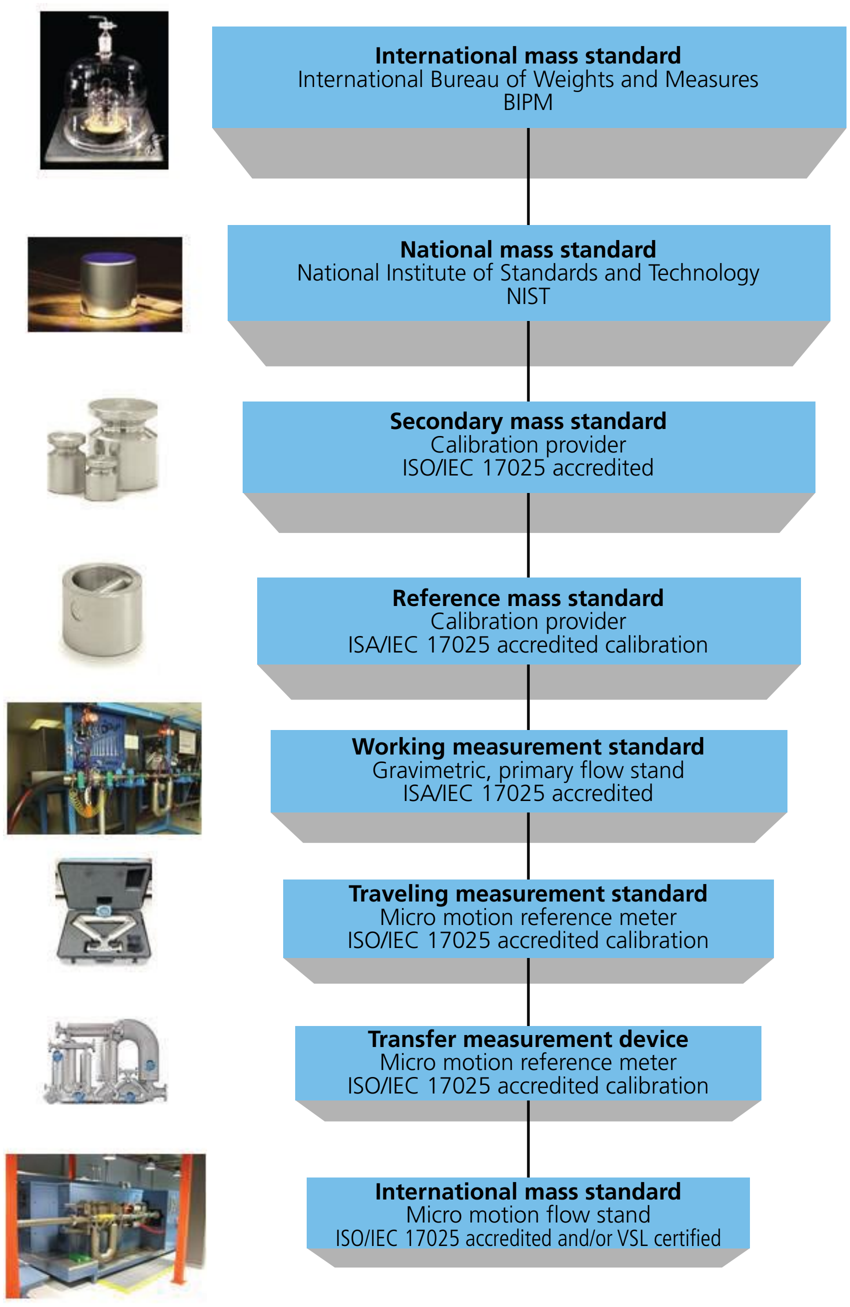

International mass standard
International Bureau of Weights and Measures
BIPM
National mass standard
National Institute of Standards and Technology
NIST
Secondary mass standard
Calibration provider
ISO/IEC 17025 accredited
Reference mass standard
Calibration provider
ISA/IEC 17025 accredited calibration
Working measurement standard
Gravimetric, primary flow stand
ISA/IEC 17025 accredited
Traveling measurement standard
Micro motion reference meter
ISO/IEC 17025 accredited calibration
Transfer measurement device
Micro motion reference meter
ISO/IEC 17025 accredited calibration
International mass standard
Micro motion flow stand
ISO/IEC 17025 accredited and/or VSL certified

Figure 1. Example traceability chain

measurement traceability to international standards helps ensure flow measurement equipment can meet those standards. In the case of mass flow measurement, such as those a Coriolis meter can provide, traceability is the chain of measurement standards going back all the way to the International Mass Standard as determined by the Planck constant. (Previously, the standard was set by the International Bureau of Weights and Measurements, but the world has recently adopted a natural standard defined by Planck's constant for greater consistency and accuracy).

Traceability documents the paths by which everything ties back to a single central starting point. In addition, traceability allows a facility to understand and apply the appropriate level of uncertainty to its measurements. Finding the right balance between the cost of uncertainty and the benefits of product quality and process efficiency can be achieved by understanding the uncertainty as documented in a traceability fact sheet or website for the meter under consideration. In all instances, the level of precision and refinement of a product will depend on the level of uncertainty found in the meter. Figure 1 illustrates a chain of traceability, which is an essential tool in achieving traceability accreditation.

Calibration procedures

The traceability of a calibration reference standard obviously matters, but how is calibration against a set standard achieved? The calibration process requires a strictly controlled procedure and an environment where a device can be put through a series of reproducible tests.

When calibrating a Coriolis flowmeter, there are two different preferred methods that can be used to reach optimal calibration. There are other methods available for other types of flowmeters that are sometimes used in applications that do not require the meter to handle flow rate transitions as well as a Coriolis meter can.

Static start/finish method

When the calibration batch begins and ends at a no-flow condition, it is a static start/finish method of gravimetric calibration. A weigh scale is used as a reference in this method, and the scale will have been calibrated using traceable mass standards. In this instance, the test fluid is water. The water is measured through the unit under test (UUT) and collected in the tank. At the end of the test, the tank is weighed again and compared to the total mass measured by the UUT.

In an application where it is necessary to obtain a better uncertainty, the mass shown on the scale will be corrected for the effect of buoyancy acting on the water in the tank, as well as for the effect of buoyancy on any immersed pipe in the setup. Fluid pressure and temperature are measured upstream and downstream of the UUT. For static start/finish, the ambient pressure, temperature, and humidity are measured during each test. Figure 2 represents graphically how this method works.

Transfer standard method

The transfer standard method (TSM) of calibration is a dynamic start-finish method where a batch starts and ends at a steady flow. Using water as the test fluid, the calibration is performed in closed conduits. Water passes through both the reference meter (RM) and the unit under test. In this example, two reference meters are used that are known as the master meters and are known good meters initially calibrated on an ISO/IEC 17025 accredited primary gravimetric flow stand following the static start/finish method. The traceability associated with this method is maintained annually using global reference meters for comparison testing.

With the TSM method the mass total from the UUT is compared to the mass total from the RM using pulse counters. Pulse counters are triggered on and off for both the UUT and RM at the same time. Upstream and downstream measurement of fluid temperature and pressure are done to ensure consistency and reproducibility. Figure 3 illustrates the TSM calibration process.

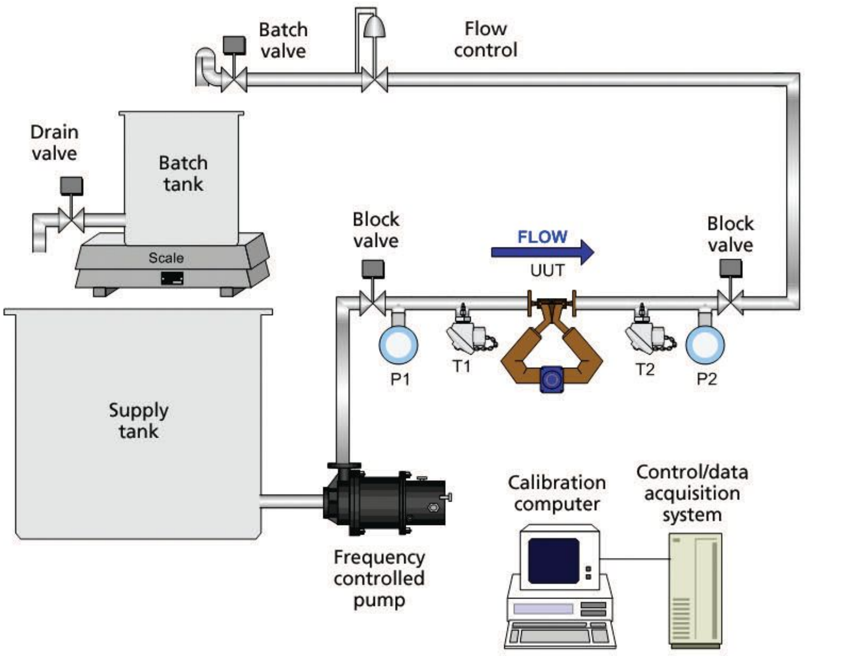


Figure 2. Static start/finish method (T = temperature transmitter, P = pressure transmitter)

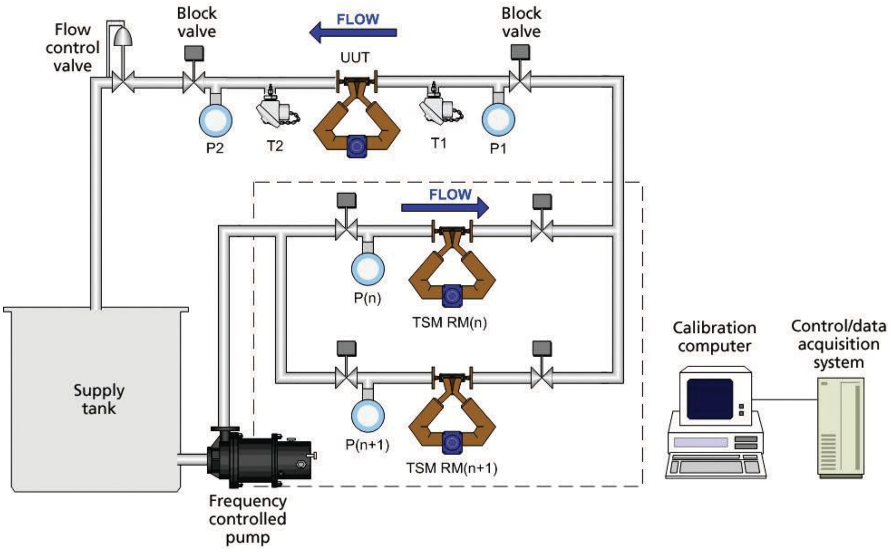


Figure 3. Transfer standard method (T = temperature, P = pressure transmitter)

Fit for purpose uncertainty

When considering calibration methods and traceability standards, it is critical to understand the cost of reaching each incremental level of improvement to the uncertainty and how tight of an uncertainty might be justified given the impact on the process where the Coriolis flowmeter is used. Determining uncertainty levels of a meter is done by the combined uncertainty of each of the traceable steps leading to the calibration of the meter. Uncertainty increases in small increments, often negligible to the results of the process, with each step further down the traceability chain.

What happens when a Coriolis flowmeter leaves the laboratory and is no longer in the controlled environment where it was calibrated? Secondary effects then come into play and add more uncertainty to the performance of the meter in situ in a process.

Calibration uncertainty and the effects of process on the flowmeter combined will determine the final uncertainty of the measurement. This is why it is important to understand both the uncertainty of the calibration and the impact and magnitude of secondary effects of a process in order to know the appropriate level of calibration uncertainty that is needed—or is acceptable—to ensure a quality final product. ■

ABOUT THE AUTHOR

Marc Buttler is the oil and gas application innovation director at Emerson for Micro Motion Coriolis flowmeters and has a BS in mechanical engineering from the University of Colorado. Buttler has been with Emerson for 32 years in a wide variety of roles. He specialized in custody transfer applications involving both gas and liquid products. He is active with the API Committee on Petroleum Measurement and with the National Conference of Weights and Measures. Previously he worked for the NIST Office of Weights and Measures.

ISA and Newsweek publish cyberrisk white paper

Newsweek Vantage recently published an independent report on cyberrisks to critical infrastructure—and ISA served as its expert partner. Titled "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure," the report surveyed 415 executives at critical infrastructure organizations to learn whether they are taking a holistic approach to security for operations technology (OT) and information technology (IT).

Among other takeaways, the survey found that a holistic approach is a priority for most—and that more than a third of respondents said a cybersecurity breach was the motivating factor. Key points of the report include:

- The design of a secure cyber-physical system depends on a clear threat analysis. The biggest sources of vulnerability are current and former employees—more so, even, than cybercriminals.
- A comprehensive approach to security is required to protect critical infrastructure against cyberthreats from within and without. Almost nine in 10 respondents have integrated some or all of their IT, OT, and physical systems. But this does not mean they are doing so to enhance security; only a few said this was the purpose. Instead, most aim to take advantage of the greater responsiveness and enhanced operational control that comes from a holistic approach.

The implementation of a holistic approach to securing cyber-physical systems faces both internal and external obstacles. The internal hurdles are largely the result of differing perspectives among IT and OT professionals, according to the report. Those internal hurdles were rated as the top technical and organizational obstacle. Externally, security standards for cyber-physical systems are available but not widely used. ■

Newsweek VANTAGE

WEATHERING THE PERFECT STORM

SECURING THE CYBER-PHYSICAL SYSTEMS OF CRITICAL INFRASTRUCTURE

Sponsored by:

NOZOMI NETWORKS SIEMENS yubico

ISA

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 Automation Professionals

Ethan Stephens, U.S.
Khalid Ismail, Saudi Arabia
Jose Guevara, U.S.

Certified Control System Technicians

Level 1

Frank Giacinto, U.S.
Lamar Atwood, U.S.
Edward Egan, U.S.
Robert McDonald, U.S.
Steven Nisbet, U.S.
Scott Okasaki, U.S.
Michael Patton, U.S.
Nathaniel Ross, U.S.
Wessley Wissinger, U.S.
Scott Breschini, U.S.
Jonathon Chandler, U.S.

Level 2

Derrick Mire, U.S.
David Stanford, U.S.
Jeffrey Rodewald, U.S.
Steve Morrison

Level 3

Manuel Aguilar Morales, Mexico
Michael Schmoll, U.S.

Unsung Heroes

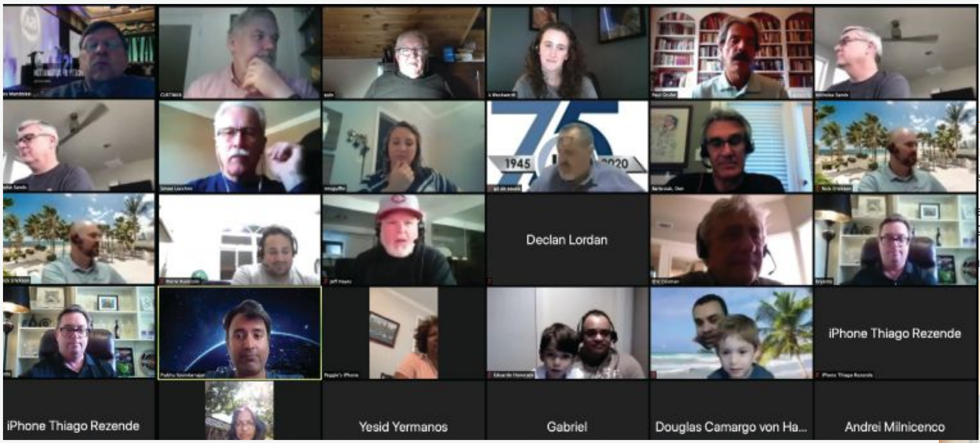
ISA and Automation.com salute the manufacturing and process industry employees keeping essential supplies available during the COVID-19 pandemic.

See page 58.

Are you up to date on instrument calibration, cybersecurity, system migration, and industrial communications? Would you like to find out more about ISA events, training, membership, and more? ISA's YouTube channel is your resource for how-to videos on all facets of automation and control, and a great way to hear members talk about their real-life plant experiences and membership networking benefits. **www.isa.org/isa-youtube**

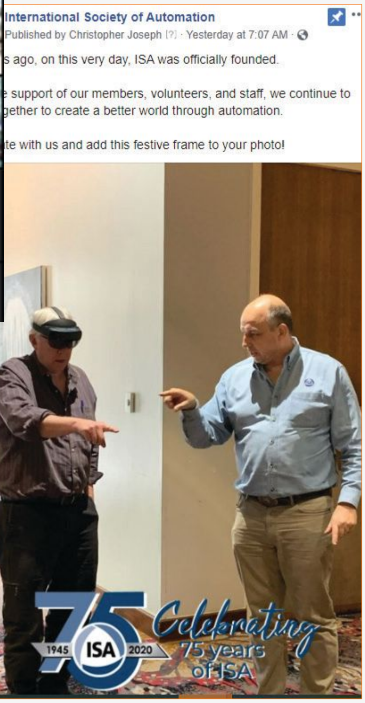
You Tube

Anniversary snapshot: ISA members celebrate via Zoom, Instagram



Zoom meeting happy hour. On 28 April, the date of ISA's founding 75 years ago, Ashley Weckwerth organized a virtual happy hour over Zoom to celebrate. Invitations were sent via ISA LinkedIn groups, email, ISA Connect, and WhatsApp, and soon about 30 participants were toasting their favorite association from their desks or home offices in the U.S., Canada, Brazil, Ireland, Colombia, and elsewhere.

On the anniversary of the actual date of ISA's founding (28 April), ISA staff unveiled a festive photo frame for members to use on their Instagram posts.


International Society of Automation
Published by Christopher Joseph [?] · Yesterday at 7:07 AM ·

s ago, on this very day, ISA was officially founded.

e support of our members, volunteers, and staff, we continue to gether to create a better world through automation.

te with us and add this festive frame to your photo!

Pledge to make a difference: #ISAGivesBack

As part of its 75th anniversary celebration, ISA is challenging members to each give 7.5 hours in service to their community this year. The ISA Gives Back program encourages members to pledge and log the completion of service hours through the ISA 75th Anniversary website at www.isa.org/75in2020. Through 21 May, 152 hours had been pledged.

Service hours can take many forms. Members may want to consider activities specific to the coronavirus pandemic, or online opportunities that allow you to volunteer while practicing appropriate social distancing. Ideas include:

- Find or transport personal protective equipment and other supplies.
- Help your local school district get involved in the Cyber Robotics Coding Competition (CRCC.io), a cloud-based robotics competition that uses simulation of virtual 3D robots that perform complex tasks and missions.
- Build disposable face shields using hardware store items (https://newbo.co/building-face-shields) or reusable face shields or mask ear protectors using a 3D printer.
- Donate blood to local health facilities that are in need.
- Tutor students in science, technology, engineering, and math (STEM) topics through organizations like www.etutorworld.com/stem-tutoring.html.

Get other ideas for helping with neighborhood enhancement, the environment, senior citizens, special needs kids, and more at SignUpGenius.com. ■

Check out the newest ISA 75th Anniversary branded items. isa.org/75in2020

#ISAGivesBack

Professional Development

New certification verifies skills of mission-critical operations professionals

By Steve Mustard

As a result of various demographic and cultural changes, there is an acute shortage of suitably qualified and experienced individuals to work in *mission-critical systems design and operation*. The term "mission critical" relates to any activity, system, or equipment whose failure can result in the failure of an organization's operations. Depending on the organization, the consequences of failure can be very wide ranging.

ISA believes that mission critical applies to the operational technology (OT) that is an integral part of oil and gas, water and wastewater, electricity generation and transmission, food and beverage, and the other critical infrastructure sectors defined by the U.S. Department of Homeland Security (DHS). However, information technology (IT) systems, such as those in data centers also can be mission critical, since their failure can severely impact operations. This is especially true as businesses shift their infrastructure to cloud providers such as Microsoft, Google, and Amazon.

The Automation Federation, founded by ISA, has been working with the U.S. Department of Labor since 2008 on the development and ongoing maintenance of an *automation competency model* (ACM). The model identifies the knowledge and skills needed in mission-critical systems design and operation.

ISA offers a range of certifications and certificate programs that provide verification of key skills and knowledge defined in the ACM. The latest is the Certified Mission Critical Professional (CMCP) certification. This is an important certification for mission-critical professionals. It is a means to verify the knowledge required for those entering the workforce. And it ensures that new workers have the essential foundations for a successful career.

The automation competency model was used by the National Center for Mission Critical Operations to define a two-year degree program for mission-critical professionals who can enter the workforce already prepared to contribute. ISA developed the certification exam that mission-critical professionals can take to achieve independent verification of their knowledge. The certification is managed by Global Skills Exchange, a nationally recognized developer of skill standards and measurement tools.

The CMCP credential is open to anyone who has a two-year degree, two years of related work experience in a mission-critical field, or any combination.

CMCP covers seven core areas:

- Concepts – what makes mission-critical operations unique, such as the high availability demands and the conflicting demands of security and accessibility.
- Standards – what standards, regulations, and guides apply to mission-critical systems.
- Technology – what devices and systems are commonly used in mission-critical operations, such as distributed control systems, programmable logic controllers, networking equipment, and cybersecurity-related hardware and software.
- Operations – what is involved in mission-critical operations, including standard operating procedures, troubleshooting, performance objectives, monitoring, and change management.
- Safety and physical security – what professionals need to be aware of when working in mission-critical environments, including the use of personal protective equipment, lockout/tagout procedures, safety data sheets, and hazardous area classification.
- Risk management – what methodologies will be used to determine the risks associated with mission-critical operations, and how these risks will be managed.
- Emergency response – what preparation goes into ensuring that emergency situations are dealt with safely and with minimal disruption to the organization and its surrounding environment.

The CMCP credential is open to anyone who:

- Has a two-year degree (with course work in an IT or an OT field), including a minimum of six months (two quarters) of related co-op experience or an equivalent apprenticeship of at least six months.
- Two years of related work experience in a mission-critical field, such as information technology, operational technology, engineering, cybersecurity, or military.
- Any combination of the requirements above, totaling two years of experience or education, provided that the minimum requirement of six months of work experience is met.

The importance of CMCP is clear. As the 16 critical infrastructure sectors grow, demographic research reveals there will be an even greater need to fill vacancies with professionals who are fully prepared to avert and avoid any and all mission-critical threats. CMCP seeks to help validate that those working in mission-critical positions have the requisite skills and knowledge needed to handle mission-critical threats, whether they are natural disasters, manmade threats, or accidents. ■

Steve Mustard has been in the engineering profession for 30 years. Much of his current work involves assessing the cybersecurity readiness of critical infrastructure organizations.

Updated guidelines for using ISA/IEC 61511 – Functional Safety

Following a week of web-based meetings in mid-May, the ISA84 standards committee, Instrumented Systems to Achieve Functional Safety in the Process Industries, is moving well ahead in developing and updating a comprehensive set of technical reports providing guidance and practical examples for the global process industries in applying the widely used ISA/IEC 61511-2018 standards, *Functional Safety – Safety Instrumented Systems for the Process Industry Sector,* Parts 1-3. Those ISA/IEC standards, the first version of which was completed by ISA84 in 1996, set forth requirements for the specification, design, installation, operation, and maintenance of a safety instrumented system (SIS), so that it can be entrusted to achieve or maintain a safe state of a process.

ISA84 has now completed an update to one of several technical reports on specific phases of the SIS life cycle. ISA-TR84.00.04-2020 Part 1, *Guidelines for the Implementation of ANSI/ISA-61511-1-2018 (IEC 61511-1)*, provides an overview of the SIS life cycle with references to several annexes containing detailed guidance on key aspects of the safety life cycle, including: "grandfathering" existing SISs, operator-initiated functions, separation of the basic process control system (BPCS) and SIS, field device and logic solver selection, manual shutdown considerations, and design/installation considerations (for example, wiring, power, relationship to BPCS, common mode impacts, and fault tolerance).

The web meetings in mid-May drew more than 90 attendees from across the globe during the main committee sessions.

Another ISA84 technical report in revision, ISA-TR84.00.02, *Safety Integrity Level (SIL) Verification of Safety Instrumented Functions*, serves as a tutorial on the fundamentals of data selection and the reliability calculations. The revision is now complete with the exception of an example on calculating the PFDavg of an automated block valve undergoing partial stroke testing. That example is being reviewed by the ISA96 committee, Valve Actuators. The revised technical report is expected to be completed by the end of this year.

This work follows the late 2019 publication of ISA-TR84.00.03, *Automation Asset Integrity (AAI) of Safety Instrumented Systems,* which presents guidance on establishing an effective AAI program that demonstrates through traceable and auditable documentation that the SIS and its equipment are maintained in an "as good as new" condition.

Previous ISA84 technical reports also include:

- ISA-TR84.00.09-2017, *Cybersecurity Related to the Functional Safety Lifecycle,* provides guidance on integrating the cybersecurity life cycle with the safety life cycle as they relate to safety controls, alarms, and interlocks, inclusive of safety instrumented systems. The scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the industrial automation and control system network. Input and collaboration between ISA84 and ISA99, Security for Industrial Automation and Control Systems, is ongoing as a new revision effort is now underway.
- ISA-TR84.00.08-2017, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers,* addresses wireless technology-based sensors that are used in independent protection layers (IPL) providing a risk reduction factor of less than or equal to 10 (non-SIS IPL) by the authority having jurisdiction (typically the owner/operator or local regulatory authority), and establishes guidance and considerations for their utilization in the process sector.
- ISA-TR84.00.07-2018, *Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness,* addresses detection and mitigation of fire, combustible gas, and toxic gas hazards in process areas. It clarifies information to be considered when developing a performance-based FGS design—including integrating the design activities into relevant portions of the safety life-cycle model for safety-critical controls.
- ISA-TR84.00.05-2009, *Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS),* is currently being revised by ISA84, with a focus on providing BMS-specific guidance/clarity to all phases of the safety life cycle, updating unit operation examples based upon the latest governing standards/practice (for example, NPFA 85, API 556), and updating based on end user feedback from the current edition.

Web meeting success

The web meetings in mid-May drew more than 90 attendees from across the globe during the main committee sessions and were well attended throughout the week. Based on that success, ISA84 is planning another week of web meetings to be held 12–15 October.

ISA standards participation and meetings are open to all interested parties, and experts from any country are welcome to join the ISA84 committee. For more information, contact Charley Robinson, ISA Standards, crobinson@isa.org.

For information on viewing or obtaining the technical reports described above, visit www.isa.org/findstandards. ■

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

How manufacturing can attract the best and brightest next-generation workers

By Paul Donnelly

As more experienced workers retire from the manufacturing workforce, the sector faces a future with a growing skills gap and a greater number of unfilled jobs. Initiatives to boost the manufacturing workforce, like the National Association of Manufacturers (NAM) "Creators Wanted" national tour that recently kicked off, are excellent steps in boosting the profile of the industry and, hopefully, encouraging younger generations to take interest in manufacturing career paths.

What will attract the next generation of workers to manufacturing is understanding the impact their career can have on solving these larger societal issues.

While established tech giants and new venture startups lure talent with ping pong tables and beer taps, manufacturing can tap into a sincere drive to solve the world's most pressing problems. A career working for a leading social media platform may come with the latest office perks, but can it really compare with a career focused on meeting the world's energy needs today while preserving the environment for their kids? Can the shine of social media–focused companies really compete with challenges like reengineering basic materials like plastics to be more recyclable and meet requirements for a true circular economy? If newer workers are shown the entire picture, I highly doubt it. That is why initiatives, such as the above-referenced NAM initiative, are sorely needed.

Education

What will attract the next generation of workers to manufacturing is understanding the impact their career can have on solving these larger societal issues. That is why a key component of the NAM initiative involves outreach to students, educators, and parents to positively influence the perception of manufacturing as a place to make a difference. Major industrial companies can work to propagate this messaging as well, even partnering with colleges and universities to make themselves and their industries more visible to students, while positioning manufacturing careers in positive ways. It is a fundamental lack of awareness and knowledge about the manufacturing world that has created a lack of students who express or show interest in pursuing careers within our field. The industry, schools, parents, and the media all have a responsibility to educate the public in order to change perceptions. To complement these efforts, the industry also needs to modernize through digital initiatives and directly connect themselves to the topics of sustainability and the future of energy.

Modernization

Most manufacturers are in the midst of significant initiatives to digitalize their operations. For example, an area in which they can see significant returns is in helping newer engineers and other workers become productive faster. Firms can leverage artificial intelligence to help provide in-context learning and guidance, so less experienced employees can more easily complete their work. Artificial intelligence and automation can also be used to remove some of the mundane, low-value tasks that turn off next-generation workers. It goes without saying that as the rest of the world modernizes, industries that do not follow suit will be at a major disadvantage when it comes to hiring new talent.

Sustainability

Sustainability is top of mind for next-generation workers. Many would easily prioritize meaningful work over other perks if it is connected to helping develop a sustainable future. As a significant portion of the world's sustainability challenges are associated with the process manufacturing industries, specifically energy and plastics, these are two fields where opportunities abound to make a difference. Digital transformation initiatives underway in these fields in particular will give new workers simply unmatched opportunities to have a real and meaningful impact on society and the environment.

Through targeted and continuous education, modernization, and sustainability efforts, we should expect to see a change in mindset when it comes to people pursuing careers in manufacturing. It is also important to consider that it is not only the future workforce who can make a difference—it is also the current workforce who can affect change and apply their skills and expertise to solving these pressing societal problems. This can aid in retaining key talent who will be critical in helping newer workers reach their potential faster. ■

ABOUT THE AUTHOR

Paul Donnelly is the industry marketing director for engineering and construction at AspenTech. Donnelly has more than 25 years of experience in engineering, construction, and supply chain management with global business responsibilities. He earned an undergraduate degree in geology and has an MBA from the University of Massachusetts.

SCADAwall™
Industrial Airgap Bridge

PLANT DATA SECURELY DELIVERED ONE-WAY FROM THE "SHOP FLOOR" TO THE "TOP FLOOR"

Securely Transfer Sensitive Plant Data to Corporate Without The Risk of Internet Exposure, Infected USBs Or Data Hard Copies

- Secure, one-way data transfer, no possibility of any network connection, unlike a firewall
- Total insulation against malware, workstation exploit propagation and back channels
- Safe replication of plant data from trusted to untrusted destinations with provable validation – examples: databases, historians, logfile sync, inventory, production and maintenance data, etc.
- Higher throughput, guaranteed delivery, no re-transmissions, and lower cost, averaging at least 30% less than competitive solutions

**SCADAwall makes use of two discrete systems operating together, still with an average savings of at least 30%*

Learn More! www.bayshorenetworks/SCADAwall
or email sales@bayshorenetworks.com

TO START THE CONVERSATION

Technical Details

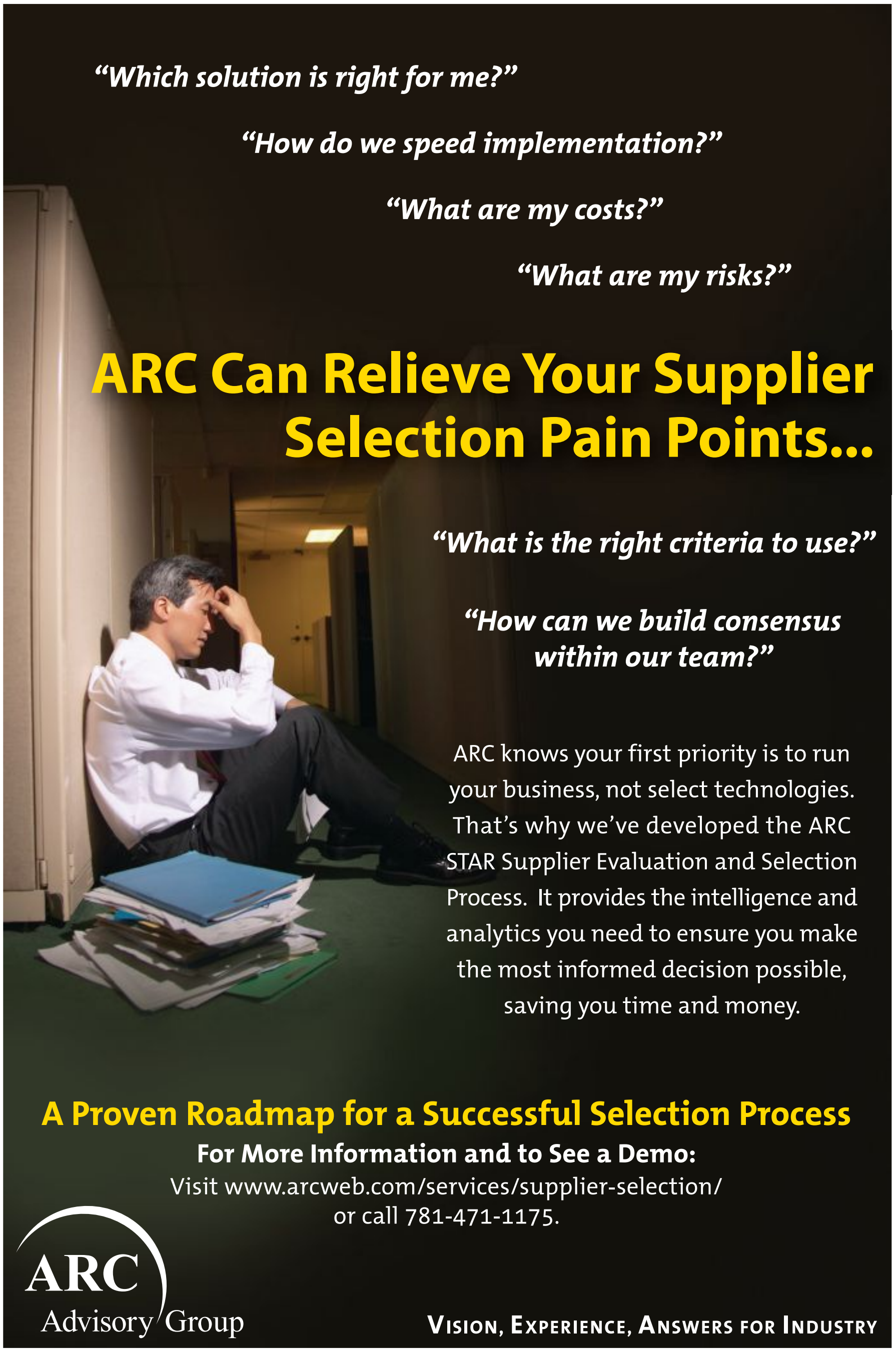
- Server Replication - Native support for real-time OPC DA, OPC AE, Modbus, others
- Database Export Replication - Oracle, MySQL, MS SQL and more
- Native unidirectional file transfer via Windows or ftp shares
- Support for any unidirectional tcp or udp socket, e.g. mqtt-sn, syslog, or tunneled SCADA applications

BAYSHORE

Bayshore Networks is the leading provider of active cybersecurity solutions designed specifically to protect the safety and integrity of industrial and critical infrastructure networks. Bayshore protects ICS/SCADA and OT devices from unauthorized changes, automatically builds security policies, delivers OT data securely to destinations outside the plant, and secures remote access.

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	**56**
Automation Direct www.automationdirect.com	**Cover 2**
Bayshore Networks www.bayshorenetworks.com	**55**
Buerklin Gmbh www.buerklin.com/en	**27**
Endress + Hauser www.us.endress.com	**3**
Inductive Automation www.inductiveautomation.com	**Bellyband**
ISA Global Cybersecurity Alliance www.isa.org/isagca	**Cover 3**
ISA Training www.isa.org	**26**
Moore Industries www.miinet.com	**6**
Opto22 www.opto22.com	**Cover 4**
ProComSol, Ltd. www.procomsol.com	**9**
Seifert Systems www.seifertsystems.com	**25**
Tadiran www.tadiranbat.com	**15**
VEGA Americas www.vega.com	**19**



The September/October issue of *InTech* will be the 75th Anniversary edition. Contact your sales rep for details.

75 1945 ISA 2020

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

Elena Pitt
Strategic Business Development
Phone: +1 919-323-4023
Email: epitt@isa.org

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

View and download the InTech media planner at **www.isa.org/intechadkit**

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.

Explosion-proof panels

The CPX series of multi-touch control panels and panel PCs is available in more robust versions, with aluminum enclosures complying with the requirements for hazardous areas classified Zone 2/22c. CPX series panels have capacitive touch technology, a large selection of display formats and sizes, and multiple installation options. Both the panels for control cabinet installation and stand-alone panels are available in the CPX29xx and CPX39xx series.

Beckhoff, www.beckhoff.com/process

HART-IP developer kit

This software, hardware, and services development platform for HART-IP enabled wired instruments is based on the Raspberry PI (3B+) system using GitHub repositories. It provides a path for process instrumentation manufacturers to prototype and demonstrate high-speed HART-IP instruments with minimal engineering effort. Initially configured to work with power-over-Ethernet (PoE) solutions, the developer kit has a replaceable Ethernet module that will be upgraded to support two-wire Ethernet-APL as components become available. Planned upgrades also include incorporation of FieldComm Group's OPC UA-centric Process Automation Device Information Model (PA-DIM) for interoperability with OPC UA–based enterprise applications, as well as support for JSON and XML–based DeviceInfo files to use with lightweight IIoT edge gateway solutions.

FieldComm Group, www.fieldcommgroup.org

Connector for battery storage modules

The wiring for lithium-ion batteries requires compact plug connections that do not heat their surroundings, even when transmitting high currents, and connector housings that ensure efficient cooling. The Han S large-scale special connector for battery storage modules meets these needs, as well as the latest standards for stationary energy storage systems (including UL 4128). Housings have space for a heavy-current contact up to 200 A, and pin contacts are mounted in the attachment housing, which is freely pivotable. The connectors can also be installed as part of the control line (BUS system) for a battery management system. They include special pin contacts in the attachment housing to support this.

Harting, www.harting.com

Thermoelectric coolers

Seifert SoliTherm thermoelectric coolers use the Peltier effect for closed-loop cooling. Because the only moving parts are axial fans, there is virtually no maintenance. The units can be mounted in nearly every position (except roof mounting), because they do not have a compressor or any moving parts other than the fans. They are resistant to extreme ambient conditions and can operate effectively in dusty and oily environments, both indoors and outdoors. Cooling capacities range from 170 to 680 BTU/H (50 W to 200 W); the operating temperature range is –4°F to 149°F (20°C to 65°C). Units are CE, RoHS, and cURus listed and washdown friendly NEMA 4X, IP66 rated.

AutomationDirect, www.automationdirect.com

classifieds

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.

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

Manufacturing and process heroes behind the scenes

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.

The impact worldwide of the COVID-19 virus is obvious, and there are amazing and dedicated people in healthcare on the "frontlines" working with patients. Many have characterized this as a fight much like a war. It certainly has those characteristics, including the quiet heroes behind the scenes who "keep the wheels turning and supply the troops." In order for society to function, many manufacturing and process industry professionals are also amazing and dedicated behind-the-scenes people who are making sure a steady flow of a wide range of essential resources, materials, and supplies is available.

Manufacturing and process industry professionals are keeping a wide range of production functioning, including:

- pharmaceutical and biotech plants (medicines, insulin, etc.)
- electric power generation, substations, and transmission lines
- natural and LP gas utilities (pipelines, compressor stations, etc.)
- water and wastewater treatment plants (distribution, lift stations, pumps, etc.)
- oil and gas production (upstream, midstream, downstream)
- ethylene plants (plastics, solvents, etc.)
- pulp and paper plants (toilet paper, masks, filters, diapers, etc.)
- food and beverage production plants (sanitizer, groceries, soup, meats, frozen food, etc.)
- manufacturing plants (medical masks, medical shields, ventilators, soap, toilet paper, etc.)
- distribution centers (conveyors, material handling, AVGs, robotics, etc.)

Consider the impact if these operations at these production plants degraded or failed.

In the ranks of these workers are many International Society of Automation members who are dedicated professionals. Since the founding of ISA in 1945, members have been committed to improving industry with members volunteering their time to develop standards and education and training, and publishing books and technical articles. ISA's 160 geographical sections connect members with technology, expert advice, and technical training.

The importance of manufacturing and production professionals in this crisis reminds me of the message Peter Martin, PhD, ISA Fellow, has given for a number of years about the high value that automation professionals' work contributes to the welfare and betterment of the world.

For those not familiar with Dr. Martin he is a recognized leader and innovator in the field of automation and control for over 37 years. He was recognized by *Fortune* magazine as a Hero of U.S. Manufacturing and received ISA's Life Achievement Award. He has a BA and MS in mathematics, an MA in administration and management, a PhD in industrial engineering, as well as a masters and PhD in Biblical studies.

Manufacturing and production professionals are another part of the "troops" in this fight behind the scenes. Others behind the scenes in these ranks include warehouse people, operators, truck drivers, grocery store cashiers, farmers, and many others.

Certainly, the medical professionals are brave, dedicated people right at the front. As automation professionals, we understand it takes an entire system with all support troops to win. ■

We salute the many amazing and dedicated behind-the-scenes manufacturing and process industry professionals in this pandemic crisis.

Manufacturing and process industry professionals around the world keep things running.

Coronavirus disease (COVID-19) is an infectious disease caused by a newly discovered coronavirus. In the designation COVID-19, "CO" stands for "corona," "VI" for "virus," and "D" for disease. Formerly, this disease was referred to as "2019 novel coronavirus" or "2019-nCoV."

Ignition 8

by inductive automation

The Unlimited SCADA Platform of the Future is Here

Download the free trial today at *inductiveautomation.com*

14:13

Back

Ignition

Start Date	End Date	Top
01/23/2019 00:00	01/23/2019 23:59	10

ALARM SUMMARY

TOTAL ALARMS	3
TOTAL DURATION	02:16:01
TOTAL UNACKNOWLEDGED	3
AVG TIME TO ACK	00:00:00
AVG TIME TO CLEAR	01:09:30
MOST FREQUENT	Day Tank - 2 (66.7%)
LONGEST DURATION	Tank 1 - 7621 (93.4%)

ALARMS BY HOUR