January/February 2018

InTech

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

- Leveraging HART
- MTConnect
- Alarm rationalization
- Remote monitoring
- Pressure spotlight

Breaking closed architecture bonds

The Open Process Automation Forum

Setting the Standard for Automation™

www.isa.org/intech

Affordable HMIs for any budget

Starting at only $98.00, you're guaranteed the savings you need

C-more micro HMIs
starting at only:
$98.00
(EA3-S3ML-RN)

C-more micro

C-more micro HMIs are perfect for small systems and cost-conscious applications. With free programming software and a starting price of $98.00, these micro HMIs can provide the visibility and cost savings your project needs.

- NEW! Reduced price 3-inch non-touch and touch screen HMIs
- 3-inch EA3 models have 12 selectable background colors while 4-inch and 6-inch models provide 32K color TFT displays
- Serial communications on all panels, with USB and Ethernet options available
- FREE C-more micro HMI programming software with simulator (EA-MG-PGMSW)

C-more

C-more HMIs
starting at:
$465.00
(EA9-T7CL-R)

C-more HMIs provide the advanced functionality needed in more complex applications including animations, logic, math, alarming, remote accessibility (web server and mobile app) and a myriad of supported communication protocols.

- NEW! 10-inch widescreen and reduced price 15-inch base model available
- 10-touch screen models offered with 7 different screen sizes supporting 64K colors
- Serial communication, USB programming, and SD card slot for data logging/program backup on all panels; Ethernet, HDMI video, and audio output options available
- C-more HMI programming software (EA9-PGMSW) $99.00

Research, price, buy at:
www.go2adc.com/cmore-micro
www.go2adc.com/cmore

Order Today, Ships Today!

VOTED Best in SERVICE 15 YEARS

AUTOMATIONDIRECT.com
1-800-633-0405 the #1 value in automation

* See our Web site for details and restrictions. © Copyright 2017 AutomationDirect, Cumming, GA USA. All rights reserved.

HEARTBEAT + MINDSET

Imagine your devices had their own pulse. They would tell you how healthy they were and what you could do to improve the performance of your process. **Heartbeat** Technology™ breathes life into your devices. It provides you with diagnostics, verifies performance and monitors process data to support optimization and predictive maintenance strategies. Our engineers listen carefully to you and understand your **Mindset**. It is their job to find the best fitting products with Heartbeat Technology to deliver increased operational availability for your plant.

Heartbeat Technology

Find out more about the Heartbeat Technology on **www.yourlevelexperts.com/heartbeat**

Endress+Hauser

People for Process Automation

InTech

COVER STORY

www.isa.org/InTech

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

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

© 2018 InTech

ISSN 0192-303X

***InTech* is published bimonthly by the International Society of Automation (ISA). Vol 65, Issue 1.**

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

Subscriptions: For members in the U.S., $10.38 annually is the nondeductible portion from dues. Other subscribers: $175 in North America; $235 outside North America. Multi-year rates available on request. Single copy and back issues: $20 + shipping.

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

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

Printed in the U.S.A.

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

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

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

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

InTech magazine incorporates *Industrial Computing*® magazine.

PRINTED WITH SOY INK

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

Instrumentation that Keeps Danger at Bay

SFY Functional Safety Frequency-to-DC Transmitter

Put a fortress of protection around your process with FS Functional Safety Series instrumentation from Moore Industries. You can be confident that it will safeguard your processes when you need it the most. Our STA, SSX, SST, SRM, STZ and the NEW SFY Functional Safety Frequency-to-DC Transmitter have been designed and built to strict IEC 61508 standards, ensuring safe and reliable function – particularly in environments where hazardous or emergency situations are likely to occur.

CERTIFIED IEC 61508 SIL 3 CAPABLE

2014 WINNER

FS FUNCTIONAL SAFETY SERIES

MOORE INDUSTRIES WORLDWIDE

Demand Moore Reliability

To learn more about our Functional Safety Series, call (800) 999-2900, or go to: **www.miinet.com/safetyseries**

IoT requires 'systems thinking'

By Bill Lydon, *InTech*, Chief Editor

Should Internet of Things (IoT) investments focus on narrow business outcomes? Keeping IoT deployments simple by focusing on a single narrow application is being sold as a way to apply new technologies. These can be worthwhile investments, but only focusing on narrow applications may put you in the position of "not seeing the forest for the trees." Basically, if you look at specific narrow applications one at a time, you might not realize that a group of separate "trees" go together to make a "forest." If everyone strictly followed this logic, nobody would have invested in a distributed control system or a factory automation system. A major value that automation professionals bring an organization is system-level thinking, analysis, and application. Rather than focusing too closely on one item, taking an overall systems view provides a broader perspective. Generally, this will reveal a whole forest you could not see before because you were too close, and focusing on the trees.

The influx of innovative and lower-cost technology provides a range of new tools for taking a systems-level approach to manufacturing and process operations to increase productivity and efficiency. The ISA95, Enterprise-Control System Integration, and ISA88, Batch Control, series of standards are two strong examples of models for applying system-level thinking that have yielded increased quality, productivity, and efficiency for manufacturers worldwide. It is worth noting that these standards are being applied using IoT and other new technology in new architectures, including Industry 4.0.

The system-focused thinking of automation professionals is critical for the future success and existence of many manufacturing organizations. Manufacturers worldwide have realized low labor cost is not a winning strategy, and this is leading to greater adoption of automation, with IoT accelerating applications. There is a revolution going on with a much wider and growing range of automation options today driven by technology advances and lower-cost solutions. It is analogous to what happened in the computer industry with the shift from mainframe and minicomputers to PCs that enabled small- to medium-size companies to leverage computing to be more competitive. Manufacturers throughout the world are automating to stay competitive and profitable. The alternative is to be overtaken.

Lack of knowledge, more than actual budget constraints, is a major barrier when these types of changes occur. It is easy to do things the way they have always been done as competitive producers with lower prices take away business. It is easy to say they are "giving away the business" rather than seeking to understand the changing competitive landscape.

The automation professional's challenge is to first evaluate production operations to understand the greatest points of inefficiency, including existing overall production processes. Lean manufacturing concepts, value engineering analysis, and logistics analysis are great tools to uncover opportunities for improvement. It is advisable to use these foundational methods on an ongoing basis for continuous improvement. Automation professionals armed with the results of these types of analysis then need to educate themselves on new solutions available through Internet searches, webinars, and industry events.

As illustrated by the changing landscape in the computer industry over the years, the established automation suppliers may not offer the best solutions to be competitive. Too often manufacturers rely on the suppliers they have used for years. This is a very narrow lens for viewing what is possible to be more competitive.

Members of ISA have great opportunities to participate in forums and standards groups to share ideas, concepts, and experiences with other automation professionals. ■

ISA *INTECH* STAFF

CHIEF EDITOR
Bill Lydon
blydon@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Colleen Casper
ccasper@isa.org

SENIOR GRAPHIC DESIGNER
Pam King
pking@isa.org

GRAPHIC DESIGNER
Lisa Starck
lstarck@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

ISA PRESIDENT
Brian J. Curtis

PUBLICATIONS VICE PRESIDENT
James F. Tatera

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

Vitor S. Finkel, CAP
Finkel Engineers & Consultants

Guilherme Rocha Lovisi
Bayer Technology Services

David W. Spitzer, PE
Spitzer and Boyes, LLC

Dean Ford, CAP
Westin Engineering

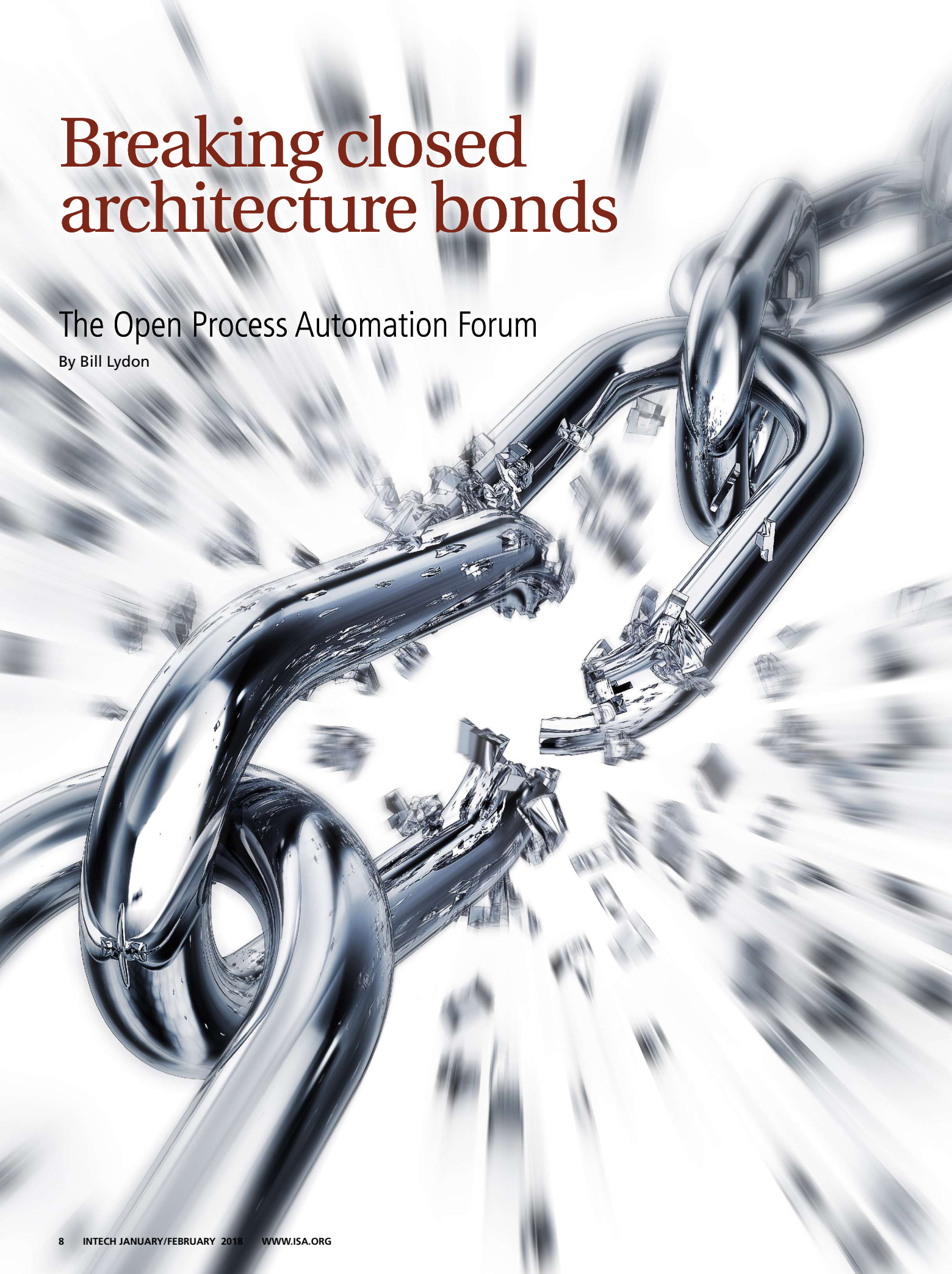
David Hobart
Hobart Automation Engineering

Smitha Gogineni
Midstream & Terminal Services

Breaking closed architecture bonds

The Open Process Automation Forum

By Bill Lydon



FAST FORWARD

- The goal is to create a process automation industry standard that generates an ecosystem of suppliers using the latest technology.
- The new standard drives change that parallels the evolution of the computer, telecommunications, consumer electronics, military defense, and avionics industries.
- A new coalition of end users throughout the industries using process control are defining the standard.

The Open Process Automation™ Forum (OPAF), launched in November 2016, is defining a standards-based, open, secure, multivendor, interoperable control architecture to satisfy the technical and business requirements of process industries. A major driver for this effort has been the widespread call for accelerating the modernization of automation technology, along with an ecosystem of suppliers that can leverage the latest technology in ways analogous to the evolution of the computer, telecommunications, consumer electronics, military defense, and avionics industries.

OPAF is a forum of The Open Group, which is a consensus-based standard group of end users, suppliers, system integrators, standards organizations, and academia with the mission to develop the Open Process Automation Standard (O-PAS). Don Bartusiak, ExxonMobil Research and Engineering, chief engineer, process control, and co-chairman of The Open Group Open Process Automation Forum project, has framed the issues by asking three thought-provoking questions:

- Would you accept your Verizon cell phone if it could not talk to a phone with AT&T, Sprint, Vodafone, or another carrier?
- Would you accept having to rewrite all your Word documents, spreadsheets, and presentations if you switched your home computer from a Dell to an HP?
- Would you accept that you must have a dedicated router from your Dell PC, a second router for your Apple computer, a third router for your Samsung phone, and a fourth router for your iPhone?

His conclusion is that this is the state of process automation control systems today. Control systems are so tightly coupled functionally that end users cannot integrate best-in-class solutions. They are trapped by the current closed architectures with highly gated vendor-managed partner ecosystems.

History

The root of the OPAF initiative was a corporate project at ExxonMobil to understand how the company would compete in the future, recognizing the significant shifts in technology as enablers for new competitors worldwide. This led the company to an understanding that open interoperable process automation systems would be required to compete.

User survey

The problem of replacing legacy systems is prevalent throughout the industry and reflected in the results of a Frost & Sullivan survey. It asked distributed control system (DCS) users: "What are the top five issues with current distributed control system architectures?" The biggest issues were:

- The difficulties associated with replacing a DCS are significantly higher than those associated with replacing or upgrading other computer-based systems (68 percent agreed).
- The cybersecurity models for currently available DCSs will be difficult to adapt to future cloud-based services or managed cybersecurity services (61 percent agreed).
- The pace of innovation for DCSs is typically slow compared to other information technology (IT) systems (61 percent agreed).
- DCSs at my facility/organization require replacement in large part due to system obsolescence (inability to integrate with newer equipment or systems) (54 percent agreed).
- DCS compatibility between generations is poor (even if the supplier stays the same) (53 percent agreed).

Note: The results are based on 53 survey completions and 13 interviews.

Birth of OPAF

ExxonMobil approached The Open Group to initiate a new open standards activity for the process control industry. From March to September 2016, ExxonMobil and The Open Group staff worked to build a "coalition of the willing" comprising end users throughout industries using process control and their key suppliers. During this time, the organizations built interest and identified potential participants via public outreach meetings, webcasts, and face-to-face conversations. As the incubation work proceeded, it became clear that there was interest from

at least seven different industry sectors that use similar systems from the same community of suppliers in their process manufacturing environments. These sectors included food and beverage, mining and metals, oil and gas, petrochemical, pharmaceutical, pulp and paper, and utilities.

The Open Group described, through its blog, a few things that quickly became very clear during the first member meeting:

- There are common pain points spanning multiple sectors (such as aging control systems and the need for more rapid technology insertion), which the proposed standards effort can address to the benefit of customers.
- There are similar pain points shared by suppliers in current business models.
- The supplier community is eager to work collaboratively on an open standard for process control.
- The participants had a common understanding that a "win-win" outcome, benefiting end users and suppliers, is essential. The members of the forum are keen to deliver this.

Adjacent industry example

At the 2016 ARC Orlando Forum, Dennis Stevens of Lockheed Martin, and Future Airborne Computing Environment (FACE™) (part of The Open Group) consortium business working group (BWG) chairman, described how standards have improved avionics and other critical military applications. He shared how the FACE software standard coupled with the OpenVPX hardware standard have spawned a multivendor interoperable ecosystem that has lowered cost, shortened project execution time, and improved functionality.

OpenVPX in avionics enables multivendor systems.

These are not ordinary products. They have to meet stringent specifications enabled in many ways by rugged electronic components developed for consumer products requiring higher durability and higher computing power, including cell phones and personal fitness devices.

ExxonMobil proof of concept

ExxonMobil engaged Lockheed Martin to build a prototype process control system based on standard hardware and software. Don Bartusiak, co-chairman of The Open Group OPAF and ExxonMobil Research and Engineering, chief engineer, process control, commented on the prototype progress: "Currently a proof-of-concept prototype by Lockheed Martin is in their facilities in Owego, N.Y., and is operational. There are two variants of the proof of concept. One runs against a simulated plant with emulated instruments. The other runs against a real, college lab type process with water tanks in series, sensors, control valves, and pumps. We are proceeding directly to the design of the prototype system for initial field trials on the basis of The Open Process Automation Standards in progress."

Organization

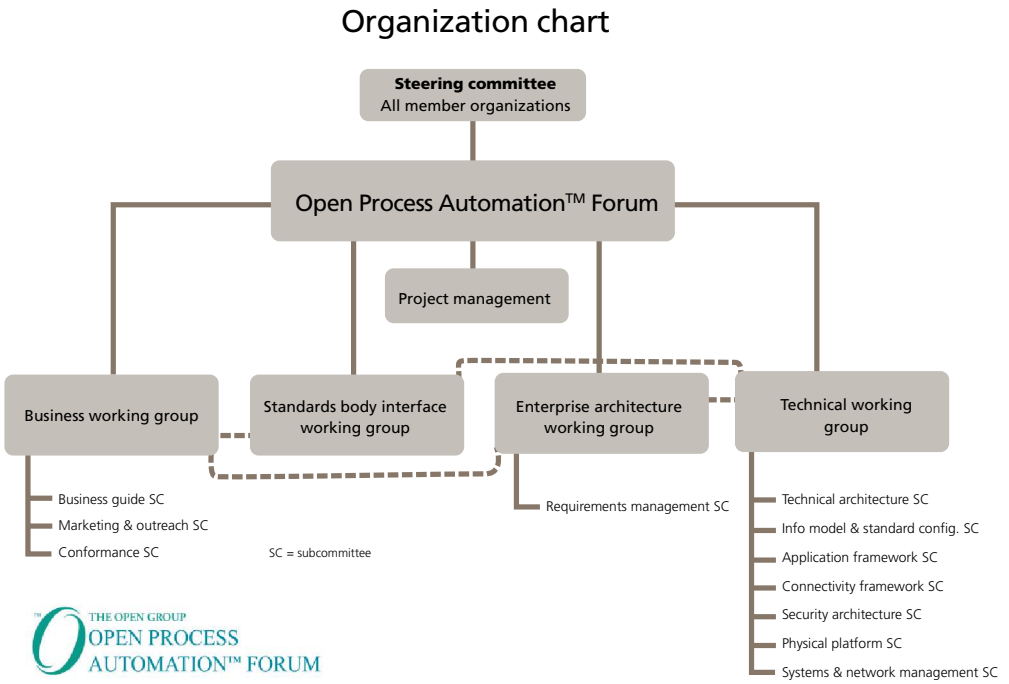
During the comprehensive first meeting, the members discussed the scope of the standards effort, while also creating the forum organization, and identified leadership roles for the forum and for specific work groups. The top Open Group Open Process Automation Forum leadership is:

- Director: Ed Harrington, The Open Group
- Co-chair: Donald Bartusiak, ExxonMobil Research and Engineering, chief engineer, process control
- Co-chair: Trevor Cusworth, Schneider Electric, VP, global account executive – ExxonMobil

This initiative has come a long way in a short time. Jim Hietala, vice president, business development and security for The Open Group, manages the business team, security and risk management programs, and standards activities. He characterizes the progress: "The Open Group is happy with the development of the Open Process Automation Forum, which now has 109 members including most of the major control systems suppliers, and significant end user representation from oil and gas, chemicals, pulp and paper, pharmaceuticals, and mining and metals. We are also pleased with the pace of progress in the forum, which started in November 2016, and now has technical, business, standards body interface, and enterprise architecture work groups; numerous subgroups, including conformance; and numerous technical subcommittees all formed, meeting regularly, and making rapid progress."

Ed Harrington, The Open Group OPAF director, commented on his role as the primary interface between the members of the forum and The Open Group. His roles include meeting organization and facilitation, as well as ensuring that The Open Group processes are followed, and all legal and vendor- and technology-neutrality guidelines are enforced.

The business working group is very active, noted Harrington, "The first formal deliverable of the forum is the Open Process Automation *Business Guide*, due for publication in January 2018. The *Business Guide* is targeted at mid- and senior-level management in both the supplier and user communities that make up the process automation ecosystem. The value propositions are key for both the end user and supplier communities. It takes a business—as opposed to technical—perspective to describe the vision, mission, and scope of the forum's effort. The guide has seven business use cases from the oil and gas, petrochemical, specialty chemical, pulp and paper, mining and metals, and biopharmaceutical vertical industries. It includes a description of the future-state process automation ecosystem and the business approach used to achieve that. Later in the year, the fo-



Source: The Open Group

rum will publish a "snapshot" of the first version of the technical standard. This document will give industry participants a strong indication of where the forum is heading from a formal technical standard perspective. This will allow industry participants not directly involved with the forum's standard development process to review and comment on its direction."

Business Guide

The *Business Guide* is a business reference for senior stakeholder leadership. It describes the vision, mission, and scope of the OPAF and details several vertical industry use cases. It also describes the envisioned future ecosystem and the approach to reaching that future through the development of a "standard of standards." The co-chairmen working on the guide are Darren Blue, Cloud Platforms, Health, and Silicon Photonics Groups senior controller at Intel Corporation, and Eugene Tung, West Point site IT lead, Merck Sharp & Dohme.

Technical working groups

Hietala and Harrington say the technical working groups are all working in parallel to facilitate development of the standard. Harrington commented, "The technical working group subcommittees are working diligently toward their aspects of standardization." Asked if these groups are working on high-level requirements at this point, Harrington responded that they are "a little bit beyond that with the business working group having come up with a couple of hundred identified requirements to the point that the technical people have a fairly detailed technical architecture."

"The plan is, and we are really pushing this in the second quarter of 2018, to publish publicly what we call in The Open Group a snapshot of where we're heading as far as the specifics of the standards are concerned. Remember what we are trying to do here, and why we are able to move it so quickly; we are not trying to invent new standards if at all possible. We may find some white spaces we are going to have to fill in, but for the most part we want to take existing standards and integrate and utilize them on a holistic basis. We are planning to publish a snapshot, then target releasing a version of the standard six months later," he said.

Jim Hietala emphasized, "It is not a serial process, not just doing the business guide and then shifting to the technology. Those things are going on in parallel. Along with the enterprise architecture working group, a conformance subcommittee has been spun up and started to meet around developing a conformance program that will be available in close proximity to when the standard comes out."

Harrington described The Open Group process where any member organizations of the group are free to participate to whatever degree they feel appropriate with as many people as they are willing to commit. "However, when it comes down to arriving at consensus, that is determined by the members of The Open Group Forum with each organization having one vote."

"We may find some white spaces we are going to have to fill in, but for the most part we want to take existing standards and integrate and utilize them on a holistic basis."
—Harrington

I asked if independent labs will be used for the conformance testing. Hietala responded, "that is all still to be determined." He said there is "a lot of blocking and tackling about what's the right policy." Hietala explained how the UNIX program, which The Open Group administers, works—vendors run a conformance test and submit results, providing a self-certification to the standards. "The goal is having products in the market that are certified to work conformant with a standard, so customers can identify a trademark and say they want a product that conforms

to that standard, delivering interoperability when it is installed."

I asked about safety. Harrington replied that "safety system standards, at least for this first go around, are off the table; it is not part of what we are standardizing." Bartusiak explained, "Given the requirements of the ISA-84 and IEC 61151 standards that there shall be separate and independent combinations of sensors, logic solvers, and final elements to achieve required safety integrity levels, the Open Process Automation Forum decided that safety instrumented systems were outside of its scope."

Sensors and controllers

I asked if the standard intended to deal with the controller and sensors. Harrington explained, "We are dealing within the controller. As a matter of fact, this includes the wire to the end devices. One of the big things the Exxon Mobils, the Shells, and other organizations throughout the world are complaining about is when upgrading systems, they end up having to move wires, which is a major cost. There is a subcommittee within the technical working group headed up by Alex Johnson, system architect – Next Generation Systems of Process Automation at Schneider Electric, looking at the physical aspects."

Control and sensor network standards?

I asked if the group intends to create a new industrial automation protocol, and Harrington clarified, "The OPAF Connectivity Framework will *not* be a new protocol. It will reference one or more existing standards. The technical working group is currently evaluating OPC UA to determine if it meets or exceeds the OPAF requirements for the Connectivity Framework."

Standards groups engagement

Because the intent is to leverage existing standards, I asked how OPAF will determine which standards to include in the new specification. Harrington described the process, "Standards to be adopted are being driven by the technical working groups, and then the standards body interface working group will develop the relationship and be responsible for the relationship between the other standards bodies. At this point in time there have been no specific standards that have been positively set in stone."

Hietala commented, "There has been a little bit of a chicken and egg in terms of The Open Group staff to put these relationships in place—needing to be driven by the standards liaison working group telling us which organizations make sense."

Harrington describe the process of using technical committee members, "we are relying on the expertise of the members of the forum who happen to be participating in the standards efforts." The technical working group committees define for the standards body interface working group the standards they would like to use as part of The Open Process Automation Standard. Harrington described the point of contact with other standards organizations, "Most times we work on a shared liaison basis where we will have an elected member of our forum represent what it is we are trying to do to the standards organization we are trying to deal with." Typically, this is a formal relationship with a memorandum of understanding. He noted the standards body interface working group leads are from Schneider and Siemens, based on the thought that the vendors are much more knowledgeable on the details of standards than users.

OPC Foundation

The OPC Foundation is currently the only standards organization outside of The Open Group that is a member of OPAF. Thomas Burke, OPC Foundation president, commented on the relationship, "OPC Foundation joined The Open Group in 2017 specifically to get engaged with the very exciting initiative called The Open Process Automation Forum. OPC Foundation recognizes the positive influence of the end-user community and the suppliers collaborating together in The Open Process Automation Forum. This initiative will clearly define the future of process automation and tie together all of the legacy systems with the systems of tomorrow. Great efforts are being made to make sure that systems are being architected that are truly open and will have timeless durability. It's very important to leverage the right technology for the right business cases when you are developing truly open hardware and software systems for the future. OPC UA is deliberately architected for complete protocol independence, platform independence, operating system independence, and vendor neutrality. We see this as the key infrastructure that the open process automation should be able to leverage easily to tie together the systems of the past with the systems of the future."

"Great efforts are being made to make sure that systems are being architected that are truly open and will have timeless durability."

—Harrington

System integrators

Discussing system integrators, Harrington said, "We have a liaison with CSIA, and an OPAF member from Lockheed Martin is our liaison with them." Discussing the relationship with Jose M. Rivera, CEO, Control System Integrators Association (CSIA), he commented, "The vision for the future of process control systems by OPAF is based on the concept of openness. This translates into significant changes in the business models of the various stakeholders, including independent system integrators. Through a formal relationship, CSIA and OPAF have been collaborating, specifically on the development of a business guide

document. A CSIA task force has shared its views to ensure that the roles and responsibilities of control system integrators, a key part of the automation business ecosystem, are adequately represented. Through this collaboration, CSIA has made its members aware and excited about the OPAF initiative." CSIA, founded in 1994, is a not-for-profit, global trade association that advances the industry of control system integration. It has more than 500 member companies in 27 countries.

What is at stake?

The industrial automation industry has dramatically lagged in the adoption of technology. A major reason for this has been closed ecosystems. Many vendors have partner programs that are promoted as "open," but they are highly gated, bureaucratically controlled, and closed systems for noncompetitive offerings. As in the computer, telecommunications, and consumer electronics industries, this closed approach is not sustainable. The dramatic technological changes, the rise of open systems in the computer industry, and the increasing implementations of Internet of Things advancements—with greater reliability, performance, and cost efficiency—is changing the landscape of system components.

Users should absolutely think about what they need to be competitive in their industries in the long term on the global stage. The intent of developing this new open process control architecture standard is to create an alternative. ■

ABOUT THE AUTHOR

Bill Lydon (blydon@isa.org) is chief editor for *InTech*. Lydon has been active in manufacturing automation for more than 25 years. He started his career as a designer of computer-based machine tool controls; in other positions, he applied programmable logic controllers and process control technology. In addition to experience at various large companies, Lydon co-founded and was president of a venture-capital-funded industrial automation software company.

View the online version at www.isa.org/intech/20180201.

RESOURCES

The OPAF
www.opengroup.org/open-process-automation/forum

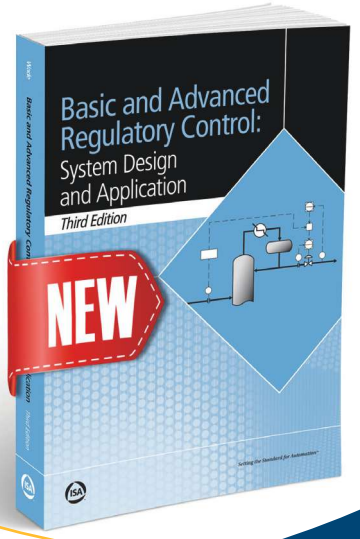
The Open Group
www.opengroup.org

The Future Airborne Capability Environment (FACE)
www.opengroup.org/face

VMEbus International Trade Association
www.vita.com/vpx

NEW! From ISA Publishing

Discover the economic benefits of applying advanced regulatory control strategies to processes and feedback control loops



An excellent resource for beginning and experienced technicians. Topics include set-point weighting controllers, dead-time processes, advanced process control (APC), cross-limiting control systems, and improving "as-found" tuning. Exercises are included at the end of each chapter.

Order your copy today at
www.isa.org/regcontrol

Setting the Standard for Automation™

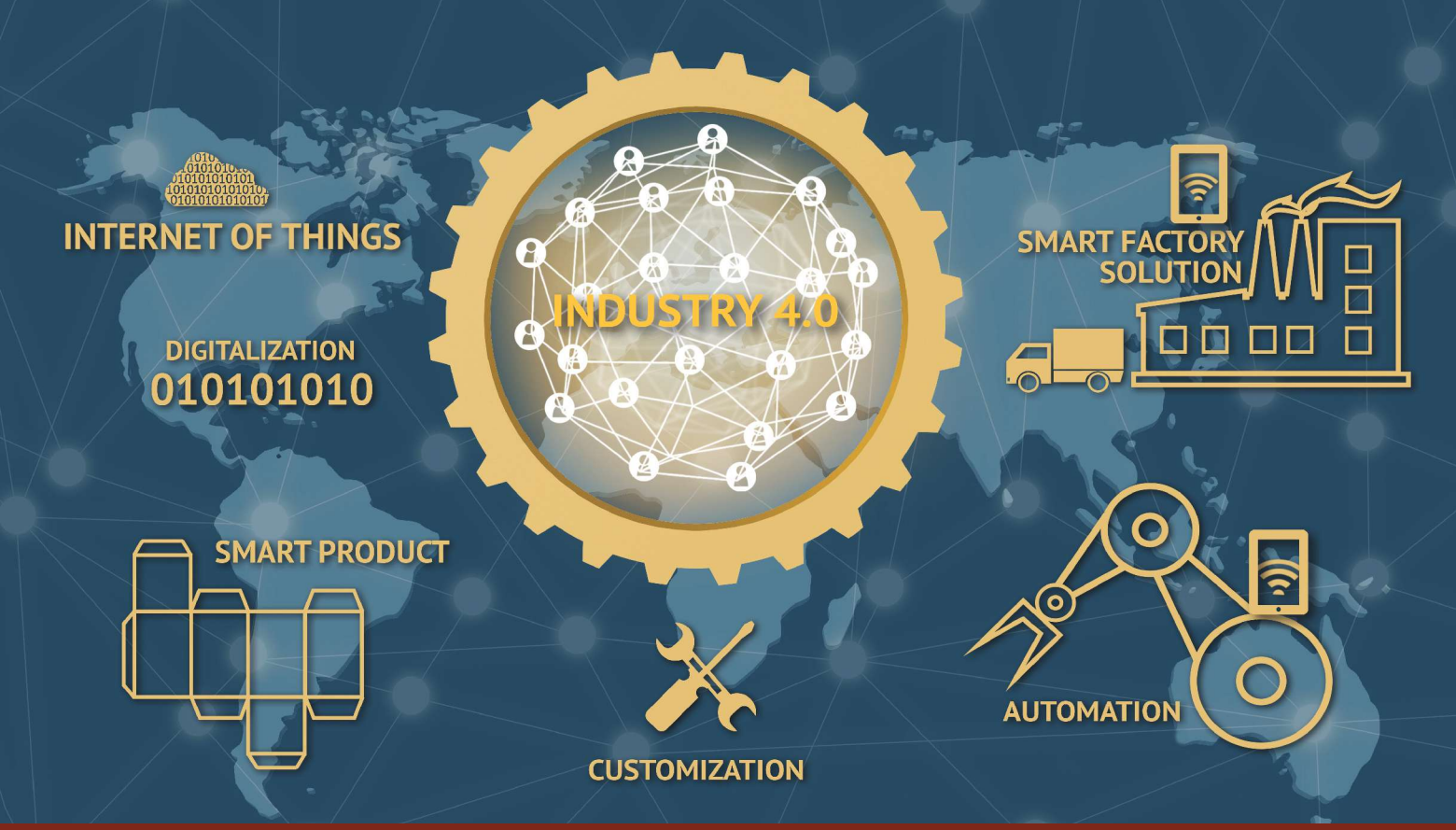
ISA

did you know?

Capacitance Probes do more than just level!

ARJAY ENGINEERING

+1 905-829-2418
MORE AT: WWW.ARJAYENG.COM



HART integration supports industrial digitalization

By Ted Masters

HART, FDI, and OPC UA collaboration simplifies applications

The vision of industrial digitalization, Industry 4.0, and the Industrial Internet of Things (IIoT) requires integration with information technology (IT) and operations technology (OT) systems to be successful. WirelessHART and HART-IP can be used to deliver the benefits of intelligent devices with digital communications for Industry 4.0 and the IIoT while preserving existing infrastructure, training, control system, and operational investments. Simplifying the bridging of information between IT and OT is the goal of the ongoing collaboration between the FieldComm Group and the OPC Foundation. They want to advance open information integration and enterprise data exchange, and streamline application engineering. The FieldComm Group has an official agreement with the OPC Foundation, creating a joint working group to develop OPC UA information models for process. At the 9 November 2017 NAMUR annual conference, there was a demonstration of field data information flowing from a HART device into FDI, then to an OPC UA cloud server, and displayed in Microsoft Azure.

The IT and OT systems have traditionally been disconnected, preventing industrial organizations from sharing and leveraging key information to improve production, quality, and maintenance. Organizations can make significant manufacturing improvements by using sensor data to make intelligent decisions about plant assets and process automation systems with the assistance of enterprise and cloud tools. Common tasks, such as preventative maintenance and tracking information to predict when machinery needs repair before failure, shift unplanned maintenance to planned and lower the cost of operations. With the right data and information, personnel can anticipate problems and take appropriate corrective actions to keep the plant up and running.

IIoT and Industry 4.0 technology and methods are being adopted worldwide, redefining manufacturing. While the interoperability of IIoT-based devices and systems will no doubt be the subject of ongoing discussion over the next few years, there are already well-established standards in industrial and manufacturing environments that can accelerate the implementation of the digital plant.

User expectations

Proprietary solutions in industrial automation are quickly becoming a thing of the past. The engineers and end users of today—primarily driven by

their experiences with consumer electronics—are no longer satisfied with products from different vendors not operating together seamlessly. This expectation now requires multivendor and multiplatform information integration from the sensor to the cloud. The days of the IT and OT worlds not communicating are also waning, with both sides seeking to convert data and metadata from plant assets into meaningful information. The joint activities of FieldComm Group and the OPC Foundation are bringing this reality into real-world focus.

FAST FORWARD

- Industrial digitalization, Industry 4.0, and the IIoT require integration with IT and OT systems.
- WirelessHART and HART-IP developments are paving the way to the benefits of intelligent devices with digital communications.
- The FieldComm Group and OPC Foundation are jointly developing OPC UA information models for process industries.

Role of HART

The large installed base of HART and WirelessHART sensors and devices is a huge resource for real-time information that is already on processes and equipment. There are more than 30 million supported field instruments worldwide. HART technology is a reliable, long-term way to leverage the benefits of intelligent devices through digital communication to improve operations.

Simply communicating raw data from field devices to OT and IT systems is not a good solution. The noncontextual data does not have meaning to be productively used for higher-level applications, including predictive maintenance, analytics, and process optimization, unless duplicate contextual definition profiles are available in the receiving systems. This approach duplicates information, contributing to lower system reliability and brittle systems that have problems when configuration changes are made in databases and field devices. The FieldComm Group and OPC Foundation are cooperating to solve these issues.

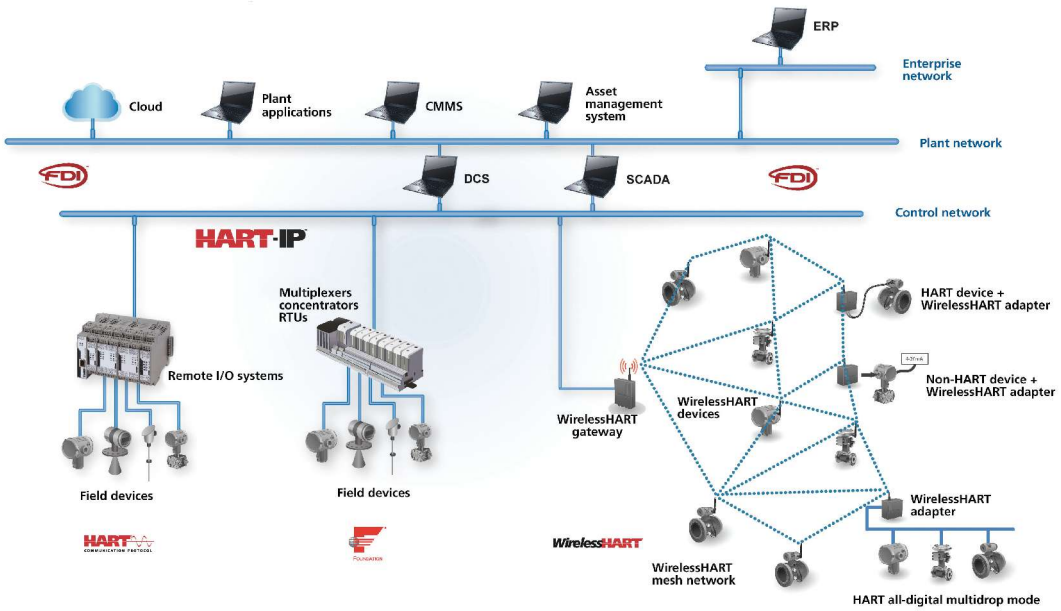
OPC UA component

OPC UA is a platform-independent, service-oriented architecture that has standard models for secure and reliable information exchange in industrial automation. Developed by the OPC Foundation, it is an established standard for integration and interoperability between factory-level devices, supervisory and control systems, manufacturing execution systems, and enterprise applications, such as enterprise resource planning (ERP) and supply chain management. As a vendor-neutral international standard, OPC UA is also published as the IEC 62541 specification.

In 2016, the OPC Foundation delivered open-source OPC UA code to the software community, paving the way for greater interoperability. This eliminated the need for rigorous multivendor testing, which was once the norm in industrial automation.

FDI and OPC Foundation collaboration

The architects of FDI partnered with the OPC Foundation to include in the design of FDI the OPC UA technology that defines field devices and field device integration in the context of FDI technology. Specifically, the technologies share the same information model that defines the context of field devices in process automation. The goal is to ensure that as systems evolve, an open pathway to field device information is assured. To complete the architecture, the FieldComm Group, which is responsible for ongoing development of FDI technology, has collaborated with the OPC Foundation to provide a solution allowing data and metadata from intelligent device networks to be consumed by generic applications. More importantly, this data is converted into information that can be communicated into the IT world and leveraged directly by cloud-based applications. Integration with IT and



The FieldComm Group accomplished sensor to enterprise and cloud integration.

OT systems is simplified, because the data communicated has the context of the data with all the information about the HART devices.

Standardization of devices, including their data and metadata, makes configuration easier, reduces application engineering labor, and simplifies training of new plant personnel, including operators, engineering, and maintenance. Training is a significant cost for any manufacturer, and having suppliers agree on data formats makes everyone's life easier.

FDI technology has been developed and supported by the automation industry's leading technology foundations and suppliers. FDI is scalable and combines the advantages of FDT® with those of Electronic Device Description Language. FDI takes account of the various tasks over the entire life cycle for both simple and complex devices, including configuration, commissioning, diagnosis, and calibration.

OPC Foundation's president and executive director, Thomas J. Burke, emphasizes, "It has been rewarding to collaborate with FieldComm Group on crucial technology initiatives. Our organizations have a common strategy and vision. We understand the value of implementing the best specification and certification processes, and providing technology to our respective communities to bring world-class products to market."

I believe the FDI standard provides a proven solution for end users to better manage their assets by having standardized device configurations that are independent of the vendors and networking technologies involved with their respective installations. With FDI, the true potential of decentralization, transparency, integration, and a central view of all data and functions can be fully realized.

FDI device packages and EDDL

In automation systems with field instruments from a variety of vendors, there is a need to reduce the effort of installation, version management, and device operation. This requirement can only be met with an open and standardized device integration solution. For this reason, the FieldComm Group has specified a standard architecture for device integration FDI (IEC 61769) that applies IEC 61804, *Electronic Device Description Language (EDDL)*, for the description of devices, including their representation in the OPC UA information model. Typical use cases for this solution include:

- interaction between users and the device (user interface)
- integration of new communication protocols (i.e., FDI communication servers)
- access to device information by OPC UA clients that are not FDI aware, such as archiving tools, maintenance tools, asset management, or ERP systems

FieldComm Group and the OPC Foundation cooperated on a companion specification defining how the information of a field device—described by an electronic device description document—is mapped to OPC UA objects, methods, and variables. The information model is primarily based on the OPC UA for Devices specification (IEC 61541-100); in fact, most of the OPC UA for Devices model has been driven by FDI requirements.

FieldComm Group's director of integration technology, Achim Laubenstein, states, "FDI technology manages information from intelligent field devices during their entire life cycle—from configuration, commissioning, and diagnostics to calibration, making one-off solutions for different devices obsolete. The standardization of field device information facilitates the development of native OPC UA applications that support the OPC UA device information model."

In addition to the device model, FDI defines how communication topologies of the automation system, representing the entire communication infrastructure, should be represented in an OPC UA AddressSpace. The comprehensive set of services provided by OPC UA enables the "how" of system integration.

Cloud applications

FieldComm Group's Integration Working Group is enhancing the FDI/OPC UA information model specification to provide semantics for machine-readable information. This specification will allow cloud-based applications to process field device information without extra configuration.

Mapping the FieldComm Group's data model to OPC UA enables frictionless OPC UA client/server and publisher/subscriber connections to the cloud. Applications that traditionally run on premise can now run globally in the cloud without having to change the interface to easily take advantage of robust cloud applications. Industrial organizations can have seamless information integration into cloud computing platforms, significantly enhancing compatibility and interoperability in the new digital world.

Future

FieldComm Group and the OPC Foundation are committed to developing complete infrastructures and solutions for seamless information integration in industrial automation applications. Both organizations recognize they must provide standards that help solve real-world problems and create new opportunities. This includes ongoing enhancements to the FDI standard, and potentially incorporating other organizations' networking technologies into a common integration architecture.

For more information, please visit the *FDI Technology Overview* (www.fieldcommgroup.org/technologies/fdi/fdi-technology). ■

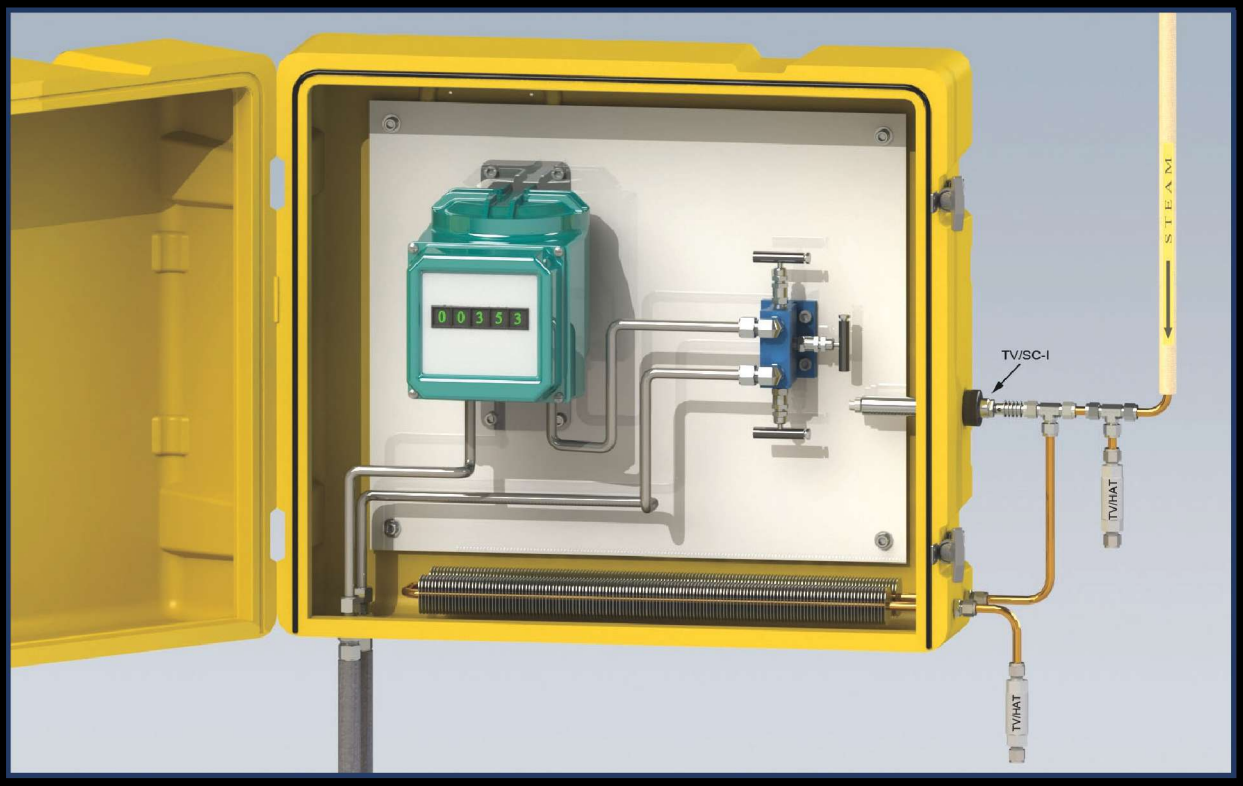
ABOUT THE AUTHOR

Ted Masters (tmasters@fieldcommgroup.org), president and CEO of FieldComm Group, has supported the process industry in leadership roles at a wide variety of technology companies for about 25 years. He has managed the growth and delivery of products, software, and service solutions to industrial markets. Masters' career has been centered around converting operational data into actionable intelligence and helping users make better decisions to capture the value by integration into business systems and processes.

View the online version at www.isa.org/intech/20180202.

Think inside the box.

Control temperature. Protect instruments.



ThermOmegaTech's innovative, self-actuating thermostatic valve technology maintains optimal interior temperature in instrument or analyzer enclosures. It's a reliable, economical and safe way to keep your instrumentation from overheating.

TVSC-A Valve

TVSC-I Valve

To learn how we can improve your systems,
please call us at (877) 379-8258
or email valves@ThermOmegaTech.com.

ThermOmegaTech®

Flow to the Nth Degree°

ThermOmegaTech.com

MADE IN USA

The next generation of MTConnect applications

By Russ Waddell

Process improvement, predictive analytics, and more

FAST FORWARD

- Manufacturing executives rank predictive analytics as the most important advanced manufacturing technology of the future.
- The decades-old vision of anticipating breakdowns before they happen can now be achieved.
- Factory connectivity coupled with the MTConnect standard is the underlying infrastructure of both predictive analytics and process improvement.

The MTConnect standard enables manufacturing equipment to provide data for predictive analytics—which is a hot topic for good reason. The vision of anticipating breakdowns before they happen is decades old, but the computing power, available data, and level of statistics and forecasting expertise in industry today puts this vision closer to reality than ever before. Production line shutdowns are exceptionally costly, and manufacturing executives are understandably enthusiastic about moving from a preventative to a predictive paradigm.

In the *Industrial Analytics 2016/2017* survey and report from the Digital Analytics Association Germany and IoT Analytics, machine predictive/prescriptive maintenance was the top industrial data analytics application. Similarly, in the *2016 Global Manufacturing Competitiveness Index* by Deloitte and the U.S. Council on Competitiveness, top manufacturing executives ranked predictive analytics as the most important future advanced manufacturing technology.

With the MTConnect standard, manufacturing equipment provides data in structured XML, rather than in proprietary formats. Uniform data opens up a world of new applications for industry. MTConnect data sources include production equipment, sensor packages, and other hardware. Applications using MTConnect data have more efficient operations, improved production optimization, and increased productivity.

Within the MTConnect community, the rise of analytics has been watched closely. The MTConnect standard drastically reduces the cost of translating between different brands or types of equipment and devices. A factory outfitted with MTConnect is an appealing target for an analytics project, because data is already homogenized and uniformly defined. The MTConnect standard defines a semantic vocabulary or dictionary of terms, as well as a structure of how terms relate to one another. The dictionary specifies units, exact wordings and spellings, and definitions. For example, "spindle speed" is normalized to "RotaryVelocity" and expressed in units of revolutions per minute. The structure or data schema specifies that RotaryVelocity is nested under a set of one or more rotary axes (for a single- or multispindle machine), and that rotary axes are in turn nested under a set of all axes, including rotary and linear.

MTConnect for monitoring

Machine monitoring was the first widely commercialized application using MTConnect data, and the standard has become closely associated with shop floor monitoring software and the companies writing and selling it. Those applications have long been used to visualize data like utilization and overall equipment effectiveness, although these days most software packages have expanded to include additional data views, calculations, or functions, such as downtime classification or data breakdowns by shift, process, or operator. Many of these features relied on MTConnect data, either by adding calculation across multiple existing MTConnect data items or by adding new data items into the standard. Despite the close association between MTConnect and shop floor monitoring companies, MTConnect is not application specific. The role of the MTConnect standard is to expose device data using a consistent dictionary of terms (data items) and predefined structure, but once that data is formatted and exposed it could be used for anything.

Predictive analytics for the factory

Building on the foundation already in place for monitoring and status reporting, predictive analytics is the most talked-about upcoming application area for MTConnect. Predictive analytics, which broadly means using data and statistical modeling to anticipate future events or conditions, has been talked about for decades in manufacturing. It may not have always gone by the name predictive analytics, but forecasting and error prediction have long played a big role in mitigating production risks.

Building on the foundation already in place for monitoring and status reporting, predictive analytics is the most talked-about upcoming application area for MTConnect.

Predictive analytics in manufacturing starts with crosscutting predictive models that apply to many different industries. It is a discipline unto itself, and the best practices, modeling, software tools, techniques, and computer processing power serving the discipline are always improving. As data science has become a full-fledged industry and a lucrative career path, many in the field have set their sights on manufacturing. Meanwhile, data connectivity in factories has become

far more common. Many companies with existing analytics capabilities in industries like finance, logistics, telecommunications, or ecommerce have been quietly seeking out new data sets to run through their algorithms and forecasting models. What starts as investigations into the Industrial Internet of Things (IIoT) often leads to industrial process improvement applications, which enjoy an appealing combination of high value-added use cases and available data. The result is a raft of new entrants into manufacturing from data analytics.

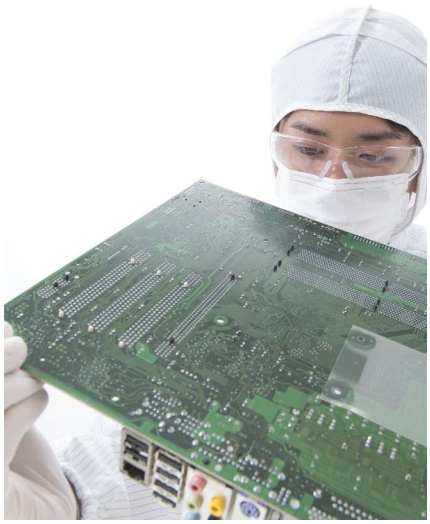
For established players in manufacturing and automation, the forecasting framework from finance, economics, and many other fields is already familiar. That framework has already been widely applied in measurement and test, quality and inspection, and statistical process control (SPC), among other manufacturing disciplines. As a result, many manufacturers are building up their analytics capability in house. Others are seeking close partners, especially from smaller companies with some manufacturing background, as well as programming and forecasting capabilities. Under the umbrella of predictive analytics, predictive maintenance is the most hotly pursued function. The concept is simple: the current maintenance paradigm is to fix or repair components once they have failed or based on a predetermined preventative maintenance schedule. In the future, predictive maintenance will dictate repair if and only if failure is about to occur.

Process analytics here today

Although predictive analytics is getting the most attention, a less glamorous area has the potential to be widely commercialized very soon. Analytics for process improvement is a logical next step from monitoring, and it avoids the complexity of building good predictive models. The *2016 IoT Analytics* report uses the more precise but cumbersome category "analytics that support process automation," which was considered far less important than "predictive/prescriptive maintenance of machines" among survey respondents. Compared to predictive analytics, analytics for process improvements and automation also lacks some of the associated jargon. Machine learning, deep learning, neural networks, and artificial intelligence, for example, are critical leading-edge technologies for predictive models. Process analytics, though, could be as simple as process visibility helping a human operator, technician, or engineer remove tedious or repetitive manual steps. Process visibility is like shop floor monitoring in that it presents data that already existed but may have been hidden to operators, engineers, or management.

In custom automated systems, continuous manufacturing or packaging lines, and high-volume production work, it is already common to include current process data to users and management. This data may include detailed views of setups, operations, or individual parts and assemblies. Shop floor monitoring, by contrast, emphasizes a complete and comprehensive view of all equipment and assets. Companies are increasingly demanding both detailed process data and comprehensive asset management views.

In commercial software packages or those integrated into automated systems, process analytics manifest as feedback to operators or improved communication between production and engineering. For example, a technician may know to periodically remove a filter for visual inspection. The inspection interval may be set at the production station or dictated by engineering, but additional automated data collection and analysis supplements and improves the process. Switching from manual inspection logs to automatically recording filter removal events saves time, improves accuracy, and decreases the number of process steps for the technician.



Layering automated data collection on top of existing processes like inspection, cleaning, or routine preventative maintenance can remove process steps, streamline production, and increase throughput.

Other application areas for process analytics include supplementing SPC and quality systems and tool path generation and tool selection for machining. In fact, there is barely a line between SPC and process analytics. Data collected for process analytics can simply be additional inputs to improving existing systems. For machining operations, linking data from a machine, cutting tool, CAM system, and even the part itself has huge implications for tooling. Established suppliers, new startups, researchers, and end users have all converged on better tool paths and better tool selection as near-term wins for analytics.

How analytics will come to market

In the near term, automated predictions will not replace human reasoning in the factory. Complex, nonlinear thinking gives humans the edge over algorithms for managing processes. Where predictive analytics shine today is in highly repetitive, high-volume operations where one or a few target variables with a big impact can be modeled. Temperature and vibration data collected from rotating parts, such as generators or turbines, is well suited for supplying data to predictive models. Those models will eventually adapt to handling more and more variation and work from smaller data sets. Human operators will still manage work with higher variation, but increasingly benefit from analytic insights. Computerized tips and inputs to streamlining processes are already available today; warnings about predictive maintenance concerns—with a human deciding when and how to act—is easy to picture in the not-too-distant future.

Manufacturers are more likely to develop process analytics applications

Predictive analytics, unlike process improvement, uses tools and techniques that are not specific to manufacturing. It is often a back-office function or is subcontracted to software or platform vendors.

in house than predictive analytics applications. Process data is often very manufacturing specific, whereas tools and techniques for predictive analytics are not necessarily dependent on close knowledge of processes. As a result, predictive analytics can be a back-office function or contracted out to software or platform vendors.

Standards landscape

Rapidly improving factory connectivity is the underlying infrastructure that allows both predictive analytics and process improvement. There is a huge demand for access to usable data, and a maturing data standards landscape in manufacturing that helps service that demand. More and more devices in the factory have a hardware or software plug for getting data out as well as just in. The data egress was initially very low-level signals, but software libraries and APIs help abstract from otherwise generic voltages, and semantic vocabularies like MTConnect standardize and supply additional context from one device to the next. The data models in MTConnect are most widely implemented in discrete manufacturing equipment, but have been used on everything from vending machines to discrete sensors to personnel data.

The standards ecosystem for manufacturing data extends well beyond MTConnect, which solves a relatively small and narrow problem for analytics. National manufacturing policies, including Platform Industrie 4.0 (Germany), Made in China 2025, and Make in India/Digital India, explicitly call out standards as enabling technology, in large part because clean and coherent data is required for the most promising next-generation applications. The broadest layer of the ecosystem is occupied by reference architectures like the Reference Architecture Model for Industrie 4.0 (RAMI) or the Industrial Internet Consortium's Industrial Internet Reference Architecture. These reference models specify functional areas that need industry (or cross-industry) collaboration and coordination to be successfully addressed.

In many cases, standards bodies are working to directly integrate standards. For MTConnect, this includes implementation guidelines for ISA-95/B2MML on device integration with higher level enterprise planning and management systems. It also includes the OPC UA/MTConnect companion specification, originally released in 2012 and currently being updated for a new version expected in the first half of 2018. The MTConnect development road map includes expanded device and asset models (e.g., robotics, additive, programmable grippers or work holding, and file transfer), but also covers integration with QIF quality standards and expanded functionality by supporting UPnP discovery.

Much more to do

Analytics is an area of tremendous opportunity for manufacturing and automation. Basic connectivity and data collection are increasingly the norm, and new applications that go well beyond status reporting are rapidly being commercialized. Meanwhile, the standards ecosystem for manufacturing data is evolving to serve demand for increasingly complex needs. Semantic definitions provided by MTConnect are part of the puzzle, but industrial policy in major manufacturing countries and global consortia are working to minimize duplicated effort. Everyone in manufacturing and automation should know that analytics are coming to the industry in a big way. Now it is time to get educated on how the hype is fast becoming reality. ■

ABOUT THE AUTHOR

Russ Waddell (rwaddell@amtonline.org) is the managing director for the MTConnect Institute and is responsible for day-to-day business operations. He also sits on the technical steering committee for the MTConnect standard. He previously worked at AMT as an industry economist, providing statistical research for sales and marketing in the manufacturing technology industry. He holds a BA in economics from The College of William and Mary.

View the online version at www.isa.org/intech/20180203.

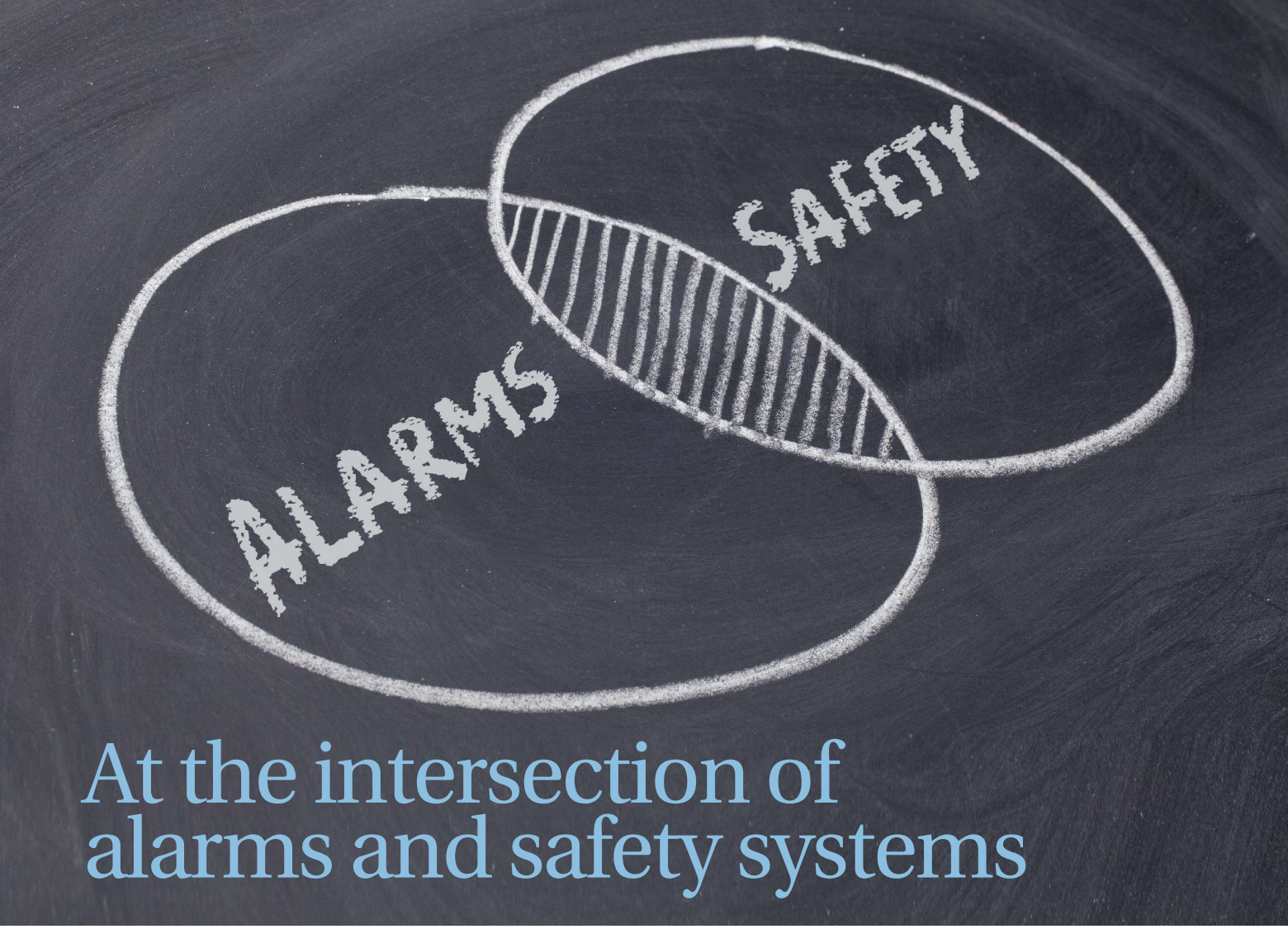
RESOURCES

Industrial Analytics 2016/2017
https://digital-analytics-association.de/dokumente/Industrial%20Analytics%20Report%202016%202017%20-%20vp-singlepage.pdf

2016 Global Manufacturing Competitiveness Index
www2.deloitte.com/global/en/pages/manufacturing/articles/global-manufacturing-competitiveness-index.html

Reference Architecture Model for Industrie 4.0
www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html

Industrial Internet Reference Architecture
www.iiconsortium.org/IIRA.htm



At the intersection of alarms and safety systems

When alarms serve the safety system, analysis must be handled with care

By Lee Swindler, PMP, Ron Carlton, and Richard Slaugenhaupt

It is not difficult to find resources related to safety instrumented systems (SISs) or alarm management, but discussions relating the two and considering their overlap are rarer. In fact, one could conclude that the two are not related at all, especially when companies address them at different times or with different personnel.

In a greenfield plant or process unit design, the hazard and operability (HAZOP) study is usually very early in the project—well before any concrete is poured or pipes are welded. Major hazards identified often trigger some equipment redesign. When the HAZOP is finished, a layer of protection analysis (LOPA) may be warranted to determine if a SIS is required (figure 1). When the automation systems are finalized later, attention turns to alarm rationalization.

An entirely new team of people, perhaps far removed from the HAZOP and LOPA efforts, may address rationalization. If a company is disciplined and fastidious about documentation, it is simple for the rationalization team to incorporate the results of the safety analysis, but this is not always the case. This is unfortunate, because details of the safety analysis play a substantial part in defining how the alarm rationalization process incorporates safeguards and independent protection layers (IPLs).

The most important layer of protection in any process is effective process control. Short of an outright mechanical failure, operations within normal boundaries produce few, if any, incidents. But no basic process control system (BPCS) can handle every possible disruption, and there will always be some process upsets.

The alarm system tells operators about disruptions that the BPCS cannot adequately handle automatically. An operator response is then required to fix or mitigate the problem before it escalates to the point where the SIS has to act. By definition, every alarm has an associated operator response, and the operator needs to know the appropriate action.

Scope limitations

It is logical to perform a HAZOP before construction has proceeded too far. For many companies, hazard analysis is tedious. A group spends many days hammering it out and might not want to extend the effort with discussions about alarm rationalization at this stage. Moreover, the automation system design may not be far enough along to make such a discussion practical. This is not a problem if the results are thoroughly documented, but poor documentation can cause significant problems for subsequent design efforts.

The HAZOP analysis identifies hazards in the process and determines the likelihood of a particular event actually happening. The LOPA considers ways to prevent the incident, or at least mitigate the result, with a preference for multiple layers of protection to prevent escalation to a full catastrophe. A LOPA study typically comes after the HAZOP, assuming a company uses it as its safety integrity level (SIL) assessment method. This is when IPLs are identified, including those defined as operator actions triggered by alarms. If the HAZOP team produced thorough documentation, this effort should be straightforward.

Operator actions as layers of protection

When the LOPA team concludes that a particular operator action can eliminate or reduce a hazard identified in the HAZOP, an alarm may be defined as an IPL within the safety system strategy. As a result, that alarm is included in SIL calculations associated with the design of the SIS. SIL calculations can take credit from the alarm's presence and may permit less drastic action in subsequent layers, as long as the operator appropriately addresses the situation.

For example, an interlock in a subsequent layer, which would have required a SIL 2-rated system, may only require a SIL 1 level of protection to achieve the same overall effectiveness when combined with the alarm. Of course, if the alarm does not cause the operator to take the designated action, the IPL fails, and the incident escalates until it encounters the next layer of protection.

With all this in mind, it is clear that key information from these studies has to survive multiple team handoffs and be implemented properly to achieve the correct alarm response to a hazard. At each handoff and time lag, gaps can form in the chain and interfere with the desired outcome.

Once it reaches rationalization

Later—possibly much later—after the other teams have done their work, the company will form an alarm rationalization team with a goal of determining the optimal set of alarms to include in the system. The idea is straightforward: deliver the right alarm to the right operator at the right time with the right importance and with the right guidance to correct or mitigate an undesirable situation. It sounds simple, but a team can become quickly intimidated by the scale and complexity of the challenge.

FAST FORWARD

- The safety instrumented system and operator alarms interact, but are usually developed by different people at different times.
- ANSI/ISA-18.2 is a very helpful tool if it is applied appropriately.
- Operator alarms that are intended to function as independent protection layers must be planned and implemented carefully.

The alarm rationalization team is supposed to review and evaluate the operation of the plant or unit, determine the undesirable things that might occur, and subsequently determine which associated alarms are appropriate under the criteria set forth in the alarm philosophy document. The team may create a preliminary design that includes the priority, set point, and other alarm attributes. An effective team might process more than a hundred alarms each day from a total of about 10,000, so the process is often long and tedious.

Most of the time, there are many more general process alarms than alarms related to safety conditions. So, within the massive undertaking of alarm rationalization, the team is supposed to give special consideration to perhaps 15 percent of the total. Any alarm intended to function as an IPL should be included as a given. There is no question about the validity of these alarms, because they have already been figured into a broader safety strategy and definitely need to be there. Further, they must be implemented in a way that supports the intent defined in the safety analysis.

This raises two questions: Will the rationalization team members fully understand the importance of those alarms, and will they select the

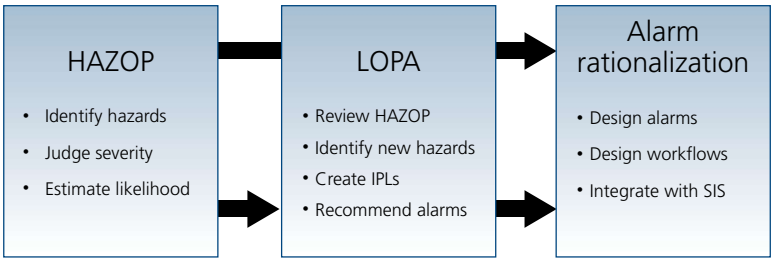


Figure 1. For most companies, the design of a safety system moves through distinct phases, each building on the previous effort. For this process to work correctly, each team must document its work thoroughly.

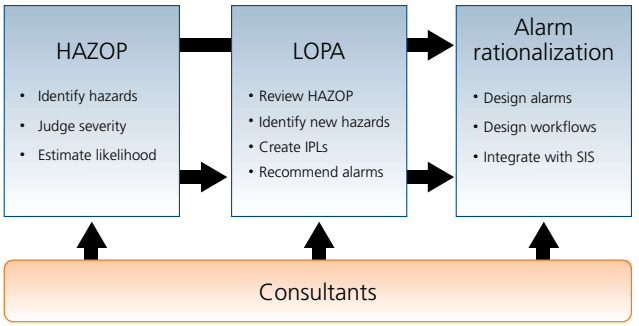


Figure 2. An experienced consultant provides continuity, so all elements are completed appropriately.

best way to design the alarm to achieve the mitigation results previously envisioned?

First, the rationalization team should not be forced to determine the difference between normal alarms and those that are truly critical. The critical ones should be clearly defined and documented by the hazards analysis, and their treatment should be defined in the alarm philosophy document. When done well, the documentation should leave no doubt which alarms are intended to be IPLs. If the documentation is insufficient, there is a chance that an alarm will not be treated appropriately or be missed entirely.

Second, the HAZOP team probably will not specify how the alarm should be implemented, given the limited information available during that phase of the analysis. The rationalization team will have to review the hazard and determine what event triggers an alarm and what series of actions the operator should perform within the necessary time window to mitigate the situation.

Not for the fainthearted

A team cannot be expected to review every hazard, and also to design the mitigation solution through layers of protection and alarming. Though ideal, it is impractical for most companies. In reality, it is common for each team—HAZOP, LOPA, alarm rationalization, implementation—to function independently, probably at different times and with different people (figure 2). There will be multiple handoffs from stage to stage. With effective documentation, these handoffs do not become points where knowledge is lost.

Because we are focusing on alarm rationalization, let's look at how this process works when dealing with safety-related alarms, many of which qualify as IPLs and figure into the larger SIS calculations. Alarm rationalization is a long and complex process, thoroughly documented in ANSI/ISA-18.2, *Management of Alarm Systems for the Process Industries* (figure 3). Many elements factor into the discussion, particularly when working with the safety-oriented alarms designed to perform as IPLs. The alarm rationalization team has to understand the methodology followed by earlier teams to recognize the hazards and generate the alarm requirements. Few companies have enough people with the depth of skill, experience, and time to do this—so outside assistance is often required.

Because any alarm, by definition, has to have an associated operator action, all alarms require workflow management. Operators need to know alarm responses from memory, or at least be able to retrieve them very quickly. Anyone auditing the system will likely quiz operators to make sure they can respond correctly and promptly. This means those individuals need to be trained. This is especially true for safety alarms where there is probably a very stringent time-of-response requirement. These alarms require the correct response within a specified time, or the opportunity to slow or stop escalation of the problem will be lost.

Consequently, anyone on the alarm rationalization team must bring a variety of skills and a thorough understanding of all the implications of the team's actions. The relationship between the BPCS and alarms within the SIS calculations is complex. Not all alarms recommended to help mitigate SIS-related hazards qualify as IPLs, so determining where credit is taken requires a deep understanding of these mechanisms.

If alarms being brought into the safety system are not implemented correctly, the IPL loses its validity, along with any credit in the larger SIS calculations. This often happens on a practical basis, whether anyone recognizes it or not. If the alarm is not implemented correctly, there may be excessive demand placed on the SIS, causing it to not have the intended availability to mitigate the hazard.

Alarm rationalization requires an engineering review before implementation, so alarms can be identified correctly, with each resulting alarm providing the protection required to fulfill the HAZOP, IPL, and the associated SIL calculations. Of course, this element of alarm rationalization is only one facet of a larger process. Most companies cannot pull it off single handedly, given the complexity and risk associated with the effort, but outside consultants are available to assist.

To understand the interplay of all these elements, everyone involved needs extensive process industry experience. Facilities and process units often handle very dangerous products with serious potential hazards. Handling them well requires discipline to avoid conditions that could cause an incident. Team facilitators, whether employees or consultants, must make sure all participants in the chain of analysis, design, and implementation know what is required to meet safety expectations.

Outside consultants, as neutral participants, can increase the likelihood of staying on track and avoiding internal

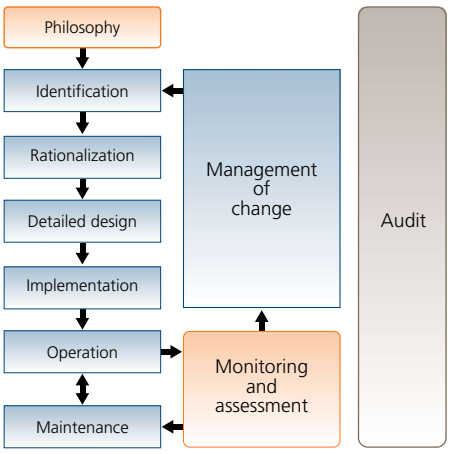


Figure 3. ISA-18.2 outlines the entire life cycle for a given alarm.

squabbles. They also bring experience from dozens of projects—more than the range of experience possible for someone working for one company or plant. ■

ABOUT THE AUTHORS

Lee Swindler, PMP, is a program manager at MAVERICK Technologies and has 30 years of automation industry experience. He is a TÜV Certified Functional Safety Engineer.

Ron Carlton, a consultant for MAVERICK Technologies with 30 years of petrochemical industry experience, is responsible for work processes and philosophy development in alarm management.

Rick Slaugenhaupt (richard.slaugenhaupt@mavtechglobal.com), a consultant for MAVERICK Technologies, has more than 34 years of industrial controls experience.

View the online version at www.isa.org/intech/20180204.

RESOURCES

"From managing to optimizing alarms"
www.isa.org/intech/20171002

"A standard grows up: The evolution of ISA's standard on alarm management (ISA-18.2)"
www.isa.org/a-standard-grows-up

"ISA alarm management standard packs a punch"
www.isa.org/isa-alarm-management-standard-packs-a-punch

"When Good Alarms Go Bad"
www.exida.com/Resources/Whitepapers/when-good-alarms-go-bad-learnings-from-incidents

"Get a life (cycle)! Connecting Alarm Management and Safety Instrumented Systems"
www.exida.com/Resources/Whitepapers/Connecting-Alarm-Management-and-Safety-Instrumented-Systems

"Alarm Management and ISA18 – A Journey, not a Destination"
www.exida.com/Resources/Whitepapers/alarm-management-and-isa-18-a-journey-not-a-destination

Safety Alarms: At the Intersection of IEC 61511 and ISA-18.2 Workshop
Texas A&M 69th Instrumentation Symposium for the Process Industries

Good documentation practices

By Joe Alford, *InTech* Editorial Advisory Board Member

Good documentation practices facilitate the management of projects as they progress from initial specifications to final system implementation. Good documentation is critical; often different aspects of a project are handled at different times and by different resource groups. The potential for missed, forgotten, or misinterpreted verbal communication is great. In all the documents discussed, it is important to note the rationale for the decisions. Many decisions are compromises, and it is important to capture their justification.

Selected documentation topics relevant to this article include functional requirements (FRs), system design, formal change control, alarm philosophy/rationalization, and system testing/commissioning.

Functional requirements: A validated system requires FRs documentation, and it is a best practice for all systems. This document is the complete list of project, system, infrastructure, and product requirements from the various project stakeholders. It is used to help select system vendors and in driving system design and testing.

System design: The design part of a project is driven by functional requirements and must be documented. It usually includes a multitude of documents, all the way down to detailed piping and instrumentation drawings. Design shows, for example, whether a separate SIS is included, LOPA information, interfaces with other plant computers, and where alarms will be generated.

Formal change control: Almost all major plant projects experience significant changes as the project progresses (e.g., a failure modes and effects analysis often results in significant plant or system redesign to reduce unacceptable risks from the original design). It is important for an organization to have a management of change procedure to drive activities associated with, for example, plant design changes, including the requirement to update relevant documentation. This enables late project activities, such as alarm rationalization, to draw on "up-to-date" design and other documents in determining what alarms to implement and what their attributes should be.

Alarm philosophy/rationalization: The requirements of alarm management are described in the national standard ANSI/ISA-18.2. This includes the need for an alarm philosophy document—which, in turn, describes the requirements for the various alarm management life-cycle activities, including rationalization. Alarm rationalization can be a daunting task with several attributes needing specification for sometimes many thousands of plant alarms. Many of these attribute values can best be determined with the help of documents from previously completed project activities, such as functional specifications, system design, and documentation generated as part of change control.

System testing/commissioning: Testing is largely driven by functional requirements (i.e., the primary purpose of testing is to show that FRs have been met). Testing includes verification that alarms work as intended, which requires that alarms are implemented in accordance with the results of alarm rationalization, which, in turn, depends on the results of previous project activities. For example, ANSI/ISA-18.2 notes that plants can designate some classes of alarms as "highly managed," because they have special administrative (e.g., reporting) requirements. Any alarms designated as "highly managed" will typically be determined from documentation of previously completed project activities like HAZOP reviews.

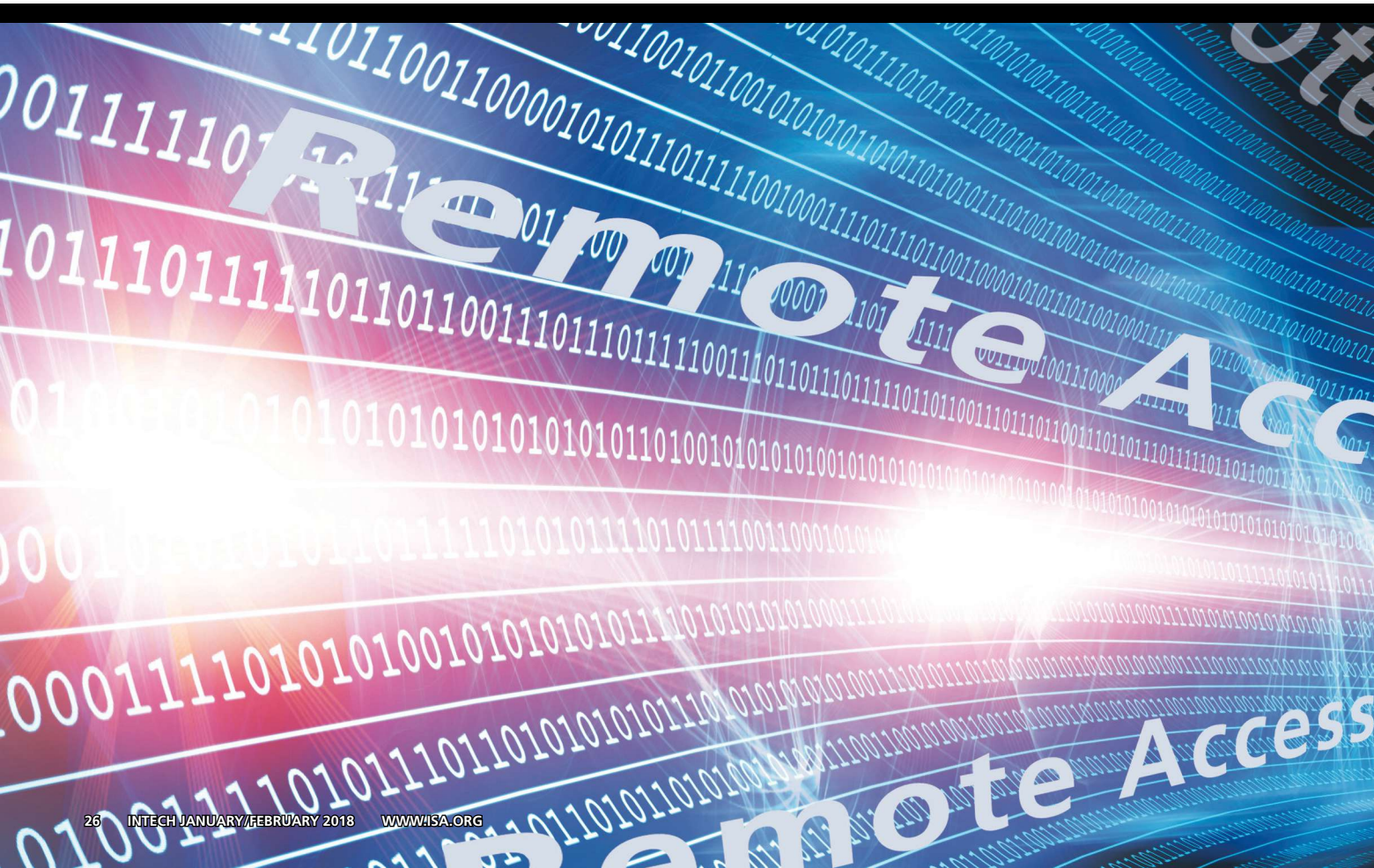
Remote access to automation system components

By Jonathan Griffith

Advantages and design considerations for the two main methods of remote VPN access

Remote access to local programmable logic controllers (PLCs), human machine interfaces (HMIs), and other automation system components is becoming a requirement for many machine builders, plants, and facilities. Although many industrial networks were previously configured with a router without a virtual private network (VPN), new installations should not do this because of the security risks.

Although a VPN is a key element in a defense-in-depth strategy, implementing remote and secure connectivity to local components presents technical, cost, and resource allocation challenges. The two options presented in this article address these issues in different ways. Each approach has advantages and design considerations (summarized in the table). Option 1 is a hosted VPN, and option 2 is a traditional VPN.



The decision to use a hosted VPN versus a traditional VPN hinges on four primary factors:

- Will all of my remote access needs fall under similar information technology (IT) conditions, with each site able to use the same router configurations?
- Is IT expertise available to support a traditional VPN?
- Is the IT team willing to support the traditional VPN?
- Will high bandwidth be required?

As shown in the decision tree (figure 1), if the answer to any of these questions is "no," then the hosted VPN solution is likely the best option. When the answers to these four questions are "yes," then a traditional VPN may be preferred.

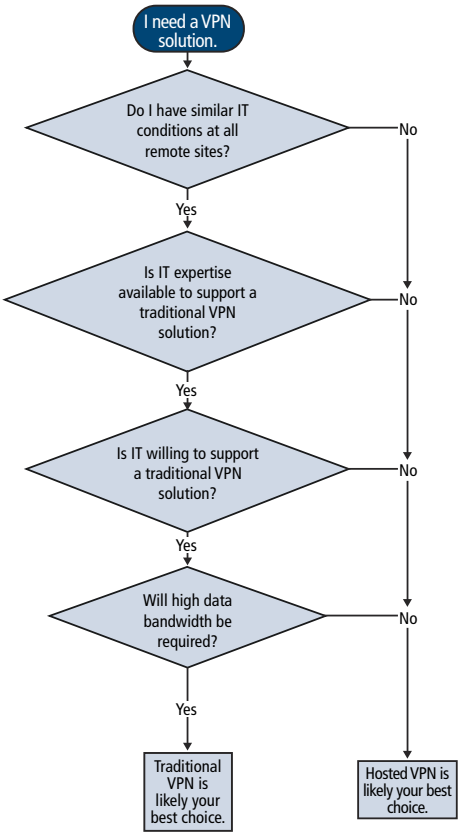


Figure 1. Decision tree

Option 1: Hosted VPN

Hosted VPNs provide a secure connection with simple setup and network configuration. Typical hosted VPN solutions include a VPN router, a hosted VPN server, a VPN client, and connected automation system components (figure 2).

A secure connection between the VPN client and the router is established after the router and VPN client each make a connection to the cloud-hosted VPN server. The router makes this connection immediately upon startup, but the VPN client only

FAST FORWARD

- The two main ways to implement secure remote access are with a hosted VPN and with a traditional VPN.
- A hosted VPN works well in most applications and is much simpler to implement and support.
- A traditional VPN may be necessary in applications with very high bandwidth requirements, but requires extensive IT involvement and support.

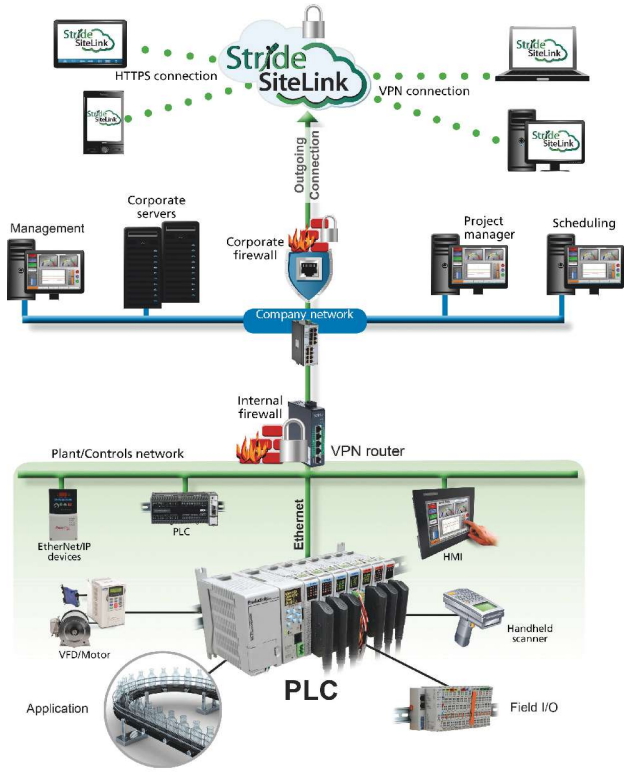


Figure 2. The STRIDE SiteLink Secure hosted VPN has no monthly charges for remote access as long as the bandwidth stays under 5 GB per month for all users in an account.

Figure 3. These VPN routers provide the functionality needed for cloud-based connectivity, simplifying implementation.

connects upon a verified request from a remote user. Once both connections have been made, all data passing through this VPN tunnel is secure.

Most hosted VPN solutions have a free monthly bandwidth allocation for basic operation, and then offer a premium plan for additional bandwidth. Normal troubleshooting and programming needs usually fall under the data requirements in the free plan, but extensive data monitoring or video surveillance may require additional bandwidth, depending on the amount of data transmitted over the VPN.

The router initiates communication to the server via an outbound connection through standard ports that are typically open, such as HTTPS. This usually requires no changes to the corporate IT firewall, and satisfies IT security concerns. By contrast, traditional VPNs require inbound firewall ports to be opened, which requires IT involvement and oversight.

Another advantage to a hosted VPN is the router configuration is extremely simple. Because the secure router (figure 3) is connected to a predefined cloud server, the router comes preconfigured, requiring only the most basic network information from the user. The router's internal firewall comes with a default setup to keep the plant floor network separate from the corporate network.

The platform and hosted servers do the complicated VPN networking behind the scenes, so non-IT staff can easily configure it. Staff members only need to know the IP addresses of the automation components connected to the local area network, and whether their ISP or corporate-wide area network router (not the hosted VPN router) provides IP addresses dynamically or statically.

In addition to a wired local area network (LAN) option, the hosted VPN should have Wi-Fi and 4G LTE connectivity options. Wi-Fi provides a simple access point or client connection, and allows plant personnel to access the router's LAN network wirelessly, rather than opening the panel to access the physical LAN connection ports. With 4G LTE connectivity, users have access from remote locations without Internet access or locations that will not provide access to the corporate network.

This approach has a very low security risk, because the client connection to the cloud server uses the proven encryption standard SSL/TLS, along with TLS 1.2. The required TLS key exchange, crucial for security, is done in accordance with the industry standard 2048-bit RSA with SHA-256. In addition, some vendors have advanced user management, event logging, and two-factor authentication—which requires a second time-based password generated at login—for an extra level of security at the user access level.

Hosted VPN design considerations

Those considering this solution must have a high level of trust in the hosted VPN vendor, as it will be responsible for securely storing data and making it available to only those who need it. Monthly costs incurred for high data bandwidth usage must also be considered, particularly as those costs are zero for a traditional VPN solution.

The hosted VPN solution does not require an IT team for support, because it is simple to implement and maintain, and most companies accept it as secure. Those companies that do not accept a hosted VPN solution for security reasons would likely not accept a traditional VPN either because of its required firewall changes.

The simplicity of this solution comes at the cost of limiting some of the advanced routing features that may be required for sophisticated networks, such as machine-to-machine networking, advanced network address translation (NAT) configuration, and access control lists. However, for most users these advanced features are not required.

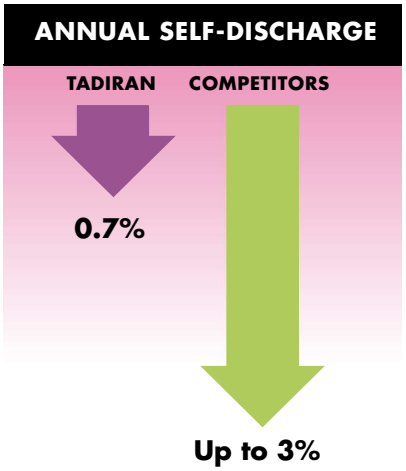
Other design considerations depend on specific features offered by the router

No place to replace a battery.

PROVEN
40
YEAR
OPERATING
LIFE*

Highly remote locations call for Tadiran batteries.

Battery replacement is costly and often dangerous work. Reduce the risk with Tadiran bobbin-type lithium thionyl chloride ($LiSOCl_2$) batteries. With an annual self-discharge rate of just 0.7% per year, Tadiran $LiSOCl_2$ batteries enable low power consuming wireless devices to operate for up to 40 years on a single battery, up to 4 times longer than the competition. Our batteries also feature the highest capacity, highest energy density, and widest temperature range of any lithium cell, plus a glass-to-metal hermetic seal for added ruggedness and reliability in extreme environments.



Take no chances. Take Tadiran batteries that last a lifetime.

TADIRAN BATTERIES

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

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

www.tadiranbat.com

Figure 4. Traditional VPN solutions often use a local HMI running on an embedded platform, like this C-more panel.

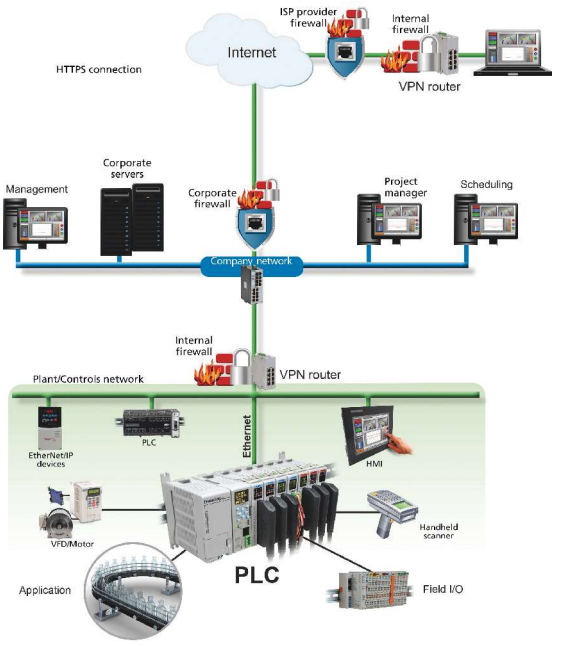


Figure 5. A traditional VPN solution using two routers is shown in this diagram. IT support is required both locally and at each remote site.

vendor. Including these key features addresses the issues, while excluding them may present problems. These key features include data logging, widgets for configuring remote access screens, a Web-based platform for router configuration, and a digital input for enabling or disabling remote access. The traditional VPN solution requires a third-party HMI, either PC based or embedded (figure 4), to provide data logging and widgets for configuring remote access screens.

Data logging provides collection, storage, and display of data via a cloud-based platform. Users can store and access a nearly unlimited amount of data, while only paying for the capacity required. Users can start with a small amount of storage, and scale up as needed. Cloud-based data logging typically requires an additional license or subscription from the router vendor to collect and store the data in the cloud, and this cost must be considered, particularly since the traditional VPN option does not have this expense.

Some cloud-based data storage and monitoring solutions allow users to configure dashboards using widgets for remote access viewing on their PC or mobile device. Alerts and notifications can be configured to inform users when parameters fall outside a predefined range. If this feature is not provided, designing remote access viewing screens can be cumbersome.

A Web-based platform lets users quickly and easily configure the VPN router, often as simply as registering an account, configuring and downloading router settings, and installing a secure client on a PC. The main advantage of a Web-based platform over a PC-based configuration is that platform updates can be made without the user having to reinstall a new version. This is particularly useful when new features are added regularly.

An important safety feature for the VPN router is a digital input for a switch to locally enable or disable communications, preventing remote control of a machine during maintenance periods. If this option is not provided, it should be added, which will add cost and design time.

Option 2: Traditional VPN

This option requires a local VPN router to connect through the Internet with a secure VPN tunnel to a second remote VPN router or software client (figure 5). Once connected, remote users can access automation components connected to the local router through the VPN tunnel.

Unlike option 1, there is no cloud server between the two devices with either method of connection: VPN router to VPN router, or VPN router to VPN software client. This option is preferred when large amounts of data need to be continuously exchanged between the local and remote sites, as to view local video remotely.

This solution is widely used, and it was the only method of secure two-way access before the introduction of cloud-based remote access solutions. It can be complex and costly in terms of internal resources required for support, both at the local and the remote sites.

Traditional VPN design considerations

The main design consideration for this option is the capability and willingness of an IT team to support this solution at both the local and remote sites for each installation. For example, an original equipment manufacturer (OEM) machine builder must consider every customer site, and make sure all of its customers are willing to provide IT support. If not, the OEM will have to customize its remote access solution for each customer.

This solution is often more expensive up front than a hosted VPN because of increased hardware costs and the IT resources required to configure the connection. Some companies have a dedicated IT staff to provide this support, but many smaller companies do not. Ongoing external costs are lower, because there are no monthly cloud service fees, but internal costs are higher due to the need for IT support.

IT must open an inbound VPN port on the firewall. This provides full remote control and monitoring, as it effectively creates one network joining local and remote users, but also presents a secu-

GET THE OPERATIONS SUPPORT YOU NEED TO RUN BETTER EVERY DAY.

24/7/365 Remote Monitoring and Support Services.

- Remote Management
- Control System Monitoring
- Asset Optimization
- Staff Augmentation
- Emergency Support

PlantFloor24® remote management and monitoring solution offers the easiest, most affordable way to improve asset utilization, allocate technical resources more effectively, reduce operational variability and lower your working capital. Each PlantFloor24 solution is as unique as the facility for which it's designed.

If operational issues arise, our technicians will either work with you to identify a solution online, or dispatch a team of automation professionals from one of our 21 nationwide locations to assist on-site as needed.

PLANT FLOOR 24®

PlantFloor24 is a registered trademark of MAVERICK Technologies.

MAVERICK® TECHNOLOGIES

A Rockwell Automation Company

ANY PLATFORM. ANY INDUSTRY. ANYWHERE. Visit **PlantFloor24.com** | 888.917.9109

Remote access option tradeoffs

	Hosted VPN	Traditional VPN
External cost		
Initial	Medium	High
Sustaining	Bandwidth dependent	Low
Internal support cost	Low	High
Required technical expertise	Low	High
Changes to existing firewall	Not required	Required
Security risk	Low	Low
Data dashboards	Available through subscription	Typically not available
Data storage and access	Available through subscription	Typically not available

rity concern. This port must be protected from unwanted access at all times. Ongoing security vigilance is required to ensure the router and VPN protocols remain up to date, and other technical considerations must also be addressed, including:

- Firewall configuration may be challenging.
- Subnet conflicts must be addressed across sites with similar network designs.
- User management and access must be well controlled.
- Event logging is not usually implemented and must be added if needed.
- Security certificates must be created and managed.
- Advanced networking knowledge is required.
- Client configuration is needed for each connection point.

Despite some drawbacks, this method is the preferred VPN solution if the IT staff is available and willing to make firewall changes, if the application requires high data bandwidth, or if the company does not want to rely on a hosting vendor.

Application example: Traditional VPN

Consider two types of OEM machine builders. The first OEM sells very large and complex printing presses with thousands of automation system I/O points, and its customers require the OEM to support the machine, including uptime and throughput guarantees. The OEM needs to remotely monitor and support its presses worldwide to make sure it meets its guarantees to customers. The OEM has considerable IT expertise and is capable of implementing a traditional VPN, and each of the customers is willing to allow the required firewall modifications.

Each press also has multiple video cameras installed for remote viewing, a necessity for solving some of the more complex troubleshooting issues. Each printing press has a full-featured PC-based HMI installed for local viewing and data storage, with high-speed remote access to the HMI and its stored data required at all times. Therefore, large amounts of operating data must be continuously transmitted to the remote corporate control center.

A traditional VPN is the right solution in this application, because of the significant amount of data exchange required, which could be cost prohibitive for a hosted VPN, and because the right IT resources are available to support the solution at the control center and at each site.

Application example: Hosted VPN

The second OEM sells a machine that does not require video monitoring. Local operator interface is provided by an embedded HMI with limited data logging and storage functionality.

The OEM machine builder needs two kinds of remote access. The first is VPN access to remotely troubleshoot, debug, and program the machine's PLC and HMI. Second, the OEM and its customers want to monitor the machine's most important operating parameters on dashboard screens from remote devices, such as smartphones and tablets.

The OEM machine builder does not have an IT department, just one part-time person who set up the internal network. The automation staff consists of one or two control systems professionals who are experts when it comes to programming PLCs and HMIs to automate their machines, but who are not very familiar with IT, VPN, and router technology. Most of the OEM's customers are not willing or able to reconfigure their firewalls, eliminating the traditional VPN option. In this case, a hosted VPN is the best choice, because it will satisfy all of the OEM's and its customers' requirements, and it can be implemented without IT staff.

Data logging is provided in the cloud, so the local HMI's limited data storage capability is not an issue. The machine builder can use widgets to create dashboard screens that many different users can view on remote devices. When full control and monitoring is required, it can be done by installing a lightweight software client on a PC, which can connect to the cloud from any location worldwide.

Many considerations

When designing a remote access solution using VPNs, there are many considerations influencing final implementation: initial and sustaining costs, technical expertise during installation and ongoing operation, site control, security risks, and data storage capabilities.

Using the information in this article, end users can evaluate each option based on their needs, budget, and internal expertise—and then select the best choice for their applications. ■

ABOUT THE AUTHOR

Jonathan Griffith (jgriffith@automationdirect.com) is the product manager for industrial communications and power supplies at AutomationDirect. Before joining AutomationDirect in 2015, he worked at ANADIGICS, a Wi-Fi networking company.

View the online version at www.isa.org/intech/20180205.

RESOURCES

Q&A with authors of *Industrial Data Communications*
www.isa.org/q-and-a-with-authors-of-industrial-data-communications-fifth-edition

Industrial Automation Cybersecurity: Principles & Application
www.isa.org/ts13

IACS Cybersecurity Design & Implementation
www.isa.org/ic34/0318nc

The choice is obvious

Pressure sensors that use metal diaphragms are susceptible to scrapes, scratches, and dents in harsh applications. All this damage creates unnecessary headaches and maintenance. But there's a better way. VEGA pressure sensors with ceramic measuring cells resist abrasion and other damage caused by caustic products or difficult process conditions and deliver consistent, accurate measurement without the headaches.

For more info about VEGA's pressure line visit vega.com/pressure

Which sensor would you trust to get the job done?

www.vega.com
1-800-FOR-LEVEL

Looking Forward VEGA

Checking cybersecurity vital signs

Industrial control system cybersecurity

By Lee Neitzel

How secure is your industrial control system (ICS)? Conventional wisdom says a comprehensive security assessment is required to answer this question. A detailed assessment may be overkill if you are just trying to get a first look at where you are on cybersecurity. Although a security assessment is a valuable tool, it is most often used for an in-depth look at threats, vulnerabilities, losses, and potential countermeasures.

So, what if you only want a checkup, not a full physical? There are 10 vital signs for self-checking your ICS—representing security capabilities that address common ICS threats, such as network attacks, connection of unauthorized devices, malware, and threats from inside the organization.

This self-check is like a checkup you get from your doctor, with the exception that there are no empirical measurements, like temperature or blood pressure, for an ICS. Because of this, and because this self-check is for your own use, scoring is left to you. Each vital sign is presented as a question (in no particular order). You can simply answer with "yes" or "no," but most answers will be a matter of degree, so scaling your answer (e.g., 0 to 10) may be more useful. Use

what is practical for you, because it is not the actual score that is important; *it is the insights you gain when answering the questions*. Once complete, you should have a good feel for the strengths and weaknesses of your ICS cybersecurity readiness.

FAST FORWARD

- Know the difference between a cybersecurity self-check and a full security assessment of your ICS.
- The vital signs represent top-level diagnostics that you can use for a self-check of your ICS's cybersecurity.
- This self-check can be performed periodically and supplemented with occasional in-depth assessments.

Vital sign #1

Is cybersecurity ingrained into your organization's culture and day-to-day operations? The answer to this question can be found in the work practices and behavior of personnel involved in the operation of the ICS, from management to operators. Are they security aware? Is the organization committed to keeping the ICS secure? Has it provided training and guidance for security best practices? Are there disciplinary measures for failing to observe them? And, for the more security-conscious, does the organization have security-certified personnel?

This vital sign should be easy to assess. Just look around. The way USB memory sticks are handled is a good place to start. Are there rules, formal practices, or polices defined for their use? Does ignoring or violating them go against the culture of the organization?

Vital sign #2

Do you maintain an inventory of all hardware and software in the ICS, and do you follow a formal process for controlling changes to them? For this vital sign, look for documentation that describes hardware and software components, when they were installed, and what changes have been made to them, including who approved the changes and who made them. It is important that all components and their change histories are documented. This vital sign makes it easy to determine if a device and its software are authorized, and if their updates (patches and upgrades) are current.

Vital sign #3

Are only necessary inbound and outbound communications between your ICS and other plant systems allowed? Unnecessary traffic has the potential to flood the network, attack internal ICS software, and otherwise disrupt operations of the ICS. Here, you are trying to identify all connections of the ICS to the plant network and beyond, and then determine if each is protected by a properly configured network security device. Typical network security devices that can be configured to control network access are firewalls, intrusion detection systems, and intrusion prevention systems.

Also, check if a demilitarized zone (DMZ) is used between the plant network and ICS network security devices. The DMZ is an intermediary/buffer zone between the plant network and the ICS that prevents direct communications between the two.

Vital sign #4

Are network access controls in place to prevent unapproved devices from being connected to the ICS? Vital sign #3 protects against unwanted traffic entering or leaving the ICS, while this vital sign lets you determine if someone can walk up and connect a device to your ICS network. For this vital sign, check if (1) network devices (e.g., switches, routers, and patch panels) are in locked cabinets, (2) unused ports of network devices are locked down, (3) the network is periodically monitored or scanned to look for newly added devices, and (4) network device ports are configured to limit the devices able to communicate through them to specific devices and to a specific number of devices.

The first two capabilities protect against plugging a device into an open port on a network device, such as an Ethernet switch, and then listening or transmitting. The third capability is used to find unauthorized devices, but network scanning should be done with care because it

can flood the network or interfere with device operations (e.g., if devices are scanned too rapidly). Testing scan rates before putting them into operation is recommended.

The fourth capability protects against someone connecting an unauthorized device to the network. For example, attackers may try to connect an unauthorized laptop to a wireless access point, or they may unplug an authorized device from the network and then connect their own device or network device in its place.

Connecting a network device in place of an original authorized device extends the network. Attackers not only can plug one or more of their own devices into the network, but can also reconnect the original device, so users will not notice a change in connectivity. When the additional network device has wireless capabilities, attacker devices can be located anywhere within wireless range. However, having capability four helps administrators find them and take corrective action.

Vital sign #5

Are your workstations and other devices hardened for security? You should check to make sure that (1) they have been stripped down to only necessary software, (2) anti-malware software is running and current, and (3) security patches are regularly installed. Security patches close vulnerabilities that attackers often successfully exploit using free hacker tool kits downloaded from the Internet. Capabilities of vital sign #2 above can be used to ensure that anti-malware updates and patches are current.

To verify that devices are stripped down, ask your vendors if they removed unnecessary software before delivery, and then look for software that may have been loaded after the device was installed. It is all too common for malware to install itself onto a computer and for users to copy their own programs to a workstation, not realizing that these programs may interfere with control system software or have vulnerabilities that can be attacked.

To find nonessential software, examine the programs in the start menu (or equivalent), and use an administrative tool, such as control panel, to check the installed programs and services. You may also search the file system of the device for executables and DLL files that should not be there. Check to make sure games, email programs, and other unnecessary or unauthorized applications are not present.

Security patches close vulnerabilities that attackers often successfully exploit using free hacker tool kits downloaded from the Internet.

Vital sign #6

Does your supply chain program require product developers in the supply chain (suppliers, their suppliers, etc.) to use security best practices? Security best practices for developers are embodied in security additions to their development and product support processes.

Upgraded product development processes are standardized in ISA/IEC 62443-4-1 and are commonly referred to collectively as a Secure Development Lifecycle (SDL). Although not all developers have upgraded their development processes to a full SDL, many follow a good number of SDL best practices. So, instead of asking the product developer if it has implemented an SDL, ask about the security practices in its current development process.

The key components of an SDL that are of interest are: (1) documenting security capabilities provided by the ICS in which the product will be used, (2) identifying security threats to which the product is expected to be exposed, (3) documenting and tracing product security requirements through design and implementation, and (4) specifying the types of security tests to which the product will be subjected.

The first two address the environment in which the product is expected to be used. The third and fourth address the security features of the product, including assurance that those features were implemented correctly and completely. The fourth, should, at a minimum, include testing of security requirements, testing for known vulnerabilities, and exhaustive testing of invalid inputs, also known as fuzz testing. Additional testing, such as threat testing and penetration testing, can provide greater confidence that the product has adequate security. Of course, no amount of testing guarantees an absence of security flaws.

Security best practices for product support are equally valuable, and are often incorporated into SDL practices. They include security patching, vulnerability handling and reporting, and security-related documentation that describes how to harden, configure, use, and securely decommission products.

Vital sign #7

Is confidential ICS data protected from disclosure, and is critical data protected from tampering? For example, are communications carrying confidential data encrypted? Are programs, configuration files, run-time parameters (e.g., set points, alarm limits), logs, and backup data protected from tampering?

Transmitting confidential data—like recipes, trade secrets, production data, and other control system information—in the clear makes industrial espionage easier. Similarly, program files, configuration files, and critical parameters/data that are not protected from unauthorized access are susceptible to being changed or even replaced by attackers. Leaving this data unprotected from tampering gives attackers an opening to insert spyware into files or to change the way the system operates.

To assess this vital sign, first look to see if ICS data is categorized or classified according to its security needs. Second, make sure that user access controls are set to prevent unauthorized reading of confidential data and unauthorized writing/updating of files and critical data. Third, for highly confidential data, like passwords and trade

secrets, verify that additional protections are used. Examples include cryptographic mechanisms (encryption and digital signatures), system partitioning architectures, and physical means, such as surveillance cameras, fences, locked rooms and cabinets, and conduits for network cabling.

Vital sign #8

Are all users authenticated and authorized using credentials (e.g., name and password) that follow best practices? For this vital sign, you are checking if all users are required to log in before they can use the system—no exceptions and no ability to circumvent the access controls. Access to your ICS should be like access to your bank account; access should be restricted to authorized personnel only.

There is often more than one way to log in, so check them all. Desktops and laptops often provide separate logins for the operating system and the control system, and potentially for control system databases. Further, if desktops or laptops are in areas where non-ICS personnel can gain access to them, multifactor authentication is recommended, such as using a smart card and personal identification number.

In addition, applications with web browser interfaces should also provide a login screen to users when access to the web server application should be restricted and when authentication is not provided to the application by the operating system.

Vital sign #9

Once they have gained access, can users access only the resources they need? Are administrator privileges given only to administrators, and are administrators restricted from performing control system operations? The primary goal of this vital sign is to see if the concept of "least privilege" is applied to both operating system accounts and control system accounts.

Operating system accounts define access privileges to program and data files, and to operating system parameters and functions. Control system accounts, on the other hand, define access to control system data and operations, such as who can download a controller, who can write run-time values, and who can calibrate a device.

Operators and engineers should be given only control system privileges that they need to perform their tasks, which should not include administrative privileges. Similarly, control system privileges should not be given to administrators. Administrative privileges should be given only to administrators. This separation of roles is important to keep operators and engineers from administering the operating system or control system, and keeping administrators from making changes to the process or factory floor.

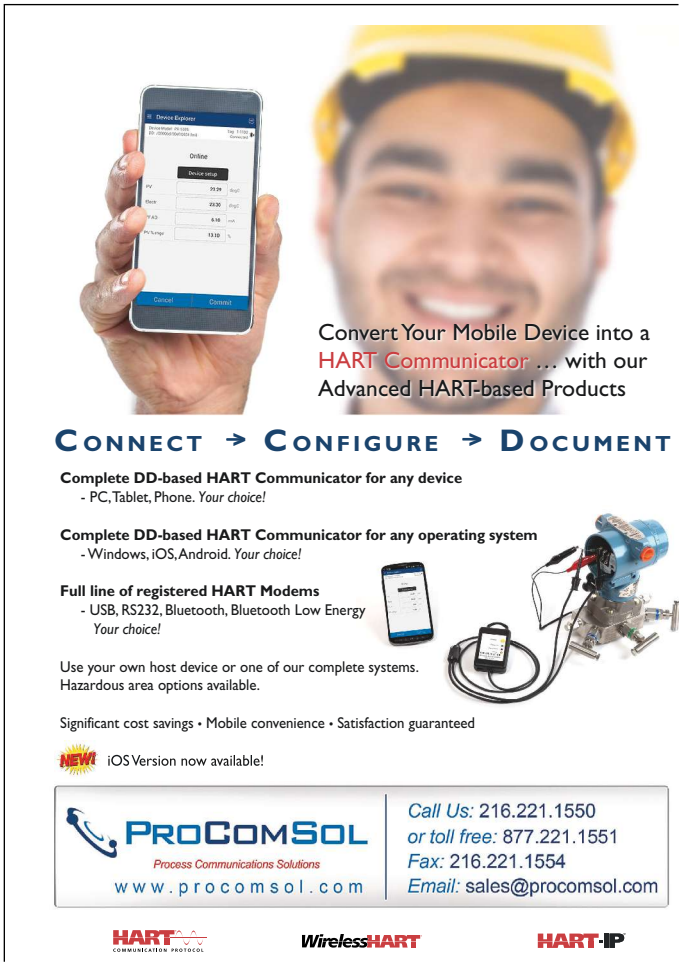
Finally, an advanced application of least privilege is making sure that operators and engineers use operating system logins that do not have administrator privileges. It is not uncommon for operator stations to go through an initial operating system login after a reboot, and then have all operators use this operating system login session when logging into the control system for their shifts. Without operators sharing this operating system session, the on-duty operator would have to log off, which would terminate all displays. Then the new operator would have to log in and reestablish the displays, causing a lack of continuity between the two.

You should check to ensure that this initial login is not done by someone with administrative privileges, since all operators would then inherit administrative privileges during their shifts. This restriction may not be supported by all control systems today, but over time this practice should be discontinued as control systems evolve.

Vital sign #10

Is the control system capable of detecting security breaches, and are there formal processes for handling breaches and associated security vulnerabilities? Breaches generally occur when protection mechanisms—such as those just discussed—are not present, are overcome, or are circumvented.

Detecting breaches is most commonly done through a combination of manual and automated activities. Many are detected by users who notice unusual or suspicious behavior from their workstations or the control system. Others are detected by programs and devices that are constantly monitoring the ICS for threats, such as



anti-malware software and firewalls. In addition, some software, like login applications, log suspicious behavior and issue event notifications to administrator or operator screens.

In many cases, logs need to be examined for suspicious behavior, for example, to determine if a failed login is an attack or just a typo by the user, or to correlate multiple control system events together to detect a pattern of malicious activity. Some software packages, like security information and event management (SIEM) systems, can be used to support these activities. However, many SIEMs are information technology oriented and are not equipped to examine control system logs.

Response teams are often used to verify and handle security breaches once they have been detected, and also to identify associated vulnerabilities and establish a way forward. In some cases, this involves restoring failed components from backups, reporting breaches and losses to authorities and customers, and notifying suppliers of vulnerabilities and requesting workarounds and patches from them.

Other considerations

As you perform this cybersecurity self-check, three additional factors may influence your score. These factors relate to the rigor with which your ICS implements cybersecurity. *First, you can consider the strength of the security measures associated with each of the vital signs.* The ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 standards formalize the strength of security measures using four security levels. Security levels represent defensive capabilities against increasing levels of attacker strength, expertise, and skill. For example, security level "1" represents defense against novice attackers, while security level "4" represents the ability to defend against nation-state attacks. For this self-check, give yourself higher scores if your system protects against attackers with higher skills.

Second, you should consider the formality of the organizational processes used with a vital sign. The IEC 62443-2-4 standard defines a maturity model for gauging how evolved (or formal) an organization's processes are. The base level in this model is for processes that the organization performs on an ad hoc basis. The remaining levels in this model are for formally defined, repeatable processes. If your organization has formal processes that it uses for a vital sign, give yourself a higher score.

Third, the degree to which your organization and its suppliers apply security can be assessed through certifications. The IECEE and other nonaffiliated test labs have formal certification programs for IEC 62443 security standards. Other certifications, such as Achilles Communications Certifications, are well known in the industry, even though they are not tied to a specific standard. Certifications provide an extra level of confidence that security is properly understood and implemented in the ICS. Give yourself higher scores for vital signs where certified devices or processes are used.

Top-level diagnostics

The vital signs represent top-level diagnostics that you can use for a self-check of your ICS's cybersecurity. Your answers to the questions about these vital signs bring valuable insights into how your ICS is poised to protect itself. This self-check can be performed periodically, and supplemented with occasional in-depth assessments, analogous to getting an annual checkup from your doctor and getting a full physical every few years. Of course, if the self-check reveals issues that need immediate attention, specially scheduled assessments can be used to investigate them.

Several types of in-depth assessments exist, such as risk assessments, vulnerability assessments, and threat models. Each has its own purpose, so you can select the ones most appropriate for your ICS. Finally, it is often advantageous to have an independent third party perform in-depth assessments to rule out bias and invalid assessments. ■

Vital sign checklist

☐ Vital sign #1
Is cybersecurity ingrained into your organization's culture and day-to-day operations?

☐ Vital sign #2
Do you maintain an inventory of all hardware and software in the ICS, and do you follow a formal process for controlling changes to them?

☐ Vital sign #3
Are only necessary inbound and outbound communications between your ICS and other plant systems allowed?

☐ Vital sign #4
Are network access controls in place to prevent unapproved devices from being connected to the ICS?

☐ Vital sign #5
Are your workstations and other devices hardened for security?

☐ Vital sign #6
Does your supply chain program require product developers in the supply chain (suppliers, their suppliers, etc.) to use security best practices?

☐ Vital sign #7
Is confidential ICS data protected from disclosure, and is critical data protected from tampering?

☐ Vital sign #8
Are all users authenticated and authorized using credentials (e.g., name and password) that follow best practices?

☐ Vital sign #9
Once they have gained access, can users access only the resources they need?

☐ Vital sign #10
Is the control system capable of detecting security breaches, and are there formal processes for handling breaches and associated security vulnerabilities?

ABOUT THE AUTHOR

Lee Neitzel (LNeitzel@wurldtech.com) is a cybersecurity consultant at GE Digital. He has been involved in security and network standards for more than 30 years and is currently leading the development of the IEC 62443 standards and conformance assessment program. Neitzel holds multiple patents in the area of control system cybersecurity and has a master's degree in computer science with a focus on computer security from George Washington University in Washington, D.C.

View the online version at www.isa.org/intech/20180206.

Awards cap productive year for ISA standards

ISA's Standards and Practices Department annually publishes 10–15 new or revised standards and technical reports that improve the safety, cybersecurity, and efficiency of industrial processes. Each year the department's governing body, the ISA S&P Board, presents department-level awards in recognition of outstanding efforts that have resulted in these documents or in other significant outcomes for an ISA standards committee.


Maurice Wilkins, PhD

For 2017, the following individuals were announced as award recipients by Maurice Wilkins, PhD, of Yokogawa and 2017–18 vice president of ISA's S&P Department, for their expertise and leadership in developing several key documents:


Graham Nasby

ISA-TR18.2.7, *Alarm Management When Utilizing Packaged Systems*

Provides guidance on how to integrate packaged systems into a basic process control system–based centralized alarm system. The technical report addresses various issues that can arise when ISA-18.2-2016 work processes are applied to facilities where packaged systems are used, providing guidance on how to successfully apply ISA-18.2 in those situations

Graham Nasby, City of Guelph Water Services, ISA18 Working Group 7 co-chair
Joseph S. Alford, consultant, ISA18 Working Group 7 co-chair
John E. Bogdan, J Bogdan Consulting
Bill Hollifield, PAS Global
Darwin E. Logerot, ProSys
Leila Myers, ILS-Automation
Bob Weibel, TiPS Inc


Hal Thomas

ISA-TR84.00.09, *Cybersecurity Related to the Functional Safety Lifecycle*

Sets forth guidance on integrating the cybersecurity life cycle with the safety life cycle as they relate to safety controls, alarms, and interlocks, inclusive of safety instrumented systems.

Hal Thomas, exida, ISA84 Working Group 9 chair
David L. Bennett, Phillips 66
John D. Day, Air Products and Chemicals
David A. Deibert, Air Products and Chemicals
Eloise L. Roche, SIS-Tech Solutions
Nagappan Muthiah, Wood Automation and Control


Kevin Klein

ISA-TR84.00.08, *Guidance for Application of Wireless Sensor Technology to Non-SIS Independent Protection Layers*

Addresses wireless technology-based sensors that are used in independent protection layers (IPLs) providing a risk reduction factor of less than or equal to 10 (non-SIS IPL) by the authority having jurisdiction (typically the owner/operator or local regulatory authority) and establishes guidance for their use in the process sector.

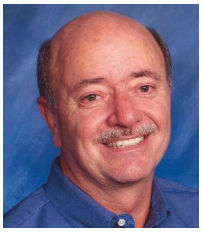
Kevin Klein, Chevron ETC Process Automation, ISA84 Working Group 8 co-chair
Greg LaFramboise, consultant, ISA84 Working Group 8 co-chair
Ted Schnaare, Emerson, ISA84 Working Group 8 co-chair


Herman Storey

ISA-TR100.20.01, *Common Network Management: Concepts and Terminology*

Provides an overview of the principles and concepts of common network management (CNM), the related terminology, and the expected benefits from adopting a CNM standard.

Herman Storey, Herman Storey Consulting, ISA100 Working Group 20 co-chair
Patrick Kinney, Kinney Consulting, ISA100 Working Group 20 co-chair
Patricia E. Brett, Honeywell
Dr. Penny Pei Chen, Yokogawa


Jim Federlein

ISA-RP105.00.01, *Management of a Calibration Program for Industrial Automation and Control Systems*

Sets forth the basic framework for developing and maintaining a consistent calibration program for industrial automation and control systems, including instrumentation used in safety instrumented systems.

Jim Federlein, Federlein & Associate, ISA105 chair
Leo Staples, Automation Solutions Advisors

For information on viewing or obtaining the documents listed above, visit **www.isa.org/findstandards**. For information on ISA standards, contact Charley Robinson (crobinson@isa.org). ■

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

Integrating cybersecurity into a greenfield ICS project

By Krish Sridhar, PE, GSEC

Industrial control system (ICS) cybersecurity is critical to companies that spend millions of dollars assessing and mitigating ICS cybersecurity risks. This is great news for brownfield systems, but how do we make sure that greenfield projects do not install new ICSs with cybersecurity vulnerabilities and gaps? Cybersecurity does not happen by accident—it must be consciously designed into the system.

Integrating cybersecurity into an ICS requires a project life-cycle approach. First, you must justify the project. The relationship between process safety and ICS cybersecurity is compelling for companies, especially if they fall under process safety regulations, such as OSHA process safety management (PSM). Preventing cybersecurity incidents that could cause costly lost production or extended service interruption follows and finishes with adherence to industry best practices and standards. The mission to "stop the bleeding" requires proactive integration and recoups losses on the bottom line.

Business challenges include acquiring buy-in from senior and project management, and support from engineering, procurement, construction (EPC), vendors, system integration (SI), and relative operations. Collective buy-in guarantees minimal impact on project scheduling.

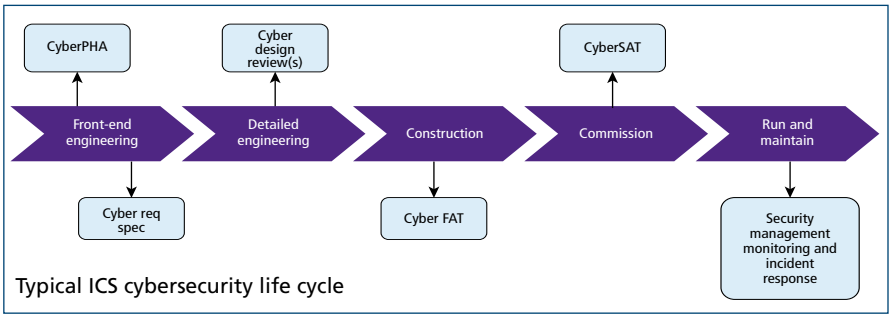
For reference, a typical ICS cybersecurity life cycle for existing systems has five phases: vulnerability/gap assessment, risk assessment, a mitigation plan, implementation, and auditing. Integration of cybersecurity into the ICS project life cycle consists of:

- front-end engineering with a cyberPHA (detailed cybersecurity risk assessment methodology)
- detailed engineering with cybersecurity requirements specifications and design reviews
- cybersecurity factory acceptance testing (CFAT) and cybersecurity site acceptance testing (CSAT)
- security management, monitoring, and incident response

Front-end engineering begins with ICS cybersecurity risk assessments, which are compliant with industry standards like ISA-62443-3-2. While conformance to standards is sufficient enough for many organizations, other factors, such as risk reduction per dollar spent, investor and regulator due diligence, and documenting to management, justify certain actions taken or not taken. An ICS cybersecurity risk assessment is meant to link a cybersecurity event and a true process hazard; a cyberPHA does so by connecting vulnerabilities and threats to consequences and likelihood of occurrence, accounting for existing countermeasures. The result gives management a road map highlighting a ranked set of risks, prioritized recommendations, and a mitigation plan.

If you want cybersecurity designed into your system, you must define your requirements and communicate them to all involved parties in the form of cybersecurity requirement specifications (CRSs). The CRS includes requirements for the monitoring and security of zones and conduit boundaries, and for hardening end points like ICS asset management, malware prevention, and access control. Include key stakeholders in the design review and have focused discussion about satisfied cybersecurity requirements and issues to document.

Conduct CFAT and CSAT on site to evaluate the cybersecurity of a system. The operating company should accept this before delivery and startup. CFAT and CSAT ensure the verification of cybersecurity requirements and proper configuration of security settings, the operating system, and antivirus software. Additionally, detection systems should be cleared as operational and able to identify and report events. Cybersecurity robustness testing must also be verified with discoveries on present vulnerabilities,



Typical ICS cybersecurity life cycle

Site	Unit	Zone	Unmitigated risk (no countermeasures)	Mitigated risk (existing countermeasures)	Adjusted risk (proposed countermeasures)
1. Anywhere	1. Remote	1. Employee remote access	8	6	3
2. Corporate HQ	1. Corporate	1. Enterprise	7	5	4
3. Terminal	1. Admin. building	1. Plant business	5	4	3
	2. Truck loading	1. Process control	8	6	5
		3. Safety	10	6	4
		5. Wireless	6	4	3
	3. Tank farm	1. Process control	9	7	4
		5. Wireless	6	4	3
3. Pumping station	1. Admin. building	1. Plant business	5	4	3
	2. Pump house	1. Process control	8	5	4
		3. Safety	10	6	4
	3. Tank farm	1. Process control	8	6	5
		5. Wireless	6	4	3

Example of an ICS risk profile

resilience to storms, and intrusion tests to verify firewall configuration. Tests in the latter coincide with the system under test, which establishes network boundaries and scope, the collaboration of CSAT and CFAT, verified configuration, and a punch list follow through.

Consider vendor-recommended settings for each control system platform: identify vendor best practices, modify default settings, review overall vendor hardening criteria, and review architecture and apply the data flow requirements.

The final life-cycle phase necessitates maintenance with the trifecta of security management, monitoring, and incident response. Security management is developed through governance policies aimed at sustaining the cybersecurity risk posture of ICS. Special consideration must be given to asset management, patch management, system backups and change management. Monitoring is the detection of abnormal activity, host and network intrusion detection, and periodic auditing.

To summarize, the benefits of integrating cybersecurity into the ICS project life cycle are:

- a common understanding of cyberrisk and securing that risk
- verification that security is properly implemented
- an operations staff security that is prepared to manage, monitor, and respond to security incidents before startup

In every stage of the project life cycle, transparency is essential, especially when future projects hinge on a clear vision of success. Practical goals aligned with CFAT, CSAT, and postcommissioning are a starting point. In summation of that, a team should consist of subject-matter experts from ICS cybersecurity, information technology infrastructure, process control, and project management. Assigning an ICS cybersecurity lead who works closely with all stakeholders from start to finish, with frequent communication along the way, ensures a successful cybersecurity program. ■

ABOUT THE AUTHOR

Krish Sridhar, PE, GSEC (krish.sridhar@aesolns.com), is a subject-matter expert on cybersecurity solutions applied to industrial control systems with aeSolutions (www.aesolns.com), a CSIA (www.controlsys.org) member company.

ISA Certified Automation Professional (CAP) program

CAP question

The purpose of an industrial control system alarm system audit is all of the following except:

A. Identify new points that should be added to the alarm list.
B. Check that the alarm system is meeting the documented alarm system objectives.
C. Ensure that alarm shelving and out-of-service procedures are followed.
D. Verify that alarm monitoring reports are active and up to date.

Certified Automation Professionals (CAPs) are responsible for the direction, design, and deployment of systems and equipment for manufacturing and control systems.

CAP answer

The correct answer is *A*, identify new points that should be added to the alarm list. Answers B, C, and D are all examples of alarm system auditing functions listed in ANSI/ISA-18.02. There are many more tasks that should be performed in an alarm system audit, including verifying that the alarm history is current, verifying that the management of change (MOC) processes have been followed, and verifying that all documented alarms are active and match the master alarm database.

Answer A is not an alarm system auditing function. The identification of points that need to be added to the alarm database begins with a management of change process. The MOC process is used to ensure that candidates for the alarm system meet the documented definition of an alarm (rationalization) and are assigned the proper classification and prioritization in the alarm system.

Reference: Trevathan, Vernon L., *A Guide to the Automation Body of Knowledge, Second Edition*, ISA, 2006.

ISA Certified Control Systems Technician (CCST) program

CCST question

What standard that defines quality policy and procedures is recognized as the "de facto" requirement for doing business in Europe?

A. ISA-12.12.01
B. ISO 9000
C. NFPA 70
D. CENELEC

Certified Control System Technicians (CCSTs) calibrate, document, troubleshoot, and repair/replace instrumentation for systems that measure and control level, temperature, pressure, flow, and other process variables.

CCST answer

The correct answer is *B,* ISO 9000. ISO 9000 is a set of standards developed in Europe that covers many aspects of quality management. The standard named ISO 9000 is titled: ISO 9000:2015: *Quality management systems – Fundamentals and vocabulary*. ISO 9000 has also been adopted widely in the U.S. as the baseline for quality management.

One standard in the ISO 9000 family is ISO 9001:2015: *Quality management systems – Requirements*. This is the standard for which organizations apply for certification. An organization applying for ISO 9001 certification is audited based on an extensive sample of its sites, functions, products, services, and processes. ISO 9001 certification is administered by qualified certification bodies.

The other answers are electrical standards, not quality standards. ISA-12.12.01 is the ISA standard for the use of nonincendive electrical equipment in hazardous locations. NFPA 70 is generally referred to as the National Electrical Code. CENELEC is the European Committee for Electrotechnical Standardization.

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

Wireless pressure tracking propels brewer's success

By Michael Koppelman

The growth of craft brewing has changed the whole American beer paradigm by separating the market from the traditional "big three." From 2004 to 2015, annual craft beer and ale production industry-wide grew fivefold to 25 million barrels, while sales of traditional brews declined.

Figure 1. Badger Hill's people come from a variety of backgrounds, but are all committed to creating innovative products for beer lovers to enjoy.

Craft brewing was born of a do-it-yourself (DIY) countercultural mentality that pushed the boundaries of style, brand, and quality beyond accepted norms. Many of the people making craft beer are not process engineers, but instead come from a variety of careers and are looking for a different path. Most have a keen entrepreneurial spirit, an independent streak, and a love of the art of brewing. They come to craft brewing with different motivations, and think differently than many of their counterparts in other industries.

At Badger Hill (figure 1), we enjoy craft brewing because we manufacture fun, making a product that is not a commodity. Our customers want us to be craftspeople—innovative and different—which is exactly what we want to be as a company. Our people understand this, and we are always looking for new ways to improve.

But, craft brewers are also manufacturers. We know we need to deliver product reliably enough to be financially sustainable, which means dealing with many of the same problems as more traditional manufacturers. The expression of the craft and the capital to innovate is made possible through good manufacturing processes. Customers expect consistency, and operations must comply with appropriate regulations. We need to learn from other companies, so we can focus on new problems rather than ones already solved.

This desire for continuous improvement has been a core tenet at Badger Hill since the begin-

ning. Each improvement extends our vision, exposing us to new technologies and applications. When we stir in DIY and Internet of Things (IoT) applications with these technologies, interesting things start to happen.

Some may find it daunting to take risks and experiment with the new IoT and wireless automation technologies, but it is possible to start small and succeed. The sensors and transmitters gathering operational data are the starting point. These technologies are scalable, making it easy to start small and grow.

Rolling our own data historian

Badger Hill does not have a traditional supervisory automation system or a process data historian. Like many craft brewers, ours is largely a manual operation with basic programmable logic controllers driving motors, valves, and pumps—and only a modest amount of instrumentation. When we installed the first wireless pressure transmitter, our initial step was to figure out the best way to extract data and post it to the cloud for analysis and archiving.

This meant getting to know Modbus, an amazingly forward-thinking protocol given its age, which was not familiar to us. Two wires provide remote data access and automation for dozens of devices. It can also be extended transparently over TCP/IP. Our first tests did just that using an industrial wireless gateway that bundled all of the transmitters into a single virtual Modbus network.

As our first experiment, we installed a pressure transmitter on our cold-liquor tank (a brewing water storage tank) to measure the differential pressure (DP) level and post it to the cloud. Given the low cost of cloud storage, we started gathering data continuously.

The data is requested by a simple Modbus master hosted on a $20 Arduino-like chip called a Particle Photon. It reads the response and posts it to a cloud-based database using a RESTful interface over HTTP. For data analytics, we have pretty graphs on the Internet, and we can download the data for analysis. In the future, we would like to tap into the big data capabilities of companies like Google or Amazon. New companies, such as Initial State and Meshify, also exist with this type of application in mind.

We also have Modbus capabilities in our temperature controllers, brewhouse, keg filler, canning line, and centrifuge. We are slowly bringing more data sources into our analysis. Security is and should be a concern, but the cloud is no worse, and probably better, than what can generally be achieved in-house by companies like ours.

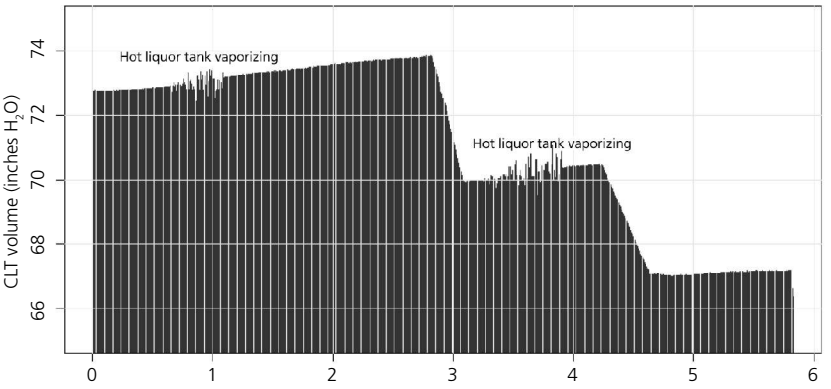


Figure 2. The scattering in the continuous level plot of the cold-liquor tank showed a steam flow problem in the hot-liquor tank. This was one of the first recognitions of the information available through inference from data collected by a Rosemount 3051 wireless pressure transmitter.

Inferring information from data

The interesting part is seeing what information can be inferred from all the data. What can you learn if you are willing to spend some time looking at the data? Inference provides information on behavior, which can relate to a person or a process, and generates four main benefits for Badger Hill:

- self-documents human activities by capturing indications of process steps
- creates information useful for training by illustrating current versus ideal practices
- provides secondary and tertiary information on top of primary functions, useful for risk management
- shows where efficiency can be improved through long-term analysis

What does this all mean in actual practice? How did we recognize the potential, and how have we realized these benefits?

More than just level

The first use of the pressure transmitter was as a DP level instrument on the cold-liquor tank, which is the initial stage for the fresh water to be used for a new batch. In the initial data (figure 2), there was normal data scatter, but in some areas, it was much more pronounced. While this might have been written off as an instrument malfunction, we realized that these areas coincided with feeding steam into the hot-liquor tank heat exchanger.

The cold- and hot-liquor tanks are next to each other and have interconnecting pipes. Heating water in the hot-liquor tank involves feeding steam through a heat exchanger immersed in the water. If too much steam is being fed into the heat exchanger, steam bubbles form in the water, which shake the tank and rattle the piping. This shows up on the pressure transmitter mounted on the cold-liquor tank. So, from this scatter we were able to infer that the steam regulation to the hot-liquor tank heat exchanger was set incorrectly.

This was an interesting realization, but it be-

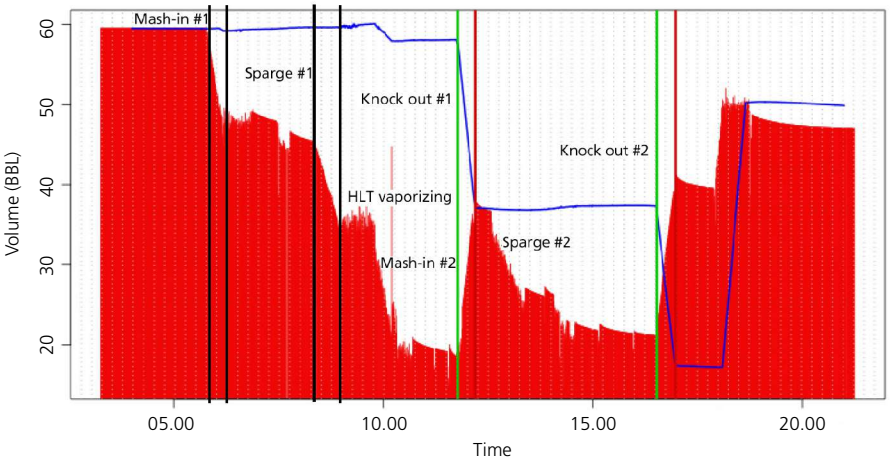


Figure 3. Watching the level indications from the hot- and cold-liquor tanks during a brewing process shows each step, documenting overall operation.

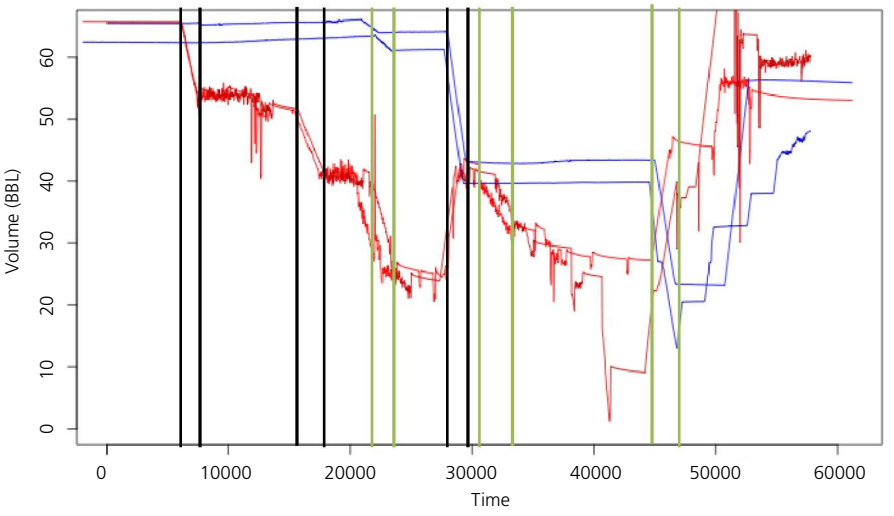


Figure 4. Multiple brewing batches can be compared, illustrating how consistently the recipe can be applied, and how individual brewers approach their craft.

came clear that much more was possible when looking at more complex operations (figure 3). The process of starting a new batch of beer in the hot-liquor tank follows a set series of steps outlined in the recipe. Usually we try to make two batches, one after the other, over 20 to 25 hours to use energy more efficiently. The hot- and cold-liquor tanks interact as water needs to be heated, and the first batch is cooled by transferring its heat to the second batch. The graph shows the levels on both tanks superimposed with the same time scale. It is easy to see the changes as liquid moves between the two tanks. By following the profile, it is possible to see each step in the process and identify changes. So how do we use this information?

These profiles document each step and put the process in a form suitable for comparing it to similar batches. This provides 90 percent of the information we were recording manually, and provides it in greater detail. When we lay profiles from multiple brewing days on top of each other (figure 4), we can see a high degree of consistency with these manual processes. This suggests we have a good recipe, and our brewers know what they are doing. It also shows us that the process does not need to be adjusted on the fly, which gives us a basis for plans to automate the process. This allows us to build our craft brewers' know-how into our automation.

We manage risk by watching the process in real time. If any values diverge from recognized norms, we know something is going wrong with the batch.

We can use this information for training as we look at the characteristics of the most effective batches and most effective brewers. Positive deviations from normal operations can be captured and analyzed, so we can duplicate improvements.

Making this kind of thing happen is not complex or expensive. It is the result of several technological approaches working together:

- continuously logging critical process variables, with perpetual data retention using the cloud
- data collection and reporting using small, cheap, replaceable devices with powerful capabilities
- strategically placed process instruments
- the ability to recognize when useful information can be inferred from all the data

The lesson for process engineers is that you should not be afraid of looking for valid inferences. These are not guesses if they are informed by the data. Data, by itself, does not help. Information comes from understanding the data and seeing what it is telling you. Insight comes from understanding the information and using it to improve what you are doing to gain competitive advantage. ■

ABOUT THE AUTHOR

Michael Koppelman (michael@badgerhillbrewing.com), former head brewer, is currently the CTO of Badger Hill Brewing in Shakopee, Minn. He is responsible for the technical aspects of brewing the company's craft beer, and for other aspects of the company's operation. Koppelman holds a BS in astrophysics from the University of Minnesota Twin Cities, and a BA in music from the Berklee College of Music in Boston.

RESOURCES

Brewers Association
www.brewersassociation.org/statistics/national-beer-sales-production-data

"Brewing Quality Beer while Increasing Production Efficiency"
www.emerson.com/en-us/industries/automation/food-beverage/beer

Empowering the digital workforce of the future

By Mike Train

Over the past 30 years, advances in automation have done fantastic things for the manufacturing sector in terms of reliability, safety, and operational efficiency. But today, despite all the hype about the promise of the Internet of Things, the industry has reached a point where those gains are leveling off. Manufacturers cannot simply "efficiency their way" to top-quartile performance any longer.

In this environment, managers have the relentless pressure to do more with less. Do they cut back on staff and ask more of the workers they keep? Will the sensational headlines claiming that automation kills jobs come true? These reports routinely miss the big picture. History has taught that while technology can unsettle the current nature of work, disruption consistently brings new opportunities for value and net employment growth, not loss.

New era of productivity

Capitalizing on these opportunities means not only investing in technology, but also fundamentally transforming the way you do business. But while it is clear manufacturers understand the need to evolve, many struggle to find a predictable path forward.

To take the next step to game-changing performance, manufacturers should focus on implementing technologies that empower the assets that will be the biggest driver of success in the future: their people. By analyzing the organizational behaviors of top-quartile industry performers, we have identified five essential competencies that are critical to helping workers achieve this digital transformation: automated workflow, decision support, workforce upskilling, mobility, and change management.

Automated workflow: One of the best ways to create bottom-line impact is to eliminate repetitive tasks and allow employees to focus on the exceptions to normal operations. They can solve problems and identify opportunities for value creation. For example, electronic logbook applications that automatically capture detailed records of user activity and track tasks during work shifts let operators access a historical knowledge base, which can help them plan work priorities and facilitate collaboration.

Decision support: Enabling workers to be more productive means arming them with actionable information for faster, better decision making. This might mean using predictive intelligence to troubleshoot the root cause of an impending pump failure. With better insight into asset health, maintenance crews can schedule repairs when it makes the most economic sense.

Workforce upskilling: Obviously, you cannot expect an employee who is used to doing manual tasks to be proficient in advanced analytics and critical problem solving right away. The good news is that there are innovative training formats today that can greatly accelerate workforce development. With both high-fidelity training environments that immerse students in real-world scenarios and on-demand expertise, it is possible for operators to gain years of experience in just months. They can immediately put the concepts they learn to work on the plant floor.

Mobility: To tap the full power of all these new tools and technologies, it is essential to put them in the hands of employees wherever and whenever they need them, securely, of course. This idea is key to enabling collaborative workflows. If control room operators need to ask a process engineer how to solve a problem or make a step change to improve performance, they can do so from halfway around the world with secure mobile applications. These applications provide process data and analysis to both parties in real time.

Change management: A recent survey conducted by Emerson and *IndustryWeek* found that 47 percent of respondents saw change management as the biggest challenge to their operational efficiency programs. An automation supplier that can bring together the right strategies, tools, and expertise will help manufacturers address this problem by simplifying the institutionalization of operational best practices. Consulting will play a central role in this process, especially as knowledge and experience becomes easier to share with customers remotely.

Bright future

Automation innovations are bringing unprecedented opportunities to evolve performance in each of these areas of transformation. Companies and employees who embrace the rapidly changing digital landscape will achieve the greatest success. Everyone has skin in the game. Employers need to offer education and upskilling opportunities, and employees need the confidence and commitment to learn new skills and embrace change. By adopting these methodologies and putting power in the hands of workers to use technology investments today, manufacturers can put themselves on the path to achieving top-quartile performance in any market. ■

ABOUT THE AUTHOR

Mike Train (Mike.Train@emerson.com) is executive president of Emerson Automation Solutions. He leads strategies and innovations to help customers enhance operations and achieve top-quartile performance. Train was also president of global sales for Emerson Process Management, overseeing five world area regional organizations.

Automatic pressure calibrator

Pressure instrument calibration requires accuracy and repeatability. The 729 automatic pressure calibrator automatically generates precise test pressures, compensates for leaks, and automatically documents the pressure calibration process to help meet compliance and regulatory requirements.

With the portable 729, technicians input a target pressure, and the calibrator automatically pumps to the desired set point while the internal fine adjustment control stabilizes the pressure at the requested value. The device has automatic pressure generation and control for multiple tests to 300 psi (20 bar, 2 MPa). Calibration documentation is done using defined templates for transmitters and switches. Input the starting and ending test pressures and number of test points, and the calibrator documents the applied pressure, measured mA, and percentage error for each test point. The bright graphical display flags test results that are out of tolerance in red.

Fluke, www.fluke.com

Pressure and vacuum gauges

The adjustable red/green zone dial face on the pressure and vacuum gauges cues when a system is out of green-zone operation. Dial-face adjustability allows companies to apply a unified visual warning system across a range of processes for quicker recognition of issues. Red indicator bands on the high and low end of the green zone delineate the upper and lower boundaries of safe operation for each pressure or vacuum system where the gauge is applied. The red band, covering the entire out-of-specification zone on the dial face, makes deviations from acceptable conditions visible. This type of monitoring/warning system is suitable for all personnel, including those new to the plant.

Festo, www.festo.com

Digital pressure sensors

EPS-series sensors are available with measuring ranges from vacuum up to 5,800 psig. Selectable engineering units, such as bar, mbar, kPa, MPa, inches of water column, and inches of mercury, can be shown on the digital display. The series withstands extreme shock and vibration and incorporates a combination of overpressure, burst pressure, and stability for each measuring range.

Encased in a stainless-steel housing, the EPS-series sensors have an IP67 ingress protection rating, and achieve their atmospheric pressure reference at the four-pin M12 electrical connection. The standard ¼" NPT male process connection allows direct installation without requiring extra fittings. With no moving parts, such as pistons or springs, that can stick or break, two solid-state switch outputs are an alternative to mechanical pressure switches. On certain models, the second output can be configured as a scalable analog signal, turning the unit into a combination pressure switch and transmitter. The built-in two-color digital display indicates the measured pressure and switch set points.

AutomationDirect, www.automationdirect.com

Low-power output

The company added a 1–5 VDC low power output option to the PMP71 pressure transmitter that draws only 17 milliwatts of power at 9 V. This draw makes the PMP71 suited for battery- and solar-powered applications, such as remote oil and gas wellheads, offshore platforms, or pumping stations where low power consumption is critical.

The PMP71 measures absolute and gauge pressure of gas, steam, or liquid and has built-in algorithms to calculate level, volume, and mass of liquids. Measuring spans are available in ranges from –6 psi to +6 psi up to –15 psi to 10,500 psi. For safe operation at process temperatures up to 752°F, it has a piezoresistive measuring cell and a metallic welded process isolating diaphragm. The PMP71 has ATEX, FM, CSA, NEPSI, and IECEx approvals and is suitable for use in up to SIL 3 hazardous applications. The voltage output version is available with the CSA C/US XP approval in North America.

Endress+Hauser, www.endress.com/en

Setting the Standard for Automation™

Need money for college?

Students can't win academic scholarships if they don't apply. ISA Educational Foundation Scholarships are awarded to college or university students who demonstrate outstanding potential in the fields of automation and control. ISA scholarships cover tuition and related expenses as well as research activities and initiatives.

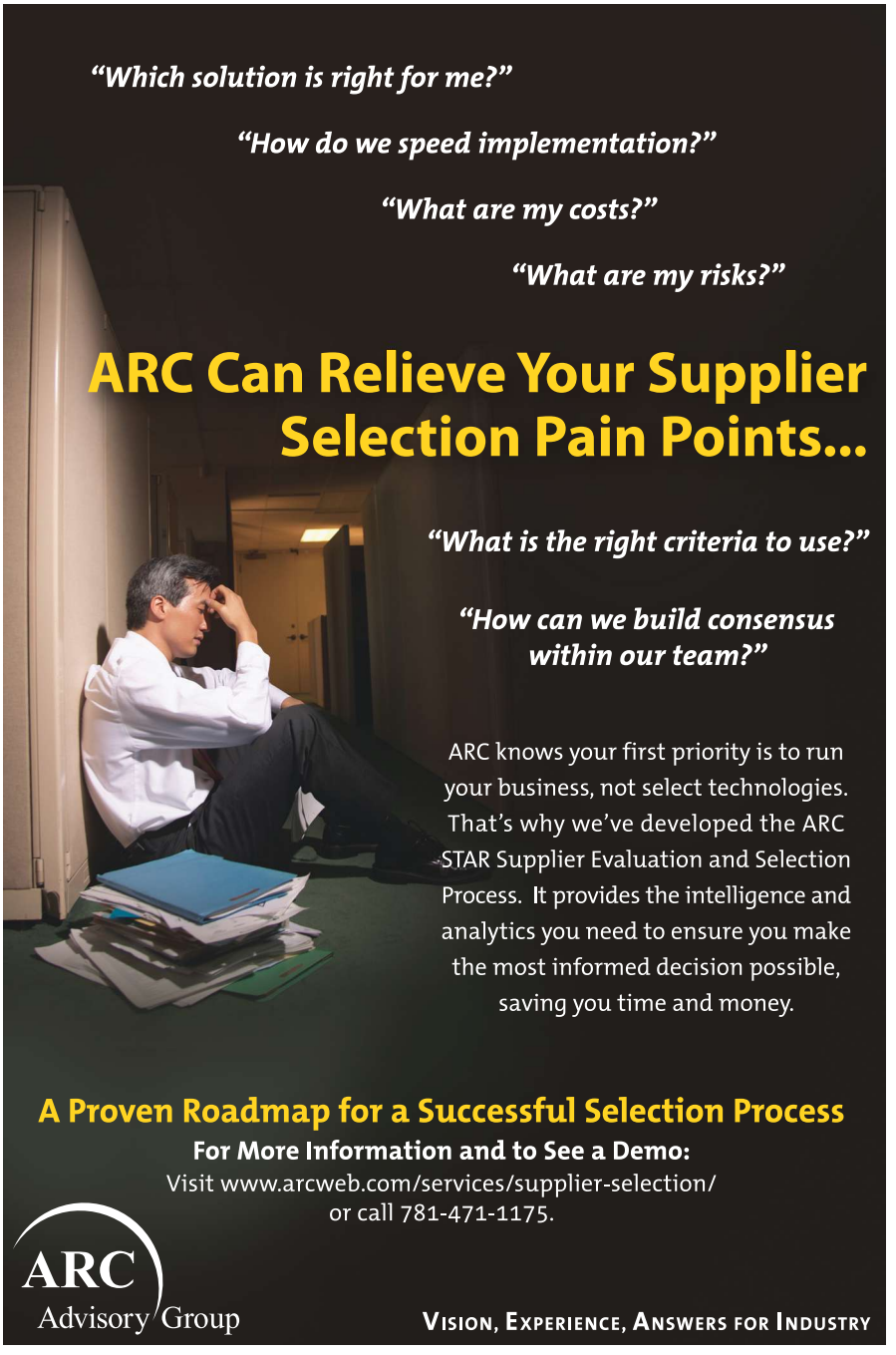
To guarantee consideration, students are encouraged to complete and submit an application as soon as possible. The deadline for application submission is 15 March 2018.

For more details, including answers to frequently asked questions, visit **www.isa.org/scholarships**, or call ISA at +1 919-549-8411.

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

ISA™

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



Contact *InTech* today:

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

Laura Martinez
Advertising Sales Representative
Phone: +1 702-810-3922
Email: lmartinez@automation.com

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

Kelly Winberg
Advertising, Classifieds Section
Phone: +1 267-718-8197
Email: kwinberg@comcast.net

Chesley Grove
Advertising Materials Coordinator
Phone: +1 919-990-9267
Email: cgrove@isa.org

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

datafile

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

COM-TABLET: COMPLETE HART COMMUNICATOR!

The COM-TABLET is a complete HART Communicator for the Tablet PC. It includes the Tablet PC loaded with the DevCom2000 Smart Device Communicator Software, the HM-BT-BAT-ER Bluetooth HART Modem, complete DD library, and a hard plastic carrying case.

All components installed, setup, and ready to go!

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

Maintenance Management Software/ CMMS

FastMaint CMMS
Your FAST TRACK to maintenance management™
For Utilities, Manufacturing Plants, Industrial & Commercial Facilities
Fast to setup. Easy to use. From US$ 995
Download 30-Day Trial/ Web Demo
www.smglobal.com (919) 647-9440
SMGlobal Inc, 5448 Apex Peakway #308
Apex, NC 27502 USA

Plus Maintenance Books, Tips & Training

NATIONAL Engineering RESOURCES INC

Serving the Controls and Process Automation Industry for over 25 years

Bringing Candidates and Great Companies together!

Go to www.nerinc.com to view available Career Opportunities

Contact: Evy Trost
Linkedin.com/in/evytrost

800-665-7610 ext. 110
Controls@nerinc.com
www.NERINC.com

Sample of Jobs Available at Jobs.isa.org

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

Instrumentation and control systems technician

City of Ann Arbor: The technician will inspect, install, upgrade, maintain and repair electrical and electronic equipment and systems for water treatment and wastewater treatment facilities and associated collection and distribution equipment, systems, and components. The successful candidate will have a high school diploma or equivalent and a journeyman electrician or federal license . . . see more at Jobs.isa.org.

Senior manufacturing engineering

Arthrex Manufacturing: The engineer, based in Ave Maria, Fla., will design, develop, and implement automated device assembly, packaging, and labeling processes to produce cost-effective quality medical device products and systems. He or she will provide manufacturing engineering expertise to create, document, and implement required procedures and documents. A bachelor's degree, preferably in industrial, manufacturing, or mechanical engineering, is required. The successful candidate will also have seven or more years of manufacturing process improvement experience and preferably medical device manufacturing or FDA-regulated environment experience . . . see more at Jobs.isa.org.

Director, cell therapy process development

Casebia Therapeutics: The company seeks a process development leader to deliver life-changing therapeutics to patients. He or she will lead the development of manufacturing processes for cellular therapies based on the company's gene-editing technology. The ideal candidate for this Cambridge, Mass., position will have strong hands-on technical experience with cell-based biologics and associated technologies in a GMP-compliant system. An MS or PhD in a relevant scientific discipline and ten or more years of relevant experience is required . . . see more at Jobs.isa.org.

Product applications engineer

NEXTracker: The engineer will be based in Fremont, Calif., and will manage product applications through the sales process. The engineer will be responsible for both configuring existing tracker products to meet customer needs and identifying requirements for new products. A BS in mechanical engineering, two-to-four years of mechanical or structural engineering experience in solar trackers, PV panels, or other ground-mounted solar tracking systems, and strong presentation skills are required . . . see more at Jobs.isa.org.

Cybersecurity compliance engineer

Johnson Controls: The successful candidate will be the compliance subject-matter expert, coaching product management and development organizations in technical cybersecurity requirements. A bachelor's degree in compliance, regulatory affairs, engineering, IT, or other technology-related discipline is required . . . see more at Jobs.isa.org.

ISA volunteer leader lessons learned

By Jim Keaveney

ABOUT THE AUTHOR

Jim Keaveney (jim.keaveney@emerson.com) was ISA president in 2016. He has been an active ISA member for more than 30 years and has served in numerous leadership positions, including society treasurer, finance committee chair, and District 2 vice president. Keaveney is the northeast regional manager for Emerson Automation Solutions.

I would like to share the top two lessons I learned as an ISA leader and the top two reasons to become a volunteer leader.

Lesson 1: Volunteer leadership or a committee role is like work with one key difference—no one directly reports to you! Indirect influence and team building are the keys traits required to be an effective leader or committee member. Volunteers are not paid to behave in a certain way, but an effective team sets expectations and engagement guidelines. Failure to learn this lesson will earn an "F" for frustration. It is important to find the right fit for volunteers with different competencies and diverse perspectives to build a team culture of inclusion. At the board level, the composition should best reflect the type of society that we strive to become. Patrick Lencioni's book, *The Five Dysfunctions of a Team*, should be required reading for any association volunteer.

Make no mistake about it, ISA welcomes and needs more new volunteers.

Lesson 2: It is all about trust; the foundation of any good team is exploring change and new approaches to old problems. Involving all in healthy discussions leads to higher quality results. With trust, team members are not afraid to be vulnerable and are willing to express their views and collaborate to resolve differences. Trust empowers us to help other volunteers become better team players and embrace change in the form of continuous improvement. A trust culture is the cornerstone of any organization, including ISA. I still cringe when I hear, "If it is not broken, why fix it?" President John Kennedy wisely noted that the best time to repair a roof is when it is not raining. It is rare that we have those light bulb "aha" moments, and we really need to drive improvement incrementally.

Trusting the various committees and task forces to do their jobs builds a strong organization. Board members or committee chairs need to stay focused on overall strategy and avoid micromanaging.

Volunteer leaders also need to trust and respect staff partners who hold the "institutional memory" of the organization. As volunteer leaders, we must hold ourselves—and each other—accountable to ensure that the volunteer-staff relationship is cohesive and collaborative. Drucker nailed it when he observed that culture eats strategy for breakfast. As volunteer leaders, we all need to contribute to a culture of trust, collaboration, and continuous improvement. *The Change Cycle* by Ann Salerno and Lille Brock is an excellent read on surviving and thriving during organizational change. The bottom line is that building and leading effective teams is always hard work.

My top two reasons for deciding to step up to a volunteer leadership role are:

Reason 1: Understanding and mastering the techniques to be an effective volunteer leader or committee member enhances skills you need to be successful on the job. The time commitment pays dividends in terms of developing a wider professional network for technical issues and professional guidance. Be sure that your company really understands these advantages, so it buys into supporting your time investment and commitments. Make no mistake about it, ISA welcomes and needs more new volunteers. There are many ways for you to contribute, including technical standards development, governance, and image and membership, to call out a few.

Reason 2: Contributing is what it is all about! We as automation professionals make the world a better place. As your professional organization, ISA helps make our world safer (cybersecurity, alarm management, safety instrumented systems) while increasing productivity (workforce development, standards best practices). Be proud of this fact, and make sure that your management, friends, and families all know that you are making a difference.

If I had to choose just two words to wrap things up, one would be *gratitude* for the opportunity to learn from so many in my volunteer leader role. The other would echo the call from Jean Luc Picard, the fictional Star Fleet officer from the Star Trek franchise, and challenge each of you to *engage!* ■

Setting the Standard for Automation™

2018 ISA Division Symposia

ISA's unbiased technical conference programming provides access to worldwide experts and content on the latest technologies, trends, real-world challenges, and industry updates needed to remain competitive in today's marketplace.

Mark your calendars and make plans to attend an ISA technical conference program in 2018!

Leak Detection and Repair/Fugitive Emissions Symposium (LDAR)
Training: 5 & 8 March • Conference: 6–7 March
Galveston, TX, USA

Analysis Division Symposium (AD)
Training: 22 & 26 April • Conference: 23–25 April
Galveston, TX, USA

Power Industry Division Symposium (POWID)
Training: 25 June • Conference: 26–28 June
Knoxville, TN, USA

Water/Wastewater and Automatic Controls Symposium (WWAC)
Training: 6–7 August • Conference: 8–9 August
Bethesda, MD, USA

Food and Pharmaceutical Industries Division Symposium (FPID)
Training: 15 October • Conference: 16–17 October
Montreal, Québec, CA

International Instrumentation Symposium (IIS)
Training: 15 October • Conference: 16–17 October
Montreal, Québec, CA

Process Control & Safety Symposium and Exhibition (PCS)
Training: 5 November • Conference: 6–8 November
Houston, TX, USA

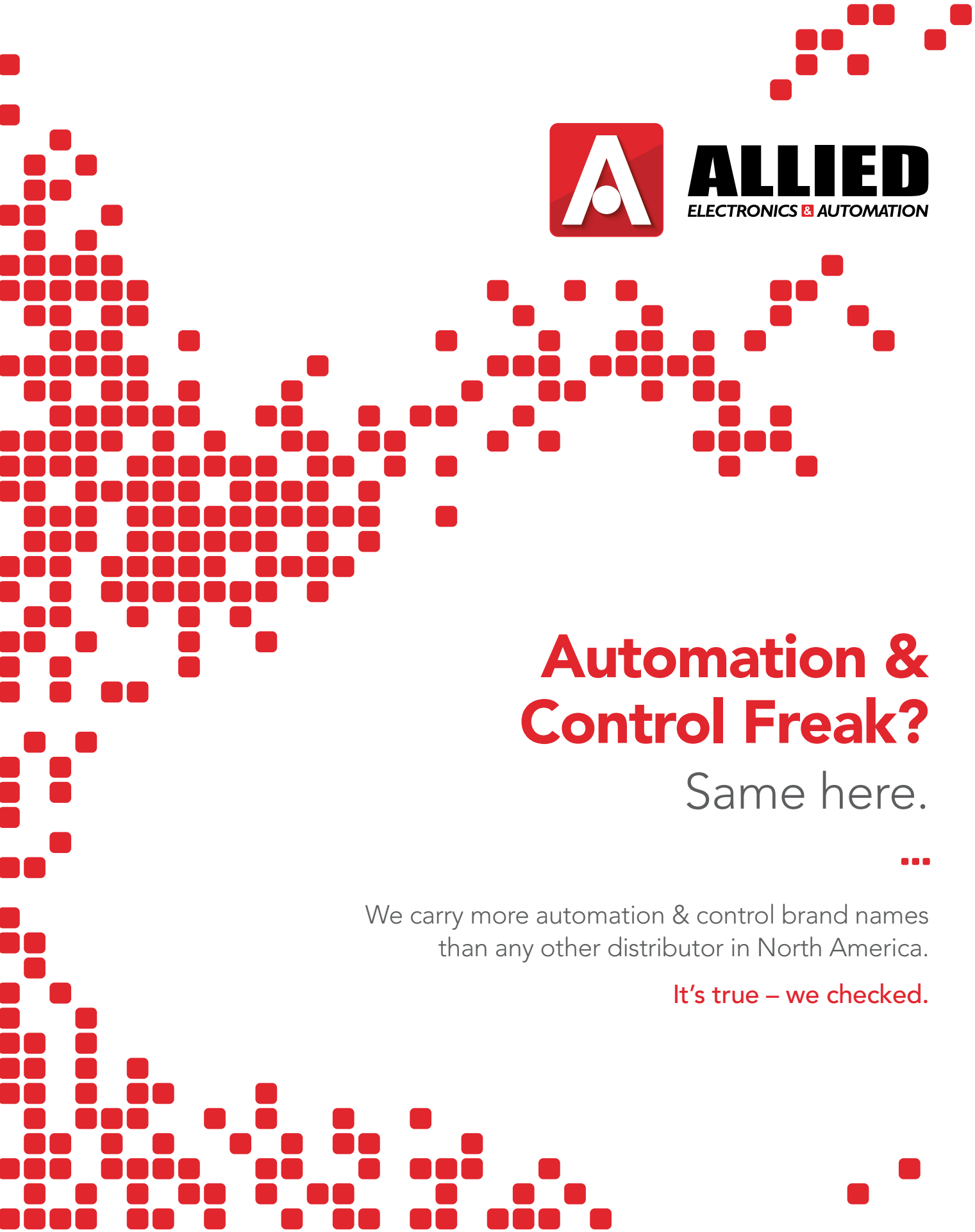
Great locations!

Awesome content!

Find developing program details at:
www.isa.org/events

ISA™

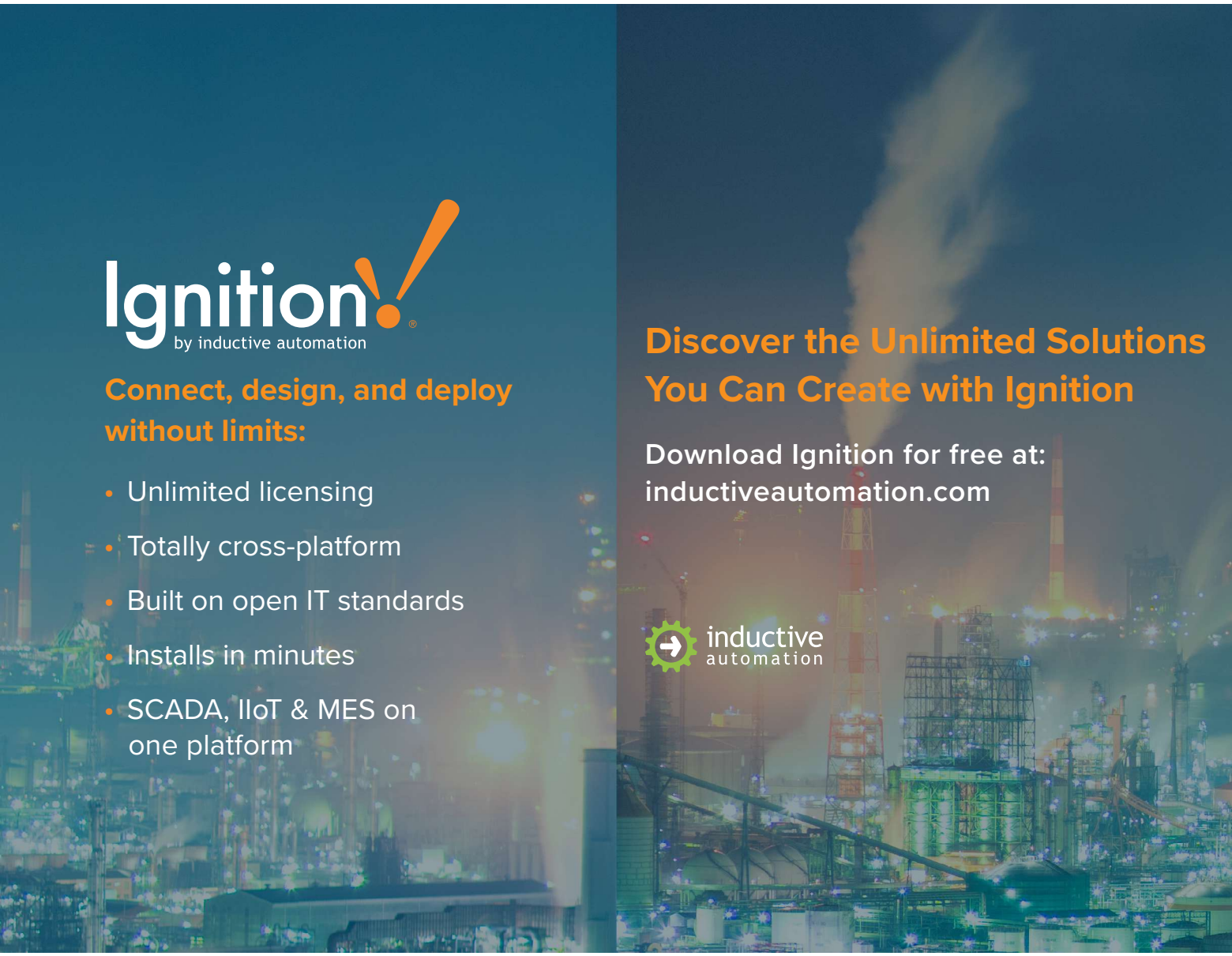
EP50-8145-0917



© Allied Electronics & Automation, 2018

Get your A&C fill at alliedelec.com 1.800.433.5700


Ignition!
by inductive automation
The Unlimited Platform for SCADA
and So Much More
See the possibilities at inductiveautomation.com/ignition


Ignition!
by inductive automation
Connect, design, and deploy without limits:
• Unlimited licensing
• Totally cross-platform
• Built on open IT standards
• Installs in minutes
• SCADA, IIoT & MES on one platform
Discover the Unlimited Solutions You Can Create with Ignition
Download Ignition for free at:
inductiveautomation.com
inductive automation