CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION • CONTROLGLOBAL.COM

EVERYDAY CYBERSECURITY

Effective cybersecurity must be a routine part of process operations—even as new defenses arrive daily

CHINA'S WANHUA CHEMICAL GROUP NAMED PLANT OF THE YEAR

TERMINAL BLOCKS TACKLE WIRES, ADD INTELLIGENCE

NOVEMBER 2022

We're sensing big savings in your future…

when you buy process sensors from AutomationDirect

Process control and measurement devices sense changing values over a set range that are transmitted during continuous or batch processing. Our process sensors give you high performance at prices that are easy on your budget.

Level Sensors

Starting at $12.50 (FLS-VM-100)

Level sensors monitor the level of liquids, pellets, powders, and other similar products in tanks and process systems.

- Ultrasonic level sensors
- Float level switches
- Vibration fork level switches
- Capacitance level switches
- Rotating paddle level switches
- Guided wave radar level sensors
- Differential pressure level transmitters

Temperature Sensors

Starting at $19.00 (FG1W-100PP-28)

Temperature sensors provide accurate and reliable feedback for temperature control and monitoring applications.

- **NEW!** Optris infrared pyrometers
- Temperature switches and transmitters
- Digital temperature switches/transmitters
- Thermocouple and RTD probes
- Thermowells and fittings

Pressure Sensors

Starting at $84.00 (QPSL-AP-42)

Pressure sensors measure pressure at a specific point in the process and transmit the measured value to a control device.

- **NEW!** Winters pressure accessories: siphons, snubbers, and isolation needle valves
- Electronic and mechanical pressure switches
- Pressure and vacuum transmitters
- Digital pressure switches/transmitters
- Differential pressure transmitters

Flow Sensors

Starting at $63.00 (FG1W-100PP-28)

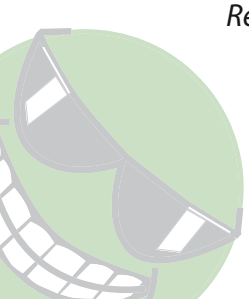
Flow measurement devices monitor liquid media and provide reliable flow indication, detection or measurement.

- Mechatronic flow switches and transmitters
- Magnetic-inductive flow meters
- Thermal flow sensors
- Vortex flow sensors
- Variable area mechanical flow meters

Also Available

Process Controllers	Digital Panel Meters	Flowline Level Controllers (LC Series)	Hour Meters & Counters
			

Research, price, and buy at: ***www.automationdirect.com/process-controllers***



Order Today, Ships Fast!

TOP RATED BY CUSTOMERS

AUTOMATIONDIRECT.com

1-800-633-0405 the #1 value in automation

Take Charge

To take charge and be sure your operations and system are in sync at optimal capacity, you need to be atop autonomy. And to get there, Yokogawa delivers resilient solutions for you, a process using our smart manufacturing and IA2IA (Industrial Automation to Industrial Autonomy), deploying OpreX as our true enabler to achieve total optimization throughout the supply chain. Integrating discrete systems in society, we move together with you toward the system of systems in which everything is intricately connected and goals are achieved beyond those of a single system. Yokogawa. Atop autonomy for the planet.

OpreX™

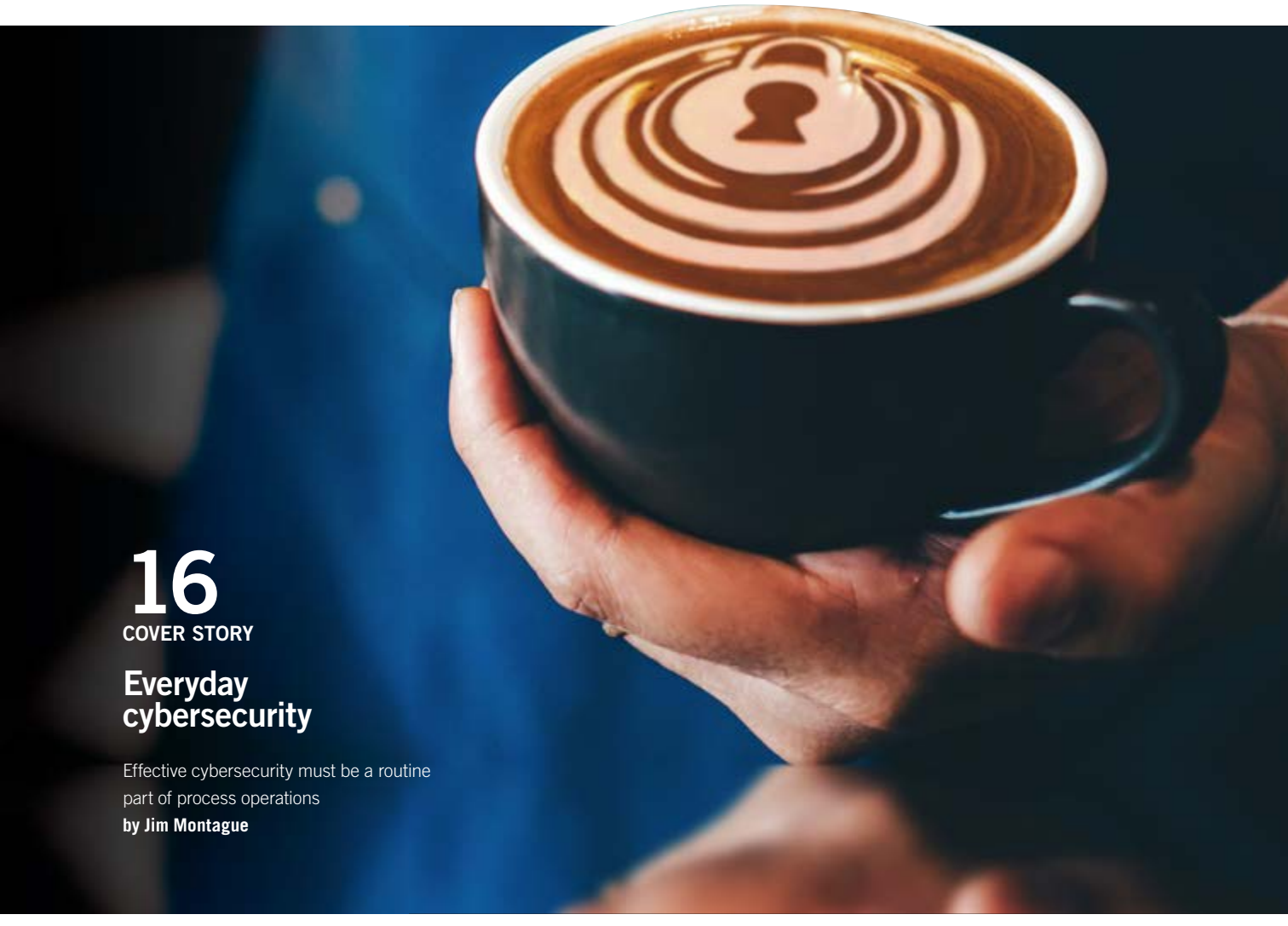
yokogawa.com/ia2ia/

YOKOGAWA

Co-Innovating tomorrow™

NOVEMBER 2022 • VOLUME 35 • NUMBER 11

CONTROL



Proline 10 - Flow measurement uncompromisingly simple

- User-friendly over the entire device life cycle - from sizing to commissioning and maintenance in basic applications
- Straightforward operation via LCD touch screen as well as via SmartBlue app
- Time-saving due to commissioning wizard and Heartbeat Technology
- Seamless system integration via HART or Modbus RS485 - over million Promag and Promass sensors successfully installed

Do you want to learn more?
www.us.endress.com/proline-10

Endress+Hauser
People for Process Automation

Departments

CIRCULATION

Food & Kindred Products	13,230	Paper & Allied Products	2,784
Chemicals & Allied Products	6,582	Pharmaceuticals	4,533
Systems Integrators & Engineering Design Firms	9,702	Rubber & Miscellaneous Plastic Products	3,297
Primary Metal Industries	6,541	Stone, Clay, Glass & Concrete Products	1,690
Electric, Gas & Sanitary Services	5,071	Textile Mill Products	1,221
Petroleum Refining & Related Industries	1,992	Tobacco Products	155
Miscellaneous Manufacturers	3,222	Total Circulation	60,020

MAKING THE COMPLICATED SIMPLE

SUSTAINABLE, FLEXIBLE, EASY

From fractional to 600 HP, Yaskawa industrial drives cover all of your application needs, with an array of features that improve your operations.

- ✓ **Intuitive Mobile-Friendly Interaction**
- ✓ **Fast Connection to Any Major Network Protocol**
- ✓ **Functional safety rated - Standard**
- ✓ **Best-in-class Efficiency**

And don't forget about everything else Yaskawa provides you with.

- ✓ **World-Class Quality and Reliability**
- ✓ **Award Winning Customer Service**
- ✓ **Product Lifetime Training**
- ✓ **Free 24/7/365 Technical Support**

Life getting too complicated?
Contact Yaskawa for help today.

For more info:
https://go.yaskawa-america.com/yai1450

IT'S PERSONAL

YASKAWA

Yaskawa America, Inc. 1-800-YASKAWA
Email: info@yaskawa.com | yaskawa.com

CONTROL

Endeavor Business Media, LLC
30 Burton Hills Blvd, Ste. 185,
Nashville, TN 37215
800-547-7377

EXECUTIVE TEAM

CEO
Chris Ferrell

President
June Griffin

CFO
Mark Zadell

COO
Patrick Rains

Chief Administrative and Legal Officer
Tracy Kane

EVP/Group Publisher
Mike Christian

EDITORIAL TEAM

Editor in Chief
Len Vermillion, lvermillion@endeavorb2b.com

Executive Editor
Jim Montague, jmontague@endeavorb2b.com

Digital Editor
Amanda Del Buono, adelbuono@endeavorb2b.com

Contributing Editor
John Rezabek

Columnists
Béla Lipták, Greg McMillan, Ian Verhappen

Editorial Assistant
Lori Goldberg

DESIGN & PRODUCTION TEAM

Art Director
Derek Chamberlain, dchamberlain@endeavorb2b.com

Senior Production Manager
Anetta Gauthier, agauthier@endeavorb2b.com

PUBLISHING TEAM

VP / Group Publisher
Keith Larson, klarson@endeavorb2b.com

Midwest/Southeast Regional Sales Manager
Greg Zamin, gzamin@endeavorb2b.com
704/256-5433, Fax: 704/256-5434

Northeast/Mid-Atlantic Regional Sales Manager
Dave Fisher, dfisher@endeavorb2b.com
508/369-6330, Fax 508/543-3061

West Coast/Mountain Regional Sales Manager
Jeff Mylin, jmylin@endeavorb2b.com
847/516-5879, Fax: 630/625-1124

Classifieds Manager / Circulation requests
Lori Goldberg, lgoldberg@endeavorb2b.com

Reprint Marketing Manager
Mossberg & Co.
Lisa Payne, lpayne@mossbergco.com

Subscriptions
Local: 847-559-7598
Toll free: 877-382-9187
Control@omeda.com

Jesse H. Neal Award Winner & Three Time Finalist
Two Time ASBPE Magazine of the Year Finalist
Dozens of ASBPE Excellence in Graphics and Editorial Excellence Awards
Four Time Winner Ozzie Awards for Graphics Excellence

It's game on for net-zero

Process control technology is equipped and ready to win the sustainability game

AS I darted around this year's Emerson Exchange, one thing became increasingly clear: you, the process control engineer, are in the starting lineup when it comes to tackling the world's net-zero goals. So, buckle up your chinstrap because we're well past the opening drive of the game when it comes to sustainability efforts.

"We need to start to turn pledges into progress," said Mike Train, Emerson's chief sustainability officer, discussing carbon emissions.

While many 2030 or 2050 (name your date) net-zero goals set forth by governments and companies worldwide have been pledged and, in many cases, even put into play, the results thus far have been fieldgoal handshakes rather than touchdown celebration dances. So, how can industry let loose and move the ball downfield? Luckily, the answer already has a helmet on and is ready to go.

Process control.

Throughout the week in Grapevine, Texas, I sat through multiple roundtable discussions and case study presentations describing the role of digitalization in turning emission-excessive operations, such as those in energy production, into carbon-reducing processes. Behind each one, the star quarterback of their business' sustainability efforts was the automated control system.

Wireless technology serves as the control room's running back in these efforts, toting digital information around plants, even plant-to-plant in many cases. Facilities are rapidly becoming digitalized, and the possibilities for making operations more sustainable are following suit. One thing is apparent, digitalized operations make for more quickly scalable sustainable businesses, and the path to building those operations comes via technology investment.

Ah, there's the rub. In keeping with our football metaphors, one way to push the ball (sustainable operations) downfield in bigger chucks of yardage is investing in talent, perhaps better draft choices and/or free agents (digital technologies), as well as a winning culture. Any football coach knows a bad locker room environment can ruin even the best laid game plan.

While many people tend to focus on the politics of net-zero, particularly in the West, where climate change action is prominent on political advertisements, process engineers have a much more productive role to play in managing carbon emissions versus politicians or even company executives. That's because we're not going to make a difference in climate change based on promises, but on action, as Emerson's Train pointed out. The action needed is investment in digital technology and expertise. ∞

LEN VERMILLION
Editor-in-Chief
lvermillion@endeavorb2b.com

"From plastics recycling to carbon capture to, yes, even beer brewing, experts representing many multifaceted industries showed examples where the star quarterback of their business' sustainability efforts was the automated control system."

Tomorrow's process automation: Open, democratized and empowering

MICHAEL MARTINEZ
Global Control Systems Leader
Schneider Electric
www.se.com

IN a recent survey designed to gauge the process industry's progress on its digital transformation (DX) journey, the vast majority of respondents indicated that such initiatives would have a high (60%) or moderate (36%) impact on their organizations' operations in the next two or three years. Also, with a new urgency instilled by the COVID-19 pandemic, more than half of respondents (51%) had already begun scaling DX across multiple facilities and business functions. (For more details on the study, see QR code that accompanies this article.)

To better understand the effects that such rising tides in user sentiment —and technological capabilities—portend for the distributed control systems (DCSs) at the heart of most process manufacturer's operations, Control caught up with Michael Martinez, global distributed control systems leader for Schneider Automation.

Q: What dynamics underly users' changing expectations of their DCSs

A: The DCSs that industry has become accustomed to using today were all built with core expectations of safe and predictably reliable control of industrial processes. Tightly integrated systems performed consistently, but that integration also limited the ability to nimbly respond to changing business conditions or smoothly take advantage of new capabilities. Users optimized plants for profitable operations as best they could, but today's envelope is more complex, and the need for "responsible profitability" involves optimization against additional constraints and measures of success, including sustainability and other ESG metrics.

Q: Over the past several years, we've seen the user community become more vocal about the need for greater system openness, flexibility and the ability to accommodate new digital ecosystem solutions such as those epitomized by the Industrial IoT. The NAMUR Open Architecture vision and the work of the Open Process Automation Forum also come to mind. How do you expect that these movements will be reflected in next-generation automation systems?

A: When we at Schneider Electric talk about the future of automation, we see it characterized by three key attributes: it's open, it's democratized, and it's empowering. These three words set the framework for what we see as the future.

Open means different things to different people and organizations, but for us its core meaning is an open automation platform that is entirely independent of the hardware on which it runs. It's more than just a decoupling of hardware and software, it also means software applications from multiple suppliers can communicate and work together on hardware from an entirely different set of technology suppliers. It's a level of independence that's more far-reaching than many of our competitors are thinking about.

In the marketplace, we see suppliers acting on three different visions of open, the first of which has to do primarily with data and communications: we all speak OPC UA, for example, so we can all communicate and share data, we can all manipulate that data and act upon it. The second vision more closely resembles the Apple ecosystem, in that all my stuff seamlessly works with all my other stuff, as long as they're all Apple stuff.

We subscribe more closely to what I would call the Android version of open, in that there's a commonly defined operating kernel, or runtime execution engine, that can run on computing hardware in a range of form factors from a variety of suppliers. This runtime, in turn, enables software from a variety of suppliers—the apps that run on your Android phone, to extend the metaphor—to run together on that hardware, sharing data and interoperating with one another. One tangible example of this third sort of openness is UniversalAutomation.org, which provides just that sort of runtimel for real-time automation systems and can enable the sort of reference architecture described in the Open Process Automation Forum's vision. More than 35 organizations already have joined UniversalAutomation.org, and we believe their model will shape the future of process automation systems. This model is also democratized in that technology providers compete on an equal footing, and users can mix and match best-in-breed applications for different functions.

Q: That explains open and democratized, but what about that third characteristic "empowering"? Something tells me you mean more than just more powerful systems than we had in the past.

A: Yes, when we say empowering, it's much more about the people and organizations who are charged with the configuration and maintenance of these systems. If we go back to those first two visions of "open" that I described, with a universal communications language among systems or a closed ecosystem of components from one supplier that plug and play together, each system still has its own configuration tools and nuances that you have to understand and master. Even more confounding, the constant reconfigurations of organizations often find them stuck with a heterogeneous mix of systems from different suppliers, each with its own unique tools and methodologies. That's a current skills-management nightmare that only promises to get worse as experienced personnel retire and companies struggle to replace them.

But with the UniversalAutomation.org vision, the runtime is consistent from one supplier to the next, and only the hardware itself varies. On the one hand, this allows you far greater flexibility from a supply-chain perspective to source hardware components from a broader ranger of sources, increasing the likelihood of both availability and proximity, compared with a single-supplier approach. And if a new instrument or new networking technology is developed, every system supplier doesn't need to take a year-and-a-half to embed it in their systems. Rather, it's a relatively simple test that this universal automation runtime will run on that hardware, and users can add that new technology to their systems almost immediately.

Q: How has the user community responded to this future vision thus far?

A: When we sit down to talk with our customers about digital transformation, about what the future holds and what success would look like, at the end of the day it all comes down to the fact they've only got so many people to do so much.

They've made investments in technologies like advanced process control (APC) and other types of high-level analytics, even machine learning and artificial intelligence in some instances, but they can't leverage it because they're spending in some instances up to 80% of their time managing the technology, managing its lifecycle. Operator consoles, for example, are often based on commercial off the shelf (COTS) workstation and server technologies and they only get five to seven years of use out of them. It's not something we did wrong, but it's the technology that was available and we've chosen as an industry. And even if the plant only gets a planned shutdown once every five years; all their time is spent planning for that next turnaround. They're spending all their time supporting the technology, not figuring out how to get the most out of their APC application.

This brings us back around to responsible profitability, in that in order to accomplish those higher-level objectives, to drive sustainability and real-time energy management, you have to have the mental space and the human bandwidth to focus on them. Right now, the more things we add to the equation, the more we make it more complex, the greater burden we're putting on the process engineer. In many cases they're only able to maintain the status quo.

We as an industry are responsible for binding these things together, and now that we can unbundle them, now that we can start to take full advantage of the automated tools and methodologies developed by our counterparts in the IT world, we can finally let our people do what they're good at and what we, as a society, need for them to do. ∞

For more information on the current state and future automation needs of the global process industries, follow this QR code to download your copy of "Taking Control of Digital Transformation."

Emerson Exchange goes fast forward

First in-person event in three years draws 2,500 attendees to more than 300 sessions in Texas

JUST as necessity is the mother of invention, innovation didn't stop during the COVID-19 pandemic. It was simply redirected by the essential process industries to enable remote work, accelerating digitalization and increased sustainability. This resilient spirit was demonstrated by close to 2,500 visitors, who attended more than 300 technical sessions and dozens of other presentations and exhibits at Emerson Exchange Americas 2022 on Oct. 24-28 at the Gaylord Texas in Grapevine, near Dallas.

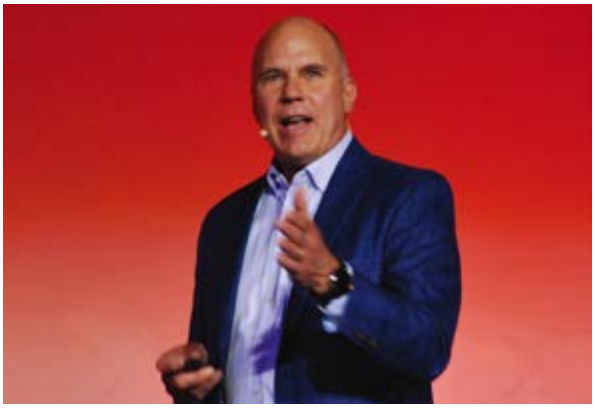
"What our operations did was critical, but our personal connections to the outside world came through the Internet," said Mark Bulanda, executive president, Emerson Automation Solutions, during his keynote address kicking off the event. "Data became accessible anywhere and at any time. Technology helped companies adapt in ways and at a pace we wouldn't have imagined."

While most industries were affected by COVID-19, Bulanda reported the biggest impact was in life sciences and pharmaceuticals, which streamlined lifesaving vaccine development from the previous record of four years to just one year, and ramped up and digitalized global production to deliver vaccines and save lives worldwide.

While companies were fighting for business sustainability due to COVID-19, Bulanda added the rest of the world refocused on another priority—decarbonization. "It's become a generational imperative," said Bulanda. "We drive innovation to make the world healthier, safer, smarter and more sustainable—and our Plantweb ecosystem is the most complete portfolio of solutions for achieving these goals, while the addition of AspenTech deepens our ability to provide asset optimization at all levels."

Mike Train, newly minted chief sustainability officer at Emerson, added that its working towards net-zero sustainability—halving greenhouse gas (GHG) emissions every decade—within its organization, as well as helping customers decarbonize with Emerson technologies, and collaborating academic, industry and government groups. "Emerson has tremendous global reach," said Train. "We can bring to these dialogues our focus and at-scale examples of solutions. Energy efficiency is the best opportunity for sustainable use of resources. Automation professionals know how these things run. We have the tools and expertise. We can demonstrate progress."

Train reported that Emerson is conducting "treasure hunts" conducted at its facilities, where teams search for energy inefficiencies, some resulting in 15% improvements. He added that new programs are relying on electrification of processes, using more natural gas, and pulling hydrogen programs and solar campaigns into the mix.



"We drive innovation to make the world healthier, safer, smarter and more sustainable," said Mark Bulanda, executive president, Emerson Automation Solutions, during his opening keynote at Emerson Exchange Americas 2022 on Oct. 24 in Texas.

Best-in-conference awards

Of the 300 live sessions delivered at the event, just 16 were nominated as finalists by Emerson Exchange 2022's board of directors for its Best-in-Conference awards. The five winners announced at the event's closing lunch were:

- "Fisher Control Valve—Reducing Maintenance Spend via Control Valve Upgrades at K+S," which was presented by Michael Holm of K+S Potash Canada, Duane Lunde of Spartan Controls and Nolan Vollstedt of Emerson.
- "Bringing Rosemount and Micro Motion together to improve brewing at New Belgium," which was presented by Matthew Gilliland of New Belgium Brewing, and Brent Pankonien and Bobby Seal, both of Emerson.
- "Transfer Assistant: Helping an Operator in a manual-Only World," which was presented by Jim Coleman of Savannah River Mission Completion (SRMC).
- "SoCalGas Hydrogen Innovation Experience Achieves Goals of Decarbonization & Digitalization," which was presented by Jennifer Medina of Southern California Gas Co. (SGC), and Brian Burkowsky and Luis Martin Del Campo, both of Caltrol.
- "Shell's Unique Approach to Alarm Management at a Major Greenfield Site," which was presented by Sandeep Pampattiwar of Shell Polymers, Pennsylvania Chemicals Project, and Darwin Logerot and Carlos Pereia, both of Emerson.

For full coverage, visit www.controlglobal.com/events/emerson-users-exchange-2022/article/21436424/emerson-automation-solutions-emerson-exchange-americas-2022

THREE INTRINSIC VALUES: ACCURACY, RELIABILITY, AND EASE OF USE.
THE 6X®. OUT NOW!

Admittedly, at first glance, you can't tell what's inside the new VEGAPULS 6X radar sensor: A high-precision level instrument that doesn't care if its measuring liquids or bulk solids. Only its color gives you a hint that it's going to be great to use.

VEGA. HOME OF VALUES.

GET TO KNOW THE 6X®
www.vega.com/radar

VEGA

Valmet buys NovaTech's process business

Finland-based Valmet Oyj (www.valmet.com) reported Nov. 9 that it's agreed to buy U.S.-based NovaTech Automation's (www.novatechautomation.com) Process Solutions business. Terms of the deal weren't disclosed, but its earliest expected completion is Jan. 1, 2023.

NovaTech's Process Solutions business specializes in process control and optimization solutions for batch, continuous and hybrid processes. It has a turnover of approximately $18 million and employs more than 90 people in the U.S. and the Benelux countries.

Valmet reports that acquiring NovaTech is in line with its strategy, and will further strengthen its recurring stable automation business with a reliable, batch, distributed control system (DCS). It also expands Valmet's automation systems business footprint in the U.S., particularly in new industries, including food and beverage, pharmaceuticals, and chemical products.

"NovaTech's process solutions complement Valmet's automation offerings and industry reach. It brings synergy and opens the opportunity to serve both companies' current and future process automation customers with a wider offering," says Toni Saarnio, VP of strategy and business development at Valmet's Automation Systems division. "Together, we'll continue to strive to fulfill our vision of becoming the global champion in serving our customers. We look forward to welcoming our new colleagues from NovaTech to Valmet."

NovaTech's Process Solutions business will transition to Valmet, including employees, technologies and customer agreements. The two organizations report they'll work together over the coming months to ensure a smooth transition. The acquired business will be integrated with Valmet's Automation Systems business line.

"Valmet is an industry leader in automation systems and process control. Their investment in research and development, direct-to-customer service model, and their global footprint make them an ideal steward of the NovaTech Automation Process offering," says Conrad Oakey, CEO at NovaTech Automation. "I know our customers and employees will benefit from their expertise and technologies." ∞

SIGNALS AND INDICATORS

- **GE Digital** (www.ge.com/digital) launched Oct. 20 its latest iFix and Cimplicity software, which is its flagship HMI/SCADA applications that's reportedly used by more than 20,000 companies worldwide. As part of the Proficy software portfolio, iFix 2023 and Cimplicity 2023 have a web-based user interface (UI), no-code/low-code environment, and new MQTT bridge to increase efficiency and accelerate development.
- Industrial thermal systems manufacturer **Watlow** (www.watlow.com) reported Nov. 7 that it's acquired **Eurotherm** (www.eurotherm.com) from **Schneider Electric Co.** (www.se.com). Terms of the purchase were not disclosed. Eurotherm provides temperature, power and process control, measurement and data management equipment, systems, software and services.
- **CXV Global** (cxvglobal.com), an alliance comprised of European- and U.S.-based **Crest Solutions, Xyntek Inc.** and **VistaLink**, reported Oct. 12 that it's combining the three businesses under common ownership with **Panacea Technologies Inc.** (www.panaceatech.com), a CSIA-member system integrator in Montgomeryville, Pa., near Philadelphia. The transaction creates a provider of automation and digitization solutions that can optimize life sciences organizations' operations worldwide.
- **ODVA** (www.odva.org) announced Nov. 8 that conformance testing is now available for EtherNet/IP network-enabled devices that communicate over the Ethernet-APL physical layer. Conformance testing verifies Ethernet-APL physical layer functionality by checking that different port types properly adhere to relevant specifications. The EtherNet/IP communication network functionality is also confirmed as a part of this process.
- **The OPC Foundation** (OPCF, www.opcfoundation.org) announced Nov. 8 that its Field Level Communications (FLC) Initiative has released the first set of OPC UA Field eXchange (UAFX) specifications, which lay the groundwork for using OPC UA for open, secure communications at the field level. These UAFX specifications passed in-depth OPCF member reviews and prototyping to ensure their implementations maintain cross-vendor interoperability.

EVERYDAY CYBERSECURITY

BY JIM MONTAGUE

Effective cybersecurity must be a routine part of process operations—even as new defenses arrive daily

JUST like brushing and flossing, putting on pants, taking a walk or grabbing a cup of coffee, cybersecurity must become routine. It must be a familiar, everyday, even comforting activity to be effective—just as eternal vigilance is the well-known price of freedom.

Locks, firewalls or other barriers that get bolted on in a one-time panic won't stay secure for long—no matter how much everyone wants a silver bullet or black box they can install and forget about. As always, there's no "set it and forget it" when it comes to cybersecurity.

Think through for best fit

"To me, cybersecurity is nothing more than specialized risk of dealing with computer systems. A lot of software and devices get put in for the sake of security, but not much thought goes into why and what the organization is trying accomplish," says Alan Raveling, operational technology (OT) architect at Interstates (www.interstates.com) in Sioux Center, Iowa, a certified member on the Control System Integrators Association (CSIA, www.controlsys.org). "We talk about reducing and mitigating risk to tolerable levels, but too often, organizations implement cybersecurity just to show how much they can put in, and they're proud of it. However, when we ask how much it reduces risk or how much money it saves, it's tough for them to quantify. Many company boards and accountants say 'we have to do something about cybersecurity,' but it's difficult later to say enough was done because no one gets in trouble for doing more. This is what leads to just adding more cybersecurity without asking what areas really need it."

Raveling reports that some users also address cybersecurity for applications and systems using Microsoft Windows, initiate endpoint protection and antivirus software, and users' behavior. But at the same time, they don't address their 15-year-old controllers that are 10 revisions behind on their firmware. "Windows does have many vulnerabilities, but it still gets too much attention, while there's not enough focus on plant-floor equipment, especially safety devices that may be linked to a network," explains Raveling. "There's also more potential danger because the number of network connections is increasing so fast, and that means increasing exposure and points for potential cyber-attacks.

Raveling has worked on several cybersecurity projects at Interstates in which the challenge was getting clients to calculate and quantify the risks they faced. This was needed before they could talk about what cybersecurity measures made the most

sense given their limited budgets. He adds it's still helpful to think about cybersecurity in the same way as process safety.

"As process hazards analyses (PHA) play out in a facility, the same process can be used for security," says Raveling. "So, when we're identifying where dangers exist, it could be an ammonia tank or a contractor using a virtual private network (VPN) portal. We've done this exercise with engineers at several clients, and it helps them learn to be more receptive to cybersecurity. Many of them aren't cybersecurity savvy, and it can be hard to translate information technology (IT) and cybersecurity concepts that can impact their processes."

Software saves mining labor

Even as network links, vulnerabilities and cyber-threats multiply, there are some tools that can streamline many cybersecurity tasks. The trick to success and security is combining them with forethought, awareness, training and follow-up.

For instance, to protect its laptops, devices and mining system endpoints worldwide, Orica Ltd. (www.orica.com) previously used antivirus software, but CISO Sean Lasinker reports it was complex to support, inefficient and drained resources because it had to be investigated and resolved manually when a new cyber-risk was detected. Endpoint detection, protection and response were basic and slow, and offered minimal visibility and limited threat-hunting. The company supplies explosives, blasting systems, mining chemicals, geotechnical monitoring, digital solutions and services. Because it's at the forefront of R&D in new mining and blasting technologies, Orica must ensure that related data is safeguarded to protect intellectual property.

"Ensuring our operational technology is used correctly, and we're prepared to respond to a cyberattack is of the utmost importance," says Lasinker. "The goal is next-generation, endpoint security as part of our overall security strategy."

Orica settled on CrowdStrike (www.crowdstrike.com) due to ease of deployment, ongoing management, and seamless integration with existing security and business systems, such as its web-secure gateways and an email security solution. It deployed CrowdStrike's FalconX automated threat detection in its IT environment, which must protect digital systems and IIoT products sold to customers, its own business systems hosted on AWS and Azure cloud-computing services, and OT and manufacturing systems that support its global plants. This environment comprises 8,700 endpoints at Orica's sites worldwide, including its engineers working at clients' mining facilities. The company also implemented Falcon OverWatch to manage threat hunting, and CrowdsStrike's Incident Response and Advisory Service that lets it prepare to react quickly to any incidents and assess and thwart potential cyber-threats.

"We've already used the CrowdStrike Incident Response and Advisory Service twice to investigate suspected security incidents that were thankfully false positives," explained Lasinker. "Speed of response and resolution were impressive, but more importantly gave us confidence and reassurance. The standout feature of CrowdStrike is its single-pane-of-glass visibility of endpoint security. As a security expert, having that information at my fingertips in real time and being able to act at the click of a button saves lots of time. With the way CrowdStrike is deployed across Orica, we know we can rely on the accuracy and validity of our data."

Lasinker reports another CrowdStrike highlight is its ability to isolate multiple hosts at the same time. It can highlight several endpoints with specific compromise indicators and act swiftly. "CrowdStrike enables us to quickly spot live incidents, gain greater visibility and discover unknown services, which is extremely efficient," adds Lasinker. For example, CrowdStrike helped Orica deal with the 2021 Log4Shell threat with no impact. This was a software vulnerability in the Java logging framework, involving arbitrary code execution that affected multiple global organizations.

Following its deployment, Orica evaluated CrowdStike's and found that during three years, it's expected to save more than $1.5 million Australian, pay for itself in 16.5 months, and deliver a 115% return on investment (ROI). In addition, CrowdStrike's real-time response and remediation virtually eliminated the three weeks it used to take to recover and rebuild devices for remote workers. Finally, CrowdStrike also reduces the workload of the

HOW TO STOP SPEAR PHISHING

The most popular path for malware and cyber-attacks is still Internet links delivered via email and social media formats. This makes it crucial for all organizations to train and retrain personnel to recognize possibly spurious messages and links by checking for authentic sender addresses before clicking on any links. There are many online guides to prevent spear phishing, such as the five-page "Capacity enhancement guide—counter-phishing recommendations for federal agencies" by the U.S. Dept. of Homeland Security's Cybersecurity & Infrastructure Security Agency (www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Counter-Phishing_Recommendations_for_Federal_Agencies_1_0.pdf). Its recommendations include:

- Secure email gateways by deploying email filters and sandboxes or detonation chambers.
- Protect outbound web-browsing by blocking known-malicious sites and top-level domains.
- Prevent specific file types from leaving the network.
- Harden user endpoints by employing multi-factor authentication and securing browsers.
- Protect endpoints blocking malicious macros by default, and deploying antivirus software and host-based, intrusion-detection and prevention systems.

small team that manages Orica's global security 24/7, for example, by reducing the four hours previously required to triage an incident down to 10 minutes.

"As a CISO, there are three aspects of cybersecurity we need to be good at: patching and vulnerability management, regular backups and testing of those backups, and endpoint security. CrowdStrike handles the latter across Orica's whole enterprise."

Cope with change—protect PLCs

Beyond simply multiplying, cyber-probes, -intrusions and -attacks are growing more sophisticated, and requiring users to protect entire systems instead of single access points.

"Cyber-criminals used to focus on taking control of a PLC, but now we're seeing them attempt to gain access to the entire network through PLCs. That access can be debilitating to a plant or public utility," says Keith Mandachit, PE, engineering manager at Huffman Engineering Inc. (huffmaneng.com), a CSIA-certified system integrator in Lincoln, Neb. "These hackers attempt to exploit the network through engineering workstations, and any disparity between your IT and OT operations can open a window for an attack we've seen called 'Evil PLC attack.1' "

To handle the everchanging risk posed by cyber-threats, Mandachit reports that users must constantly and consistently educate and communicate among their staffs, contractors and clients. "Looking outside your organization to learn about real-life examples and passing that knowledge to your stakeholders is imperative. The stakes are high as these attacks grow more sophisticated, so it's not just about controlling your internal processes," he explains. "Limiting access points is key to defending against attackers weaponizing PLCs. This includes managing the risk of allowing a third party's external team to connect a laptop to your network."

Mandachit reports that cybersecurity mitigation strategies should include:

- Conduct a cybersecurity risk assessment (RA) and asset inventory to determine risk tolerance and budgetary plan;
- Communicate with all stakeholders, such as operators, IT, automation engineers and management;
- Limit access to PLCs with policies and procedures that control access, and allow only approved and vetted personnel access to applicable systems;
- Monitor network traffic and analyze it for unusual events, such as uploading and downloading PLCs with automated notifications;
- Segment networks to reduce the risk of an attack infecting overall networks; and
- Stay current with patches and other software updates.

"Reputable system integrators will regularly monitor and communicate updates with customers," adds Mandachit. "These strategies used in conjunction can provide a unified front across your organization to help combat attacks."

Armor up during upgrades

One of the best ways to normalize and improve cybersecurity is to make it part of planned maintenance and upgrades. For example, to clean Silicon Valley's wastewater, the San José-Santa Clara Regional Wastewater Facility (www.sanjoseca.gov/your-government/environment/water-utilities/regional-wastewater-facility) operates the largest, advanced treatment facility on the West Coast, and processes an average of 110 million gallons of wastewater per day (mgd), with a capacity of up to 167 mgd.

Because the region is a prime target for cyber-attacks, the city's leadership knew it needed to keep updating the plant's cybersecurity, and recently enlisted ABB (www.abb.com) to modernize its waste-

FIVE FACES AND ACTIVITIES OF CYBERSECURITY

Here are the five primary elements required for an effective cybersecurity program, according to SANS Institute (www.sans.edu):

- **Operations technology (OT) incident response**—includes operations-informed incident response (IR) plan with focused system integrity and recover capabilities during an attack, as well as exercises to reinforce risk scenarios and use cases tailored to the industrial control system (ICS) environment.
- **Defensible architecture**—consists of architectures that support visibility, log collection, asset identification, segmentation, industrial demilitarized zones (DMZ) and process communication enforcement.
- **OT network monitoring**—employs continuous network monitoring of the ICS environment with protocol-aware toolsets and system-of-systems interaction analysis to inform operations of potential risks to controls.
- **Remote access**—identifies and inventories all remote access points and allowed destination environments, on-demand access and multi-factor authentication (MFA) where possible, and jump-host environments to control and monitoring points in secure segments.

- **Risk-based vulnerability management**—understands existing cyber-digital controls and device-operating conditions that aid in risk-based vulnerability management decisions to patch vulnerabilities, mitigate impacts, and monitor for possible exploitations.

Here are the five essential activities from SANS that are needed to establish the five elements and carry out a successful cybersecurity program:

- Identify the most important sites, such as safety, health, business, environment, national security, etc.—*know yourself.*
- Align with the risk and threat scenarios that can impact your business—*what will a cyber-attack on you look like?*
- Provide the staffing levels and training needed to deliver the necessary tools, technologies and capabilities to your practitioners—*people will save the day.*
- Develop a prioritized, tactical and strategic plan that's aligned with operations—*what's needed and when to operate through a cyber-attack?*
- Establish essential supplier partnerships for ICS environments—*identify needs and overlapping interests.*

water system, implement a cybersecurity infrastructure, deploy required security controls, apply more than 2,000 security patches, conduct a cybersecurity assessment, and do it all in five days.

Consequently, during one business week, ABB revamped San José-Santa Clara's legacy DCI controllers with its HPC 800 Symphony Plus controllers, installed ABB Ability Cyber Security software, and customized the plant's cybersecurity to protect it from malware and other cyber-threats. The plant implemented ABB Ability's:

- Cybersecurity Updates to ensure the automated deployment of validated Microsoft security updates to system nodes.
- Cyber-Malware Protection to enable automated deployment of validated McAfee updates to the nodes.
- Cybersecurity Backup & Restore to provide a backup solution configured to safely take backups from the DCS.
- Cybersecurity Fingerprint for reports of the current cyber security posture, detect any gaps in protection, and have a baseline for future reference.

The wastewater facility adds that a cyber-attack could lead to significant downtime, which could result in wastewater polluting the local environment. However, with its new cybersecurity controls, the city is confident that the plant has sufficient cybersecurity controls to continue producing clean water and protecting public health. "By implementing solutions to improve efficiency at the wastewater treatment facility, ABB has enabled us to protect the environment, public health and safety of our citizens," says Jerry Au, network engineer at City of San José Wastewater.

Robert Putman, global manager of cybersecurity products and services in ABB Group's Process Automation business area and Energy division, adds that it defines two cybersecurity macrosegments. The first is security for its System 800xA distributed control system (DCS) and other products, and making sure its software, connectivity and reference architecture have enough cybersecurity to make their environment defensible. Once this is achieved, the second macrosegment is adding whatever added cybersecurity software or mechanisms are needed, but weren't baked-in earlier.

"Commercial cybersecurity has three procedural pillars," says Putman. "The first is identifying and assessing risks, and deploying antivirus and whitelisting capabilities; adding backup and restore soft-

CONTROLS FOR OT CYBERSECURITY

Operations technology (OT) cybersecurity is finally getting more of the attention it deserves, but Dragos Inc. (www.dragos.com) reports that executive buy-in and five control policies/procedures are needed for a successful cybersecurity program. To gain executive understanding and support, cybersecurity supporters should present them with real-world examples of cyber-attack impacts and how much they cost, research prior incidents including U.S. Security and Exchange Commission (SEC) filings by firms that were impacted, and explain the difference between information technology (IT) and operations technology (OT) and stress that they must support OT cybersecurity as well as IT. The five controls for cybersecurity are:

- Create a dedicated **industrial control system (ICS)-specific incident response plan** that addresses OT device types, communication protocols, procedures, tools and languages. Include points of contact, such as employees with cybersecurity skills in each facility, and add thought-out steps for specific cyber-scenarios at each location. Consider performing tabletop exercises to test and improve response plans.

- Establish a **defensible architecture** by hardening the environment—remove extraneous OT network access points, maintain strong policy control at IT/OT interface points, and mitigate high-risk vulnerabilities. Invest in training people in skills for adapting to new vulnerabilities and cyber-threats.
- Maintain **visibility and monitoring** with an inventory of assets. Map vulnerabilities against assets and mitigation plants, actively monitor network traffic for cyber-threats, and respond as needed. Visibility of assets validates implemented security, and threat detection enables scaling as networks grow.
- Implement **multi-factor authentication** (MFA) across OT's systems for an extra, low-cost layer of cybersecurity. If MFA isn't possible, consider using a jumphost with focused monitoring to manage devices in a separate security zone. Focus on connections in and out of a network, rather than links within the network.
- Perform **key vulnerability management** by maintaining timely awareness of vulnerabilities that apply to the environment with correct, updated information and risk ratings. Also, maintain alternative mitigation strategies to minimize exposures.

ware such as Quest, Acronis and Veeam; and performing orchestration of patch updates for HMIs and engineering workstations. We can do all three with ABB Cybersecurity Workplace (CSWP), Version 2.0, released earlier this year."

ABB is also working with Nozomi Networks and Forescout to develop asset inventory software to help users prepare for their cybersecurity programs. This package combines network host information and combines it with node-level detail collected from the DCS itself. The combined network and DCS node details are then summarized in the CSWP 2.0 web-based frontend.

"This approach lets users view node-level details and scale up to a fleetwide summary," explains Putman. "For example, one chemical manufacturer has 135 System 800xAs across 2.5 square miles with approximately 2,400 nodes, so when an antivirus event fires, they need to know 'where' details and coordinate a response. We can deliver this monitoring and automate patch updates, so operators don't have to deploy them manually, node by node."

Putman reports the second cybersecurity pillar is maintenance and service, and the challenge of having internal staff with the capacity and expertise to do it, or contracting with ABB or a similar provider. "The patch update service enables operators to orchestrate validated updates securely downloaded from a remote repository or uploaded to a local directory," says Putman. "How the validated patch is made available depends on the customer's policy on remote connectivity."

The third pillar is operations and data, and securing them as OT and IT converge. "This is our highest potential growth area with IT coming into OT environments," adds Putman. "The automation environment is largely deterministic, and can be characterized by 'what must always work' and 'what must never happen.' Passive network analysis provides good information, and is easy to implement, but falls short of providing actionable, deterministic details needed to prioritize and mitigate process disruption. We can do better with the combined approach of automation system event analysis and passive network insights."

Converge and coordinate

Just as cooperation between OT and IT can aid digitalization, it's also one of the best ways to achieve cybersecurity.

"It's always a challenge to get the IT and OT departments to work together. Both have important initiatives to accomplish but finding an effective balance for the organization can be difficult," says Huffman's Mandrachit. "Vulnerabilities can be exposed when the IT and OT departments can't find the middle ground between security risk and production. If OT won't budge on allowing the latest security updates, that exposes them to the risk of the newest cyber-attacks. If IT doesn't recognize the importance of a continuous schedule, production goals can't be met. These two have to find a middle ground, and a certified control system integrator, who understands the importance of both areas when it comes to cybersecurity, can often stand in the gap and bring them together."

However, Interstates' Raveling cautions that translating between IT and OT must be a two-way street, with OT communicating its concerns back to IT, especially when operations has to manage software patches and reboots.

"If OT is required to run some antivirus software that could interact with their plant-floor SCADA system, they must get IT to help make sure it won't stop that SCADA system." says Raveling. "There are many cybersecurity guides and prescriptive documents, but many users

don't know they exist. Also, many engineers had bad experiences with IT, so they're hesitant to try again. Once again, Interstates sometimes mediates in these situations, and tries to get OT to give IT a second chance. OT can review what IT is planning, and maybe tweak their approach."

System integrators can further reassure OT by demonstrating that digitalization and IT technologies won't break their processes, and that the risk of unplanned downtime is small and manageable. "We worked with a consumer packaged goods (CPG) client on the IT side of their network, whose corporate level switched antivirus products, and wanted to do the same on their OT side. The plant-floor people were worried about performance and compatibility, and how the new antivirus software would impact operations," says Raveling. "Consequently, Interstates engaged them in a small, pre-pilot project, set up an independent testing environment, and copied their HMIs and production lines. Next, we collected metrics, put the project under a regular load, and found that the new antivirus on their HMIs would affect them the same or less than the antivirus they were using before. This pre-pilot gave OT the confidence to pilot their new Crowdstrike antivirus software on several lines and plants. Those tests were successful, too, and gave the user even more confidence to implement these protections."

Interstates was involved in all three phases of the CPG client's antivirus effort, including the pre-pilot, pilot and larger implementation. "The biggest hurdle to cybersecurity wasn't the technology. It was giving the stakeholders the assurances they needed to feel good about moving forward," explains Raveling. "Again, this begins with identifying OT's concerns about safety, plant stoppages, quality issues and revenue. Engineers' reputations are typically closely tied to their production lines, and many feel like it's a personal attack if they're not running. Meanwhile, IT often focuses on documentation driven by the CIO, CISO, accountants and board. However, IT often takes on these mandates without enough background on why OT is concerned. Good companies know why OT's concerns exist. Bad companies just push IT mandates forward without taking the time to understand OT's concerns."

To repair these rifts and build bridges between IT and OT, Raveling reports that plant-floor people can form relationships with individuals at or near the same level on the IT side.. "They also need to talk to each other more often than just when they're mad," says Raveling. "If they want to, OT engineers can learn cybersecurity concepts. If not, they'll have to find someone to act on their behalf. Just like with translating, Interstates has been asked by OT people to reframe their concerns into forms that IT can understand. System integrators can also add value by sharing their experiences with other OT clients, and give IT specific examples of bad experiences due to pushing through IT-based mandates without considering OT's concerns. These are much more effective than hypotheticals, and will often cause IT to pause and be more sensitive to the OT side. We want them to engage with each other." ∞

Asset-specific insights to transform service workflows

BRIAN FRETSCHEL
Director, Digital Customer Experience, Emerson
Emerson.com

THE digital transformation of industry doesn't only apply to the real-time control and optimization of industrial processes. It also applies to the documentation, supply chains and context-specific workflows that support industrial assets across their lifecycles—and that includes the instruments, software and systems that make modern automation possible.

To better understand how, when it comes to industrial automation, the digital technology at our disposal can make online retailers' estimated delivery times little more than entry stakes, *Control* caught up with Brian Fretschel, director of digital customer experience for Emerson.

Q: To start things off, perhaps you can outline for our readers the broader MyEmerson platform, and its initial focus on digitalizing and streamlining the engineering and specification processes involved in buying the company's instrumentation products.

A: MyEmerson is the personalized access point to Emerson.com, and it serves as your portal to all the functionality relevant to your individual Emerson products, including as-purchased configurations, sizing calculations and the like. There's also quote and order history, as well as the ability to reorder, validate prices, check lead times and other e-commerce functionalities.

More recently there's been on lot more focus on MySoftware, where you can manage and maintain your software licenses, as well as MyTraining, which is a new functionality around personalized training plans. So, MyEmerson is becoming an increasingly holistic experience across Emerson.com and your engagement with our solutions. But I think our most exciting effort of late has been our MyAssets buildout.

Q: How is the MyAssets offering different than the device-specific engineering and e-commerce information that you already had?

A: At its core, MyAssets provides a comprehensive record of all of the Emerson instruments at a particular customer's site. It contains access to historical information, device timelines, technical documents, certificates, upgrades, spares—a wealth of information specific to the installation and operation of a particular asset.

We hear from customers that not only is it great for troubleshooting problems more quickly, but all of this supporting data can also help keep processes up and running longer. The data it provides can assist in maintenance or obsolescence planning for your next turnaround or outage. A central use case for MyAssets is to reduce the number of trips back and forth from the field. Rather, engineers and technicians on the go always have access to all the information about a particular instrument at their disposal. They can find troubleshooting manuals and guides or reorder anything they might need. That's really been a huge help for customers.

Q: It seems that with the pandemic, the QR codes that seemed to have fallen out of style came roaring back. And beyond restaurant menus, I understand they've also found their place onto millions of Emerson devices in the field, each with a unique, device-specific QR code. What further functionalities do these codes enable when it comes to instrumentation?

A: I agree that the pandemic really reminded us of what a QR code could do, but I think mobile technology had really came a long way as well to make that renaissance possible. It's now much easier to scan a QR code; there's no app to download, it's at people's fingertips. What's really interesting is the level of support, troubleshooting and training you can now get while you're at the device. You can scan the code, watch a quick video on how to do something with a particular instrument, or summon support if you need it. I believe the QR code has really unlocked a new high-water mark for troubleshooting and support while at the device—and that's really exciting.

Q: I imagine you can also start to combine "see what I see" access to remote subject matter experts with the resource access MyAssets brings to the field.

A: Absolutely. You can get a much clearer picture of what's going on with the instrument, how it's installed, what the ambient conditions are like. It really helps from a troubleshooting perspective.

Q: Although MyAsset's first efforts have been focused on instrumentation and other hardware devices, I can't help but think of how important it could be for making sure that software and firmware is properly updated and patched. How is that handled now, and how does Emerson's vision of Boundless Automation that was announced this week at Emerson Exchange impact the delivery of this value proposition in the future?

A: Today, the act of retrieving a download is pretty straightforward. You go to a website, you apply a few filters, you find the file you're looking for, you grab it and go. So, I think in this world of Boundless Automation and all this interconnected data, especially through MyAssets, we're starting to find those use cases of proactively notifying people when there's new firmware revisions or software updates that need to be applied.

We've been thinking a lot about device access and license management and how all that gets controlled, stored and managed. It's all evolving really quickly, and we'll soon be able to see the current firmware on a device and quickly access and install the next firmware upgrade. That used to be a lot of emailing back and forth, searching around on websites. That will soon be more streamlined, with MySoftware and MyAssets working in tandem to be able to deliver that for customers. It's a perfect example of delivering on that vision of the intelligent field integrated seamlessly up into the cloud.

Q: So, what's next? Are there other things your customers are asking for and what's the next high priority for you?

A: One of our next steps is to look at enabling and streamlining the procurement workflow coming out of the field. Why not connect the asset data information to the procurement organization to streamline the procurement process after troubleshooting gets done? MyTraining, too, is new, and we'll continue to build that out, adding troubleshooting primers and support tactics to the experience. There's a lot yet to do; these are just some of the areas to watch out for.

For more information on the MyEmerson suite of capabilities and to register to create your own free account, visit https://www.emerson.com/en-us/automation/digital. ∞

SPECTRUM
CONTROLS
An Allied Motion Company

HART® + Analog for Process with Allen-Bradley Systems

1734 POINT I/O

1769 Compact I/O

HART®
COMMUNICATION PROTOCOL

Analog Input & Output Modules

1734sc-IE2CH	2-Ch Analog+HART Input
1734sc-IE4CH	4-Ch Analog+HART Input
1734sc-OE2CIH	2-Ch Analog+HART Output
1769sc-IF4IH	4-Ch Isolated Analog+HART Input
1769sc-OF4IH	4-Ch Isolated Analog+HART Output
SCX-3000	Connecting Your Asset Management Software to Your HART I/O

spectrum@spectrumcontrols.com
spectrumcontrols.com

Compatible with Allen-Bradley by ROCKWELL AUTOMATION

China's Wanhua Chemical Group

transforms plant into finely tuned testimony to digitalization

Chemical materials producer makes full use of FieldComm Group FOUNDATION Fieldbus, HART and WirelessHART technologies in large-scale operation

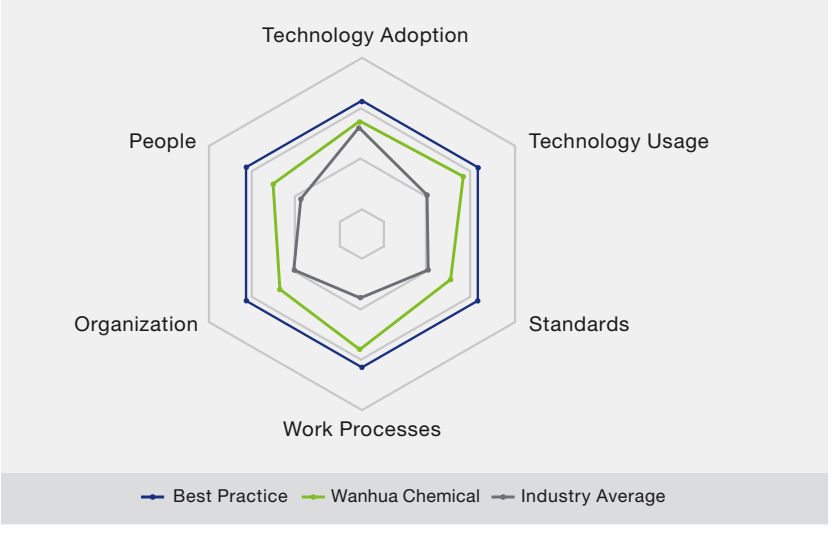
BY LEN VERMILLION

WANHUA Chemical Group is one of the largest chemical product manufacturers in the world. The China-based company serves four main industries: polyurethanes; petrochemicals; fine chemicals, such as high-performance materials and nutritional chemicals; and emerging materials, such as those used in batteries and electronics. Because it serves such fast-moving and growing sectors, maintaining a competitive edge in its operations, and gaining value from its control systems is of the utmost importance. That is why the company turned to FieldComm Group's FOUNDATION Fieldbus, HART and WirelessHART technologies to serve as the centerpiece of its digital transformation.

The company's operations are extensive. In addition to its world-class, highly competitive manufacturing technology for producing manmade chemicals, it boasts complete industry chain manufacturing technology of Nylon-12 and citral, as well as a complete C2/C3/C4 petrochemical industry chain. Wanhua Chemical Group currently has manufacturing bases in Yantai, Ningbo, Zhuhai, Meishan and Fujian, China, as well as locations in more than 10 countries and regions including Europe, Middle East, U.S., Japan and India. But it's the digital transformation of its Wanhua Yantai Industrial Park that has earned it the honor of FieldComm Group's 2022 Plant of the Year.

Wanhua Chemical's Yantai, China, facility has been named FieldComm Group's 2022 Plant of the Year. Source: Wanhua Chemical Group

INTELLIGENT DEVICE REVIEW GAP ANALYSIS CHART



"We have five sites in China and Yantai is the largest," says Lee, Caihua, director of instrumentation for Wanhua Chemical's Yantai Industrial Park, via a translator. "We also have a plant in Europe and other office locations all over the globe."

The installation of FieldComm Group's technologies has been the basis of the plant's improved operations, maintenance and asset productivity in real-time applications. In addition, FieldComm Group's technology has helped the company save tens of millions of dollars in operational costs ranging from reductions in configuration and commissioning times to remote maintenance capabilities.

Instrumentation with FieldComm Group's technologies is prominent throughout the Yantai plant. "Wanhua Chemical's Yantai Industrial Park features about 30 sets of production equipment with a production scale of nearly 500,000 I/O points," says Lee. "Intelligent measuring instruments and valve positioners in the plant make full use of FieldComm Group's FOUNDATION Fieldbus, HART and WirelessHART technology, which operate in up to 180,000 I/O points and account for 96% of the analog instruments and valves."

Wanhua Chemical uses two Emerson AMS Asset Optimizers to cover the total number of points.

Among its four major industries, Wanhua Chemical has installed tens of thousands of FieldComm Group's FOUNDATION Fieldbus and HART instruments and valves in its facilities, according to Wanhua Chemical Group representatives. Among them are:

- Polyurethanes (5,000 FOUNDATION Fieldbus and 30,000 HART)
- Petrochemicals (4,000 FOUNDATION Fieldbus and 56,000 HART)
- Fine chemicals (70,000 HART)
- Emerging materials (15,000 HART)

In Yantai Industrial Park, Wanhua Chemical uses more than 50 sets of Emerson's AMS Device Manager featuring FOUNDATION Fieldbus, HART and WirelessHART. AMS is used for startup and commissioning, online monitoring, predictive maintenance and valve diagnostics.

FieldComm Group's technologies are the basis of the plant's improved operations, maintenance and asset productivity. Source: Wanhua Chemical Group

Adding value and savings to operations

Wanhua Chemical's representatives state there have been numerous value-added benefits to using FieldComm Group's technologies at Yantai Industrial Park. "Intelligent instruments with FOUNDATION Fieldbus and HART can provide valuable health information about themselves, which can be well integrated with control and asset management systems to save time during commissioning and throughout the plant's life," Lee says. "By using FOUNDATION Fieldbus and HART instruments and AMS, [we] reduced commissioning time, and provide more efficient and dependable operations."

Among the value-added benefits, according to Wanhua Chemical:

- Intelligent instruments were configured with FieldComm Group technology, which eliminated the need to go into the field for configuration. The streamlined process saved 60% on time and reduced potential risks to workers in the field.
- Device commissioning was faster and easier, and saved 30% on commissioning time.
- Routine field maintenance was reduced because a "healthy status" can be indicated online;
- With FOUNDATION Fieldbus and HART predictive maintenance implemented, instrument failed alerts and shutdowns were reduced.
- Online valve diagnostics improved plant maintenance.

Configuration costs controlled

Thanks to the 60% reduction in configuration time, Lee says the plant saved an estimated $3 million. In addition to configuring instrumentation from the control room, the company was able to create its own user configuration templates for the same type of instruments.

Meanwhile, bulk transfer user configurations could also be bulk edited in the research and testing phase. The majority of these savings are from bulk/automated configuration of installed devices from predefined templates. This also helps ensure consistency of configuration for similar devices.

Commissioning times cut

With control systems and instrumentation often on the project's critical time path, reductions in commissioning time map directly to faster time to production and

Wanhua Chemical's Yantai Industrial Park is the global company's largest operation. Source: Wanhua Chemical Group

> "FieldComm Group's technology has helped Wanhua Chemical Group save tens of millions of dollars in operational costs ranging from reductions in configuration and commissioning times to remote maintenance capabilities."

associated earnings. The commissioning time reduction resulted in $14 million in savings, according to Lee. Those savings are mainly the result of loop tests that can be done with a HART communicator. Interlock verification further reduced loop checkout time by using HART communicatons. In addition, bulk valve diagnostics and health curve establishment could be performed before startup.

According to Wanhua Chemical's representatives, intelligent commissioning of the instruments enabled the site acceptance test (SAT) period to complete tens of thousands of devices per day. The control system helped engineers identify errors in configuration or in instruments themselves, so they only needed one week to complete their work.

Maintenance gets predictive

Another benefit of FieldComm Group technologies at the Yantai facility is that devices are monitored online, in real-time, so unhealthy devices can be found easily. Routine maintenance frequency was reduced by half, according to Lee.

When it comes to predictive maintenance, Lee indicated that potential shutdown instances caused by failed instruments dropped from 42 in 2017 to only two in 2020.

The plant also reduced debugging and cyclic maintenance time by 80%, while remote access to advanced diagnostic functions help the staff perform pre-maintenance on equipment, according to Wanhua Chemical's instrument department committee.

Smart terminals are connected to the distributed control system (DCS) or safety instrumented system (SIS) via FieldComm Group technology at the plant. The smart terminals can then achieve maximum use of management and control efficiency by using the intelligent equipment management platform.

In addition, maintenance personnel can view the status of individual equipment and conduct in-depth analysis through the management system. Based on this information, mainte-

REAL-TIME MONITORING AT WORK

Wanhua Chemical Group's maintenance personnel conduct real-time monitoring across its multiple locations via remote access. The functions they perform via an intelligent equipment information platform include:

- Real-time alarm monitoring and manual file association. Engineers can get alarm information, causes and treatment suggestions as soon as the alarm occurs.
- Alarm history management and statistical analysis of alarm causes.
- Alarm event filtering, providing a multi-level filtering mechanism to eliminate invalid and useless alarms.
- Improve equipment account management.
- Maintain configuration parameter changes during the life-cycle of the equipment, and provide configuration parameter comparison functions..
- Provide key performance indicator (KPI) reports and customized report functions.
- Provide weekly email notifications, alarm events records and alarm equipment rankings, and guide equipment maintenance.
- Deliver customized reports.

nance engineers can perform pre-maintenance to eliminate hidden dangers before problems occur.

For example, AMS Device Manager reported an alarm from a field device in an acrylic plant. The device is for SIS single-point interlocking. The device was replaced after notifying field engineers to bypass the process. A major hazard was found and resolved immediately, and an unscheduled shutdown was avoided.

Data on the equipment can also be quickly accessed by staff in other locations via industry-standard OPC communications.

"Not only [can] the plant's field instrumentation engineers get the device's internal information, but enterprise-level, full-time instrumentation engineers can get each device's information via Asset Optimizer management platform using OPC," explains John Wang, a China-based technical services engineer for FieldComm Group. "Enterprise instrumentation engineers can comprehensively monitor the fault diagnoses of all smart devices onsite, manage the overall failure rate of all brand instruments onsite, and assess the timely rate of fault elimination at present and for subsequent improvement."

Using the AMS Device Manager system, instrument control engineers can configure field equipment and adjust transmitter ranges. Because the control system is fully compatible with the AMS Device Manager system, the control system can automatically detect equipment status and adjust control strategies accordingly. According to the company, all procedures are transparent.

FOCUS ON INDIA

Each year, FieldComm Group receives fantastic applications for the Plant of the Year award from companies located in India, and in fact two of the recent winners were from India. This year was no exception, as once again there was a great application from SRF, which deserves a special commendation. It's a company that we just might be hearing more about in the future.

SRF is an Indian, international, multi-product industrial group. Its Dahej, Gujarat, facility produces specialty chemicals including technical textiles, relying on more than 40,000 FOUNDATION Fieldbus, HART and WirelessHART devices. In the 1990s, the site embraced the Total Quality Management (TQM) methodology for quality improvement, with FieldComm Group technologies strongly contributing to all TQM phases.

Jagdish Pranami, associate vice president for electrical instrumentation and advanced IoT at the Dahej facility, is responsible for innovative projects, designing concepts, project management and maintenance initiatives as part of SRF's digital transformation journey. A passionate advocate of his team's work, two areas in particular are worth highlighting.

WirelessHART

SRF's WirelessHART technology adoption is upper quartile. Some examples covering process, reliability and safety illustrate the company's TQM methodology of "monitor, analyze, act" being applied to WirelessHART.

- In a trial, four steam traps were monitored using WirelessHART technology and SRF's in-house algorithm. Analysis of the business benefits of these trials resulted in the deployment of WirelessHART technology on 400 steam traps across the facility.
- Another worthy example is WirelessHART monitoring vibrations on four troublesome vacuum pumps, which reduced their historical 16 failures per year down to zero.
- Online monitoring of ethylene and CO_2 gases at remote sites for personnel safety, resulting in a 30% productivity improvement in personnel deployment.

With more than 1,000 WirelessHART devices on 100 WirelessHART gateways connected to the plant's 13 Emerson and Honeywell control systems, WirelessHART technology is delivering business benefits helped by SRF's TQM approach.

HART and SOUL in the organization

Also commendable is SRF's incorporation of FieldComm Group's FOUNDATION Fieldbus, HART and WirelessHART technologies into its organization and personnel development programs. These initiatives include:

- The necessary technology knowledge and skills identified for specific job roles from technicians up to managers.
- A structured training curriculum defined to develop appropriate knowledge and skills from "working knowledge"' to "subject matter expert" according to job roles.
- Incorporation into the SRF Online University of Learning (SOUL), which is SRF's digital platform for learning and development that provides management overview, training metrics and deployment efficiencies.

An annual budget for training ensures that SRF staff can continuously improve TQM initiatives.

There's no doubt we'll hear more in the future from Pranami and SRF on their digital transformation journey with FieldComm Group technologies.

Valve diagnostics are routine

There are several important benefits realized when it comes to valve diagnostics, Lee says.

For key valves:

- Online diagnostic can be performed every week;
- Data analysis can be done every month; and
- Maintenance plans are improved.

For importance valves:

- Online diagnostic can be performed every month;
- Data analysis can be done every other quarter; and
- Maintenance plans are improved.

For general valves:

- Online diagnostic can be based on the valve alert; and
- Data analysis only needs to be done when there is a valve alert.

When all was said and done, Wanhua Chemical Yantai Industrial Park was fully fitted with FieldComm FOUNDATION Fieldbus, HART and WirelessHART instrumentation. Wanhua Chemical's ratings on the "Intelligent Device Review" chart illustrates its technical and organizational adoption of these technologies, so their results should not be a surprise! The business benefits realized have set one of the world's largest producers of chemical products up with a highly competitive operational advantage. ∞

Beware action bias: Sometimes the right thing to do is nothing!

PETE DIFFLEY
Global Partnerships Leader,
Trihedral, A Delta Group Company
VTScada.com

IN a world where change is inevitable and timing is everything, leaders are increasingly under pressure to make fast, strategic decisions in technology and investments. The journey through digital transformation has been a bumpier ride than many anticipated. Sometimes slow adoption rates and poor return on investment have led to industry confusion and a lack of clarity in where to go next. Inflated claims of control algorithms with artificial intelligence or predictive capabilities have only added to the noise. And when larger technology providers rush to acquire these companies in a bid to keep up with the rapid pace of 'cool tech' and present to the public that they are as current as everyone else, expected growth expectations may not be realized.

As a longtime end-user and integrator in the world of automation, Pete Diffley has frequently been asked to provide his thought leadership and guidance to global organizations when it comes to go-to-market strategies and making the right investments in technology. In his role as leader of global partnerships for Trihedral, a Delta Group Company, he's been looking at the challenge facing industry leaders in this arena. *Control* caught up with Diffley to discuss his experiences and to provide some practical advice for those browsing the technology portfolios out there.

Q: In relation to investments in technology, what are some of the reasons that companies jump to what they consider to be the latest trend in technology, only to be underwhelmed by the results?

A: I pondered this myself for some time and was brought around to the notion of action bias. It's covered well in a book I use as a reference from time-to-time, *The Art of Thinking Clearly*, by Rolf Dobelli.

Studies were carried out by researcher Michael Bar-Eli, who evaluated hundreds of penalty shootouts in soccer—football for my friends outside the U.S.! During a penalty kick, the ball typically takes less than 0.3 seconds to travel from the penalty taker to the goalkeeper; not enough time for the keeper to wait and see what trajectory the ball has and adjust accordingly (very similar to a professional baseball player's 0.35 seconds to react to an incoming pitch).

In Bar-Eli's study, he found that one third of the time the ball was kicked to the left, one third to the middle and one third to the right, yet rarely do the keepers remain standing in the middle, regardless of the fact that one in three times the ball landed there. Mostly you will see them diving to save a goal, even in completely the wrong direction, rather than staying where they are. We tend to respond like this because being seen to do something, or "looking active," is considered instinctively to be better—even if it achieves nothing, or results in a poorer outcome.

In relationship to technology, this bias sometimes makes leaders succumb to the latest buzzwords. Solution providers may rush to acquire start-ups or release solutions that then don't live up to expectations. Users and technology providers alike may also think that the well-proven solutions they have invested in are now out of date and should be cast aside.

Q: At the end-user level, doesn't this reinforce a certain level of cynicism towards technology claims?

A: That's right. The muddying of the waters in terms of what to invest in and what to discard is becoming almost like the format wars of the past… remember VHS versus Betamax, CD versus vinyl, MiniDisc versus Digital Compact Cassette?

Claims by companies that something is "the new thing" and that "you're all being screwed" need to be taken with a proverbial pinch of salt. So should claims of "unlimited" when it comes to licensing. Some systems have significant performance limitations that are reached way sooner than expected, forcing end users to purchase more and more "unlimited" licenses and/or hardware to reach the

performance that other systems can more easily provide.

Q: You recently returned from a major tradeshow where certain smart technology was showcased to an otherwise conservative industry. What kind of insights did you gain?

A: Yes. I attended WEFTEC, the Water Environment Federation's Technical Exhibition and Conference in New Orleans—the largest water conference in North America. Water is in the news almost every day now—water scarcity, water quality, water access and water flooding—so this was a great event that was very well attended, bringing tens of thousands of attendees and exhibitors together over three days. I spoke to leaders of organizations both large and small and on both the provider and user sides of the equation to get some perspective on the challenges they and the rest of the water industry were facing.

While overall there was a positive vibe of opportunity and optimism, they also expressed a common frustration that certain perceived industry trends ultimately didn't result in a sustainable solution to end customers or achieve a good ROI. Perhaps some action bias at work? Some leading technology providers were now focusing on their company's core strengths, pushing the proven solutions they are good at, whittling down the number of "difficult to implement, might work solutions" and using a more customer focused, value-driven approach to tackling water challenges.

On my many meetings with start-ups and new-to-market companies, representatives often reported that market penetration and final adoption were a challenge. This seemed to be partly due to collateral damage from unfounded claims of "intelligence" by others. The truly innovative companies and solutions were being confused with the false prophets and go-to market strategies for legitimate players suffered as well.

Q: What advice would you give manufacturers, solution providers and end users regarding innovation adoption?

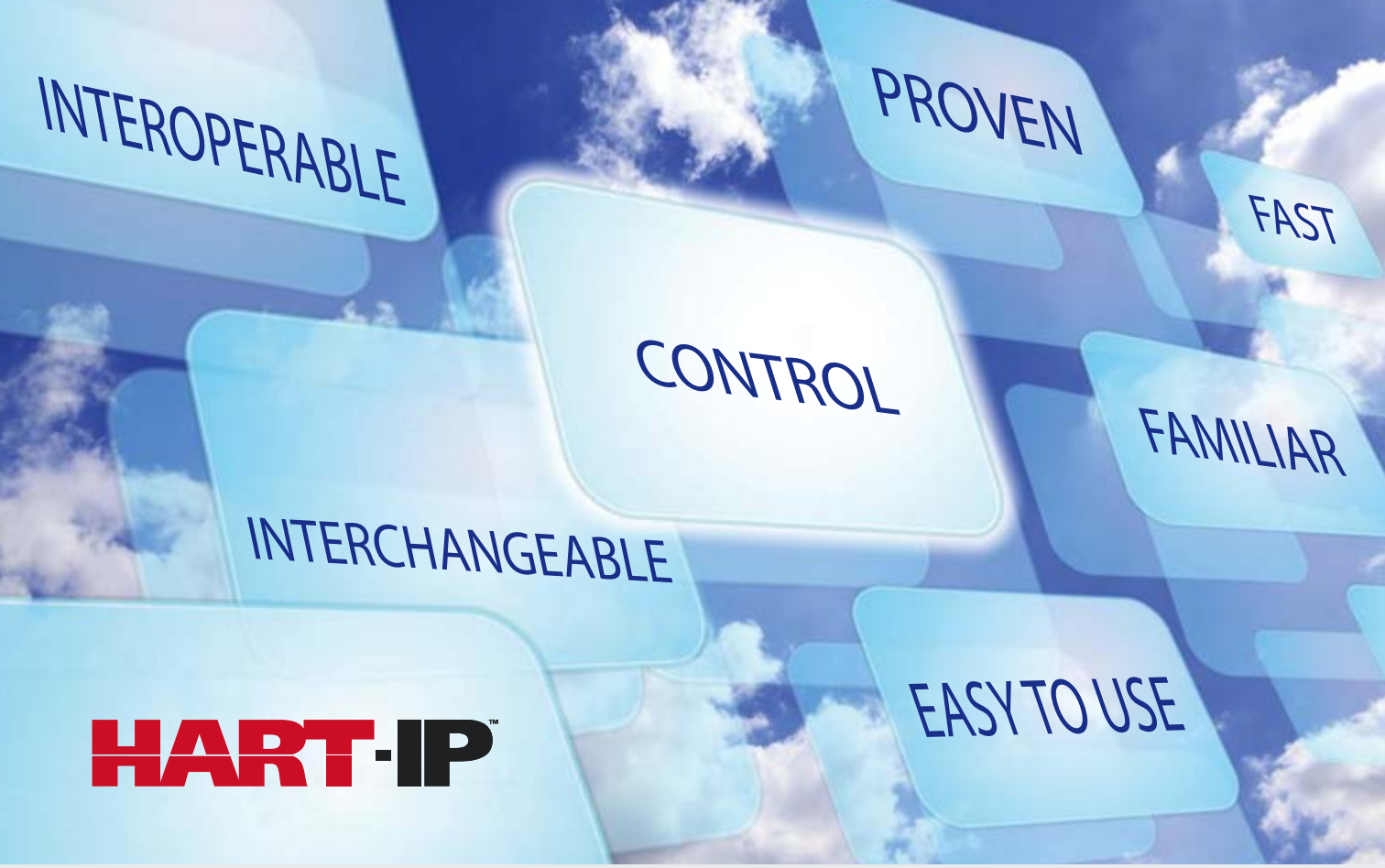
A: The water industry, which I would note is mostly built on public funding, is called critical infrastructure for a reason. It requires solutions that can perform excellently in less-than-ideal conditions. Those that don't measure up to this standard are, or will be, called out. "Cool walls" of logos claiming that Utility X uses this or that solution do not prove their use in mission-critical contexts. Track record helps a lot, but be prepared to show your credentials and prove your claims.

In the case of start-ups, try not to be too disillusioned, you may well have an amazing product or solution that could revolutionize industry. Be prepared to seek out end users or public utilities that will do rigorous, verifiable testing or maybe partner with organizations that will help do that with you.

If your solution has some form of "intelligence," ask yourself if it is using a control algorithm or some form of machine learning before laying any claim to AI. You'll do yourself a favor in the long run if you can clearly and simply differentiate your solution from all the hype.

Finally, to the leaders of large companies not sure if they should follow the latest trend or not, make sure that you are not just succumbing to action bias, that those advising you aren't simply building their own empires, and make sure your own goals are realistic and transparent.

Find out more at VTScada.com ∞



HART-IP®: Future-Proof Evolution

HART technology is evolving for the future of digital process control with secure HART-IP! HART is the mainstay technology of process automation installations and work practices, and has been for decades. HART-IP extends HART technology to IP-enabled plant architectures and is ideally suited for the new intrinsically-safe Ethernet-APL standard. With HART-IP, control is a reality.

Take advantage of simple, secure and flexible HART-IP to achieve faster commissioning, configuration, monitoring, and now control.

Ask your suppliers for instrumentation and systems that support HART-IP.

Find out how you can transition to HART-IP today!

fieldcommgroup.org/technologies/HART-IP/transition

YouTube

FieldComm Group™
Connecting the World of Process Automation

FieldComm Group is a global organization with a mission to develop, manage and promote process automation standards.

Learn more at fieldcommgroup.org

Blocks tackle wires, I/O adds intelligence

Terminal blocks handle stranded cables; I/O components network and process data

IO-LINK SMART FIELD I/O

As the interface between field devices and controllers/information systems, IO-Link master modules from Stride and Murrelektronik handle field I/O signals and diagnostic data from intelligent field devices. These two IO-Link master modules convert IO-Link signals to and from EtherNet/IP, OPC UA and MQTT. Stride IO-Link master converts IO-Link data to EtherNet/IP messages, while Murrelektronik premium module provides the same advantages as a low-cost version, with the added capabilities of OPC and MQTT.

AUTOMATIONDIRECT
www.automationdirect.com/io-link

MULTI-LEVEL SAVES SPACE

TopJob multi-level installation terminals have added pushbutton and hybrid variants to their open-tool slot version, and allow fusing or blade-style disconnects, as well as direct ground connection to the DIN rail. They share accessories with TopJob S, and conductor termination is fast and simple thanks to Push-in Cage Clamp. They're also available as a hybrid of two actuation types, so users can choose the most appropriate. These multi-level terminals also save space, and provide through terminal blocks in the same profile, giving assemblies a clean, seamless look.

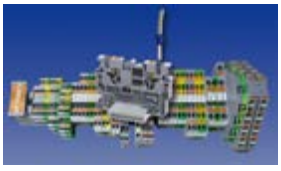
WAGO
800-DIN-RAIL (346-7245); www.wago.com

DIRECT WIRING FOR ALL CONDUCTORS

XTV terminal blocks can accommodate direct insertion of all conductor types, such as ferruled, solid or stranded wires. They're the first products to feature Phoenix Contact's Push-X connection technology, so users only need to apply enough force to unlatch the spring and directly insert any type of wire. To release the conductor, the user presses the orange pushbutton, which is the same with PT. XTV presently includes three cross-sections: 6, 10 and 16 mm^2.

PHOENIX CONTACT
www.phoenixcontact.com/us-push-x

THIN WITH PUSH-IN AND MANY LEVELS



CP Series DIN-rail terminal blocks are 3.5 mm wide for greater wiring density, and feature stainless-steel, push-in springs for toolless wiring and pushbutton release of solid wires and flexible wires with ferrules. They include blocks that are single-level, feed-through, double-level and multiple-level. CPs can be used for grounding, sensing, actuating, marshaling and potential distribution. Other features include a universal jumper system with two-jumper channels and step-down jumpers, standard test plugs and a large marking area.

ALTECH CORP.
https://www.altechcorp.com/CP

INTRINSIC SAFETY IN IP67 FORM FACTORS

EPX Series EtherCAT I/Os provide intrinsic safety (IS) in IP67 form factors by combining EtherCAT Box and IS I/O modules that enable decentralized acquisition of Ex i signals from zones 0/20 and 1/21 to enhance insights in hazardous environments. Interface options are available for HART, NAMUR and FDT/DTM standards. As a robust alternative to IP20 solutions with added enclosures, EPX modules enable reliable data collection, even in hazardous areas where no control cabinet or terminal box can or should be installed.

BECKHOFF AUTOMATION
https://tinyurl.com/2cmnd4n3

DUPLICATES, SPLITS DISCRETE SIGNALS

R90C IO-Link hub from Banner Engineering duplicates and splits discrete signals from legacy devices of nearly any manufacturer, allowing factory operators to use existing machine-sensor equipment to leverage the IIoT. R90C IO-Link hub converts and consolidates signals into an IO-Link data stream that's compatible with other devices, including Banner's IO-Link master or traditional IO-Link systems, enabling signal transmission of large numbers of discrete inputs/outputs to higher-level control systems.

DIGI-KEY ELECTRONICS
www.digikey.com

SWITCH EXPANDS REMOTE I/O APPS

The ioLogik E1200 Series from Moxa is a 16DI, two-port switch for expanding remote Ethernet I/O applications. Its universal controllers and I/O products use Click & Go control logic, which includes patented, active-monitoring technology, and supports a versatile set of operations teachnology (OT) and information technology (IT) protocols to help users easily configure, deploy, and realize industrial Internet of Things (IIoT) applications such as energy monitoring, facility monitoring, and machine OEM applications.

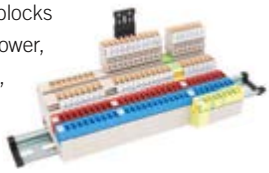
ALLIED ELECTRONICS & AUTOMATION
www.alliedelec.com

I/O CONTROLLER AND BLOCK

Melsec-A Series remote I/O controller from Mitsubishi Electric features several model types that run on the CC-Link communications protocol, including the hard-to-find AJ65FBTA4-16D part. Used for cabinet installations, AJ65FBTA4-16D offers an IP67-rated waterproof and dustproof terminal block with 16 remote DC digital inputs. Also, the I/O block includes two 7/8-inch connectors, eight M12 I/O connectors, and two M12 communication connectors, making it versatile for applications.

MISUMI USA
800-681-7475; https://misumi.info/AJ65FBTA4-16D

FLEXIBLE SENSOR, ACTUATOR CONNECTIVITY



DP2.5SG modular sensor/actuator blocks provide compact, reliable signals, power, and grounding connectivity for two-, three- and four-wire sensors and actuators, while saving up to 75% on panel space. They're 5.08 mm wide, and their modular design is a single-level, pass-through that's mountable on a standard DIN rail for flexible installation. An optional, pluggable terminal block is available for more convenient factory-to-field wiring. Contact materials are tin-plated copper alloy, using push-in design (PID) for reliable wire terminations over an -40 to 115 °C temperature range.

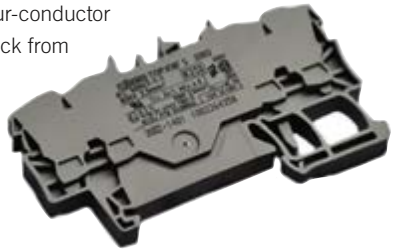
DINKLE INTERNATIONAL
https://www.dinkle.com/en

WIRELESS I/O USES LoRaWAN

Wise-4610P-NA advanced, industrial LoRa/LoRaWAN wireless I/O module offers a variety of I/O combinations. It also has an IP65 enclosure with M12 connectors, solar panel-rechargeable battery and low-power consumption that make it ideal for outdoor deployments, such as smart agriculture and cities. Wise-4610 is independent, so users don't have to worry about the signal coverage of base stations once the gateway is deployed, and can also enjoy the high flexibility for infrastructure applications.

ADVANTECH
www.advantech.com

FOUR-CONDUCTOR AND FEEDTHROUGH



2002-1401 TopJob-S four-conductor feedthrough terminal block from Wago is IEC/EN 60947-7-1 and 800 V, 8 kV and 24A rated. They're also UL 1059 600 V/20 A Group B and C approved. With Push-In Cage Clamp technology, front-entry wiring, 5.2 mm width and DIN-35 rail mountable, this 2002-1401 terminal block is ideal for installations and safety applications with minimal space.

GALCO
www.galco.com

I/O FOR SAFETY

LB Remote I/O system for Zone 2/Div. 2 connects sensors and actuators to the DCS using one standardized fieldbus connection, such as Profibus or Modbus. A wide range of single- and multi-channel I/O modules is available. With up to eight channels per I/O module, LB's modules are plugged into a backplane, while the energy-saving power management system and low power dissipation allow maximum packing density. LB I/O modules can be inserted into any slot, enabling a customized mix of I/O signals. In addition, the relay outputs are hot-swappable.

PEPPERL+FUCHS
www.pepperl-fuchs.com

FERRULES, CRIMPING, ETC

S3TL series ferrules, wire strippers, crimpers, and screwdrivers provide dependable wire terminations to screw and push-in terminals. S3TL ferrules accommodate wire gauges from AWG 26 to AWG 8, each with one or two wires. Each ferrule has an electrically insulated cover that's color-coded. These ferrules are UL 486F certified when used with S3TL crimping tools, which include two wire strippers (6-10AWG and 10-28AWG), three crimping tools (6-10AWG, 10-24AWG and 12-30AWG), and three insulated screwdrivers.

IDEC CORP.
800-262-IDEC (4332); https://lp.idec.com/push-in-S3-usa.html

REMOTE MODULES ADD COMPUTING

BusWorks NT Ethernet-expandable (NTE) remote I/O modules have conditional logic on their web configuration page, which has rules that allows complex decisions based on yes/no questions. For example, reading an analog or digital input value can trigger an action, and this value could control a relay when one or more conditions occur. No programming is required. The modules support up to 64 conditions using if/then/else statements for rule-based I/O operations. Each I/O module adds up to 16 input or output signals.

ACROMAG
248-295-0880; www.acromag.com

SCREW-IN, BOLT-ON, TENSION-SPRING, PUSH-IN

SRK series features screw-connection terminal blocks in single- and double-tier versions for wire cross sections from 0.08 mm^2 to 240 mm^2. HSKG-type high-current bolt-on terminals are designed for energy transmission applications over 296 A. They provide current-carrying capacities of up to 520 A and rated voltages of up to 1,000 V. In addition, ZRK/ZSL feed-through, PE terminals in single and double-tier versions, and ZIKD three-tier terminals use tension-spring connections for wire cross sections from 0.2 mm^2 to 16 mm^2.

CONTA-CLIP
www.conta-clip.com

EQUIPMENT & MATERIALS

AD INDEX

Do your chores

Cybersecurity points out familiar tasks we should have performed earlier

JIM MONTAGUE
Executive Editor
jmontague@endeavorb2b.com

"We aren't just resisting what's new and different. We resent that they turn the light on and make visible what we've been neglecting all along."

MOST of the sources I interviewed for this issue's cover story, "Everyday cybersecurity" (p.16), reminded me that avoiding cyber-threats and preventing probes, intrusions and attacks is relatively easy in the short-term, but increasingly difficult as time goes by.

The basic best practices—using passwords and authentications, implementing antivirus software, segmenting networks with firewalls, and enabling network traffic monitoring and threat detection—are always good advice and certainly worth repeating. However, they're just the table stakes for getting into a game that runs all night, throughout the next weeks and months, and for all of our foreseeable futures.

Similar to most things we build, a little time goes by, and rust, weeds, version creep, erosion, maintenance gaps and other problems crop up. This happens to everyone, in this case, even the best cyberspace experts and most proactive organizations.

For example, a few highly qualified sources for this month's cover article tried to pass off the same old slides and bullet points they'd already providing for years. I know it helps to repeat the essentials, but the cybersecurity field evolves quickly, and I figured there had to be more detailed news about the profound ways that software is automating cybersecurity. Not so much.

I'm pretty sure there's more up-to-date information and best practices that apparently aren't getting out, or at least aren't reaching me—and I apologize for not finding them and relaying them to you. I'm aware pesky reporters may not get the latest intel, but I shudder to think that many users may not be getting what they need to protect their people, processes and facilities.

This situation triggered my own mental alarm because it was similar to when the U.S. Dept. of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) started out years ago as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). I recall they initially posted a bunch of generalized white-papers, and then nothing for a while. It looked like they were scrambling to put anything up on their website to cover their rear ends. Not a good omen. Since that time, they eventually rallied, and now regularly provide updated alerts and other useful cybersecurity guidance.

In both cases and others, expertise can get stale and lag behind accelerating technical advances. Many sources, myself included, have to look like we still know what we're doing, and fall back on old information. I remember that some of the surgeons I used to interview telling me that crucial sections of their know-how were one breakthrough study away from being obsolete, especially in the mid-1990s when innovations minimally invasive surgery procedures were developed and improved in rapid succession. Sound familiar?

What to do? Well, first off, don't wait for me or others when we apparently don't have useful input on cybersecurity or any other topic that can help users do their jobs more securely and effectively.

Go out and get second, third and fourth opinions about cybersecurity software and other tools to will be the most helpful to you and your colleagues, processes, facilities and organizations. You can't wait for useful solutions to just come to you. Trust me. Almost everything that comes in unsolicited are sales pitches, which logically require promotion because they're almost entirely useless.

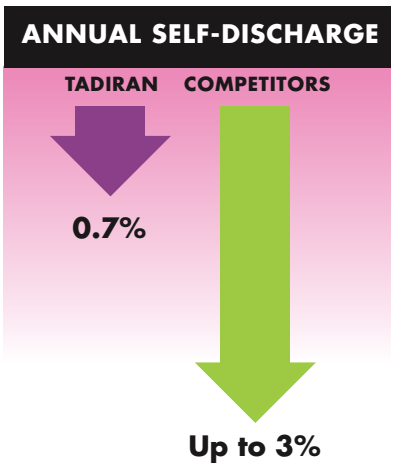
Likewise, aggressive initiative is also required as cybersecurity policies and procedures transition from being responses to one-off incidents to regular jobs like process safety and routine maintenance. As usual, it's easier to jump up for an exciting novelty than it is to maintain long-term focus on routine tasks we should have been doing all along, especially when many of them have been neglected up until now. In fact, I think this may be why reluctance to adopt cybersecurity, digitalization and other productive change is so persistent. We aren't just resisting what's new and different. We resent that they turn the light on and make visible what we've been neglecting all along. ∞

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 $LiSOCl_2$ 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.

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

www.tadiranbat.com

Go digital brain.

Go Boldly™

Emerson's Plantweb digital ecosystem is the brain for smarter, safer and more sustainable process performance. With data that's contextualized and prioritized, all your plants can now be connected and optimized seamlessly as one enterprise.

EMERSON™