December 2021

InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

Using Control Valve Installed Gain Calculations

Industrial Autonomy on the Horizon

Extreme OT Data Makeovers

Applying ISA/IEC 62443

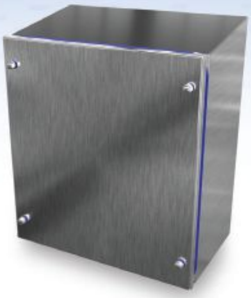
Advanced Analytics Improve Predictive Models

www.isa.org/intech

Now with over 7,000 top brand enclosures...

you'll surely find the enclosure you need, for less

High Visibility Pushbutton Enclosures



Slope Top Enclosures

NEW!

Sanitary Enclosures

SCE SAGINAW CONTROL & ENGINEERING

Your Enclosure Source®

STARTING AT ONLY $40.50

More Saginaw Enclosures

We just added more quality models to our very popular offering of Saginaw enclosures. These great new additions include:

- ***NEW!*** RAL 1018 yellow pushbutton enclosures for safety applications or ones where a highly visible enclosure is needed
- ***NEW!*** Sanitary enclosures designed to protect electrical equipment in sanitary environments, such as food and beverage applications, where resistance to intensive cleaning is essential
- ***NEW!*** Sloped-top enclosures that prevent water from gathering on top of the enclosure, as well as, providing space for mounting controls

The full line of enclosures from Saginaw, one of the most trusted names in the industry, includes:

- Wall-mount
- Junction boxes
- Pushbutton enclosures
- Floor-mount
- Freestanding
- Disconnect enclosures
- Internal mount disconnects
- Consoles and consolets
- Desktop workstations
- Wire troughs
- Stainless steel and carbon steel enclosures
- And much more...

And we keep adding to these great lines too!

HAMMOND MANUFACTURING

AttaBox™ A BRAND OF ROBROY ENCLOSURES™

WIEGMANN®

INTEGRA ENCLOSURES

Plus thousands of low-cost accessories for all the brands we carry.

- Filter fans
- Thermal management including heaters, air conditioners, vortex coolers, etc.
- Enclosure lights
- Smart sensors
- Enclosure door switches
- Subpanels
- Mounting accessories
- Locks and latches
- Electric interlocks / defeaters
- Folding shelves
- Window kits
- Casters
- And many more...

Research, price, buy at:

www.automationdirect.com/enclosures

Order Today, Ships Fast!

TOP RATED ★★★★★ BY CUSTOMERS

AUTOMATIONDIRECT.com

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

* See our Web site for details and restrictions. © Copyright 2021 AutomationDirect, Cumming, GA USA. All rights reserved.

December 2021 | Vol 68, Issue 6

InTech

FEATURES

COLUMNS

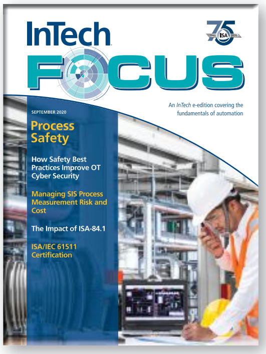
DEPARTMENTS

www.isa.org/InTech

October 2021
InTech
Benefits of a closed-loop digital twin
Wireless networks for condition monitoring
FDI digital sensing device standard explained
NEC Class 2 circuits for machine power distribution
Beyond the Pyramid: Using ISA95 for Industry 4.0 and Smart Manufacturing
www.isa.org/intech

InTech Magazine

The most current issue of ISA's flagship print publication is available online in a Digital Edition—an easily sharable format that lets you flip virtual pages on your tablet or desktop screen or download a PDF of the entire magazine. Also online, you can access the *InTech* Magazine Archives—digital magazine articles from 2016 to the present.


InTech
FOCUS
75
An InTech e-edition covering the fundamentals of automation
September 2020
Process Safety
How Safety Best Practices Improve OT Cyber Security
Managing SIS Process Measurement Risk and Cost
The Impact of ISA-84.1
ISA/IEC 61511 Certification

InTech FOCUS Ebooks

The InTech FOCUS series of ebooks, published in PDF format, covers fundamental automation and instrumentation topics through technical articles contributed by industry experts, including ISA members.

Also available: InTech Plus Newsletters

InTech Plus newsletters combine technical articles, automation basics, event coverage, book excerpts, and more in an easy-to-scan format delivered to your inbox. Subscribe through the website: www.isa.org/intech-home/subscribe.

InTech
MAGAZINE

© 2021 InTech

ISSN 0192-303X

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

Volume 68, Issue 6

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

Subscriptions: ISA Members receive *InTech* as part of their annual membership. Become an ISA Member at: http://www.isa.org/join. Other subscribers: 175 USD in North America; 235 USD outside North America. Single copy and back issues: 20 USD + shipping.

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

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

Printed in the U.S.A.

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

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

To order reprints of *InTech* print or digital articles, contact Nathan Swailes at reprints@mossbergco.com or 800-428-3340.

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

PRINTED WITH SOY INK

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

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

Honoring a Man by Building on His Legacy

By Renee Bassett, *InTech* Chief Editor

In this issue (p. 8), we mark the passing of one of the most recognized and widely published names in industrial process control: Francis "Greg" Shinskey, holder of 18 patents and author of more than 100 published papers and seven seminal books, died peacefully in September at the age of 89.

Although the first versions of the proportional-integral-derivative (PID) controller were used almost 100 years ago, Shinskey spent almost 50 years detailing the PID's uses for different applications. Known as "the genius behind feedforward control," he won numerous awards over his long career, including the ISA Life Achievement Award in 2008.

Shinskey's legacy lives on in the many he instructed and inspired. "He showed how the PID is the best controller for handling unmeasured process input (load) disturbances, and also how the PID can handle interactions by relative gain analysis (RGA), decoupling feedforward signals and valve position control," says Greg McMillan, in an article in *Control Design.*

"Sigifredo Nino, a Shinskey protégé, has continued his legacy, particularly in using RGA in refineries, and my entire career, except for an occasional dabbling in model predictive control, has been to make the most out of PID control," says McMillan. "My 2015 Momentum Press book *Tuning and Control Loop Performance, Fourth Edition* seeks to build on what I learned from Shinskey, confirming revelations by test cases to show what a PID can do employing often underutilized key features."

McMillan also honors Shinskey through his ISA standards-related activities. A few years ago, noting that most of the capability of the PID is underutilized, McMillan spurred the formation of ISA5.9, *Controller Algorithms and Performance.* This ISA working group functions under the ISA5 committee, *Documentation of Measurement and Control Instruments and Systems,* and seeks to clarify the algorithms used in industrial control systems and aid in their selection and application to improve manufacturing processes.

Participation in the group by leading experts has been exceptional, reports McMillan, and a 137-page ISA 5.9 technical report titled *PID Algorithms and Performance* has been issued for general review and comment by the committee. Ultimately, automation engineers could use the report to increase knowledge and appreciation of PID control. A digital twin with simple dynamic process simulations could enable automation engineers to build their foundation of knowledge and improve existing PID controllers, he said.

A digital twin with simple dynamic process simulations could enable automation engineers to . . . improve existing PID controllers.

Key ISA 5.9 contributors—McMillan, Yamei Chen, Pat Dixon, Mark Darby, Cheri Haarmeyer, Peter Morgan, Sigifredo Nino, Russ Rhinehart, Michel Ruel, Nick Sands, Jacques Smuts, Hunter Vegas, and others—also plan a series of writings that will build on Shinskey's impressive body of work and ensure that his knowledge continues to be shared.

Many people learned control engineering from Greg Shinskey. And thanks to the efforts of ISA volunteers, many more will. "The depth and extent of knowledge in his books will never be approached and may be lost to future generations," says McMillan. "I am trying to keep his legacy alive." ■

ISA *INTECH* STAFF

CHIEF EDITOR
Renee Bassett
rbassett@isa.org

CONTRIBUTING EDITOR
Bill Lydon
blydon@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Lisa Starck
lstarck@isa.org

GRAPHIC DESIGNER
Bonnie Walker
bwalker@isa.org

ISA PRESIDENT
Steve Mustard

PUBLICATIONS VICE PRESIDENT
Joao Miguel Bassa

EDITORIAL ADVISORY BOARD
CHAIRMAN
Steve Valdez
GE Sensing

Joseph S. Alford PhD, PE, CAP
Eli Lilly (retired)

Joao Miguel Bassa,
Independent Consultant

Eoin Ó Riain
Read-out, Ireland

David W. Spitzer, PE
Spitzer and Boyes, LLC

Dean Ford, CAP, PE
IB Abel, Inc.

David Hobart
Hobart Automation Engineering

Smitha Gogineni
Midstream & Terminal Services

James F. Tatera
Tatera & Associates

ADVERTISING & SPONSORSHIP
https://tinyurl.com/InTechAcom2022mediakit

Greg Shinskey, "the genius behind feedforward control," circa 1975.

In Memoriam: Francis "Greg" Shinskey

Francis Gregway "Greg" Shinskey, of North Tonawanda, N.Y., was born 29 October 1931, and passed away peacefully in North Smithfield, R.I., on 25 September 2021. He was 89.

Shinskey graduated from the University of Notre Dame in 1952 with a BS in chemical engineering and as a commissioned naval officer. He served two years in the U.S. Navy during the Korean War before beginning his career with Olin Chemical Company in New York. In 1960, he hit his stride with The Foxboro Company in Massachusetts, where his stellar career as a control systems engineer spanned more than three decades.

Shinskey was not only an expert, but an innovator and visionary. In *The Foxboro Company, 1908–2008, 100 Years,* Jack Authelet writes that Shinskey is "considered by many in the industry as the genius behind feedforward control," and that he retired "as the most recognized, widely published name in the industry, holder of 18 patents, author of more than 100 published papers on process control and seven books that became standards within the industry."

The prolific industry author shared his expertise as a frequent lecturer and in the seminal textbook *Process Control Systems,* published by McGraw-Hill and used in college courses across the country. He penned *Feedback Controllers for the Process Industries* after he retired. His materials continue to be used, carrying on his legacy of mentorship.

Shinskey was the recipient of many prestigious awards in his lifetime. He was one of the first two Bristol Fellows—he and Hoel Bowditch were honored simultaneously—named by The Foxboro Company. From ISA, Shinskey earned the Donald P. Eckman Award in 1983, the Albert F. Sperry Award in 1988, the status of Fellow in 1990, and the Life Achievement Award in 2008.

"I often thought that there was nobody that had more impact on forwarding the mission of ISA during my lifetime than Greg Shinskey," said Peter Martin, a retired executive from Schneider Electric, which had previously acquired Invensys and, before that, Foxboro. "ISA was like the automation and control leader of industry, and Greg was the *control* leader of industry. If I think back during my career, there are probably only a few names that come up that are even close to that. He kind of set the path for them."

Martin adds, "Greg was also probably one of the world's leading controls people around distillation columns, which are particularly tricky to control. Even after he retired, he would monitor the distillation columns of Petro-Canada from his barn." Shinskey's own bio made brief mention of his contributions in the application of feedforward controls and relative gain analysis, as well as nonlinear and self-tuning controllers with deadtime compensation.

Martin recalls encountering Shinskey for the first time in the 1970s. "When I first joined Foxboro, Greg Shinskey was *the* person. Everybody said, 'Oh, have you met Greg Shinskey?' He was almost a demigod at that time. It was fascinating, because when he walked in the room, everybody just got quiet: 'Here comes Greg. Let's see what Greg has to say.' Certainly, he was an engineer, probably the ultimate engineer—he graduated from Notre Dame, and he really knew his stuff. But the thing that surprised me was what a complete 'gentle man' he was, in the truest sense of the word. He was just about the nicest person you'd ever meet."

Authelet shares the same sentiment. "He was very humble. He was incredibly talented in his contributions to the products being developed by The Foxboro Company and was held in great esteem in the industry and different industrial groups, but he himself was very quiet and unassuming."

Indicative of Shinskey's ability to transfer his knowledge via books, Martin recalls, "As smart as he was, he was just such a good teacher. When I came in, I was not a control engineer, so I had a lot of questions. He'd just take the time, and he'd explain it. Very often people who know the most can explain it the simplest. They know it so well that they can just tell it to you, and Greg could explain things in such a simple way. I learned control engineering from Greg."

While his curiosity and scientific mind afforded him and The Foxboro Company much success, at the same time Shinskey was an artistic soul and beloved family man of great faith who was highly active in his church and community. For years, he had a column in the local newspaper, of which Authelet was the editor, called "God in Our Lives." Says Authelet, "It was nondenominational—just comments about faith-based people and the choices we make and the lives we live and how do we care for each other. It was just remarkable in and of itself."

Shinskey took great pleasure in his historic Foxboro, Mass., farm home built in the 1770s. He also enjoyed oil painting, hiking, gardening, and his self-restored 1959 Morris Mini bicycle. Peter Martin recalls him wearing his Harris tweed jacket, riding that bicycle from building to building to talk to customers or teach a course if the weather was right.

Says Authelet, "Greg was definitely a very unusual individual. Incredibly, incredibly talented, yet asked absolutely nothing for himself. But he lived his faith, and that took him to the heights."

Shinskey continued to serve as an independent consultant when he retired in 1993 to Sandwich, N.H., with his wife, Elizabeth. He is survived by his three daughters, five sons, 17 grandchildren, and five great-grandchildren, as well as his brother and two sisters. ■ *–By Lynn DeRocco*

Event Review: Ignition Community Conference 2021

Inductive Automation took virtual networking to the next level at its 2021 Ignition Community Conference.

The 2021 Ignition Community Conference (ICC) was another high-energy and informative event—the company's second held virtually. Under the theme "Evolve to be Smarter, Faster and Stronger," the September event billed itself as "taking virtual networking to the next level" with an interactive video chat platform. Attendees could start video chats in virtual rooms with a simple point-and-click and make conversations public or private.

In his opening keynote, the founder and CEO of Inductive Automation, Steve Hechtman, discussed the importance of the company keeping a finger on the pulse of the business: "I started the company to address pain points experienced as a system integrator," he said, citing his 25 years of experience in that segment of industrial automation. "Without experience as an integrator, how could you run an industrial software company?" He emphasized the company's commitment to collaboration, sharing and working with the industrial automation community to improve the industry.

The ICC conference again featured the Discover Gallery, showcasing a wide range of interesting applications. The annual Ignition Firebrand Awards recognized system integrators and industrial organizations that use the Ignition software platform for projects that include human-machine interface, supervisory control and data acquisition, manufacturing execution systems, and the Industrial Internet of Things (IIoT).

The system integrator panel this year included Brian McClain, business development manager for Corso Systems; Cody Warren, senior controls engineer for Tamaki Controls; Dustin Wilson, senior project manager for Phantom Technical Services, Inc.; Jake Hall, business development manager for Feyen Zylstra; and moderator Shay Johnson, sales engineer for Inductive Automation.

One of the topics addressed by the panel involved the digitization of work instructions. Digital information and work-process instructions for machine setup and operation are becoming important to bring on new workers that can be effective quickly, they said. This is valuable for every manufacturer grappling with the labor shortage and skills gap. In addition, this simplifies cross training of existing workers on new systems and platforms. ■

–By Bill Lydon

The Future of Automation: CODESYS Tech Talk Fall 2021

The CODESYS Corporation North America hosted a distinguished live speaker panel during its October CODESYS Users Conference and Tech Talk Fall 2021 event. The goal was to provide the latest insights on the "future of automation and the changes in automation communication and IIoT integration." Panelists included Albert Rooyakkers, CEO/CTO from Bedrock Automation; Jose Rivera, CEO from CSiA; Don Bartusiak, president of CSI; Brandon Williams, cofounder of CPLANE.ai; and Dieter Hess, CEO of CODESYS Group. The moderator of this panel was Bill Lydon, automation industry expert, consultant, and Automation.com contributing editor. Here is an excerpt of some remarks by panel participants. Visit Automation.com for a full report.

Don Bartusiak: Industries that are not embracing digital technologies are not very appealing to the very people, the digital natives, who companies need to make the digital transformation. Companies have to show an appealing career perspective to people coming out of college who are math, computer, and communications oriented, or they all will go to tech companies. You have to give them a workplace where they feel productive, and if you're a manufacturing company that doesn't do that, you're not going to get the talent you need to survive.

Albert Rooyakkers: You need a blend of old and new with several generations. We have people on our team who are in their 60s, 70s, and 20s. You need the mix and match of the wisdom and historical perspective of automation in addition to the young talent who are digitally astute. When the new talent is exposed to the real-world production and physics, they gain a broader understanding and appreciation of industry. Putting the young and experienced talent together can help the younger generation get excited about the industry, factory and process automation. I don't think it's hard to find people who not only are smart, innovative, and flexible, but also have a curious mind that's willing to learn new things.

Dieter Hess: It is really about combining the abilities of people who are able to create a software architecture with people who know how processes and machines work. It is unbelievable what you can do if you combine both together.

Jose Rivera: As things get more complex, we will have to rely more and more on diverse good working teams.

Brandon Williams: Modern and open systems provide an incredible toolkit that is a broader canvas, removing a lot of closed system barriers and enabling creation of new applications. The application of AI, analytics, and other open features using a container or virtual machine inside a control system with access to an OPC UA data flow in real time unlocks opportunities that cannot be realized today with proprietary closed systems. I think it will be somewhat like the Renaissance with new tools and platforms that are going to unlock creativity.

Don Bartusiak: To be successful in the application of AI and other technologies, in my experience you need collaboration between the data scientist and people with domain knowledge; one or the other is not sufficient. ■

Hannover Messe 2022 Plans Focus on Digitalization and Sustainability

Restarting after two years without a physical trade fair, the organizers of Germany's Hannover Messe 2022 trade fair focused on transformation and their next event's themes of digitalization and sustainability. At an October press conference, Deutsche Messe AG, Hannover, spokesman Onuora Ogbukagu recognized how the digital Hannover Messe offerings provided during the pandemic helped the event and its exhibitors to reach a broader audience through linking the physical trade fair with new digital products. Hannover Messe is dedicated to providing important content for industry in both the physical trade show and virtual worlds going forward, he said.

Jochen Köckler, PhD and CEO of Deutsche Messe AG, which puts on the event, noted the "continuous stream of innovations to improve industry" that Hannover Messe has showcased for the past 70 years: "Industrial innovations that manufacturing organizations can implement for competitive survival and continued prosperity. This is even more compelling today with the most profound industrial digitalization and sustainability transformation challenges occurring, including resource efficiency, carbon neutrality, and sustainability."

Onuora Ogbukagu said the physical trade fair will be combined with digital for 2022.

Köckler emphasized, "We face the greatest transformation since industrialization towards a resource-saving, climate-neutral, and sustainable industry." He discussed the importance of collaboration between industry, innovators, and politicians to achieve sustainability goals.

"Hannover Messe provides a unique event bringing together industry, technological innovators, and politicians participating in constructive discourse to collaboratively explore major issues seeking clarity, creating ideas, and setting new directions," he said. Hannover Messe is the showcase for products industry will use to become carbon neutral and sustainable, and "digitalization and sustainability will be the driving force for Hannover Messe topics for years to come."

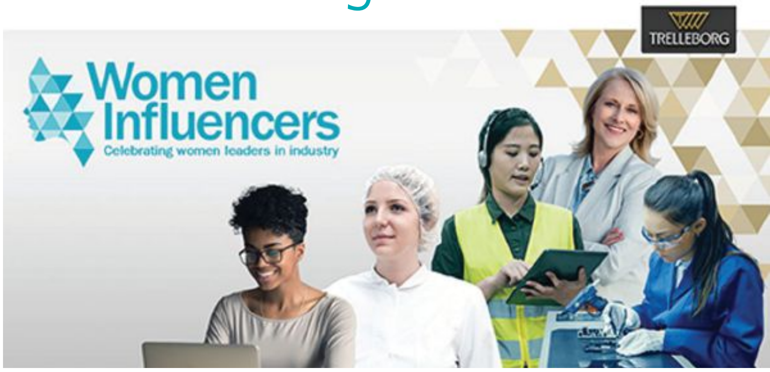
Portugal is the official partner country of Hannover Messe 2022. As Germany's third most important trading partner, Portugal will showcase its focus on engineered parts and solutions, digital ecosystems and energy solutions, and clusters of excellence such as mechanical engineering, metal, mobility, aeronautics, textiles, technical plastics, production technologies, and renewable energy. ■ *–By Bill Lydon*

Trelleborg Launches Women Influencers Program

For the inaugural event of the Trelleborg Sealing Solutions Women Influencers program, seven women in the manufacturing, technology, and supply chain industry participated in a virtual panel discussion about how to bridge the gap for women in their fields, particularly in aerospace.

The discussion, moderated by Sudha Chandrasekharan, general manager of the Trelleborg Sealing Solutions facility in Denver, Colo., U.S., and Greg Jones, director of Trelleborg Sealing Solutions Aerospace Hub Americas, explored the panelists' leadership philosophies and their views on gender diversity and inclusiveness in manufacturing, technology, and supply chain roles.

Participants voiced their opinions on common misconceptions about women in leadership and how to overcome them, the importance of mentorship programs, and the value of being bold in the workplace. Panel participants also shared stories about their successes and the challenges they have faced in their academic and career journeys.



Chandrasekharan, the catalyst for the Women Influencers program, said, "The strongest women are those who build each other up. If we want to see more women leaders, it's important for women to develop a strong supportive network of mentors. I am delighted to see this program take off and watch the partnerships form between women influencers."

Panelists included Heather Castleman, senior director of strategy and marketing, Trelleborg Sealing Solutions; Nancy Getz, product line director, Trelleborg Sealing Solutions; Kathy Hamrick, financial analyst, Boeing; Tara Heller, ITAR compliance manager, Magpul Industries Corporation; Tricia Heller, director of compliance, IP, and brand protection, Magpul Industries Corporation; Honorata Hencel, regional director, Poland Boeing Global Services; Kelsie Soneson, director of project management, IHS. ■

Industrial Digital Transformation: What Makes a "Top Company"?

By Greg Gorbach

Industrial innovation is accelerating, and leading companies have their transformation initiatives well underway. Digital champions are leading designated teams that focus on resilience, disruptive technologies, remote work, autonomous operation, sustainability, the circular economy, climate change, and other critical business-level objectives. We all hear anecdotes about companies that have had success with machine learning, augmented reality, robotics, additive manufacturing, data management, autonomous operations, cloud and edge, Internet of Things (IoT), or other core transformational technologies, but who are the leaders in digital transformation and what makes them so?

Leading companies take a strategic approach, integrating digital technology throughout their value chains. Design and engineering, production operations, maintenance, logistics, supply chain, business systems, customers, products, and organizational structure are subject to innovative change as processes are examined and updated and new tools and technologies are deployed.

The core business model by which a company produces or offers services to the marketplace can be replaced by new business models that leverage cognitive analytics, digital twins, predictive technologies, or other technologies that enable the company to expand its worldview and embrace competitive excellence as a goal. Companies thereby move beyond production efficiency to a much more dynamic, responsive, and resilient business model.

To be sure, digitalization in production, whether known as Industry 4.0 or smart manufacturing, plays a crucial role in opening new opportunities for highly flexible, fast, and high-quality production systems. Top companies know that "digital" cannot be bolted on. They must intimately weave digital together with their internal and external processes. Traditional organizational silos must be broken down; multifunctional teams must innovate around customers, processes, and employees; and workforce hesitancy must be addressed and overcome.

In one form or another, software is key to digital transformation. For industrial companies, there is a correlation between investment in software and transformational technologies and corporate valuation. Software powers digital transformation, necessity drives innovation, and the whole cycle is accelerating year after year. Many leading companies have been at it for some time, but the best understand that the successful, ongoing transformation relies not only on getting the technology right, but also on empowering the right people to guide, interpret, and leverage the technology.

Another massive driver for digital transformation is the pressure companies feel to become more sustainable and significantly change their operations to address climate, environmental, and circular economy concerns. Leading companies recognize that they cannot make these changes quickly and effectively—or maybe at all—without substantial digital transformation.

Determining the top 25

So, who are the real leaders in digital transformation? Advisory Group has been conducting research designed to identify them and is releasing a new report. For this research, digital transformation was defined as: "The integration of digital technology into all areas of business, fundamentally changing the way companies operate and deliver value to customers. The organization is typically charged to innovate and improve across multiple dimensions such as: digital/disruptive technologies, culture and leadership, operational agility, workforce engagement, customer experience, environmental, social and governance, and competitive performance."

A summary of the *Top 25 Industrial Companies in Digital Transformation* report will be available at the 26th Annual ARC Industry Forum, held February 14–17, 2022 in Orlando, Fla.

While it is not straightforward to identify leaders in such a complex space, ARC has developed a rigorous process based on financial performance, a community-intelligence-based ranking system, and software and sustainability data. Publicly available financial information, ARC primary and secondary research, data from ARC's market database, and the opinions of members of ARC's community of end users were all factored into a report and ranked list. The *Top 25 Industrial Companies in Digital Transformation* report will be released in January. Think your company is doing digital transformation well? ARC would love to hear about it! ■

ABOUT THE AUTHOR

Greg Gorbach (ggorbach@arcweb.com) chairs the Digital Transformation Council of the ARC Advisory Group and is VP and manager of the digitization and IoT Group for ARC. He is based in Suffolk County, Mass.

IIoT Disruption Potential Gets Tested

By Renee Bassett

ABOUT THE AUTHOR

Renee Bassett (rbassett@isa.org) is chief editor of *InTech* magazine and Automation.com, a subsidiary of ISA. She is a career journalist, editor, and content creator with a focus on industrial automation.

A potential network vulnerability has emerged: Attackers can target Industrial Internet of Things (IIoT) networks by using drones to bypass physical barriers. These drones can be equipped with signal jamming technology to automatically locate and disrupt part of the industrial communication infrastructure.

Nozomi Networks Labs investigated the likelihood of attacks against the low-power radio frequency WAN (LoRaWAN) technology used in IIoT networks. The company's research focused on the viability of discovering the transmission frequency of the IIoT network and jamming the signal to disrupt network communication. The results revealed potential attack vectors that industrial security professionals should consider as technology matures.

LoRaWAN wireless technology is based on low-power, wide-area networks (LPWAN). LoRaWAN is an open standard promoted by the LoRa Alliance (https://lora-alliance.org), mostly for IIoT deployments. Technology usage includes devices that benefit from wireless communication and have requirements for long-distance communication and low power consumption, such as intelligent utility meters.

A downside to LoRaWAN is that LoRa sensors are susceptible to interference attacks that can make the LoRa signal unavailable to the recipient. Such an attack would not be pragmatic because of the long-distance applications in which these sensors can be placed, and because of countermeasures from modulation (such as frequency hopping). But Nozomi wanted to test whether signals could be made unavailable.

Jamming the signal

LoRa sensors send a few countable packets per day, usually in a predefined time range, which allows the LoRa packets to be timed. Another approach is to initiate an attack when the sensor starts its transmission with the goal of sending the jamming signal the moment the transmission starts from the sensors to disrupt the payload. Nozomi Networks Labs used the second approach because it has an advantage over frequency hopping. However, the jammer must be close enough to the sensor to jam the signal.

Locating a device from a radio signal can be easily done. Any wave that propagates in a medium has a specific direction as it distances itself from its source. By using an array of antennas, one can derive the source location of a signal. Such an approach would need the proper synchronization of devices to calculate the time difference of arrival of the signal and the direction. Another attribute of a wave is its power. Under certain conditions, one can estimate the distance to the sensor by measuring how strong or weak the signal is.

Making the attack real

For the jammer, Nozomi used a software-defined radio (SRD) module. These devices are programmable signal processing devices that allow modulation and demodulation of a signal. To identify and jam the LoRaWAN signal, Nozomi used a localization strategy based on the strength of the LoRa signal, and a jamming attack that activates when the sensor sends data. For the localization, Nozomi used the received signal strength indicator (RSSI) value.

The jammer attack consists of two phases:

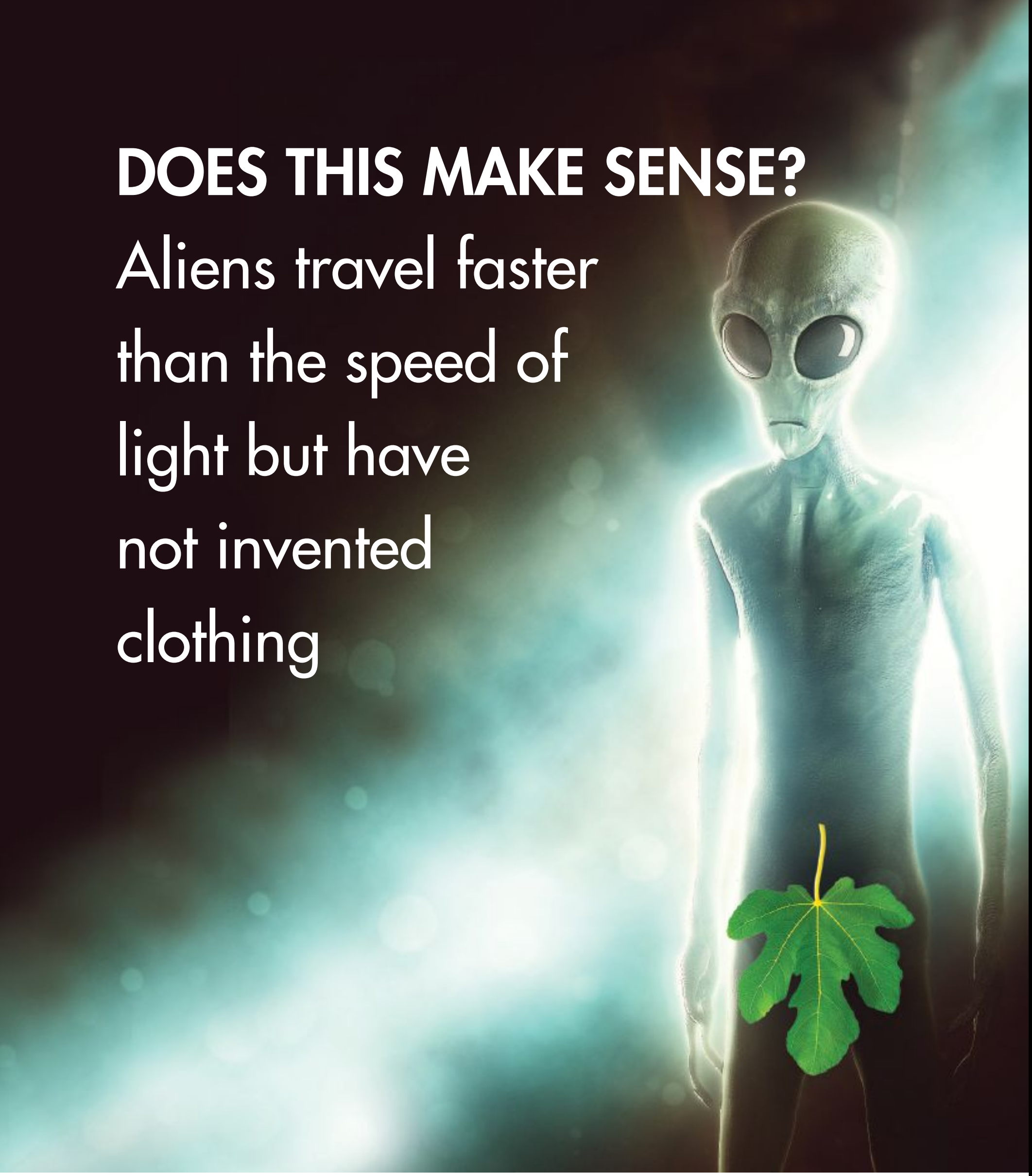
1. Detection of the LoRa signal. Nozomi used a series of band-pass filters to check the available channels in the LoRa range. This allowed monitoring of multiple channels to capture any possible packet transmission.
2. Jamming the LoRa signal. This involves sending a burst of energy to the frequency to be jammed. This results in the destruction of the LoRa signal. The legitimate gateway is forced to drop the packet, and valuable information is lost.

Results of the tests

Packets were either dropped or the cyclic redundancy check of the packet was invalid. This meant part of the packet was received from the gateway, but it was malformed so the gateway could not validate it and was forced to drop it.

Nozomi used drones to apply this approach in the real world. A drone can move across any terrain and gain adequate altitude to receive the signal. The RSSI can be accurate after a few measurements in the same general location by averaging the values. An attacker could select a random location close to a facility within a 5 to 10 km radius. Once within the receiving area of the LoRa signal, an attacker can take multiple measurements to establish a good averaging RSSI value. The process must be repeated in at least two arbitrarily selected locations if they are not the same point. The final stage is to approach the sensor and activate the selective jammer.

Nozomi reported that lab simulations prove attacks like these can occur. Those who would do harm may not be far behind. Find out more at www.nozominetworks.com/blog/the-long-range-disruption-of-industrial-iot-lorawan-networks. ■



Advanced Analytics Improve Predictive Models

By Joseph Reckamp

Inaccurate or overlooked alerts on manufacturing data can be reduced with proper data handling when developing and deploying predictive models.

FAST FORWARD

- Models are often used to predict process plant problems before they occur.
- The quality of these predictive models, and the input data supplied to them, can be greatly improved with advanced analytics.
- The result is more accurate predictions further into the future, giving process plant personnel information to improve operations.

Data analytics, and specifically predictive analytics, are meant to reduce the number of alarms for process improvements, trend forecasting, and predictive maintenance. However, deploying predictive analytics often leads to excessive nuisance alarms, a common problem in process manufacturing control rooms.

Process engineers typically spend days or weeks reducing and eliminating nuisance alarms to ensure control room operators respond with the correct vigilance to the critical alarms that could cause safety incidents or quality deviations. Predictive analytics help drive data-driven decisions for process improvement and optimization, but data and insights must be handled properly.

Predictive analytics 101

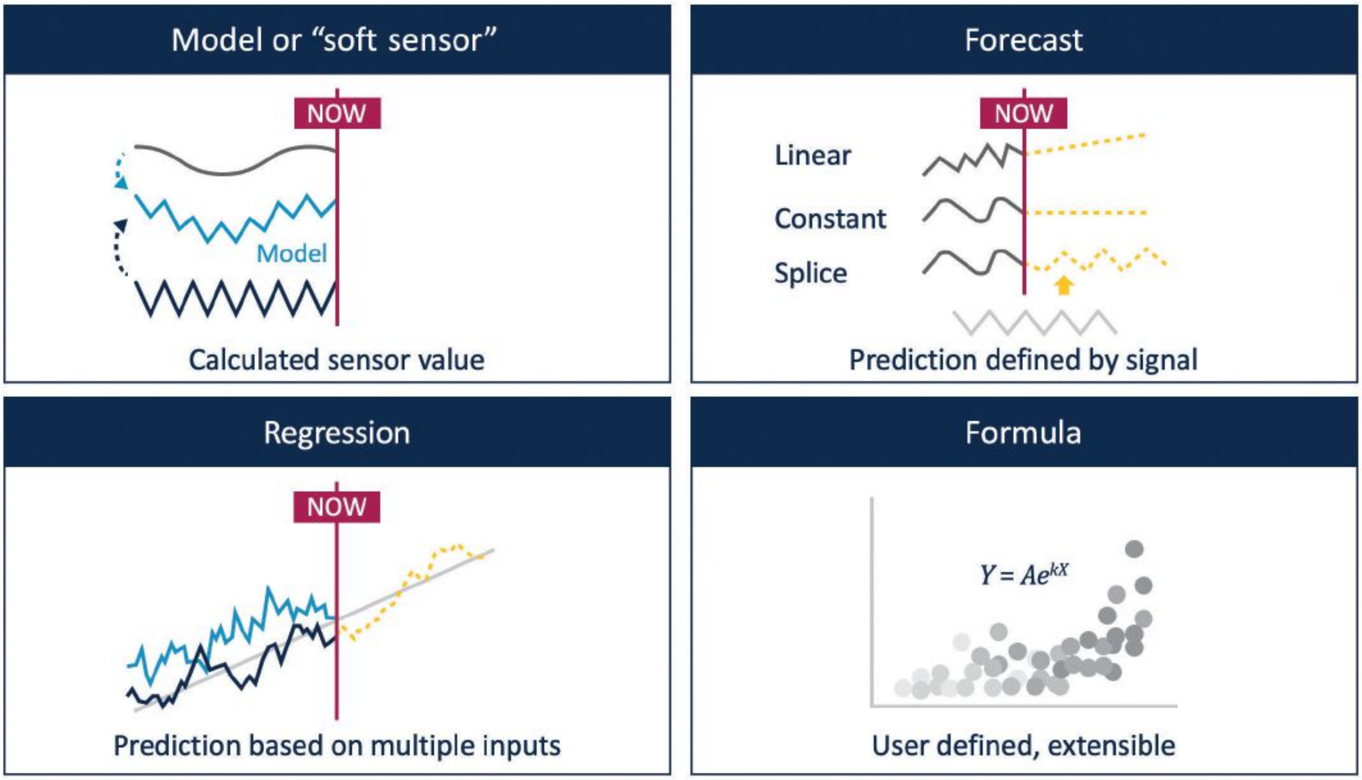
Predictive analytics are a method of data analysis whereby future projections of data are estimated as a function of modeled historical data sets. Some common techniques for creating predictive forecasted data include regression, event or profile, and classification.

Regression uses a quantifiable model applied to historical data and extrapolated for new or future data. Event or profile predictions denote when a particular data trend is preceded by a pattern or shape of the data. Classification predictions leverage normal data in a model to detect anomalies or abnormalities in the new data (figure 1). Each of these methods requires a model to be trained on historical data, with the model then used to predict future data or events.

Predictions have three potential outcomes: an accurate prediction, a false positive, or a false negative. An ideal model uses accurate data as an input to accurately predict issues well in advance. False positives occur when the model predicts a nonexistent issue. False negatives occur when the model predicts normal operation and overlooks an issue.

In practice, most predictive analytics display some amount of the two false error types, because every possible combination of inputs to and outputs from the model are unlikely to be known and accounted for in the model. False negative errors can result in significant cost to the organization for missing issues, and false positive errors often cause unnecessary adjustments or maintenance. Psychological costs are also incurred, because operators change behaviors due to a loss of trust in the model results.

Figure 1. Predictive analytics models create a projection of future data, typically based on a quantifiable method such as regression.



Regardless of whether the predictive analytics algorithms used are transparent, open-source formula, or proprietary and compiled algorithms, all methods require historical data for training and fitting the predictive model. Making sure the historical input data to the models is understood, cleansed, contextualized, and well prepared for modeling is critical for deploying accurate predictive models.

Leveraging hybrid first principles models

Most predictive analytics models are empirical, meaning that the quantitative model algorithm is fitted to the data using the method best fitting the data. Therefore, if the training data portrays a linear relationship between variables, a linear regression is used for fitting the model. However, inherent noise within data sets, complex relationships among variables, and even the selection of the specific data set used for model training can all result in a training data set that is not representative of all data available. For example, a training data set may show a linear trend, resulting in selection of a linear model; whereas the full data set may show curvature or edge effects that suggest a higher order model should have been applied.

A better method is to use first principles engineering equations that describe the relationships among variables. These first principles equations are laws or theorems taught in engineering education or published in literature. They were derived from analyzing significant amounts of data.

For example, the performance of a filtration membrane can be analyzed by membrane resistance, which is described by Darcy's law to be a linear direct relationship with the transmembrane pressure and linear inverse relationships with the viscosity and flux. Alternately, a chemical reaction with a known nth order power law equation would indicate that an nth order polynomial fit should be taken for the concentration of the components to describe the change in concentration over time.

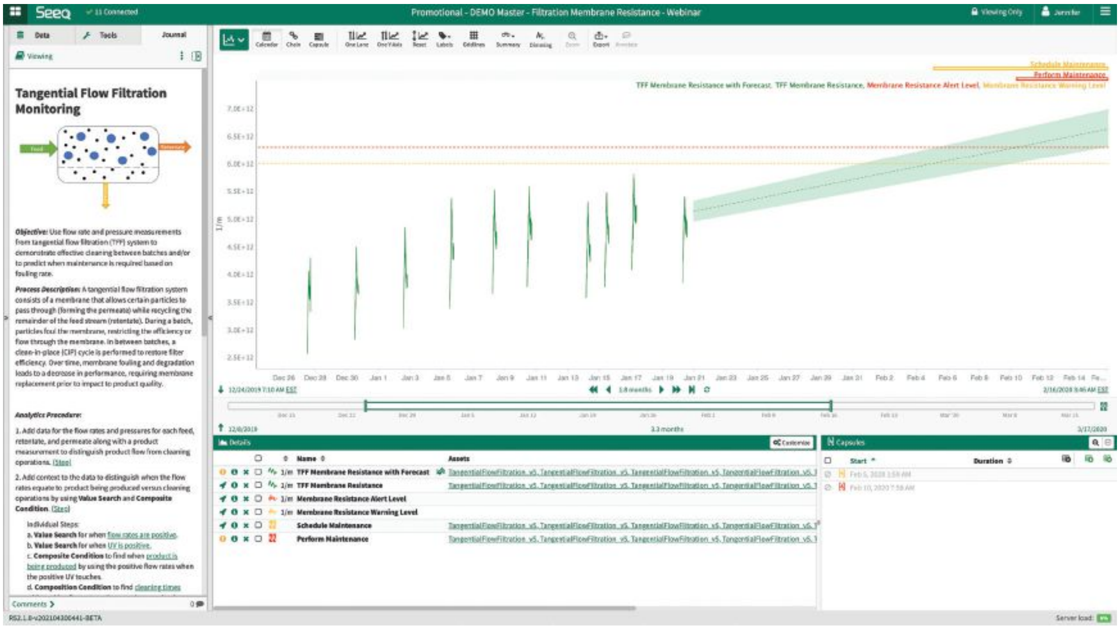
Understanding and applying first principles models typically has two major benefits. First, the predictive analytics models are often dimensionally reduced by default. In the Darcy's law example, multiple parameters, such as pressures, flow rates, surface area of the membrane, and viscosity, are reduced to a single membrane resistance variable (figure 2).

Second, the model fit is more likely to represent data outside of the training window, as the engineering principle should hold true beyond the training data range in most cases. Overfitting is a major concern with model development, as it often degrades results. Leveraging specific relationships with a basis in engineering laws based on first principles addresses this issue, because it avoids using a higher order model than necessary.

Reducing noise with data cleansing

Oftentimes, data cleansing is related to removing invalid or not-a-number data before running it through an algorithm, but there are many more considerations to improve the model and reduce false alerts. Process data often has inherent noise in the data set that causes a noisy model output, which triggers false alerts from small spikes in the data. These alerts can be minimized through data cleansing methods such as smoothing filters to eliminate or reduce the noise present in the model.

Numerous smoothing filters exist, with the most common types being low-pass filters such as the Loess method, Savitzky-Golay method, or a moving average filter. Applying these filters to the process data reduces the noise in the model inputs, resulting in a model with reduced noise that is less likely to trigger a false alert by oscillating above the alert limit. In addition to



Tangential Flow Filtration Monitoring

Objective: Use flow rate and pressure measurements from tangential flow filtration (TFF) system to demonstrate effective cleaning between batches and/or to predict when maintenance is required based on fouling rate.

Process Description: A tangential flow filtration system consists of a membrane that allows certain particles to pass through (forming the permeate) while recycling the remainder of the feed stream (retentate). During a batch, particles foul the membrane, restricting the efficiency or flow through the membrane. In between batches, a clean-in-place (CIP) cycle is performed to restore filter efficiency. Over time, membrane fouling and degradation leads to a decrease in performance, requiring membrane replacement prior to impact to product quality.

Analytics Procedure:

1. Add data for the flow rates and pressures for each feed, retentate, and permeate along with a product measurement to distinguish product flow from cleaning operations. [Step]
2. Add context to the data to distinguish when the flow rates equate to product being produced versus cleaning operations by using **Value Search** and **Composite Condition**. [Step]

Individual Steps:
a. **Value Search** for when flow rates are positive.
b. **Value Search** for when UV is positive.
c. **Composite Condition** to find when product is being produced by using the positive flow rates when the positive UV touches.
d. **Composition Condition** to find cleaning times

	Name	Assets
1/m	TFF Membrane Resistance with Forecast	TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, T
1/m	TFF Membrane Resistance	TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, T
1/m	Membrane Resistance Alert Level	
1/m	Membrane Resistance Warning Level	
	Schedule Maintenance	TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, T
	Perform Maintenance	TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, TangentialFlowFiltration_v5, T

Start	Duration
Feb 5, 2020 1:59 AM	
Feb 10, 2020 7:59 AM	

R52.1.0-v202104300441-BETA

Figure 2. An advanced analytics application, such as Seeq, can leverage Darcy's law on a tangential flow filtration system. Three pressure sensors, three flow rate sensors, viscosity, and the surface area of the membrane were dimensionally reduced to a membrane resistance soft sensor that can be regressed and projected into the future to determine the appropriate maintenance period.

signal smoothing, other types of data cleansing include outlier removal, time shifting data to adjust for process dynamics, and eliminating data that is not relevant, such as when the process is not running.

It is important to note that when data cleansing methods such as signal smoothing, time shifting, or outlier removal are applied to the training data, those same methods should be applied online to the live data when the model is operationalized. Failing to apply the same logic to the live data set as the training data set can result in a completely different set of false positives or false negatives. The model is trained on clean data and then applied to noisy data.

Similarly, persons developing predictive models of time series data should understand historian data archiving methods such as compression. Training data is typically post-compression data in the data historian, but online or live data may be precompression. Applying a model trained on post-compression data to precompression live data can cause lack of model fit issues, resulting in numerous false positives and negatives.

Providing context for alerts

Predictive analytics models are often not applicable 24/7. A certain model may only be applicable when a particular product is being produced, in a specific mode of operation, or even simply when the equipment is running. The most common time for models to falsely alert is immediately after a process change, which is when operators are often flooded with nuisance alarms.

As part of the model development process, determine which sections of the process make sense for alerts, and which ones do not. From there, build context to automatically segment or suppress alerts during time frames that are not periods of interest.

A common method of providing context to reduce false alerting is to suppress alerts during equipment startup, shutdown, or product changeovers. Additionally, model alerts occurring within a certain period of time after a manual adjustment to a process set point are often segmented into a separate visual indicator instead of a notified alert. Those deviations are expected until the process returns to steady state at the new set point (figure 3).

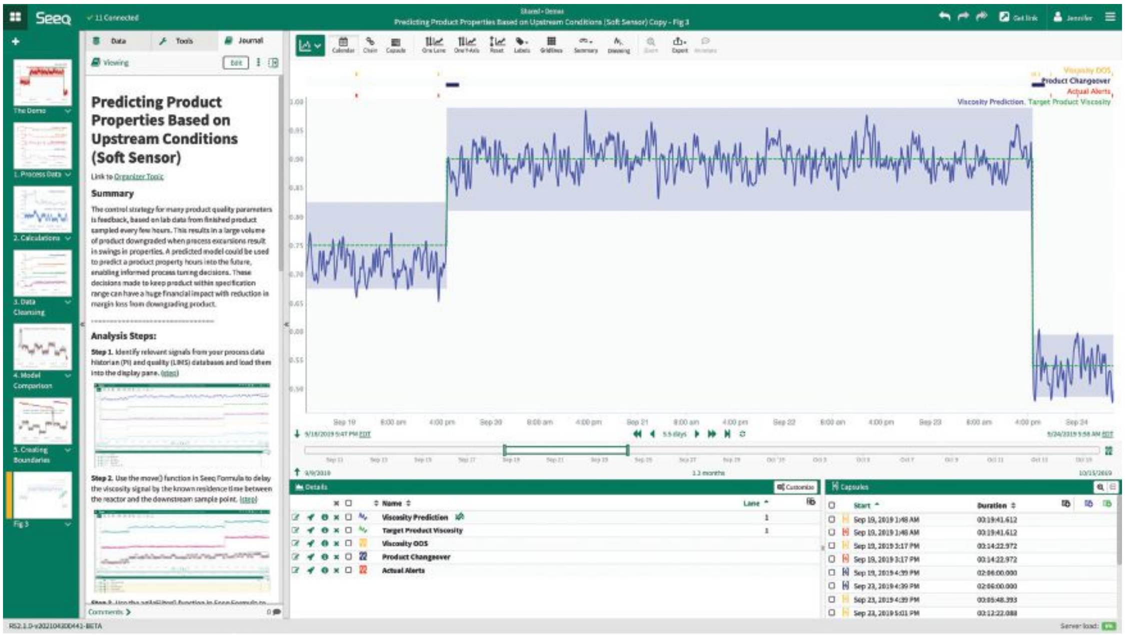
Understanding model validity

Analogous to alerts not being valid during all modes of operation, models are not valid for all possible input parameters. A predictive analytics model is only able to predict situations that the model has been trained upon. For example, if a predictive quality model was created for a reaction with training data between 40°C and 60°C, it cannot reliably predict what the quality will be if the reaction temperature is 70°C.

Models are only valid in the range of the process inputs provided to the predictive model. For continuous processes, this generally is distilled down to upper and lower static limits for each model input, whereas batch processes require a batch profile of inputs that could adjust over time. It is important for the model to build in checkpoints for valid process input ranges to avoid causing false alerts when the model is not valid.

Oftentimes, the results of predictive analytics models are displayed to operators through dashboards of the results, which include alerts or notifications. However, these operators are typically not responsible for model development or understanding when the model is valid or invalid. Therefore, it is up to the model developer to input that information and make sure the operators are aware of these conditions.

The modeler can decide the best method for dealing with model validity. Some common approaches are to create boundaries around each of the input signals represented by most of the training data. For example, a setting of ±2 standard deviations is commonly



Predicting Product Properties Based on Upstream Conditions (Soft Sensor)

Link to Organizer Topic

Summary

The control strategy for many product quality parameters is feedback, based on lab data from finished product sampled every few hours. This results in a large volume of product downgraded when process excursions result in swings in properties. A predicted model could be used to predict a product property hours into the future, enabling informed process tuning decisions. These decisions made to keep product within specification range can have a huge financial impact with reduction in margin loss from downgrading product.

Analysis Steps:

Step 1. Identify relevant signals from your process data historian (PI) and quality (LIMS) databases and load them into the display pane. (step)

Step 2. Use the move() function in Seeq Formula to delay the viscosity signal by the known residence time between the reactor and the downstream sample point. (step)

Name	Lane
Viscosity Prediction	1
Target Product Viscosity	1
Viscosity OOS	
Product Changeover	
Actual Alerts	

Start	Duration
Sep 19, 2019 1:48 AM	00:19:41.612
Sep 19, 2019 1:48 AM	00:19:41.612
Sep 19, 2019 3:17 PM	00:14:22.972
Sep 19, 2019 3:17 PM	00:14:22.972
Sep 19, 2019 4:39 PM	02:06:00.000
Sep 23, 2019 4:39 PM	02:06:00.000
Sep 23, 2019 4:39 PM	00:05:48.393
Sep 23, 2019 5:01 PM	00:12:22.088

Figure 3. False alerts during product changeover can be easily suppressed to a visual indicator using Seeq and not notified to operators as alarms.

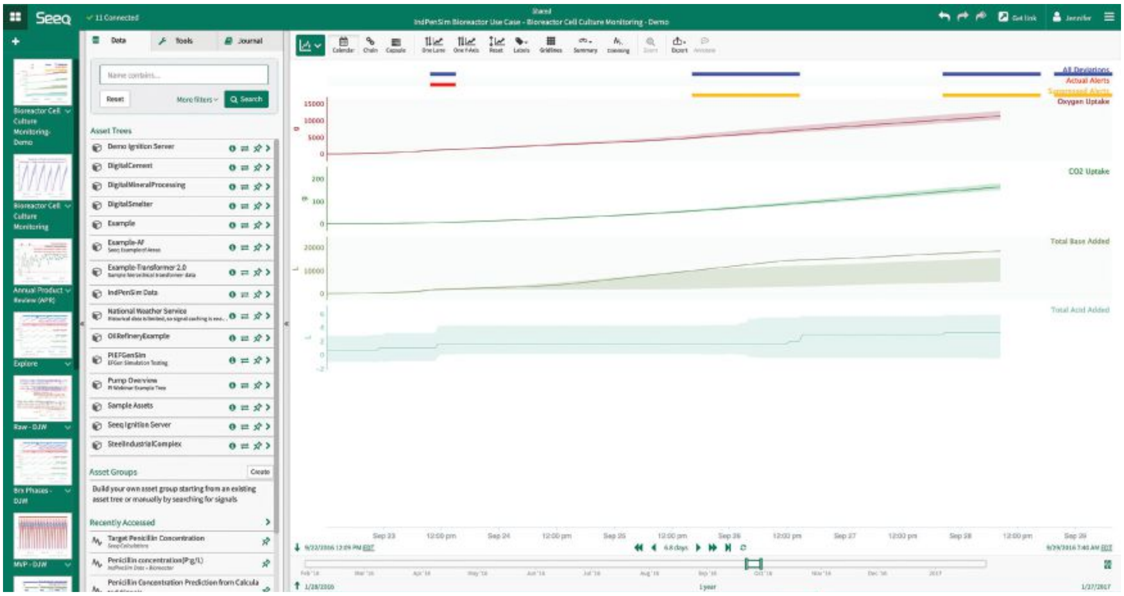


Figure 4. Seeq was used to create these reference profiles, which were applied against model input parameters to determine when the batch model was invalid. In this graph, the total base added went beyond the model validity period, so all suspected alerts beyond that point in time were suppressed.

used to account for 95 percent of the training data, which is then turned into static limits for continuous processes, or reference profiles for batch processes (figure 4).

Excursions from these model validity bands can then be used to suppress model results, along with associated alerts to operators, when the model is not valid. The model developer should be notified of these excursions, so he or she can extend the training data to expand the model validity range.

Transferring knowledge from R&D

One limitation with predictive models is the amount of data available about the process to build the predictive model. Since predictive models require a breadth of input parameters to create a wide validity range to predict future events, new processes are often at a disadvantage in the quantity of data available.

However, it is important to realize that in most cases, the data does not have to be data from the same equipment, size, or manufacturing site. Although some parameters will be affected by process configuration and scale up, a research and development (R&D) organization typically attempts to minimize the impact of scale up. Therefore, process data from R&D laboratory experiments, or even manufacturing at other sites, can often be used for model development.

One of the advantages of R&D laboratory experiments is that oftentimes there are design of experiments (DoEs) executed on the process, with a wide range of process inputs tested. These DoEs provide data regarding additional failure modes and wider process parameter ranges than would typically be observed in the manufacturing environment. Using R&D data alongside available manufacturing data provides a much greater model validity range, along with more accurate model development to reduce false positives or false negatives.

Errors will always occur, even when all the correct engineering procedures are followed for model development. These will increase, along with a decrease in confidence in the accuracy of the model, as the time horizon for predictions increases. Despite these difficulties, employing the techniques and tips described in this article will substantially decrease false positives and negatives, with corresponding improvements to plant operations and maintenance. ■

All figures courtesy of Seeq

ABOUT THE AUTHOR

Joseph Reckamp is an analytics engineering group manager at Seeq Corporation, specializing in the pharmaceutical industry. He enjoys working with engineers across manufacturing industries to improve processes and realize value using process data analytics. He received his BS and MS in chemical engineering from Villanova University and has worked in the pharmaceutical industry throughout his career, including stints in R&D with GlaxoSmithKline and production with Evonik.

RESOURCES

"Process Manufacturers Leverage Cloud Computing for Advanced Analytics"
https://bit.ly/3c8mpXm

"The Quest for the Most Magical Algorithm"
www.isa.org/intech/202004exe

"Analytics for Predictive, Preventative Maintenance"
https://bit.ly/3bjOkmN

"Analytics Next: Beyond Spreadsheets"
https://bit.ly/3bhjJX2

Download
your free
trial today

Industrial Autonomy on the Horizon

Continuous-process industries are at an inflection point regarding what they can do with automation, making now an ideal time to address inefficiencies and hazards.

By Joe Bastone

The era of the remote workforce has brought to light a cross-industry need for resilient, futureproof industrial control systems supporting more efficient, sustainable, and safe manufacturing plants. Through the integration of autonomous software and technologies along the production line, and the innovation of process control systems, plant operators can achieve long-term operational benefits.

Ongoing advancements in process automation have enabled users to create steady-state and dynamic models for plant and control design, assess equipment performance and troubleshoot issues, evaluate process design, and resolve operating problems. By using software, including advanced control and alarm management, industrial organizations have optimized industrial processes to improve business results and safety. This progress has also provided greater visibility into process risk—notably, advanced control-defined optimal limits and rigorously executed controls to maintain those limits.

Today, the introduction of new digital technologies at the plant and enterprise levels has the potential to augment people and processes to an unprecedented degree. Advanced functions, such as artificial intelligence and machine learning, are changing how people work in industry.

Autonomous control systems fulfill the growing need to streamline plant communications, provide support for the next generation of industrial workers, and gain a more comprehensive view of process inefficiencies. Autonomous solutions enhance workforce safety and performance while reducing environmental impact and operating costs with more adaptable and accessible system assets.

Process industries have never been under greater pressure to meet production targets, minimize costs, and maximize asset efficiency, all while ensuring health and safety. Moving forward, companies in these sectors will need to better align production strategies with market demand to maximize revenue growth. They must also embrace the adoption of digital technologies to drive efficiency and make investments in plants to reduce carbon footprints. From safety to sustainability and productivity to reliability, the hurdles presented in the remote-work environment amplified the need for more resilient, interconnected plants.

Yet even as industries grapple with structural changes, and as societies and economies pivot to the "new normal," process industry companies themselves have a window of opportunity: Now is the time to adapt strategies and technologies to help reduce disruption to operations and achieve new levels of performance and profitability.

Current state

Automation systems in continuous-process plants are constantly evolving due to competitive industry pressures, customer demands, external events, and security requirements. Like it or not, most existing systems have changed as a result of numerous small actions taken over the years. A control system originally installed 25 years ago may include a patchwork of small additions made over time, leading to a system that is difficult to maintain because of all its unique quirks. Only some system owners take a strategic lifecycle approach to their control systems. Others are typically reactive, making changes only as needed to correct problems.

Many industrial sites also suffer from the lack of a consistent philosophy in integrating various plant subsystems. The prevailing information technology (IT) focus on the operational technology (OT) space has only exacerbated this problem.

In addition, the current generation of experienced industrial engineers, operators, and technicians is in the process of retiring. As these workers leave the plant, they take with them valuable tribal knowledge of the control system design and evolution, the production processes, and the associated control strategies. This departure is causing the loss of their collective know-how. Recruiting workers to backfill retirements is just one part of addressing this industrial skills gap. Once new employees are on site, they must be trained efficiently so they can up-skill quickly and produce results.

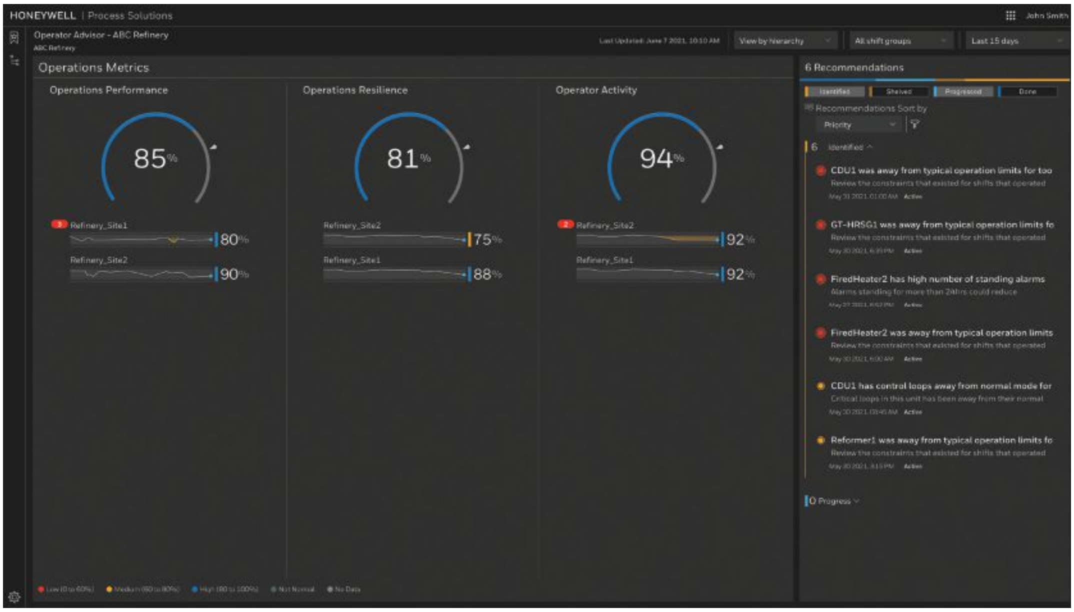
All of these challenges set the stage for a new approach to the control system of tomorrow. The continuous-process industries are at the beginning of an inflection point regarding what they can do with automation solutions. Today's objectives should be to leverage decades of process know-how, find ways to integrate subsystems and streamline communications, and become more flexible in how to work with control technology in general.

What is (and is not) industrial autonomy?

The topic of "industrial autonomy" is gaining significant interest, with many diverse views—and compelling opinions—on what constitutes the autonomous operation of an industrial facility. According to a recent study by LNS Research,

FAST FORWARD

- Ever-improving process automation technology grows along with the industries and plants that employ it.
- Current trends and events, including remote working due to the pandemic, highlight the need for systems and people to be able to function autonomously.
- Increased efficiency and safety inform built-for-today autonomous processes and result in higher profitability and quality.



CDU1 was away from typical operation limits for too
Review the constraints that existed for shifts that operated
May 31 2021, 01:00 AM Active

GT-HRSG1 was away from typical operation limits fo
Review the constraints that existed for shifts that operated
May 30 2021, 6:30 PM Active

FiredHeater2 has high number of standing alarms
Alarms standing for more than 24hrs could reduce
May 27 2021, 4:52 PM Active

FiredHeater2 was away from typical operation limits
Review the constraints that existed for shifts that operated
May 30 2021, 6:00 AM Active

CDU1 has control loops away from normal mode for
Critical loops in this unit has been away from their normal
May 30 2021, 03:45 AM Active

Reformer1 was away from typical operation limits fo
Review the constraints that existed for shifts that operated
May 30 2021, 3:15 PM Active

AI-generated guidance, such as that found in Experion Highly Augmented Lookahead Operations (HALO), equips operators with advanced tools for enhancing performance.

approximately 50 percent of industrial transformation leaders have an autonomous plant initiative formalized, and an estimated 41 percent of these leaders are accelerating their autonomous plant efforts because of the global pandemic.

The world of industrial autonomy is a crucial part of what ultimately comprises Industry 4.0, which will enable industrial assets and operations with robust adaptive capabilities. Autonomous control systems will respond without operator interaction to situations within a secure, bounded domain that was not preprogrammed or anticipated in the system design.

Industrial autonomy lets industrial companies harness innovative technologies to create a true digital transformation of operational strategies. Because digitization is not a one-step process, understanding a facility's capabilities, digital maturity, and state of operations is crucial in identifying its next steps in the industrial evolution.

It is apparent that industrial process plants can move on a trajectory toward industrial autonomy and make similar step-change improvements in benefits by harnessing new technology. In an industrial environment, the trend toward autonomous operation is truly focused on optimal advanced sensing and automation technology in plants.

Industrial autonomy is about leveraging technology for better situational awareness. It is about allowing a system to take an optimal action that achieves desired outcomes in the best way possible. And those outcomes are better production, improved quality, more reliable operation, and a much more efficient workforce.

Industrial autonomy helps automate a host of plant floor tasks and verify that they are performed flawlessly and consistently. Most importantly, autonomous operations can mean moving humans out of unsafe environments without inhibiting their access or view to process information.

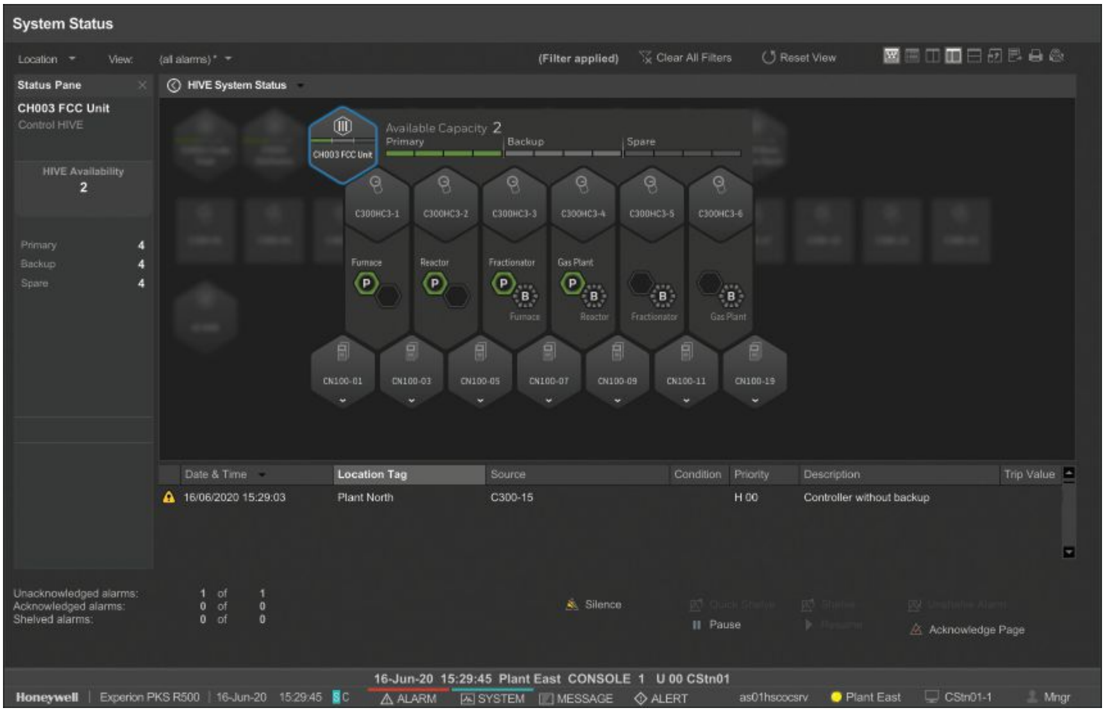
Levels of autonomous operation

When considering the wide range of operational tasks involved in a typical process plant, from the control room to the field to planning and scheduling, it appears that fully autonomous operations may be out of reach for many companies. The process industries will, however, continue to deploy more intelligent, semi-autonomous subsystems that allow the plant workforce to focus on higher-level tasks, even while simultaneously making the operation safer, more reliable, and more efficient.

To move toward autonomy in industrial processes, it is important to look at what can be fully automated, what elements will require human supervision, and which areas will remain manual. Once this clarity is established, it is possible to set a path to autonomy following six progressive levels:

Manual operations. With traditional manual operations, every aspect of the plant enterprise, including instructions and paper-based recordkeeping, is performed manually. Here, no automatic actions occur, with operations relying on humans to make all decisions and perform all functions. Most industrial sites began with significant human intervention required to run and maintain the operations.

Controlled and optimized operations. Given the widescale adoption of control systems and advanced control software, many industrial process facilities fall into the category of controlled and optimized. But just because most are in this category does not imply that most excel at it. Often an abundance of control loops are still running in manual mode or tuned incorrectly. Control loops running manually or those that are poorly tuned hinder optimization of the process. A large percentage of sites also have advanced control models that do not reflect current process dynamics or equipment performance, leading to poor results. In extreme cases, this situation can



CH003 FCC Unit
Control HIVE

HIVE Availability
2

Primary	4
Backup	4
Spare	4

	Date & Time	Location Tag	Source	Condition	Priority	Description	Trip Value
⚠	16/06/2020 15:29:03	Plant North	C300-15		H 00	Controller without backup	

Unacknowledged alarms:	1	of	1
Acknowledged alarms:	0	of	0
Shelved alarms:	0	of	0

16-Jun-20 15:29:45 Plant East CONSOLE 1 U 00 CStn01

Honeywell | Experion PKS R500 | 16-Jun-20 15:29:45 S C as01hscocsrv ● Plant East CStn01-1 Mngr

Resilient operations will reallocate the control application to available system resources, ensuring operations continue undisturbed, with no intervention required by operations. Sample screen is an Experion PKS HIVE system view.

result in sites giving up on advanced control altogether. Advanced control and optimization must be viewed as a lifecycle solution—one that is continually kept up to date.

Intelligent operations. The shift to intelligent operations is the essence of Industry 4.0. It is all about software analytics—collecting data, analyzing it, getting recommendations, and taking specific action. Companies can use digital twins to compare current process and equipment performance against expected performance. The benefit of using a model-based approach is that process and equipment performance is evaluated according to known or physical characteristics of plant processes. Users can model changes in the plant and current behavior, see if models are delivering the expected results, and employ the digital twin to close the loop between process dynamics and process design.

Remote operations. Once process operations are optimized and intelligent, users can think about leveraging the power of remote operations. From remote project execution, service, and support to centrally located remote operations centers, these capabilities are an opportunity to improve workforce efficiency, collaboration, and problem solving, and to effectively serve multiple sites or projects. Remote operations centers are used extensively in the industrial world, particularly in areas with distributed assets.

Resilient operations. Now, more than ever, plant owners require robust technology to help them withstand faults without having a large number of workers on site. They need resiliency measures such as backup power systems to keep equipment operating. Being resilient means that when failures do occur, the system or operation continues to run normally, and recovery is automated. There are many examples where this method occurs—for instance, in process automation systems with redundancy. Control systems are typically built with redundant controllers. If a controller fails, the redundant partner takes over, ensuring normal operations. At the same time, this controller is now nonredundant, and a process upset will occur if the controller also fails. Resilient operations will reallocate the control application to available system resources, ensuring that operations continue undisturbed, and that system resiliency is maintained, completely automated, with no intervention required by operations.

Autonomous operations. Ultimately, the destination of autonomous operations is enabling every day to be the best day of production and all staff to become experts in their assigned roles. The journey to autonomy is characterized by making use of all available digital technologies to realize advances in safety, reliability, and efficiency.

For the most part, the far upstream oil and gas business is one of autonomy—wellheads and pipelines are largely unmanned. By reducing the physical presence of people on an offshore platform to the few times it is absolutely necessary, operating companies can dramatically improve human safety while lowering operating costs. The mining industry is also rapidly moving toward autonomy, substantially decreasing the number of people at often very remote process locations in favor of centralized operations.

Although the aforementioned maturity model does have a natural sequence and evolution—it is recognized that most facilities will have a varying degree of capability at each level—plant operators might find that there are manual procedures for some operations, and they also have pieces of equipment that operate largely autonomously. So, it is instructive to assess existing capabilities at each level.

Trending toward the future

The trends are unmistakable: Autonomy is a critical technology that will lead process industry operations into the future. As technology moves beyond automation, autonomy and autonomous systems will bring improvements in many areas.

The latest developments around industrial autonomy provide a timely response to several key industry trends, including the desire for post-COVID-19 preparedness and resilience, growing operational complexity, the aging industrial workforce, and upskilling needs.

Regardless of an enterprise's current tools, design, or talent, integrating autonomous solutions at any level of production serves as a catalyst for increased operational performance by addressing safety, efficiency, and reliability issues to help promote business continuity. An unencumbered vision is necessary to plot the incremental steps to achieve a more autonomous future. This vision requires investing in automation systems in a strategic and consistent manner with the total lifecycle of the plant in mind. ■

Images courtesy of Honeywell Process Solutions

ABOUT THE AUTHOR

Joe Bastone is the director of product management for Experion® PKS with Honeywell Process Solutions, covering products such as Experion PKS HIVE, LEAP, Universal Channel Technology, Series-C IO, the C300 Controller, Experion Orion Console, and Virtualization solutions. He earned a BS in chemical engineering from Rensselaer Polytechnic Institute in New York. Bastone has been with Honeywell for over 20 years.

RESOURCES

LNS Research Report: *On the Road to Industrial Transformation (IX)*
https://www.lnsresearch.com/research-library

Honeywell Case History: *How Artificial Intelligence Keeps this Oil Company Running*
www.honeywell.com/us/en/news/2020/03/how-artificial-intelligence-keeps-this-oil-company-running

Honeywell Whitepaper: *New Approach to Control System Modernization*
www.honeywellprocess.com/library/marketing/whitepapers/Remote-Migration-Services-Whitepaper.pdf

Extreme OT Data Makeover

By Oliver Wang

Address challenges to quality operational data by paying attention to four key data aspects.

Industrial digital transformation had its beginnings in the Industry 4.0 initiative, unveiled in Germany in 2013. Since then, industrial digital transformation has morphed into an imperative that underpins business vitality. However, according to the *2020 Industrie 4.0 Maturity Index in Industry* released by the German National Academy of Science and Engineering (Acatech), more than 90 percent of businesses are still only in early stages of industrial digital transformation.

Most firms are still grappling with how to record and aggregate data generated by their operational technology (OT), equipment, and workforce. Such OT data is still far from delivering what the decision makers at most businesses initially hoped for. Their vision is having big data analysis results—completed and readily available—right on their screens, so that business insights can be implemented to lower cost, increase efficiency, or drive business model innovation. Companies still have a long way to go to get industrial digital transformation to this level.

Why are companies still behind in the industrial digital transformation race? One of the main reasons is that big data analytics, artificial intelligence (AI), and other innovative technologies are only implemented in the later stages of digital transformation. But if you do not obtain enough data in the early stages, then even the smartest AI or machine learning solution will have little value for you.

As we know, in the industrial digital transformation landscape, data comes mostly from OT environments—for example, a drilling well in the middle of a desert baking at temperatures of 40°C to 50°C, an oil pipeline system stretching for hundreds of kilometers in a freezing area, or a transportation system of a fast-moving and vibrating train. It does not require a huge stretch of one's imagination to perceive how difficult it is to capture data from these harsh environments.

Hence, kick-starting a transformation initiative first requires a failproof strategy on how to accurately capture OT data from industrial automation equipment. Furthermore, this is-

FAST FORWARD

- Most firms are still grappling with how to record and aggregate data generated by their equipment, systems, and workforce.
- Before trying to source OT data, consider data acquisition, data preparation, data transmission, and data security.
- Armed with these four capabilities, high-quality OT data can lay a solid foundation for transformation.

sue requires deep thinking. OT data has shifted from monitoring-oriented to optimization-minded—looking not just at the present but also to the future. Errors in data collected from its sources may lead to defects in subsequent analyses.

Therefore, the focus can longer be just capturing "stable data." Overcoming obstacles to quality data is the deciding factor of any transformation program's success. Industrial automation and business professionals need to pay attention—early in the digital transformation process—to four key pillars of data quality: acquisition, preparation, transmission, and security.

Challenge: Insufficient data

One of the challenges to data quality is insufficient data. This is mostly because automation systems were not designed for data analysis. Even in cases of data transmissions on a shop floor, data is tapped to support control equipment operations only, which is not enough by any measure for distilling business insights.

For example, a factory may have a bottleneck machine on its production line through which everything gets made or processed. If the machine goes down, the entire line shuts down. To minimize downtime, the plant needs to predict which key components inside the machine could fail and purchase the replacement components in advance. However, these devices seldom provide data regarding their key parts and components. Therefore, the company needs to install sensors in them and convert the generated analog signals to digital ones via remote I/Os. The digital signals can then be sent to servers in the upper layer or to the cloud to enable predictive maintenance. This demonstrates the capability, or attribute, of OT data acquisition.

In this scenario, only one machine needs to be worked on. If you are dealing with an entire factory with myriad communication protocols, it goes without saying that the complexity of conversion will be much greater. Because OT systems are typically used for a few decades or more, equipment from various vendors is often applied in the same system. Moreover, each piece of equipment has its own proprietary hardware

OT data has shifted from monitoring-oriented to optimization-minded—looking not just at the present but also to the future.

design, communication interface, and communication protocol to deliver operational availability.

If the equipment works independently, this silo approach is effective for ensuring system reliability and optimal performance. However, data silos will have formed over time. For instance, two production lines in the same plant may use different programmable logic controllers (PLCs) from two different vendors, each with its own communication language for the respective PLC. When seeking to aggregate data from different systems across multiple silos, a factory will find each system speaks its own language.

Fortunately, the market is aware of this problem. Many solutions are available, such as implementations of consistent and open standards like OPC UA or industrial protocol gateways to allow the extraction of data from a machine using an unfamiliar protocol. For example, with the help of Modbus-to-BACnet industrial protocol gateways, a heating, ventilation, and air conditioning system can obtain Modbus remote terminal unit data through the BACnet protocol.

Challenge: Meaningless data

The next challenge to data quality is unusable data. Equipment-generated data comes in the form of raw data or values. Information technology (IT) or business analysts cannot make use of the data as is, and manual data processing inevitably inhibits real-time response. If OT data is converted into meaningful IT values first, data can then flow in the edge-to-cloud architecture seamlessly and quickly.

OT data is structured as a series of time-related digits, each representing an event that happens to a specific device or sensor at a specific time, for example, the current magnitude of a certain motor every 10 seconds in the past seven days. Contrarily, IT data is database-residing data with rigorous structures and descriptions that must be given a meaning before being applied for various analyses. Of the OT data mentioned previously, only the numbers 7 and 10 are shown, and preprocessing is required to provide the data with complete meanings (dates, seconds, etc.) by adding the missing context. Only then can further analysis be conducted.

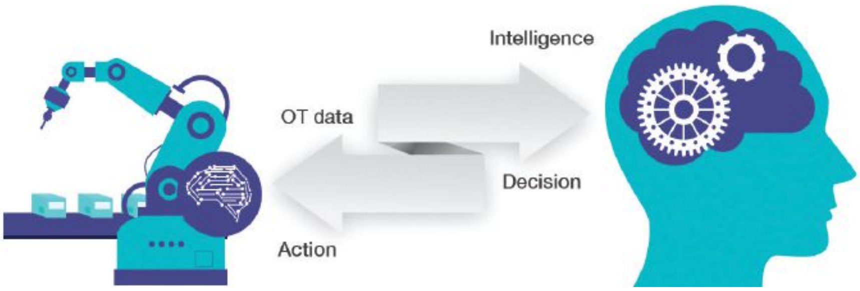
In addition, for the sake of control precision, OT equipment often produces a piece of data in intervals of a second or a millisecond. If every piece of raw OT data is transmitted to an IT system, the IT system will be overwhelmed and not able to do anything purposeful. Even worse, sending meaningless data to the cloud not only reduces operating efficiency but also increases data transmission and storage costs.

To tackle these problems, smart Internet of Things devices are used to regulate the frequency of data distribution. In doing so, OT systems can work in alignment with the needs of IT systems, such as uploading data once an hour, or processing data on the OT side first and only uploading it when a bigger deviation is observed. It takes these steps to excel at OT data preparation.

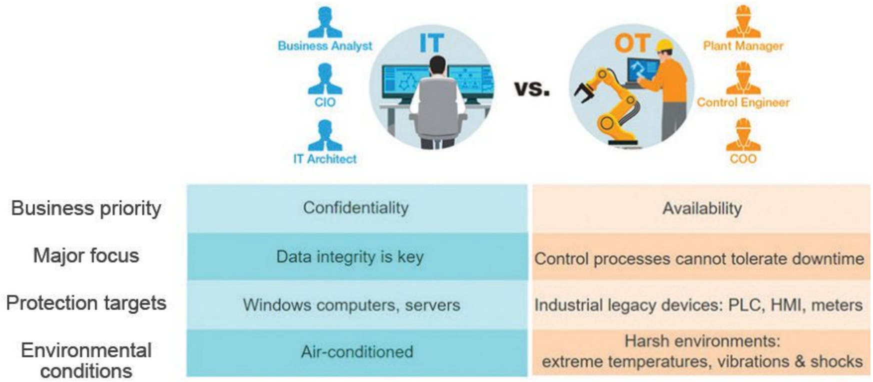
Challenge: Incomplete data

Digital transformation calls for more diverse and real-time data, and consequently, much more OT data to be transmitted. Although OT networks traditionally transmit data to meet control requirements, industrial digital transformation necessitates data transmission for analysis and decision making.

Take the smart factory as an example. To achieve zero failures, production lines must be able to provide immediate feedback every step of the way. When an aberration is detected—a sign of a problem in the previous station—the next station will instantly notify the previous one of the problem to prompt immediate reset, preventing small deviations from piling on top of each other and ultimately causing failures. In other words, lots of data will have to move through OT networks, including control information and defect images.



OT data's reach has expanded from controlling end devices to making business decisions.



	IT	OT
Business priority	Confidentiality	Availability
Major focus	Data integrity is key	Control processes cannot tolerate downtime
Protection targets	Windows computers, servers	Industrial legacy devices: PLC, HMI, meters
Environmental conditions	Air-conditioned	Harsh environments: extreme temperatures, vibrations & shocks

OT cybersecurity (right column) prioritizes very different values compared to IT cybersecurity.

At the same time, a new challenge will emerge: How does the factory avoid obstructing OT control data transmission with the addition of IT data?

Why is this a concern? It is because industrial Ethernet networks, the most-used industrial networks, do not have real-time control mechanisms for mass data. The proposed solution has been to have two separate networks for sending images and control commands. The advantage is the two streams of data do not compete for network bandwidth; the disadvantage is the cost of network implementation and maintenance doubles. Time-sensitive networking (TSN), the new-generation Ethernet, is designed to schedule transmissions according to the importance of the data, ensuring important data reaches the device at the scheduled time. This is what robust OT data transmission capability entails.

In addition, environmental disturbances, such as extreme temperatures or electromagnetic waves generated during the startup of a device, can cause network disruptions and the potential for data to be lost. Contingency plans should be made for all kinds of incidents to avoid losing data in transit during disturbances.

As an illustration, when a wired or wireless network is down, the network backup mechanism can immediately activate another section to resume transmission. Or, when the network is temporarily congested or disconnected, a certain amount of the latest data can be stored locally to ensure the data, if lost, will be retransmitted or retrieved to avoid delivering fragmented data.

Challenge: Vulnerable data

OT data becomes not trustworthy mostly from cybersecurity issues. In the past, OT systems did not need to be Internet connected and could be protected simply through physical controls, such as limiting access to an operational area or banning the use of USB sticks and personal computers. As industrial digital transformation takes off, Internet access becomes essential.

With increased connectivity, all vulnerabilities are suddenly laid bare to ruthless computer viruses or thrust onto the radar of profiteering hackers, providing channels to invade systems or disrupt operations. With cyberattacks becoming common, data security and cybersecurity are emerging as required items on every digital transformation agenda. To safeguard production capacity and keep production lines safe from data-tampering attempts, companies must pay attention to OT data security.

> Time-sensitive networking (TSN), the new-generation Ethernet, is designed to schedule transmissions according to the importance of the data, ensuring important data reaches the device at the scheduled time. This is what robust OT data transmission capability entails.

A misconception among businesses is that mature IT security solutions can be directly replicated in the OT world. In reality, security tools meant for IT environments are not entirely fit for OT system protection. For example, because OT devices do not run the operating systems compatible with antivirus software, installing it on OT systems is out of the question. Further complicating the antivirus situation is the importance of capacity availability in OT environments; the fear that production capacity will be hurt by data packets being wrongfully blocked has kept many machines away from antivirus software solutions.

Another OT data security issue is the fact that many manufacturers have deployed all devices on the same intranet for the sake of connection stability and convenience. However, once ransomware breaks into that environment, it can easily spread throughout the entire system. It is thus recommended to secure OT environments in three incremental stages: endpoint security, cybersecurity, and security management.

To enhance OT data security capability, industrial firms should:

- Apply intrusion protection system (IPS) technology to OT automation devices to secure critical infrastructure. An industrial-grade IPS monitors data flowing in and out of critical devices, segregates malicious traffic, and notifies administrators the instant an anomaly is detected.
- Take advantage of network layering to curb ransomware attacks. Firms will benefit from upgrading their Ethernet switches to managed Ethernet switches and activating the layering feature to divide an OT network into segments.
- Use network management software to overcome the interoperability hurdles among various OT communication protocols to effectively spot faulty or risky devices via visualization.

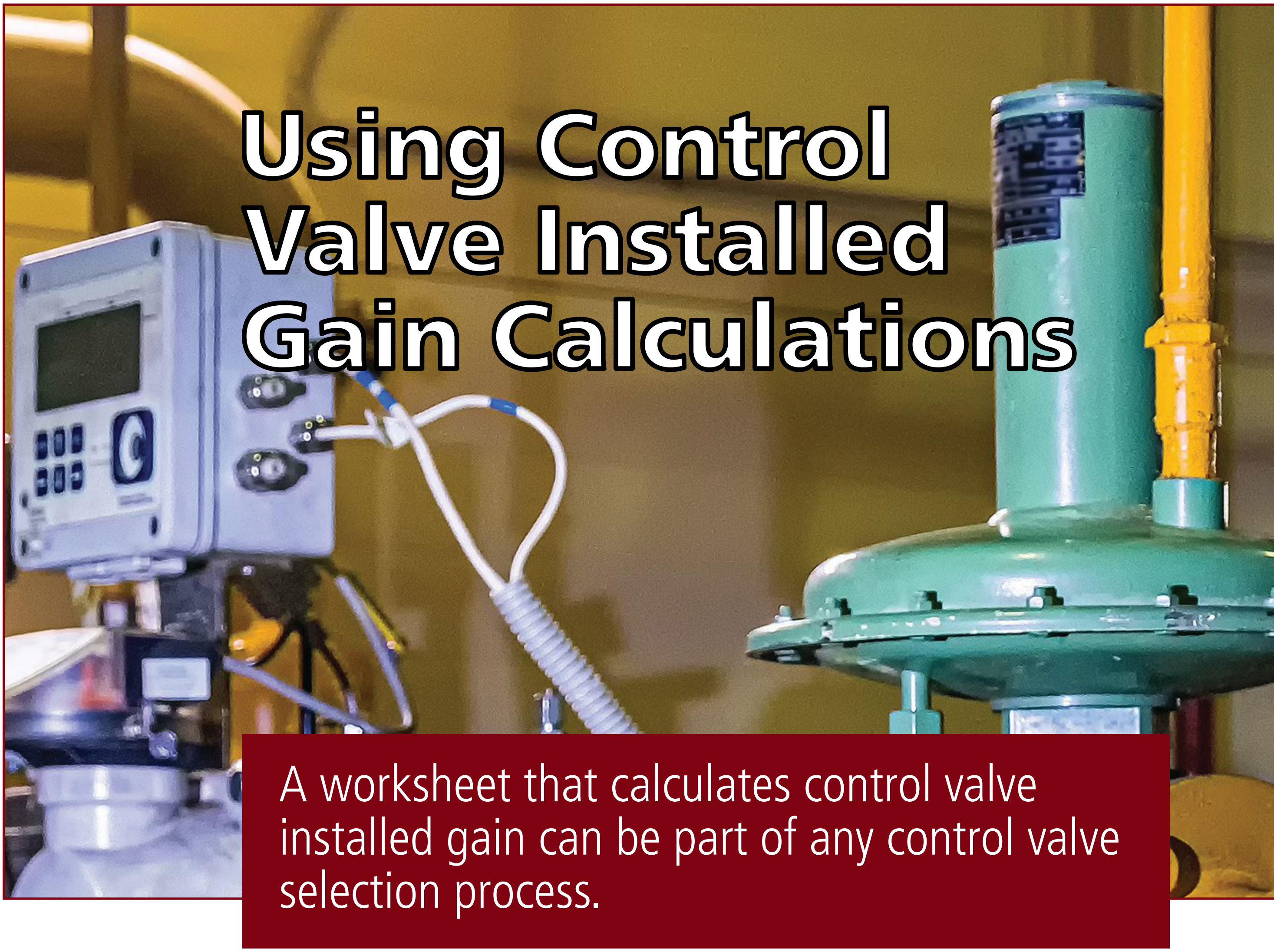
Use the four OT data capabilities

As the old saying goes, do not put the cart before the horse. It is critical to get your priorities straight in industrial digital transformation. Do not let poor-quality raw data undermine the results of your big data analyses.

Before trying to source OT data, consider where you are in terms of data acquisition, data preparation, data transmission, and data security. Armed with these four capabilities, you will be able to tackle the challenges head on and leverage high-quality OT data to lay a solid foundation for transformation. ■

ABOUT THE AUTHOR

Oliver Wang (www.linkedin.com/in/oliver-wang-6873a329) is product marketing manager, edge connectivity and computing, for Moxa, where he has worked for more than 15 years. Wang has a degree from the University of California, Berkeley. Access Moxa’s library of white papers at https://moxa.com/en/case-studies.



Using Control Valve Installed Gain Calculations

A worksheet that calculates control valve installed gain can be part of any control valve selection process.

By Jon F. Monsen, PhD, PE

For many years, the author has used, and promoted the use of, control valve installed flow and gain graphs as part of the control valve selection process (references 1–3). For all those years, the author has had the benefit of being associated with a valve manufacturer with a publicly available control valve-sizing application that included installed flow and gain graphing capability. Users who preferred other brands of control valves, and thus those manufacturers' control valve-sizing applications, were hesitant to learn to use a new application to take advantage of the graphing capability.

Recently, the author published an article that included detailed instructions for constructing a Microsoft Excel worksheet (www.control-valve-application-tools.com) that generates installed flow and gain graphs in conjunction with valve-sizing calculations made with any valve-sizing application. This makes it practical for anyone to incorporate graphing installed flow and gain into their valve selection process (reference 4). This article explains how to use control valve installed gain calculations.

Figure 1 is an example of a properly sized valve compared to an oversized valve. One valve manufacturer suggests the following gain criteria for installed gain within the specified flow range:

- Gain > 0.5
- Gain < 3.0
- As constant as possible
- As close to 1.0 as possible
- Gain (max) / Gain (min) < 2.0.

Extremely low gains are undesirable, because a low gain means when the valve moves, the flow does not change by much. It might not be as obvious why high gains are undesirable. An audio amplifier with a high gain may be desirable. But control valves are mechanical devices, and parts that move while in contact with each other tend to stick when not moving. If a valve, because it tends to stick when not moving, can only be positioned within 2 percent of the desired position and has a gain of 4, the flow can only

FAST FORWARD

- An Excel worksheet makes it practical to include the graphing of installed flow and gain in the valve selection process.
- Extremely low gains are undesirable, because a low gain means that when the valve moves, the flow does not change by much.
- Pump selection affects installed gain and installed flow.

be adjusted within 8 percent steps, which may not be desirable. The reason for limiting the gain change within the required flow range to 2:1 is so it will be easier to tune the controller for stable and fast response throughout the required flow range.

To calculate and graph the installed flow and gain using the reference 4 worksheet, the process model and the worksheet require the following information about the process:

- The minimum design flow, Q_{min}
- The maximum design flow, Q_{max}
- The valve inlet pressure at the minimum design flow, $P_{1\ minQ}$
- The valve inlet pressure at the maximum design flow, $P_{1\ maxQ}$

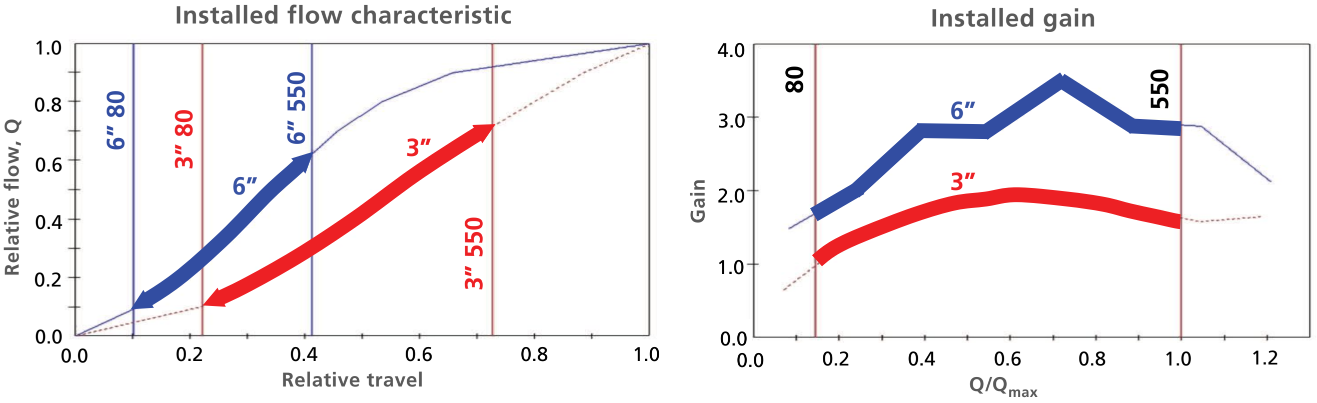
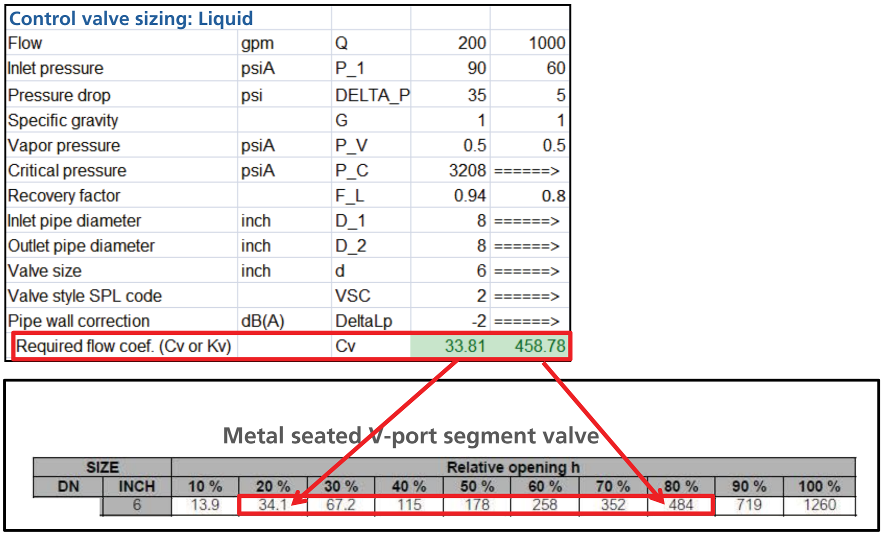


Figure 1. Control valve installed flow and installed gain characteristics comparing a properly sized 3-inch valve and an oversized 6-inch valve in the same system. Emphasis is added to show the portion of the graphs that fall within the user's specified flow range between minimum and maximum required flow of 80 to 550 gpm.



Control valve sizing: Liquid

Flow	gpm	Q	200	1000
Inlet pressure	psiA	P_1	90	60
Pressure drop	psi	DELTA_P	35	5
Specific gravity		G	1	1
Vapor pressure	psiA	P_V	0.5	0.5
Critical pressure	psiA	P_C	3208	======>
Recovery factor		F_L	0.94	0.8
Inlet pipe diameter	inch	D_1	8	======>
Outlet pipe diameter	inch	D_2	8	======>
Valve size	inch	d	6	======>
Valve style SPL code		VSC	2	======>
Pipe wall correction	dB(A)	DeltaLp	-2	======>
Required flow coef. (Cv or Kv)		Cv	33.81	458.78

Metal seated V-port segment valve

SIZE		Relative opening h									
DN	INCH	10 %	20 %	30 %	40 %	50 %	60 %	70 %	80 %	90 %	100 %
	6	13.9	34.1	67.2	115	178	258	352	484	719	1260

About 20% to 78% open

Figure 2. User's calculation of required valve C_V at maximum and minimum design flows and valve manufacturer's C_V table for a 6-inch segment ball valve.

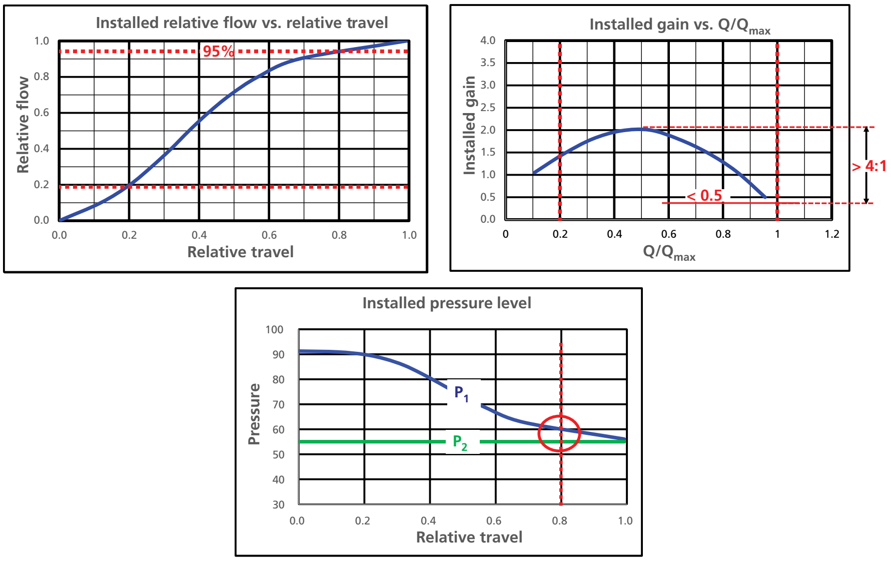


Figure 3. Installed characteristics of the valve proposed in figure 2.

- The valve outlet pressure at the minimum design flow, $P_{2\ minQ}$ (calculated from the user's input of the valve pressure drop at the minimum design flow, DELTA P_{minQ})
- The valve outlet pressure at the maximum design flow, $P_{2\ maxQ}$ (calculated from the user's input of the valve pressure drop at the maximum design flow, DELTA P_{maxQ}).

The values of P_1 and P_2 at the minimum and maximum design flow need to be obtained by an analysis of the frictional pressure losses and static pressure changes in the system upstream and downstream of the control valve (references 5–6).

Reference 4 prompted several inquiries as to what applications would be candidates for installed flow and gain graph analysis. Below are some of the most common.

Surprising results

Figure 2 shows a user's Excel control valve-sizing worksheet. The calculated C_V range appears to show a 6-inch segment ball control valve would be operating at about 20 percent to 78 percent open from the minimum design flow to the maximum design flow. An installed flow and gain calculation yielded surprising results (figure 3).

The installed flow graph shows the minimum specified flow intersecting the installed flow graph at 20 percent relative travel, and the maximum design flow intersecting the installed flow graph just a bit below 80 percent relative travel, which agrees with the user's calculation. What the user's calculation did not show is 95 percent of the valve's fully open flow is at the maximum design flow, leaving no safety factor at the high end.

At about 60 percent travel (relative travel of 0.6), the installed flow graph starts rounding off to a much shallower slope. This fact is identified on the installed gain graph where the installed gain drops to below 0.5, emphasizing the fact that changes in valve position would have only a small effect on flow in the system. The gain change from the maximum design flow (Q/Q_{max}) and the maximum gain on the graph is greater than 4:1, making it difficult to tune the controller for fast and stable control. It turned out the problem lies with the user's pump choice.

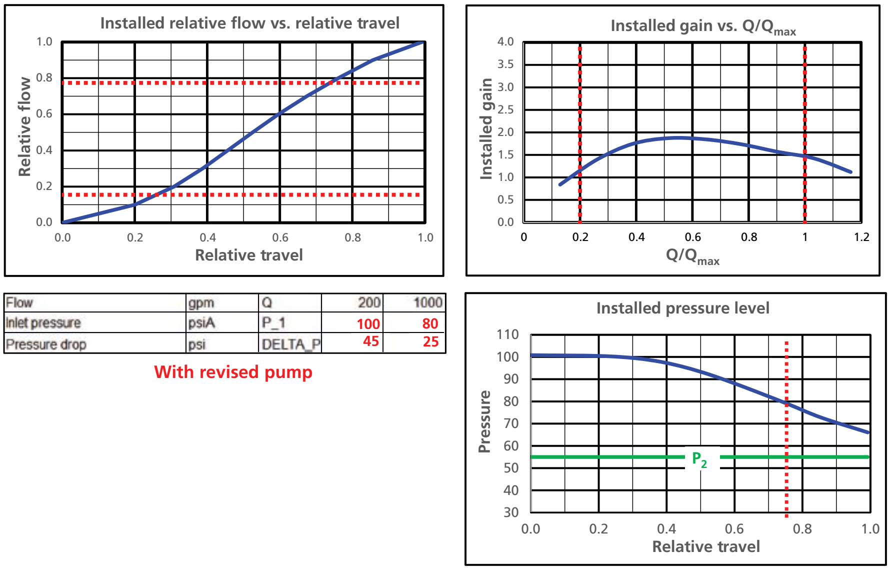
Reference 4 does not include the ability to graph what is happening to P_1 and P_2, and thus the pressure differential available to the valve. However, the reference 4 worksheet has a tabulation of P_1 and P_2, so constructing a graph of P_1 and P_2 versus relative valve travel was simple. In the installed pressure level graph, as valve relative travel approaches 0.8 (80 percent valve travel), the pressure drop available to the valve decreases rapidly.

Different pump, different valves

The user found a pump with a slightly higher and flatter head curve. A new analysis of the upstream system gave the revised values of P_1 and DELTA P shown in red in figure 4. Putting these new values of P_1 and DELTA P into the user's valve-sizing program and into the reference 4 worksheet gives the graphs of figure 4. The valve is now operating between 25 percent and 75 percent travel. The maximum design flow is now at slightly less than 80 percent of the fully open flow, giving ample safety factor at the high end of the range. The installed gain graph is much flatter and well within the suggested limits.

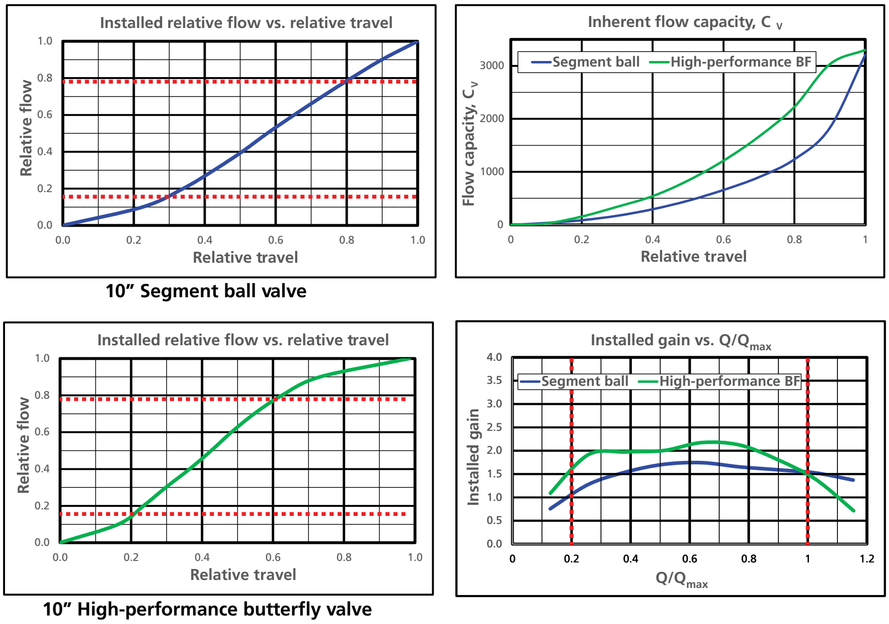
Figure 5 is based on an application where the system designer recommended a 10-inch segment ball valve after examining the installed flow and gain graphs and determining the segment valve was a good choice. The purchasing agent commented that a 10-inch high-performance butterfly valve would cost approximately one-third less than the segment ball valve. The system designer agreed to investigate the applicability of a high-performance butterfly valve, knowing the two valve styles have quite different inherent flow characteristics. Segment ball valves tend to have a nearly perfect equal percentage characteristic. High-performance butterfly valves tend to have an inherent flow characteristic between linear and equal percentage.

The upper right graph in figure 5 compares the inherent flow characteristics of the two valves being considered. The installed characteristics are linear between the design minimum and maximum flows. The installed gain of each valve meets the suggested gain limits between the minimum and maximum design flows. The gain of the segment valve is slightly closer to 1.0. The maximum gain change of the butterfly valve is 1.4:1, where the maximum gain change of the segment valve is 1.6:1. In this system, either valve would likely control satisfactorily. In a system with different valve pressure drop versus flow characteristics, this might not be the case.



Flow	gpm	Q	200	1000
Inlet pressure	psiA	P_1	100	80
Pressure drop	psi	DELTA_P	45	25

Figure 4. Installed characteristics of the valve with the revised figure 2 pump pressures shown in red.



10” Segment ball valve

10” High-performance butterfly valve

Figure 5. Comparison of a segment ball valve and a high-performance butterfly valve in the same system. The installed gain of both valves is plotted on a single graph.

Which pressure drop?

A question arose regarding the pressure drop to use when sizing a control valve. Assuming a system that has already been designed, the sizing pressure cannot be arbitrarily assigned, but the values of P_1 and P_2 need to be obtained by an analysis of the frictional pressure losses and static pressure changes in the system both upstream and downstream of the control valve. The ideal situation is where the person selecting the control valve has a say in determining what the control valve pressure drop will be, most often by specifying the pump that will be used. Using an installed gain analysis of various pumps that might be suitable can be helpful.

To demonstrate how this can be done, three possible pumps for the system shown in figure 6 will be considered, and the one that allows satisfactory controllability while minimizing energy consumption will be selected. Curves of P_1, the pressure just upstream of the valve, are shown for each of the three pumps, along with the power required by each at a normal flow rate of 400 gpm. These curves slope downward in proportion to the flow squared from the 100 gpm pump head (45, 60, and 75 psig, respectively, for pumps A, B, and

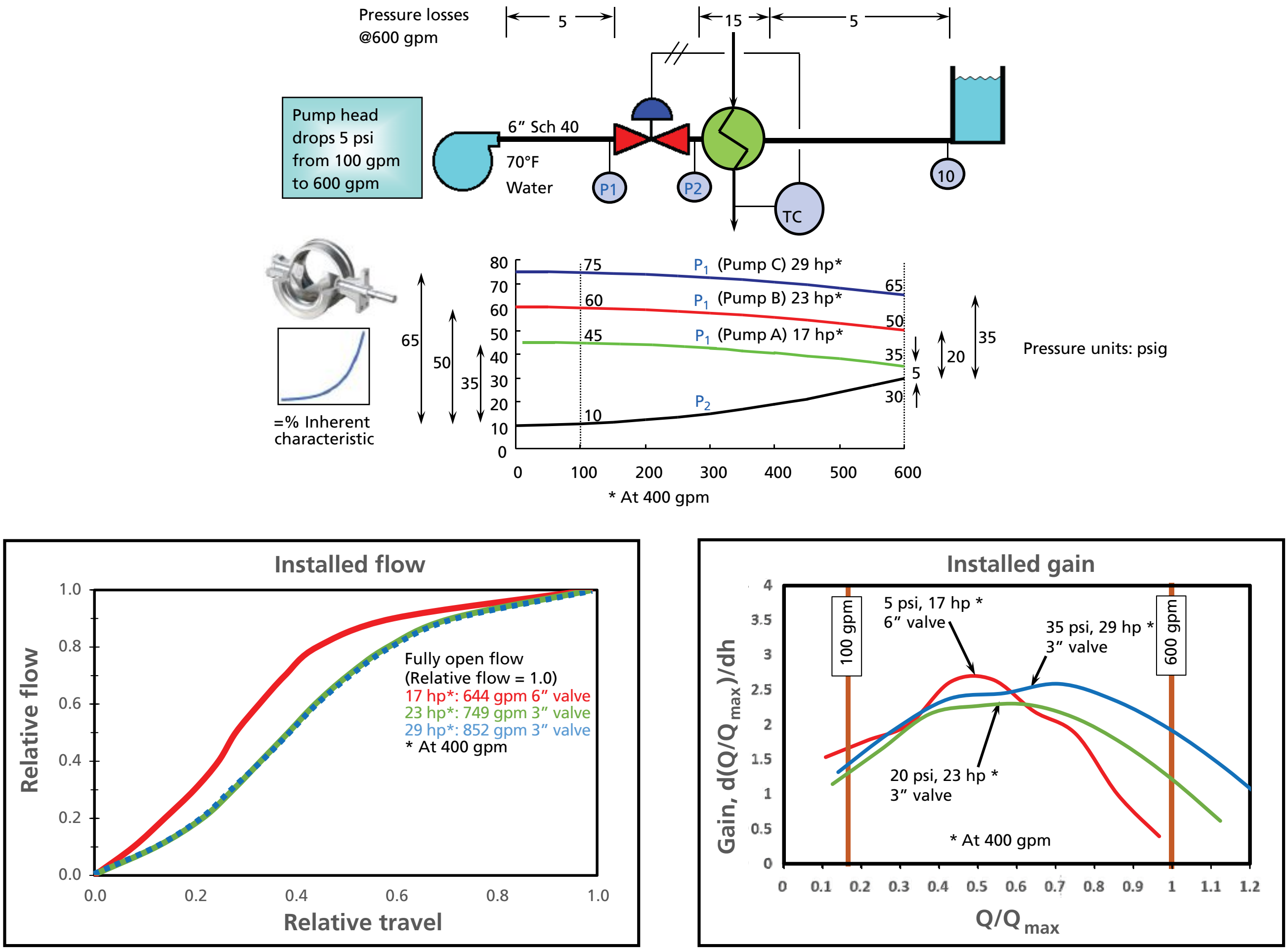


Figure 6. Control valve installed gain analysis helps balance pumping energy and process controllability.
Segment valve graphic courtesy of Neles

C) to a pressure 10 psi lower due to the combined effect of the 5 psi pressure loss in the upstream piping and the 5 psi decrease in pump head from 100 gpm to 600 gpm stated in the figure. The curve for P_2, the pressure at the control valve outlet, starts with the 10 psig static head of the tank at very low flows and increases in proportion to the flow squared to 30 psig as the downstream piping and heat exchanger pressure losses increase to their 600 gpm values.

The ideal situation is where the person selecting the control valve has a say in determining what the control valve pressure drop will be, most often by specifying the pump that will be used.

The control valve pressure drops (the difference between P_1 and P_2) are indicated in the figure by the arrows at the left side of the figure for 100 gpm and at the right side of the figure for 600 gpm.

The analysis is performed based on using a segment ball valve. The graph in the lower left of figure 6 shows the calculated installed flow characteristics. Keep in mind the installed flow graphs generated by the worksheet of the reference 4 graph is relative flow, so 1.0 is 100 percent of the fully open flow, which is different for each of the three cases. What is interesting is the installed gain graphs.

With the 17-hp pump, besides requiring a more expensive 6-inch valve, the gain graph looks terrible. The installed gain is the highest of the three (meaning a larger flow error for the same valve position error), it drops to 0.4 as it approaches the maximum design flow (the red vertical line at 1.0 on the Q/Q_{max} scale), and the variation in gain over the flow range is almost 7:1, much greater than the recommendation of 2:1. This is large enough that it would be difficult to come up with proportional-integral-derivative (PID) tuning parameters that would provide good and stable control over the entire required flow range. The gain graphs of the 23-hp and 29-hp pumps fall within the recommended gain criteria, but the 23-hp pump is the winner, because its gain is closer to 1.0, and it also is the more economical of the two to operate. ■

ABOUT THE AUTHOR

Jon F. Monsen, PhD, PE, (jmonsen@valin.com) is a control valve technology consultant for Valin Corp. , the author of the chapter on "Computerized Control Valve Sizing" in the *ISA Practical Guides Book on Control Valves,* and the author of the book *Control Valve Application Technology: Techniques and Considerations for Properly Selecting the Right Control Valve*. With his more than 40 years of experience, he has lectured nationally and internationally about control valve application and sizing, and he hosts a website (www.control-valve-application-tools.com) where he offers free information and Excel worksheets for those who specify or use control valves.

REFERENCES

1. Monsen, Jon, Rules of Thumb, *Flow Control*, November 2012 pp. 24–26

2. Monsen, Jon, An Insider's Guide to Installed Gain as a Control Valve Sizing Criterion, *Flow Control*, May 2015, pp. 22-25.

3. Monsen, Jon, Modern Tools for Sizing Control Valves & Actuators, *Processing* January 2018 pp. 12-14

4. Monsen, Jon, Calculating the Installed Flow and Gain of a Control Valve, *Process Instrumentation*, March 2021, pp. 26–30. (The worksheet described in the reference, along with an enhanced version, can be found at www.control-valve-application-tools.com.)

5. Jessee, Peter, Determining Pressure Drop for Control Valve Sizing, *Flow Control*, August 2000, pp. 12-14.

6. Coggan, D. A, ed., "Fundamentals of Industrial Control," Second Edition, Research Triangle Park, NC: Instrumentation, Systems, and Automation Society (ISA) (now the International Society of Automation—ISA), 2004. pp. 278–280.

RESOURCES

"Choked Flow in Control Valves"
www.automation.com/en-US/Articles/August-2021/Choked-Flow-Control-Valves

"Using Flowmeter Diagnostic Data"
www.automation.com/en-US/Articles/February-2021/Using-Flowmeter-Diagnostic-Data

"Secure Industrial Control Systems with Configuration Control"
www.automation.com/en-US/Articles/May-2021/Secure-Industrial-Control-Systems-Configuration

Electrical Panel Connectivity

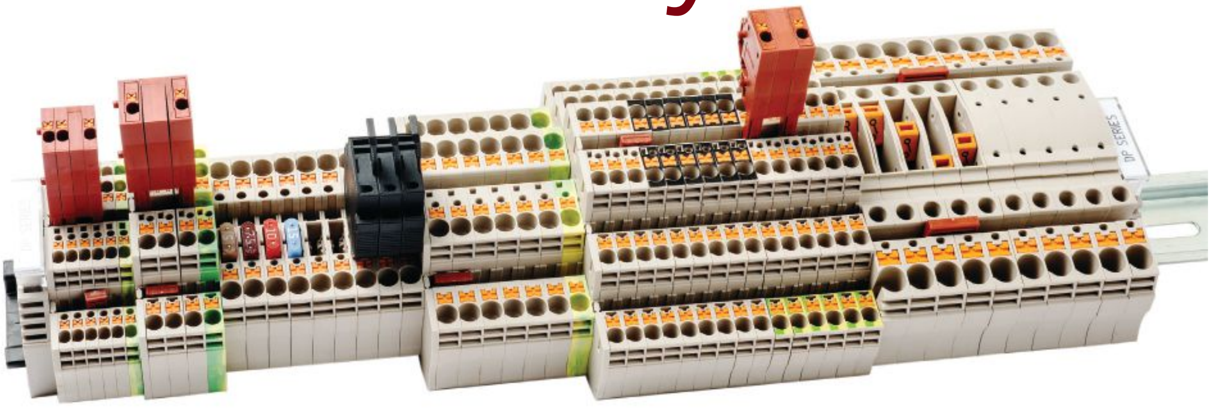


Figure 1. Push-in design terminal blocks are available in many configurations with a variety of connection technologies that reduce wiring labor compared with traditional screw terminals.

By Matt Hou

Terminal blocks, connectors/cordsets, and interface modules connect electrical and control panels to the outside world.

Much of the focus of electrical and control panel designers is on selecting, arranging, and protecting internal components. After all, locating power and automation equipment in the field, close to the loads and devices they serve, is the main purpose.

However, it is also important to properly select, design, and install components to make associated electrical connections. Even though wireless is becoming popular for certain types of communications, it is often still necessary to connect electrical wires using terminal blocks or other connectors.

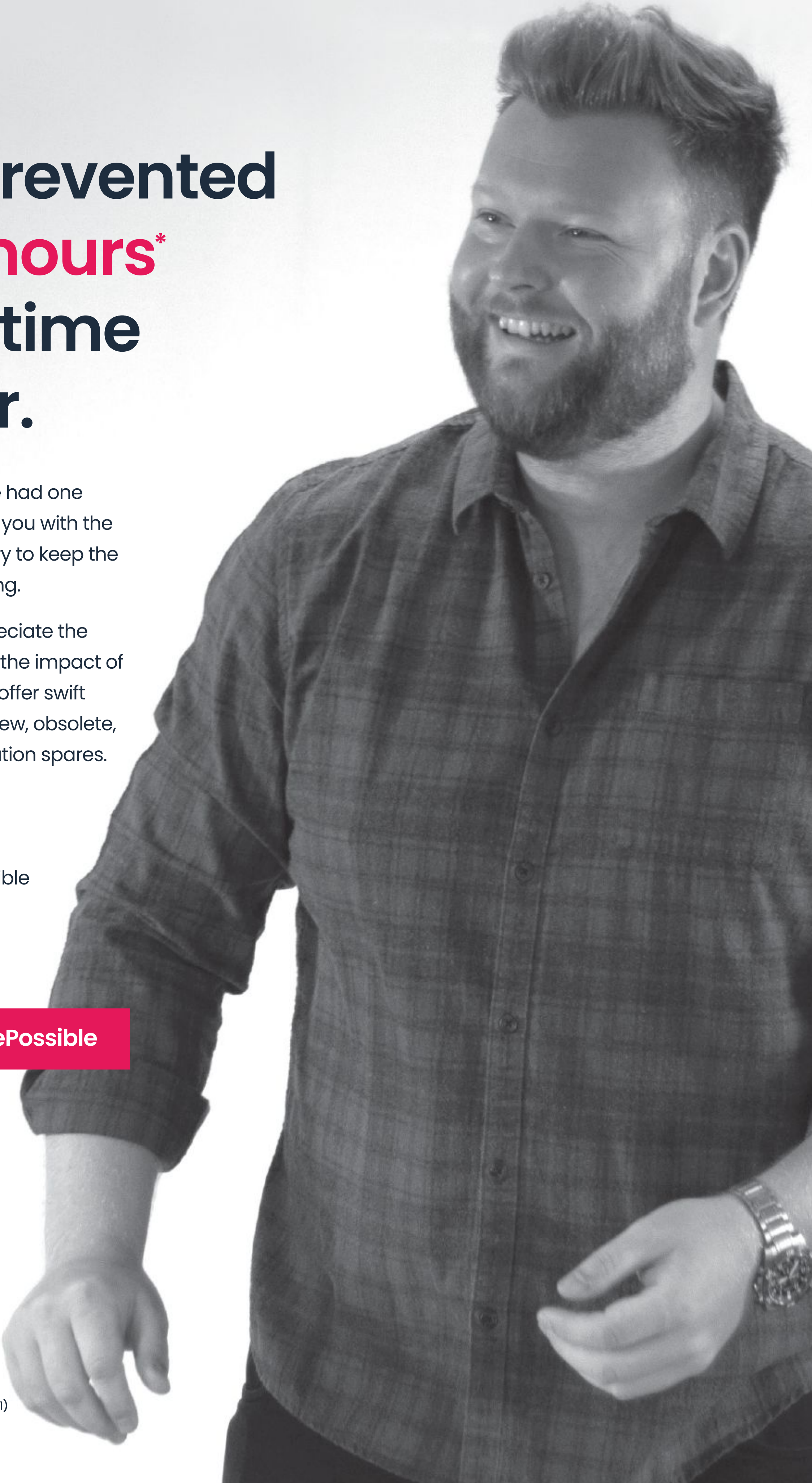
Whether for commercial or industrial use, these panels and the associated connections can be in harsh environments, with extremes of temperature, liquids, chemicals, vibration, and more. To ensure that the electrical interfaces between panels and field wiring perform reliably for the long haul, panel designers need to consider the best connectivity options. Terminal blocks, connectors/cordsets, and interface modules are the basics worthy of attention.

Classic connectivity: Terminal blocks

Terminal blocks have long been the standard way for landing field wires—both individual conductors and multiconductor cables—into a panel. But that does not mean there has been a lack of innovation for this termination style. The major terminal block connection technologies (shown in figure 1) are:

Screw terminal. This traditional technology uses screws, with or without pressure plates, to terminate wires directly or via a crimp lug. A wiring cage can compress on bare wire or a ferrule, or a ring or fork lug can be connected to the wire and inserted under the screw. Users must torque the connection properly to ensure a long-lasting, positive connection. To prevent the wires from loosening over time, some manufacturers have designed the structure to lock the screws in place and be maintenance-free. The screw terminal method is universal, recognized globally, and can handle the widest range of wire sizes.

Spring clamp. This technology uses spring force on the conductor to provide maximum contact reliability, even in high-vibration environments. A tool,



usually a screwdriver, is needed to push open the terminal points as the wire or ferrule is inserted, but completing a termination is faster and easier than it is with a screw terminal. This type of connection is beneficial to use in high-vibration environments such as railway and marine applications.

Push-in design (PID). PID terminals are also spring loaded and allow users to directly push in solid wires or stranded wires with ferrules without a tool. It is the fastest and most efficient connection possible. This technology reduces wiring labor by at least 50 percent compared with traditional screw terminals, and it provides a durable connection, similar to spring cage technology. A tool is needed to remove a wire.

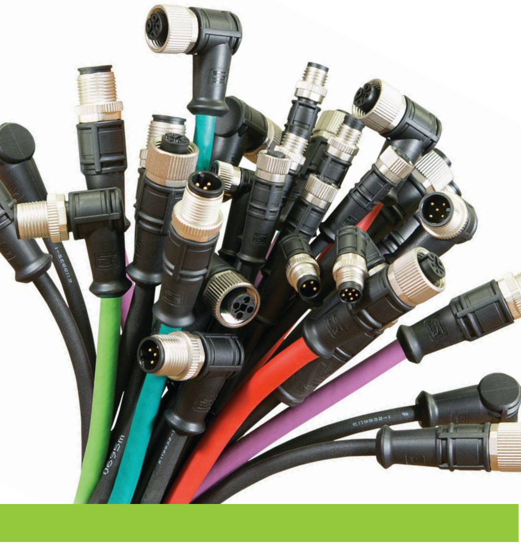


Figure 2. Circular connectors and cordsets provide reliable and flexible connectivity options, even for the most challenging industrial conditions.

Larger-size conductors and higher-power connections typically use screw terminals. Smaller conductor sizes for lower power and signaling applications work well with either spring cage or PID terminals. Many terminal blocks click on to standard DIN rails for easy and secure installation, but some traditional or larger sizes must be mounted to a backpanel.

Users must also consider what functional arrangements are needed. These could include:

- Feed through, the most common and simple type of terminal block. It is single level and provides one wire-to-wire connection. Some types have multiple connections for one-to-two or two-to-two connectivity.
- Multilevel, which is like the feed-through style, but with two, three, or more isolated levels stacked together for substantial space savings.
- Grounding, where the terminals are electrically connected to the DIN rail or panel on which the terminal is mounted. This provides a ground connection, without having to purchase and install a separate ground wire.
- Disconnect, which is like the feed-through style but incorporates a knife switch to easily open (disconnect) the circuit without removing wires.
- Fused, which is like the disconnect style, but the switch houses a fuse for downstream circuit overcurrent protection. It may also include an LED blown fuse indicator for troubleshooting convenience.
- Sensor/actuator, which is like the multilevel style but may also include a grounding connection. This is especially suitable for common multiconductor cable wiring that is often used for connections with sensors and actuators.

Flexible connectivity: Circular connectors

Circular panel casing-mount connectors, and the associated molded-connector cordsets, have become the industry standard in many industries for connecting devices to electrical and control panels (figure 2). They reliably transmit signals, data, and power, while providing the physical flexibility desirable for many installations. Furthermore, they offer a simple way to quickly disconnect circuits for service, making work safe and convenient for maintenance technicians.

Device connectors are designed to mount on the exterior casings of equipment and panels, via threaded or precut holes, while maintaining the environmental rating. There are also PCB-mount versions in straight or right-angle configurations.

The associated cordsets have matching fittings—commonly in metric sizes M8 or M12—and insert into the connector. The knurled fitting is then tightened to secure and seal the connection. Cordsets are available with straight or right-angle ends, in male or female, as needed.

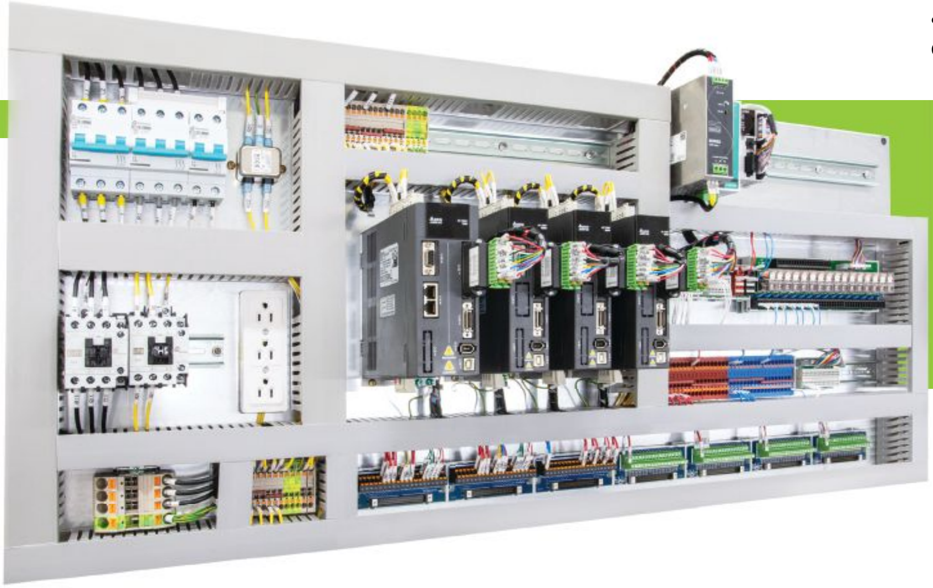


Figure 3. Interface modules (shown at the bottom and right of this picture) are a universal way for designers to provide compact and high-density connectivity, especially for control panel I/O signals.

Designers should ensure the materials are rated for the environment. For instance, nickel-plated die-cast fittings can withstand high humidity, large temperature changes, and vibration. PVC cables are best for solvent resistance and washdown environments, while PUR cables are better for the abrasion resistance often required in high-frequency movements, such as for robotic arms.

High density connectivity: Interface modules

Interface modules combine terminal blocks and connectorized cables to provide the highest possible connection density, and they are typically used for programmable logic controller and similar signaling and I/O module applications (figure 3). One wire harness connects between an I/O module and the interface module, with the interface module installed on a DIN rail. The harness may use industry-standard IDC, D-Sub, or MDR connectors as needed.

This connection method transfers anywhere from two to 40 signals as individual points, and it provides compact terminals for the field wiring connection. Installers save significant time on the panel side connections and avoid installation errors.

Effective panel connectivity

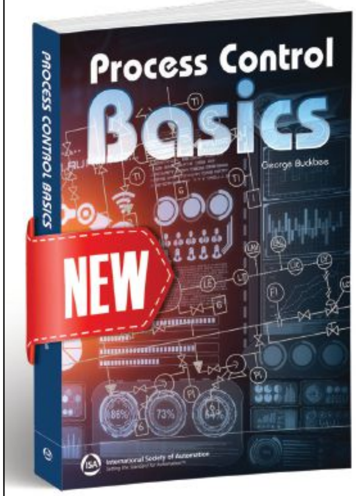
Regardless of what combination of terminal blocks, circular connectors, and interface modules designers choose for panel connectivity, there is more to consider. All components should be recognized or rated by the proper agencies with regard to standards such as UL508, UL1059, and IEC 60947. These standards ensure the materials and component construction are sufficient for industrial use. Furthermore, designers should think about usability features such as color coding, along with easy provisions for marking and tagging.

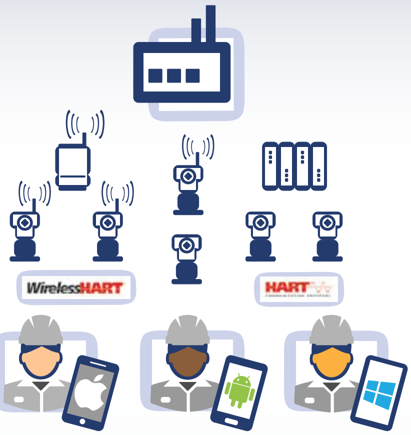
Electrical and control panels are necessary for almost any application using electrical power or automation. By using modern connection options, designers can save significant panel space and create equipment that is easy to fabricate, install, and maintain. Labor costs are reduced, and the right connection products provide improved reliability, functionality, and safety throughout their lifecycles. ■

Figures courtesy of Dinkle International

ABOUT THE AUTHOR

Matt Hou is a sales engineer for Dinkle International and has been an integral part of the development of the Dinkle Corporation's USA subsidiary since 2018. Hou holds a BS in electrical engineering from the University of Waterloo in Canada.





ISA Names Claire Ramspeck New Executive Director

ISA has announced that its new executive director will be Claire Ramspeck. She is the founder of Hobbs Barrett, a private consulting firm that specializes in association management with a focus on development, adoption, and dissemination of standards and other technical products and services. Prior to that, she built a successful career as the director of technology at ASHRAE, the American Society of Heating, Refrigerating and Air-Conditioning Engineers, and as the managing director of standards development at the American Society of Mechanical Engineers (ASME).

In addition to her 25-year history of leading standards and technology businesses within associations, Ramspeck also brings a wealth of volunteer experience, chairing and serving on several boards and committees for the American National Standards Institute (ANSI) and Underwriters Laboratory (UL.)

ISA President Steve Mustard, who chaired the executive search committee to recruit and select Ramspeck, highlighted her standards experience as a key factor in the committee's decision. "Claire has an impressive history of collaborating with volunteers and subject-matter experts to develop standards, research, and other projects that meet the needs of industry," said Mustard. "ISA's value is rooted in our standards development, and we build our portfolio of market offerings around key standards that help industries lower costs, boost productivity, and improve safety and cybersecurity. Claire's background will empower her to take ISA's valuable content to the next level."

ISA's current executive director, Mary Ramsey, will retire at the end of the year. "The time I've spent with ISA has been a rewarding chapter of my career, and I'm grateful for the collaboration and support of our members, leaders, and professional staff," said Ramsey. "We have been able to accomplish great things, including the creation of the ISA Global Cybersecurity Alliance, a group that continues to advance automation cybersecurity on the world stage. Given Claire's focus on technology adoption, I'm confident ISA will continue to build on its considerable strengths and continue to bring value to the industries we serve."

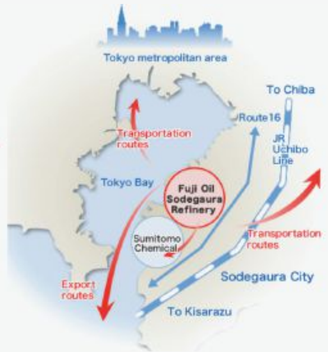
Ramspeck holds a BS in mechanical engineering from North Carolina State University and an MBA from Georgia State University. Before working with associations, she was a design engineering contractor for the Department of Energy through Bechtel Savannah River. Ramspeck has been honored with the Meritorious Service Award from ANSI and the Norman R. Harbaugh Scholastic Achievement Award from the Georgia State University College of Business. ■

Fuji Oil Company Ltd. Wins ISA100 Wireless Award

Each year, the ISA100 Wireless Compliance Institute (ISA100WCI), a subsidiary of ISA, presents the ISA100 Wireless Excellence In Automation Award to a global end-user company that has demonstrated outstanding leadership and innovation with ISA100 Wireless technology. Earlier this year, the ISA100WCI announced that the 2020 award had been presented to Fuji Oil Company, Ltd.

The company's contributions and achievements in the promotion of wireless instrumentation over the years through the ISA100WCI have been highly regarded in the industry. The company has improved safe operations and maintenance efficiency by using ISA100 Wireless technology to visualize the operating status of existing refinery facilities.

With the introduction of a wide variety of ISA100 Wireless products, Fuji Oil Company, Ltd., has achieved many results, including safer operations and improved maintenance efficiency through enhanced site monitoring and risk management. The company was also recognized for its efforts to promote wireless instrumentation by sharing on-site know-how to maintain the stable operation of wireless networks, and disseminating requests and feedback to wireless product vendors through ISA100WCI user seminars. Find out more at isa100wci.org.



The Fuji Oil Company, Ltd., Sodegaura Refinery is located on the corner of Keiyo Seaside Industrial Zone in Tokyo Bay and has a production system that can flexibly respond to changes in product demand. It produces various petroleum products from crude oil from around the world, and supplies them domestically and internationally.

The company has various shipping facilities, such as sea shipping, tank truck shipping, rail shipping, and pipeline shipping. In particular, the marine shipping facility is equipped with one of the largest dedicated piers in Japan, where 120,000-ton class tankers can directly land. Strengthening on-site monitoring through the introduction of wireless instruments has contributed to their safe operation, environmental protection, and operational efficiency, and is drawing out the strengths of the Sodegaura refinery, according to the company. ■

ISA, Endress+Hauser Collaborate to Expand Training Offerings

ISA and Endress+Hauser are collaborating to provide expanded training and certification course offerings to automation and instrumentation professionals. ISA will offer select certified training courses in conjunction with E+H's instrumentation training courses at E+H's process training units (PTUs) located across the U.S. These 11 full-scale process units provide hands-on experience with the types of configurations, operations, diagnostics, and troubleshooting found in modern process plants.

"We are thrilled to collaborate with Endress+Hauser and leverage the strengths of our respective organizations," says Geri McGrath, director of global education and outreach at ISA. "The combination of Endress+Hauser's PTUs and ISA's training services offers increased workforce development opportunities for industrial automation and control professionals."

Through this collaboration, ISA will bring its renowned expertise in controls, valves, and drives to more students in a real-world setting. ISA will send a representative to Endress+Hauser PTUs to teach its standards-based, vendor-neutral training using a seamless, holistic approach. This joint effort helps provide a one-stop shop where automation professionals can propel their education and careers forward.

"Combining a selection from the deep ISA training offering with the many choices of instrumentation training provided at Endress+Hauser's world-class PTUs provides a powerful set of options for instrument technicians who need help with their professional development," says Jerry Spindler, customer training manager, Endress+Hauser USA.

ISA has long provided certification for automation professionals through its Certified Controls System Technician (CCST) program. ISA and Endress+Hauser will focus on providing training for Level 1 certification, which affirms that technicians possess extensive knowledge of calibration, maintenance, repair, and troubleshooting.

The two have also codeveloped an online assessment tool for identifying technical strengths and knowledge gaps, allowing individuals to develop a training plan to meet specific needs. The tool is based on ISA's CCST Body of Knowledge, and will be offered through both the ISA and Endress+Hauser websites in 2022. ■

Dow Technology Leader Keynotes Digital Transformation Virtual Conference

"Obtaining value from digital transformation is only possible if culture change is achieved," said Dow Global Process Automation technology leader Paul Tomlin. His presentation, "Utilizing Digital Technology to Gain Competitive Advantage," was the keynote speech of the ISA's Digital Transformation Virtual Conference, held on 31 August 2021. The presentation set the tone for the day-long virtual event, highlighting current industrial automation operational paradigms, identifying opportunities in digitalization, and emphasizing the importance of user involvement in digital transformation.

Tomlin, who has worked with Dow since 2005 and has held his current title since 2012, noted that industrial automation professionals need to challenge their operating assumptions if they want to move forward into digital manufacturing. "When you're improving value in a plant, there are two levers you can pull: operating cost improvement or asset utilization improvement," he said.

Tomlin highlighted several strategies for identifying opportunities: target specific pain points, plan to measure value, and engage champions. "Champions" can be executive leadership, plant leadership, and operators, he emphasized. The operator, or end user, is the most important person to get onboard.

Before moving forward, consider user interface improvement, data platform integration, and connectivity. "The best way to get a person to adopt a tool is to make it substantially better than what they had in the past," Tomlin said. Just because a new tool is available does not mean operators will immediately adopt it. "Make sure the end user experience is very seriously considered in terms of building those tools, because that's going to be a very important factor in adoption." He also reminded listeners that digital technologies are a tool, an enabler. ■

–By Melissa Landon

ISA Hosts Multitrack Cybersecurity Conference

ISA celebrated Cybersecurity Awareness Month with the debut of a dual-track Cybersecurity Standards Implementation Virtual Conference (CSIC). The 19 October event featured industrial cybersecurity specialists and other speakers hailing from Pfizer, the NATO Energy Security Center of Excellence, the U.S. Department of Commerce, and the U.S. Forest Service to address operational technology (OT) cybersecurity issues.

This second annual CSIC again offered strategies for mitigating organizational threats and vulnerabilities through the use of the ISA/IEC 62443 series of standards. ISA/IEC 62443, endorsed by the United Nations and globally recognized, was the centerpiece of many presentations. The ISA99 committee developed the ISA/IEC 62443 series of standards to provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).

Track 1 kicked off with a keynote from Zach Tudor, associate laboratory director of Idaho National Laboratory's National and Homeland Security (N&HS) directorate. His presentation was called "Action Plan for ICS Competencies." In his closing remarks, he offered a few key steps to move forward in OT environments: "We have to make sure everyone realizes that industrial cybersecurity is different. . . . Collaboration is key; none of us is as smart as all of us…. We have to make standard curricular materials widely available."

Track 2 introduced listeners to six panelists, including ICS Cybersecurity Advisor's Johan Nye and OIT Concepts' Eric Cosman, who participated in the 62443 Standards Update Panel Discussion.

HEXAGON
CSIC
CYBERSECURITY STANDARDS IMPLEMENTATION CONFERENCE
VIRTUAL CONFERENCE SERIES
ISA
Cisco IoT

Attendees who chose track 1 heard about Pfizer's plant floor cybersecurity journey, observed a supply chain risk management panel featuring ISA President Steve Mustard, and learned about applying ISO/IEC 27001/2 and the ISA/IEC 62443 series in OT environments from Pierre Kobes of Siemens AG, among other great sessions. Track 2 listeners heard an ISA security update from Andre Ristaino, learned from Verve CEO John Livingston, and saw several technology demonstrations and trainings.

Because this multifaceted event offered many choices, registered attendees were encouraged to come later and view what they missed in the following 30 days. A full list of all presenters can be found on the event's website (https://virtualcsic.vfairs.com).

A related event, the Cybersecurity Standards Implementation Virtual Conference – Middle East, is scheduled to debut 7 December, running live 8:00–14:00 GMT +3. Registered attendees will also be able to watch it later on demand. Information and registration links for all ISA virtual conferences and webinars are at https://isaautomation.isa.org/virtual-events-program. ■

Johnson Controls Earns World's First ISASecure CSA Certification for a Smart Buildings Product

The ISASecure Program announced that Johnson Controls has earned the first ISASecure Component Security Assurance (CSA) certification for its smart building products featuring YORK YK and YZ centrifugal chillers. Industrial control suppliers can earn ISASecure certifications for robust products that are free from recognized liabilities. The ISASecure CSA certification assures Johnson Controls customers that each chiller product meets the technical security requirements for industrial automation and control system (IACS) components, as defined in the internationally recognized ISA/IEC 62443-4-2 cybersecurity standards, and is developed in accordance with the internationally recognized ISA/IEC 62443-4-1 cybersecurity standard.

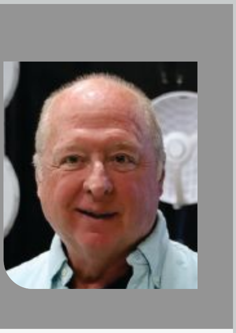
The ISASecure program has provided IACS cybersecurity certification for more than a decade, and has now demonstrated the effectiveness of the ISA/IEC 62443 family of standards for securing smart buildings technology. Cybersecurity threats are rising, and businesses are considering the potential vulnerabilities of unprotected building infrastructures.

"We understand what's at stake for our customers," said Jason Christman, vice president and chief product security officer, Johnson Controls. "That's why Johnson Controls is committed to bringing cyber-resilient building solutions to market. The ISASecure certification recognizes this commitment and provides reassurance at a time when cyberthreats to operational technology are increasing."

Johnson Controls received the ISASecure CSA conformance certificate from exida LLC, an ISASecure- and ISO 17065–accredited certification body. "Johnson Controls continues to demonstrate leadership in cybersecurity for smart buildings," said Mike Medoff, director of cybersecurity certification at exida. "The CSA certification of Johnson Controls YZ and YK centrifugal chillers is an industry first." The company previously had earned the ISASecure Security Development Lifecycle Assurance (SDLA) certification.

The ISASecure CSA certification indicates that the security capabilities of components, such as software applications, embedded devices, host devices, and network devices, conform to requirements in the ISA/IEC 62443 standards. The ISASecure SDLA certification assures that Johnson Controls' product-development security practices, including its OpenBlue platform, conform to the ISA/IEC 62443-4-1 security lifecycle standard. ■

Meet 2021 ISA Fellow Peter Fuhr



Peter Fuhr, PhD, was named a 2021 ISA Fellow in honor of his pioneering work in networked sensor systems for structures, wireless technologies, and mobile platforms; and for designing secure integrated network architectures for petrochemical, pharmaceutical, and military needs.

He has been involved in industrial wireless, sensors, and secure systems for more than 30 years. He has served as a NASA space optical physicist, university professor, serial entrepreneur, and distinguished scientist at Oak Ridge National Laboratory (ORNL) (www.ornl.gov/staff-profile/peter-l-fuhr), where he is the technology director for the Unmanned Aerial Systems Research Laboratory. In the photo, he is shown standing in front of 5-GHz and 60-GHz radio transceivers, which he uses for doing research and development for rural broadband communications.

Concurrently, Fuhr also is a professor of electrical engineering and computer science at the University of Tennessee, which allows him to help direct and participate in graduate student doctoral research. "I think I'm a teacher at heart," says Fuhr. "I get asked how I know so much in the application space, specifically inside industrial applications. It's all by being educated from people I've met through the International Society of Automation [ISA]. It may seem like [teaching is] only one way, but I've been getting taught, too—by friends, colleagues, and other individuals inside ISA."

Fuhr is a technical instructor for ISA and is the former director of its Communication Division. He also served as the co-chair of the Secure Infrastructure Controls Society, is the co-founder and past chair of the Wireless Industrial Networking Alliance, and co-chairs the Association for Advanced Agricultural Technology.

Automation in space

In addition to the people he has met along the way, Fuhr humbly credits much of his success to being in the right place at the right time, including for his role as a space optical physicist. "I was very fortunate to go straight from school as a neophyte to work at NASA Goddard Space Flight Center and get trained on how to build a complicated automation system that's up in space," he says.

Two of the satellites he worked on are still in orbit. When he speaks of them, it seems like he is remembering a couple of old friends. "If the conditions are right, I can look up in the sky and every 90 minutes see the satellites go overhead. And that's nice."

He next had the opportunity to start a program in optical sciences at the University of Vermont, and he credits a support system there with helping to get him established in the technology area. Then, the timing was right for the professor "to start doing smart structures funded by the National Science Foundation, integrating systems into an application area, putting sensors in hydro dams and nuclear containment vessels, etc."

Flying sensors on drones

"Then came my introduction to ISA," he adds, "where I got to meet so many people and hear about different needs. I was lucky to be educated by a lot of people in intersecting technologies. We put it all together. Now I'm the technology director for our national lab's drone activities, and we're flying those [sensors] on drones."

He is also a contributing member of a number of ISA, IEEE, and SPE work groups and committees. Fuhr's R&D interests are broad but principally involve secure communications, sensors, multidisciplinary applications, and control systems. He has embedded sensors into various structures worldwide, including buildings, dams, airplanes, hot air balloons, spacecraft, nuclear power plant containment vessels, and even humans. He has also deployed wireless systems in innumerable industrial, agricultural, underwater, underground, and even outer space settings.

"I've been lucky over the years to be on some pretty hot horses in technology, right at the forefront of different things," says Fuhr. "Or to use a surfing analogy, it's just riding the wave. Then you jump over to another wave—now let's ride that technology application for a while. That's the thing: It's all application. I'm an engineer. I have degrees in physics and electrical engineering and mathematics, but I'm an applied engineer. That's why we're in this field right here [see sidebar]."

His recent activities have included R&D pertaining to sensors and systems appropriate for environmental monitoring of fracking; water quality sensing for industrial enterprises; sensing and communication systems for operation in harsh settings, such as deep water, within nuclear reactors, and in corrosive environments; and examining the intricacies of printed electronics in an additive manufacturing (3D printing) environment.

A great visionary

Penny Chen, senior principal technology strategist at Yokogawa US Technology Center, says, "Peter has a great vision of what technology is to come, and when he believes that technology can make a difference in certain ways, he is just full energy, full effort. He goes for it. That also shows in his entrepreneurship."

As a subject-matter expert (SME) for Smart Grid Secure Communications, Fuhr has written numerous briefs for the Department of Energy, the FCC, and Congress on electric utilities' implementation of advanced technologies. He is a frequent speaker and has served in a variety of capacities for technical meetings, symposia, and conferences around the world.

In addition to authoring and presenting more than 800 technical journal and conference publications and presentations,

(continued on next page)

In Memory of "The Genius Behind Feedforward Control"

Industry innovator, ISA Fellow, and "the genius behind feedforward control" Francis Gregway "Greg" Shinskey died peacefully in September at the age of 89.

"I often thought that there was nobody that had more impact on forwarding the mission of ISA during my lifetime than Greg Shinskey," says retired Schneider Electric executive Peter Martin. "ISA was like the automation and control leader of industry, and Greg was the control leader of industry. If I think back during my career, there are probably only a few names that come up that are even close to that. He kind of set the path for them."

Read more on page 8 or online at Automation.com. ■

ISA Fellow, continued from p.41

Fuhr has been an expert witness in communications and sensor court cases; patented technical innovations; performed many technical assessments of companies soliciting venture capital funding; and has provided technical consulting services to companies large and small. He served as an SME for JP Morgan's venture investment division, and, as a faculty member, founded and directed the Institute for Sensors and Wireless Networking.

He continues to be a technical reviewer for proposals submitted to various governmental organizations, and routinely delivers technology overview and fundamental research presentations to cross-disciplinary audiences throughout the world.

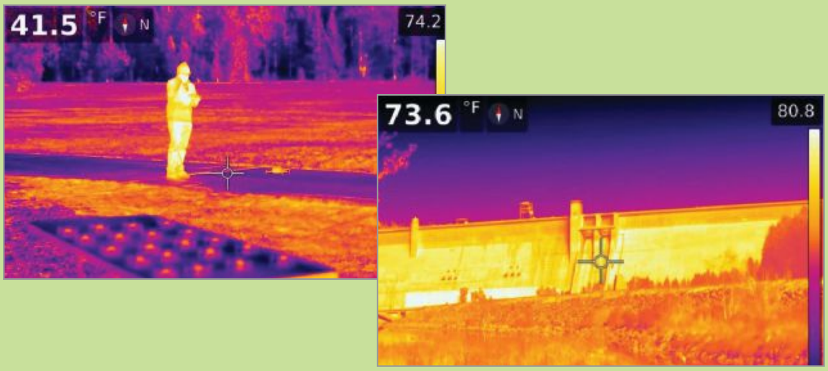
Fuhr is the recipient of the Presidential Award for Excellence in Research and is a Senior Member of both the Institute of Electrical and Electronics Engineers and International Society of Automation. Find out more about ISA Fellows and other awards at www.isa.org/members-corner/isa-honors-and-awards. ■

–By Lynn DeRocco

Doing a Whole Bunch of Sensing

Automation.com caught up (remotely) with ISA Fellow Peter Fuhr, PhD, in the mountains of Northwest Montana. His joy in doing what he loves was evident in the energetic, cheerful voice on the other end of the line and his easy laughter. "I'm with some of my colleagues working on a Department of Energy activity related to wildfires associated with things like transmission lines and cracked insulators," he said. "It's just beautiful today—about 65 degrees, blue skies, light winds. We're flying drones and doing a whole bunch of sensing and stuff like that. Just another day!"

The photos show Fuhr's current activities in the field. Even as ISA's interview ended, his latest adventure was calling. "I'm going to go back out," he said, "I want to fly some more drones by the trees and water here. . . ."



Thermal images of R&D conducted in Montana by Fuhr and his team. Left: a thermal image of Fuhr about to launch a batch of handheld drones. Right: Image taken from a sensor-laden drone of a hydroelectric dam.

New CAPs and CCSTs

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

Certified Control System Technicians

Level 1

Andrew Boone, U.S.
Sean Keane, MillerCoors, U.S.
Brad Koenig, Iowa State University, U.S.
Mansour Nasser Al Rifi, Saudi Arabia
Christian G. Ransdell, U.S.
Christian M. Smith, U.S.
Charles A. Thompson, U.S.
Thomas Michael Vigue, U.S.

Level 2

Ibrahim A. Al Meftah, Saudi Arabia
Danny Cooper, MillerCoors, U.S.
Justin Wade Davis, Transcanada, U.S.
Raymond J. Eye, M Davis & Sons Inc., U.S.
John Gowder, MillerCoors, U.S.
David Halter, MillerCoors, U.S.
Autumn D. Hansen, U.S.
Paul Kaczorowski, MillerCoors, U.S.
Jorge Maldonado, U.S.
Doug Mohr, U.S.
Zach A. Otto, U.S.
Jorge A. Vega, U.S.
Zachary Weber, Eagle River Water and Sanitation District, U.S.
Seth Young, MillerCoors, U.S.

Level 3

Brian Bruner, Xcel Energy, U.S.
JD Glenn, Dorada Foods, U.S.
Michael John Sneddon, U.S.

Certified Automation Professionals

Eric J. Anderson, U.S.
Alexander Cottengim, U.S.
Eric Kimball Jaime, U.S.
Muzammal Saud Khan, Pakistan
Sarbottam Pant, Meiden America, Inc., U.S.
Christian Djateu Pettang, DC Water & Sewer Authority, U.S.

ISA/IEC 62443 Cybersecurity Series Designated as IEC Horizontal Standards

The ISA/IEC 62443 standards, *Industrial Automation and Control Systems Security*, have been officially designated as a horizontal series by the Geneva-based International Electrotechnical Commission (IEC), establishing primacy across the wide range of IEC standards projects on matters related to cybersecurity in industrial and related applications.

The IEC defines horizontal standards as those that are widely applicable and are to be used by all relevant committees to ensure consistency and coherence in IEC standards. The status is granted following an enhanced IEC review process and approval by the Standardization Management Board, which is responsible for the management and supervision of IEC standards work.

The ISA/IEC 62443 standards are developed primarily by the ISA99 committee with simultaneous review and adoption by the IEC. ISA99 draws on the input of cybersecurity experts across the globe in developing consensus standards that are applicable to all industry sectors and critical infrastructure, providing a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems.

IEC horizontal status is the latest of several notable recognitions in the ongoing development and growing global application of the ISA/IEC 62443 series. These include:

- A decision by the United Nations Economic Commission for Europe to integrate the standards into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe.
- An agreement at the request of the NATO Energy Security Center for Excellence to establish official collaboration and exchange of information.

The IEC horizontal recognition also follows completion of several key standards in the ISA/IEC 62443 series:

- ISA/IEC 62443-3-2: *Security Risk Assessment for System Design*, defines a comprehensive set of engineering measures to guide organizations through the essential process of assessing the risk of a particular industrial automation and control system (IACS) and identifying and applying security countermeasures to reduce that risk to tolerable levels. The standard can be effectively applied across all industry segments and critical infrastructure sectors that depend on secure IACS operations, providing guidance to all key stakeholder categories, including asset owners, system integrators, product suppliers, service providers, and compliance authorities.
- ISA/IEC 62443-4-1, *Product Security Development Life-Cycle Requirements*, which specifies process requirements for the secure development of products used in an IACS and defines a secure development lifecycle for developing and maintaining secure products.
- ISA/IEC 62443-4-2, *Technical Security Requirements for IACS Components*, which provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications.

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

In addition, ISA offers extensive training resources on cybersecurity, as well as safety, fundamentals, and other topics in industrial automation and control systems. Visit www.isa.org/training for information.

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

ISA88 and IEC to Collaborate in Updating ISA/IEC Batch Standards

The ISA88 standards committee, Batch Control, will soon begin work in concert with IEC SC65A on an update of *Batch Control Part 1: Models and Terminology.* The standard, last published as ANSI/ISA-88.00.01 in 2010, defines reference models for batch and related procedure-oriented manufacturing as used in the process industries and terminology that helps explain the relationships between those models and terms.

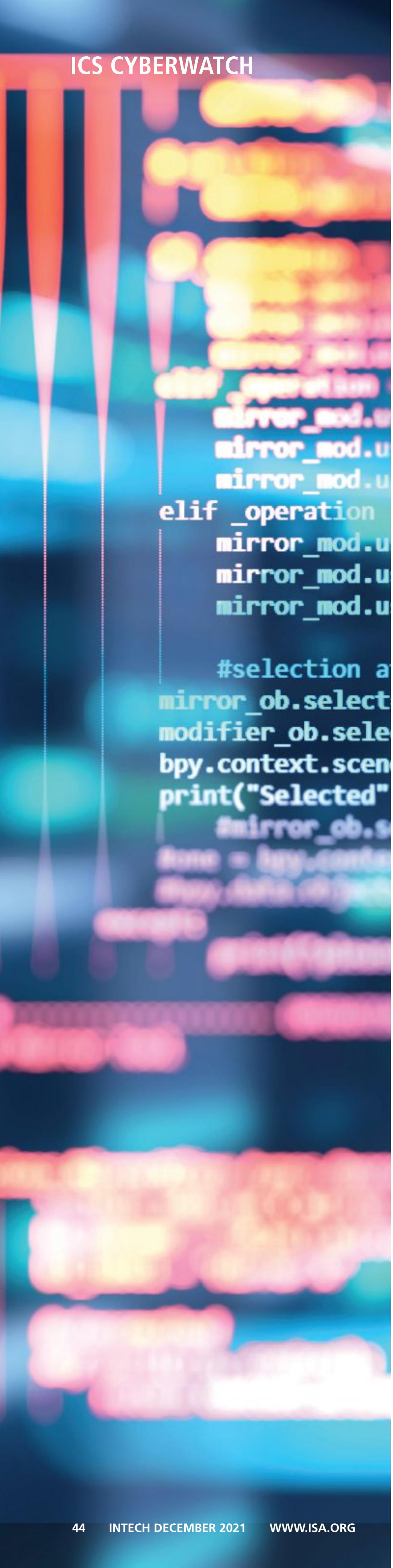
Leading the collaboration will be David Board of Rockwell Automation in the U.K. He will serve as both the chair of the ISA88 committee and convenor of the related working group within IEC SC65A, which is MT 61512. Board has previously served as a working group leader within ISA101, *Human-Machine Interface*, for which he received an ISA Standards & Practices Department Award in 2017 for his leadership in developing ISA-TR101.02, *HMI Usability and Performance*.

Following the revision of Part 1, work is expected to begin on updating the other standards in the ISA-88 series. These include:

- *Batch Control Part 2: Data Structures and Guidelines for Languages*
- *Batch Control Part 3: General and Site Recipe Models and Representation*
- *Batch Control Part 4: Batch Production Records*

All of the ISA-88 standards may be accessed at www.isa.org/findstandards.

ISA88, like all ISA standards committees, is open to all who are interested. Please contact Charley Robinson, crobinson@isa.org for information or to join ISA88. ■



Two Standards, One Integrated Industrial Cybersecurity Plan

By Pierre Kobes

New ISAGCA whitepaper explains how to apply ISO/IEC 27001/2 and the ISA/IEC 62443 series to secure operational technology environments.

Author's note: This is an excerpt of a new whitepaper available for download (www.isa.org/isagca). It offers guidance for organizations familiar with ISO/IEC 27001 that are interested in protecting the OT infrastructure of their operating facilities based on the ISA/IEC 62443 series. The paper describes the relationship between the ISA/IEC 62443 series and ISO/IEC 27001/2 and how both standards may be used effectively within one organization to protect both IT and OT. 62443 does not require the use of an underlying information security management system (ISMS). However it requires that, if the organization has an established ISMS, the security program in the OT environment should be coordinated with it. The whitepaper, and this article, are assuming an existing ISMS based on ISO/IEC 27001/2. Other information security standards similar in scope to 27001 might be used effectively together with ISA/IEC 62443.

Many organizations (especially very large ones) have established policies and procedures governing the information technology (IT) security in their office environments. Many of these are based on ISO/IEC 27001/27002. Some have attempted to address their operational technology (OT) infrastructure under the same management system, and have leveraged many IT/OT commonalities.

Although it would be ideal to always select common controls and implementations for both IT and OT, organizations have had challenges in doing so, such as OT operator screen locking creating unsafe conditions, antivirus products that are incompatible with OT equipment, patching practices that disrupt production schedules, and network traffic from routine backups blocking safety control messages. The ISA/IEC 62443 series of standards explicitly addresses issues such as these; this helps an organization maintain conformance with ISO/IEC 27001 through common approaches wherever feasible, while highlighting differences in the approach of IT versus OT where needed.

Background

Scope of ISO/IEC 27001/2. The standard ISO/IEC 27001 provides requirements for establishing, implementing, maintaining, and continually improving an underlying information security management system and a list of commonly accepted controls to be used as a reference for establishing security requirements (ISO/IEC 27000, the glossary and introduction to the 27000 series, defines the term *control* as "measure that is modifying risk"). In addition, ISO/IEC 27002 provides further detailed guidance for organizations implementing these information security controls. It is designed for organizations to use as a reference for selecting controls within the process of implementing an ISO/IEC 27001–conformant ISMS.

IT and OT. "IT" is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. "Operational technology" or "OT" is hardware and software that detects or causes a physical change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. Increasingly, IT products and systems are used in OT infrastructures, and recently, the advent of Internet of Things (IoT) and Industrial Internet of Things has further blurred the IT/OT distinction. However, the main difference is that OT environments in general must comply with strict integrity, availability, and performance constraints due to the fact that operation outside of the constraints may affect health, safety, or the environment.

Scope of the ISA/IEC 62443 series. The scope of the ISA/IEC 62443 series of standards is the security of industrial automation and control systems (IACSs) used in OT infrastructures. This includes control systems used in manufacturing and processing plants and facilities, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production, and distribution facilities. The ISA/IEC 62443 series has also gained acceptance outside its original scope, for example in building automation, medical systems, and industries and applications such as transportation networks that use automated or remotely controlled or monitored assets.

Figure 1 is an overview of the scope of some core documents of the ISA/IEC 62443 series. Part 62443-2-1 is targeted at organizations that are responsible for IACS facilities, which includes owners and operators (termed "asset owners" in the series). It provides requirements for asset owner IACS security programs. Note: The present document refers to the most recent version of part 62443-2-1, which is not finally approved as an international standard and may be subject to changes. It is not expected that these changes will impact the recommendations of this paper.

In addition, the ISA/IEC 62443 series provides conformance requirements for all entities supporting asset owners in the implementation of technical and procedural security measures for the protection of operating facilities from cyberthreats. Part 62443-2-4 provides security requirements for integration and maintenance service providers supporting asset owners in the development and operation of OT-specific technical solutions. Parts 62443-3-3 and 62443-4-2 define requirements for security capabilities of systems and components, respectively. Part 62443-4-1 includes lifecycle requirements for product suppliers for the development and support of products with adequate security capabilities. In addition, the ISA/IEC 62443 series includes guidance documents for specific issues like patch management and risk-based system partitioning in zones and conduits.

A two-part approach to OT cybersecurity

ISO/IEC 27001/2 and the ISA/IEC 62443 series address two complementary parts of an overall OT cybersecurity approach (figure 2). ISO/IEC 27001/2 standards have been broadly used for many years as a base for organizing the information security of organizations. The processes and overall management structure of organizations responsible for OT environments may be integrated with an ISMS based on these standards, as will be described here. The ISA/IEC 62443 series addresses specific needs of OT infrastructures and complements the ISMS. The OT infrastructure of operating facilities may be embedded in the IT infrastructure of the responsible organization or autonomously organized. In both situations, ISO/IEC 27001/2 and the ISA/IEC 62443 series can be used for addressing complementary parts of an overall cybersecurity approach for OT environments.

ISO/IEC 27001/2 addresses the establishment of an information security management system for the IT infrastructure of an organization. ISO/IEC 27001/2 specifies generic requirements that are intended to be applicable to all organizations, regardless of type, size, or nature. The requirements for establishing, implementing, maintaining, and continually improving an ISMS are described in clauses 4 to 10 of ISO/IEC 27001. Excluding any of the requirements specified in these clauses is not acceptable when an organization claims conformity to this standard.

In addition, ISO/IEC 27001/2 includes a set of controls addressing security topics that it requires to be given consideration in a comprehensive security strategy. In a risk-based approach, an organization can ultimately select controls from the list provided by ISO/IEC 27001/2 or from other control sets, or design new controls to meet specific

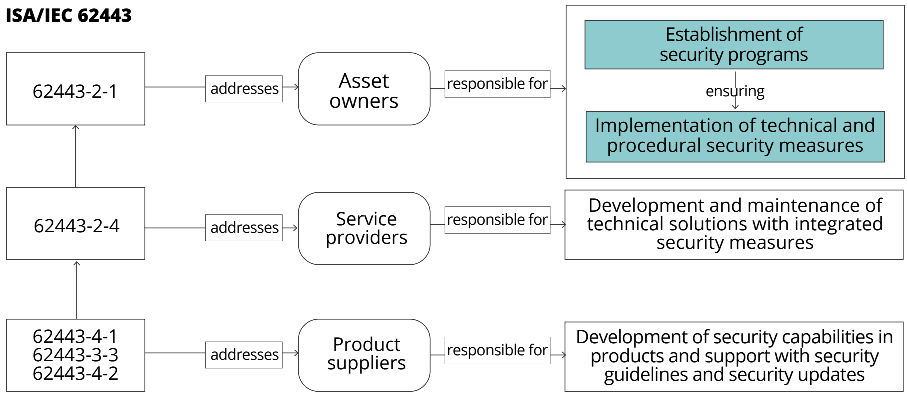

ISA/IEC 62443
62443-2-1
addresses
Asset owners
responsible for
Establishment of security programs
ensuring
Implementation of technical and procedural security measures
62443-2-4
addresses
Service providers
responsible for
Development and maintenance of technical solutions with integrated security measures
62443-4-1
62443-3-3
62443-4-2
addresses
Product suppliers
responsible for
Development of security capabilities in products and support with security guidelines and security updates

Figure 1. ISA/IEC 62443 addresses all entities involved in the protection of operating facilities. Note: This represents the next edition of the ISA and IEC versions of part 62443-2-1, which is not finally approved as an international standard and may be subject to changes.

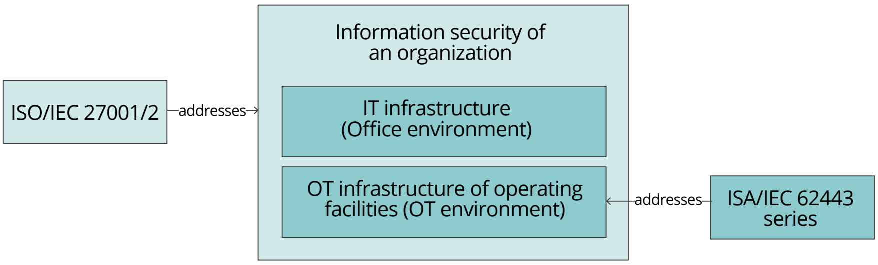

Information security of an organization
ISO/IEC 27001/2
addresses
IT infrastructure (Office environment)
OT infrastructure of operating facilities (OT environment)
addresses
ISA/IEC 62443 series

Figure 2. Scope of ISO/IEC 27001/2 and ISA/IEC 62443

needs as appropriate. The distinction between ISMS requirements and information security controls found in ISO/IEC 27001/2 is illustrated by a few examples shown in figure 3.

The ISA/IEC 62443 series addresses specific needs required for cybersecurity in OT environments. The OT infrastructures of operating facilities must fulfill specific requirements of integrity, performance, and availability to ensure operational continuity. Loss of operational continuity may, for example, manifest as an explosion, a blackout, or an incorrect formula or dose of a life-saving medicine. Many operating facilities implement dedicated safety systems to prevent operational conditions that would have health, safety, and environmental consequences. Security requirements in ISA/IEC 62443 are designed so they do not prevent or disrupt safe operation.

Further, dedicated safety functions require unique protections, and therefore are subject to unique security requirements in the standard. As examples, the challenges mentioned above, often faced when extending existing IT security control implementations to OT, are addressed by 62443. The ISA/IEC 62443 series includes requirements addressing various security topics to be handled in a comprehensive security program, in the same way that ISO/IEC 27001/2 includes a list of controls addressing these security aspects. The ISA/IEC 62443 requirements address specific needs in the OT environment and complement the list of controls of ISO/IEC 27001/2 by adding critical details relevant to that environment.

ISO/IEC 27001/2 and ISA/IEC 62443 should be combined to protect the OT infrastructure of operating facilities. The above discussion shows how ISA/IEC 62443 augments ISO/IEC 27001/2 by incorporating specifics unique to the OT environment. However, ISA/IEC 62443 does not include all elements needed to secure OT. In particular, ISO/IEC 27001/2 provides ISMS requirements and controls/guidance that are entirely common to IT and OT and are not found in ISA/IEC 62443. Therefore, a method for applying both standards to OT infrastructure is recommended. The full whitepaper describes one such method.

Comprehensive protection

ISO/IEC 27001/2 and the ISA/IEC 62443 series complement one another for implementing a comprehensive, risk-based, defense-in-depth strategy for the protection of operating facilities including the contribution of all entities:

- The combined requirements and controls of ISO/IEC 27001/2 and 62443-2-1 are the basis for asset owners to establish security programs and ensure the design and implementation of technical and procedural security measures.
- The requirements of ISA/IEC 62443-2-4 are the basis for service providers to support asset owners by designing and maintaining technical solutions providing the required security capabilities.
- The requirements of ISA/IEC 62443-4-1 are the basis for product suppliers to support asset owners and service providers by employing secure development processes and providing guidelines and support for integrating and maintaining the security of products used in OT infrastructures.
- The requirements of ISA/IEC 62443-3-3 and 62443-4-2 are the basis for providing product security capabilities necessary for the implementation of protection schemes by asset owners and service providers.

To implement the approach, a mapping of the set of related ISO/IEC 27001/2 controls to the elements of the security program of IACS asset owners specified in 62443-2-1 is required. An organization may use the approach that relies on the structure of 62443-2-1 in security programs, or any other approach they find convenient for merging ISO/IEC 27001/2 controls with 62443-2-1 requirements. A reference mapping could be developed for this purpose as a commonly used resource, and ISA's Global Cybersecurity Alliance (ISAGCA) is considering developing such a reference. Organizations could use such a mapping as a starting point for the development of their OT security programs and adjust it to their specific needs as necessary. ■

ISO/IEC 27001/2

Security Management (ISO/IEC 27001 clauses 4 to 10)	Security Controls (ISO/IEC 27001 Annex A and ISO/IEC 27002)
5.1 Leadership commitment	6.2.2 Teleworking
6.2 Information security objectives and planning to achieve them	8.1.1 Inventory of assets
	10.1.1 Policy on the use of cryptographic controls
5.3 Organizational roles, responsibilities and authorities	9.1.1 Access control policy
	11.2.9 Clear desk and clear screen policy
7. Resources/Competence/ Awareness/Communication/ Documented information	12.3.1 Information backup

Figure 3. Examples of ISMS requirements and security controls

ABOUT THE AUTHOR

Pierre Kobes is a writer for the ISA Global Cybersecurity Alliance, which is made up of 50 member companies dedicated to furthering the ISA/IEC 62443 series of standards to secure industrial and related business systems. For more information about ISAGCA, visit www.isa.org/isagca.

2022 Executive Board

The International Society of Automation is pleased to introduce the 2022 Executive Board.

President
Carlos Mandolesi
Trinity College Dublin

President-elect Secretary
Marty Bince
Schneider Electric

Past President
Steve Mustard, P.E., Eur Ing, C.Eng, CAP, FIET, GICSP, CMCP
National Automation, Inc.

Treasurer
Scott Reynolds
Johns Manville

Ardis Bartle
Apex Measurement and Controls LLC

R. Donald Bartusiak, PhD
Collaborative Systems Integration

Ken Belteau
Belith Consulting Services

Dr. Paulina Chan
Global Mutual Innovation Consortium

Jim Garrison, P.E., CAP, CFSE
aeSolutions

Eddie Habibi
PAS Global

Maxym Lachance, P.Eng
BBA inc

Claudio Makarovsky
Microsoft

J. Parsons, P.E.
Jacobs

Claire Ramspeck
ISA

Rajesh Rathi
Control Infotech Inc.

Debashis Sadhukhan
NASA Glenn Research Center

Jagdish Shukla
Servilink Systems Ltd.

Prabhu Soundarrajan
Republic Services

Ashley Weckwerth, P.E.
Burns & McDonnell

Dr. Maurice Wilkins
Yokogawa Global Marketing Headquarters

2022

International Society of Automation
Setting the Standard for Automation™

Sample of Jobs Available at Jobs.isa.org

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

Principal site reliability engineer

Glowforge: The company, although based in Seattle, is a remote-first company looking for an engineer to help manage and scale its growing infrastructure to ensure an outstanding experience for customers. The engineer will lead, mentor, and help grow a team of site reliability engineers to work with application developers; ensure services are properly instrumented, resilient against outages, and responsive to appropriate mediations; and partner with the product and data teams to ensure systems are appropriately provisioned. Qualifications include at least 10 years of combined professional experience in software development and system engineering, a relevant four-year degree, successfully managing the services of a web product, and comfort in various programming languages (including Ruby, Python, NodeJS, and Rust) . . . see more at Jobs.isa.org.

Assistant chief engineer

JLL: The engineer in Tampa, Fla., will supervise and direct maintenance staff and monitor the performance of their assigned responsibilities. The engineer will also check malfunctioning equipment and determine corrective action, provide training to expand the capacities of the operations staff, and supervise and implement the preventive maintenance program, including scheduling preventative maintenance with minimal disruption to building services, performing or delegating PM tasks, ordering parts, and maintaining inventory. The position requires two years of trade school in electrical system design, refrigeration, and HVAC and at least five years of experience in facility engineering maintenance . . . see more at Jobs.isa.org.

Electrical designer

Samuel, Son & Co.: CAID Automation, a division of Samuel, Son, & Co. in Tucson seeks solutions for challenging manufacturing processes by designing and building automated robotic systems. The electrical designer is responsible for the electrical engineering of control systems on automation equipment specific to customer and project requirements. Specific duties include designing and developing electrical systems, supporting electrical technicians, collaborating with other engineers and purchasing personnel, and preparing detailed working engineering drawings and schematics of electrical and pneumatic components and requirements. Requirements include an associate's degree in a technical field, one to three years of experience, and strong experience in AutoCAD . . . see more at Jobs.isa.org.

Process engineering manager

Omeros Corporation: This position in Seattle is responsible for developing and supporting processes for the manufacture of protein-based therapeutics. The individual will work with internal and external resources for the development of these processes and their transfer to clinical and commercial stage manufacturing plants. The successful candidate will manage technical relationships with CMOs responsible for manufacturing GMP drug substance for Omeros, be responsible for supporting CMC aspects of the company's drug substances from development through manufacturing, and troubleshoot cell culture, fermentation, and purification process and equipment challenges. The position requires a BS or MS degree in chemical engineering or a related scientific field, at least 10 years of biotechnology and/or pharmaceutical industry experience, demonstrated knowledge of cell culture and downstream protein processing and demonstrated problem solving capabilities . . . see more at Jobs.isa.org.

System integration technician

Data-Linc Group: The company is looking for a candidate who has been in the automation industry for several years, has a demonstrated record of success with design and implementation of wired and wireless data communications systems (including PLCs), and is well-versed in the logical process of troubleshooting. We seek a team player who likes to tinker and solve problems. The technician will perform in network design and troubleshooting . . . . see more at Jobs.isa.org.

STATEMENT OF OWNERSHIP MANAGEMENT AND CIRCULATION

(Required by 39 U.S.C. 3685)

Title of Publication: InTech **Publication Number:** 0192-303X
Filing Date: 9/30/21 **Frequency:** Bimonthly
Number of Issues Published Annually: 6
Annual Subscription Price: 8.65% of dues
Mailing Address and Business Headquarters:
ISA, 67 T.W. Alexander Drive, Research Triangle Park, NC 27709
Publisher: Rick Zabel **Editor:** Renee Bassett

	Average # of copies each issue during preceding 12 months	Actual # of copies of single issues published nearest to filing date
Total number of copies: Net press run	36,246	34,747
Total paid or requested circulation	32,918	31,425
Free distribution by mail	1,041	1,003
Free distribution outside mail	331	307
Total free distribution	1,372	1,309
Total distribution	34,290	32,734
Copies not distributed	1,320	1,313
Returns from news agents	None	None
Total	35,610	34,047
Percent paid or requested circulation	96%	96%
I certify that these statements are correct and complete: Rick Zabel, Publishing Manager		

InTech advertisers are pleased to provide additional information about their products and services. To obtain further information, visit their websites shown here or reach out using the contact details in their advertisements.

Advertiser	Page #
AutomationDirect www.automationdirect.com	**Cover 2**
Deviceworx Tech https://deviceworx.com	**33**
Endress + Hauser www.us.endress.com	**6**
EU Automation www.euautomation.com	**35**
Inductive Automation www.inductiveautomation.com	**bellyband**
ISA www.isa.org	**47**
ISA Pubs www.isa.org	**37**
ISA Global Cybersecurity Alliance www.isa.org/isagca	**Cover 3**
Maverick Technologies, a Rockwell Automation Company www.mavtechglobal.com	**Cover 4**
Opto 22 www.opto22.com	**3**
ProComSol, Ltd. www.procomsol.com	**37, 49**
Siemens www.siemens.com	**19**
Tadiran www.tadiranbat.com	**13**

InTech Advertising

View the Media Planner

https://tinyurl.com/InTechAcom2022mediakit

Contact a Representative

Richard T. Simpson
Account Executive
Phone: +1 919-414-7395
Email: rsimpson@automation.com

Chris Nelson
Account Executive
Phone: +1 612-508-8593
Email: chris@automation.com

Gina DiFrancesco
Account Executive
Phone: +1 216-509-0592
Email: gina@isa.org

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

Print + Online = Success

Download the ISA InTech/Automation.com Media Planner:

https://tinyurl.com/InTechAcom2022mediakit

Purchase Reprints

An *InTech* representative can work with you to create a customized reprint package, including hardcopy reprints, PDFs, or mobile-friendly products.

Contact Nathan Swailes at 800-428-3340 or reprints@mossbergco.com

datafiles

Datafiles list useful literature on products and services available from manufacturers. To receive free copies of this literature, contact each manufacturer directly.

USB HART MODEM

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

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

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

INDUSTRIAL CYBERSECURITY QUICK START GUIDE

GLOBAL CYBERSECURITY ALLIANCE
Quick Start Guide: An Overview of ISA/IEC 62443 Standards
Security of Industrial Automation and Control Systems

The ISA Global Cybersecurity Alliance's Advocacy and Adoption work group's guide to the ISA/IEC 62443 series of standards includes lists of specific standards documents applicable to various roles within the security environment. The ISA Global Cybersecurity Alliance is a collaborative forum to advance industrial cybersecurity awareness, education, readiness, and knowledge sharing. Membership is open to any organization involved in industrial cybersecurity.

To download a PDF copy of the whitepaper, visit https://gca.isa.org/isagca-quick-start-guide-62443-standards. To talk about how your company or organization can join ISA GCA, contact Rick Zabel at rzabel@isa.org.

Mary Ramsey Has Advanced ISA, Creating a Better Organization

By Bill Lydon

ABOUT THE AUTHOR

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

The International Society of Automation's current executive director, Mary Ramsey, will retire at the end of the year. She leaves behind her many accomplishments, including alignment of ISA's goals, objectives, and actions, and the creation of the ISA Global Cybersecurity Alliance (ISAGCA). In my opinion, Mary Ramsey has done a great job as executive director, both by advancing ISA's stature in the industry and in dealing with the unexpected COVID-19 pandemic.

A mix of serendipity and intuition let me play a part in Mary's coming to ISA. I have been close to the organization ever since I was introduced to it as a young engineer at Johnson Controls in the 1970s. A vice president who was an active member recommended I join, and my first formal contact was attending an ISA three-day short course in 1975. The leading-edge topic was "applying microprocessors for control."

I had known Mary professionally for many years—she had already had more than 20 years of experience in industrial automation when Schneider Electric promoted her into the role of senior vice president of its U.S. Industry Business in 2012—when ISA began searching for a new executive director in 2017. At that point, I was aware Mary was available for another challenge, which was serendipitous. I then followed the advice given me years earlier by that Johnson Controls vice president who said, "To make things happen, it is important to have knowledge and respect your intuition."

Serendipity and intuition explain my call to Mary Ramsey, during which I described the position and why I thought she would be a good fit. With her permission, I introduced her to the search committee, and, after a rigorous search-and-evaluation process, Mary was chosen as the new ISA executive director. She brought skills in leadership, change management, and strategy development and execution, and I will simply state that her achievements met all my expectations.

There are always opportunities and challenges moving an organization forward, but neither Mary nor any of us foresaw the world-changing COVID-19 pandemic and its impact. She sought out opinions from throughout the organization and navigated that difficult challenge well.

Even more importantly, Mary understood that organizations need to periodically recalibrate based on member and industry needs, and she has done a great job of collaborating with staff and member volunteers to craft clear definitions of ISA guiding principles:

- Vision: Create a better world through automation.
- Mission: Advance technical competence by connecting the automation community to achieve operational excellence.
- Values: Excellence, Integrity, Diversity and Inclusion, Collaboration, Professionalism.

The strategic objectives and programs that followed this realignment have advanced ISA's stature in industry. Mary will be leaving ISA at the end of 2021 with the satisfaction of a job well done. She turns over an improved organization to the new ISA executive director, Claire Ramspeck. I invite all to join me in giving Mary a big thank you for a job well done and wish her well. ■

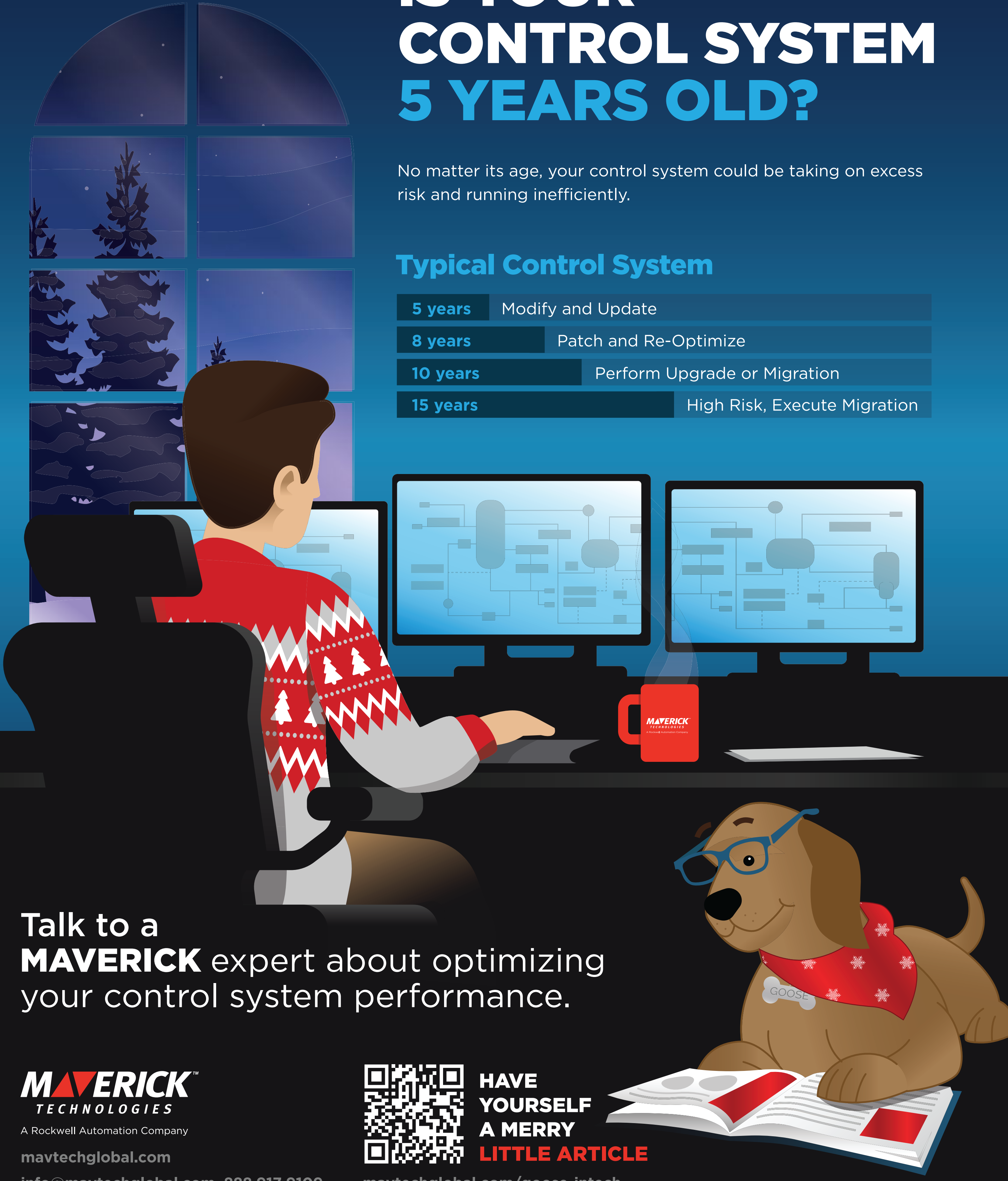
Mary understood that organizations need to periodically recalibrate based on member and industry needs, and she has done a great job of collaborating with staff and member volunteers to craft clear definitions of ISA guiding principles.

IS YOUR CONTROL SYSTEM 5 YEARS OLD?

No matter its age, your control system could be taking on excess risk and running inefficiently.

Typical Control System

5 years	Modify and Update
8 years	Patch and Re-Optimize
10 years	Perform Upgrade or Migration
15 years	High Risk, Execute Migration



Talk to a **MAVERICK** expert about optimizing your control system performance.

MAVERICK™
TECHNOLOGIES
A Rockwell Automation Company

mavtechglobal.com

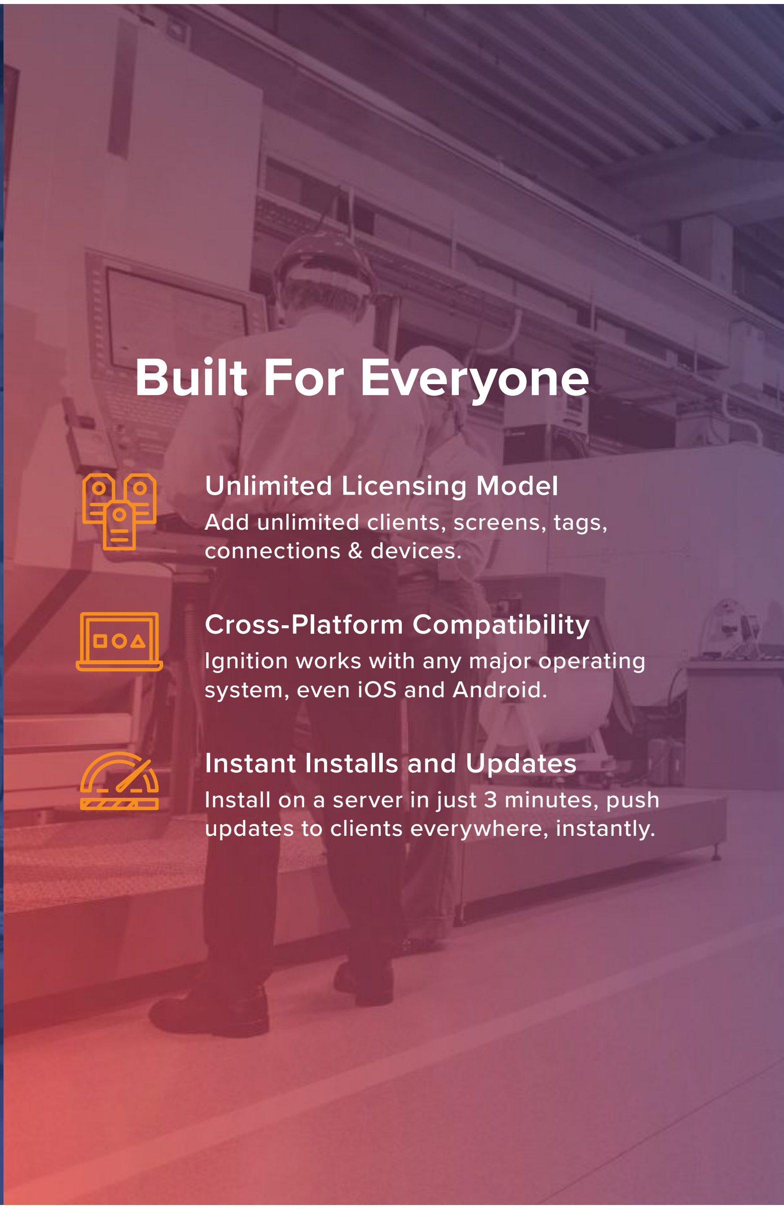
info@mavtechglobal.com 888.917.9109

HAVE
YOURSELF
A MERRY
LITTLE ARTICLE

mavtechglobal.com/goose-intech

8.1®

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



Built For Everyone

Unlimited Licensing Model

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

Cross-Platform Compatibility

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

Instant Installs and Updates

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