March/April 2018

InTech

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

Alarm management

Robotics

Wireless sensor

EdgeX Foundry

Controllers spotlight

Combining IoT, Industry 4.0, & energy management suggests exciting future

Reduce costs and improve performance with intelligent design and common sense

Setting the Standard for Automation™

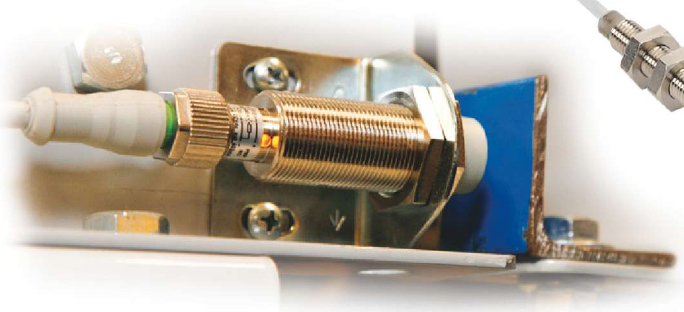
www.isa.org/intech

Proximity Sensors for Less

Over 700 models to choose from…

Proximity Sensors

We've got the high-quality, industrial proximity sensors you need at the low cost you're looking for. Our vast selection of inductive, magnetic, capacitive and ultrasonic sensors is constantly growing and includes many sensing options and ranges, sizes, body styles, etc. All at prices you won't find anywhere else.



NEW!

Inductive Proximity Sensors

Starting at $13.50 (AES-AN-1A)

- Industrial and harsh duty applications
  - Food and beverage (IP69K) variants
  - Stainless steel variants
- Standard, extended and triple sensing distances
- Tremendous variety of sizes:
  - 3mm, 4mm and 5mm round
  - 6.5mm round
  - 8mm round
    ***NEW!** AC Powered Models*
  - 12mm round
    ***NEW!** AC Powered Models*
  - 18mm round
    ***NEW!** AC Powered Models*
  - 30mm round
    ***NEW!** AC Powered Models*
  - Rectangular
- Ratings from IP65 up to IP69K
- Quick-disconnect or axial cables
- cULus & CE approvals
- Lifetime warranty

Ultrasonic Proximity Sensors

Starting at $89.00 (UK6A-DN-0E)

- Industrial automation models
- Sensing distances from 300mm to 600mm
- Discrete and analog output models
- Wide variety of sizes:
  - 18mm round
  - 30mm round
  - Rectangular
  - Flowline® liquid level sensors
- IP67 protection rating
- Quick-disconnect or axial cables
- cULus & CE approvals
- Lifetime warranty on most models

Magnetic Proximity Sensors

Starting at $40.00 (MDR-AP-1F)

- Industrial and harsh duty models
- Wide variety of sizes:
  - 8mm round
  - 12mm round
  - 18mm round
  - Rectangular
- IP65/IP67 or IP68/IP69K rated
- Quick-disconnect or axial cables
- cULus & CE approvals
- Lifetime warranty
- Damping magnets also available

Capacitive Proximity Sensors

Starting at $59.00 (CR1-00-2A)

- Industrial automation models
- Wide variety of sizes:
  - 12mm round
  - 18mm round
  - 30mm round
  - Rectangular
- IP65 or IP65/IP67 protection rating
- AC powered models (30mm)
- Quick-disconnect or axial cables
- cULus & CE approvals
- Lifetime warranty

Research, price, buy at: www.go2adc.com/sensors

VOTED Best in SERVICE 15 YEARS

Order Today, Ships Today!

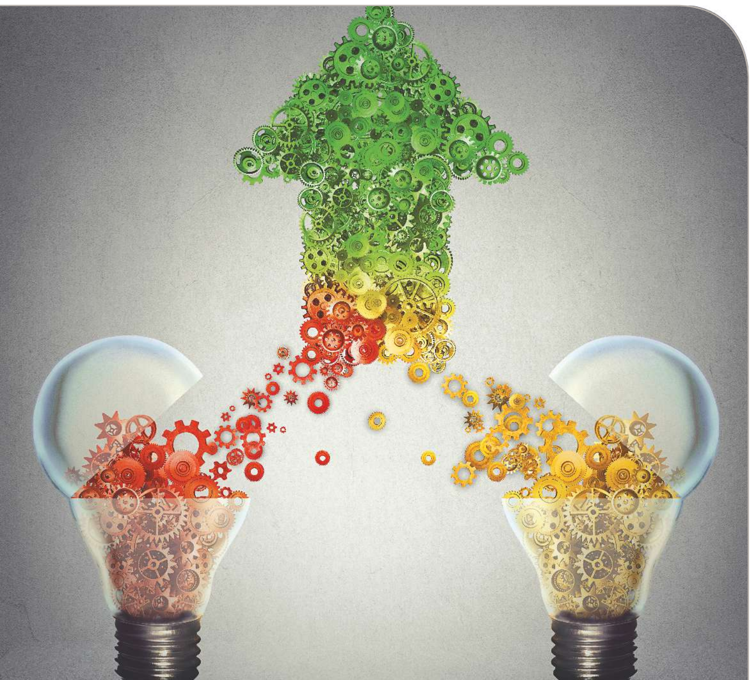
AUTOMATIONDIRECT.com

1-800-633-0405

the #1 value in automation


SIEMENS
Ingenuity for life
Making the most of air
Industrial Wireless LAN – SCALANCE W
With increasing digitalization, industrial communication networks are becoming more and more important. Particularly with wireless data transmission, demands on network components are high. Our comprehensive IWLAN portfolio offers the right solution for every application – whether in harsh industrial or moderate environments. When it comes to your wireless applications, choose performance and reliability with SCALANCE W from Siemens.
Expertise in industrial networks.
Hannover Messe
April 23–27, 2018
Hall 9
siemens.com/hm18
siemens.com/iwlan
PDPA-A10249-00-7600

InTech



DEPARTMENTS

COLUMNS

RESOURCES

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**

ISSN 0192-303X

***InTech* is published bimonthly by the International Society of Automation (ISA).**
Vol 65, Issue 2.

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 · exida

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, Industry 4.0, finding value?

By Bill Lydon, *InTech*, Chief Editor

I have already attended four industry conferences in 2018, including one in Germany, and the intensity of application of Internet of Things (IoT), Industry 4.0, and related technological innovations to improve manufacturing continues to grow. Common themes presented refer to industry studies that indicate:

- applying these technologies will significantly improve productivity and quality
- manufacturing executives believe new technologies need to be implemented to remain world-class competitors
- manufacturing executives believe they have done little to apply these technologies

Users I have talked with who have successfully applied new technologies first learn and understand the new technologies and then rethink manufacturing operations.

As I talk to industrial automation users, these themes sound reasonable. Many have told me their management groups have been asking them what the company should be doing relative to IoT and Industry 4.0—a great opportunity for automation professionals. This has empowered automation people to learn about these technologies and, in some cases, launch small pilot projects.

Vendors with new technologies to offer are certainly trying to create a sense of urgency among potential buyers to sell their products. An interesting phenomenon has been vendors asserting that they have been doing IoT for years with their existing products. Functionally this may be valid, but the implementations have been expensive, inflexible, difficult to use, and closed architectures. New IoT technologies, in contrast, are significantly less expensive and are flexible, easy to use, and open architectures.

Finding value

Users I have talked with who have successfully applied new technologies first learn and understand the new technologies and then rethink manufacturing operations. The analysis reviews how new technology could be used to improve production/process flow and improve lean manufacturing methods. This leads to new ideas and applications that improve productivity, uptime, quality, other success factors.

Automation professionals

In this new environment many higher-level management teams are getting the message that the application of technology and change are required to be successful in the future. This creates great opportunities for automation professionals to show how they can add value in the organization. Automation professionals applying good system analysis to understand their manufacturing and process are in the best position to propose applications leveraging new technologies.

Creating proposals for small pilot projects to determine the value of new technology and concepts is a good way to accomplish this. Key points in a pilot project proposal:

- problem to be addressed or improvement desired
- goal(s) of the pilot project
- technology to pilot
- questions to be answered by the execution of the pilot project
- pilot project description
- resources needed
- cost/benefits analysis
- projection of benefits if successful and broadly deployed

In addition to their day-to-day functions, helping the organization move forward and improve is an important way automation professionals contribute value. ■

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

AVEVA combines with Schneider Electric

AVEVA combined with Schneider Electric's industrial software business, bringing together AVEVA's design, engineering, and construction capabilities with Schneider Electric's industrial software business, which ranges from simulation to real-time manufacturing operations management. It creates a provider of engineering and industrial software, expanding the markets and industries the company serves.

AVEVA has more than 4,400 people across 80 locations in over 40 countries, and its global headquarters is in Cambridge, U.K. Industries served include chemical; food and beverage; infrastructure and smart cities; life sciences; mining, minerals and metals; oil and gas (upstream, midstream, and downstream); power and utilities; shipbuilding; and water and wastewater. ■

Process automation system multivendor interoperability

The OPC Foundation and FieldComm Group formed an alliance in late 2017 to advance process automation system multivendor interoperability and simplified integration by developing a standardized process automation device information model. A joint working group will develop a protocol-independent companion specification for process automation devices. The group will use FieldComm Group's experience with the HART and FOUNDATION Fieldbus communication protocols to standardize data, information, and methods for all process automation devices through FDI using OPC UA. The OPC UA base information model and companion Device Information (DI) specification will be extended to include the generic definition and information associated with process automation devices.

A joint working group will develop a protocol-independent companion specification for process automation devices.

The OPC Foundation and FieldComm Group have worked together for more than a decade, initially working on the development of the Electronic Device Description Language (EDDL) specification and most recently on the creation of FDI technology.

The joint working group plans to release an extensible process automation information model specification during the first quarter of 2019. The working group is open to all members of both organizations, as well as collaboration partners of the organizations. ■

Slight growth for U.S. valve industry

The U.S. industrial valve industry will grow by 1.45 percent in valve shipments in 2018, bringing the value of those shipments up to $4.615 billion for the year, according to the Valve Manufacturers Association's *2018 Market Forecast of Industrial Valve Shipments.* That rate of growth is slightly behind 2017's rate of 1.89 percent, which translated to shipments worth $4.549 billion.

While overall industry growth is not huge from 2017 to 2018, "it translates to $66 million more in valve shipments for the year, which is a positive sign for the industry," said VMA president William Sandler. Looking back at shipments over the past decade, the industry has gained $615 million in valve shipments, he pointed out.

The industry also has been growing since 2009, when a tumble in the petroleum and power industries meant the year saw almost no growth. "However, last year and this year, we are continuing the slow steady climb upward that has been part of our industry for the last 10 years," Sandler said.

The largest growth for 2018 will come from the petroleum production industry, which will increase by more than $42 million and gain almost a percentage point share in the market.

The largest growth for 2018 will come from the petroleum production industry, which will increase by more than $42 million and gain almost a percentage point share in the market. It now holds 11.4 percent of the market compared to last year's 10.5 percent.

Remaining in top place of valve end-user industries is the chemical industry, which holds 18.3 percent of the market, a share that did not change significantly this year. The second largest market share belongs to water/wastewater, which holds 17.7 percent of the market, slipping by half a percentage point in 2017, or about $2.3 million less for the year.

Other energy markets continue to rank among the top users, including power generation at 11.8 percent and petroleum refining at 11.7 percent. Slight gains have occurred in commercial construction and in oil and gas transmission. Those industries each hold about 6 percent of the market. Slight losses have occurred in pulp and paper and in iron and steel.

As far as the type of valves, automatic valves are the most-often used valve being shipped today. "Automatic valves are outpacing conventional manually operated versions, as end users seek to remove variability and human error from the process," said Mark Nahorski, president of PBM Inc. and chairman of VMA. "Automation and controls continue to play a major role in the valve industry—the segment represents 31 percent of VMA industrial valve shipments for 2018 compared to 18 percent for ball valves." ■

Combining IoT, Industry 4.0, and energy management suggests exciting future

By Brian Dwyer, C.Eng MIEI,
and Joao Bassa, MSc

Reduce costs and improve performance with intelligent design and common sense

The Internet of Things, Industry 4.0, and energy management can be combined to make a heady cocktail that suggests an exciting future with reduced costs and improved performance. However, as is the case with any cocktail, you could be left with a severe hangover, wondering where all the promise and money went.

Disruptive technologies are emerging at an unprecedented rate. It is difficult to know which technologies offer genuine savings versus those that may be rendered obsolete before they achieve their potential. It is challenging for organizations to cut through the hype and identify those technologies that are applicable to their needs and can deliver an immediate positive return on investment.

This article examines the Internet of Things (IoT) and Industry 4.0 from the perspective of realizing energy cost and consumption savings. What options, if any, are cost effective now? How can an organization introduce the IoT and move toward Industry 4.0 without compromising its financial performance?

Say what you mean so you can mean what you say . . .

As with any newly arrived and rapidly evolving arena, terminology can become fashionable and be erroneously applied to all sorts of situations. Buzzwords can become the tool of marketers and sales people. So, it is worth taking a moment to define what exactly what we mean by the Internet of Things and Industry 4.0.

The Internet of Things

The term is becoming ubiquitous, but there are many different definitions. The research consultancy Gartner defines the IoT as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." The International Telecommunication Union describes the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting physical or virtual things."

These definitions indicate how broadly the IoT can be conceived. Any device that can collect and transmit data, as well as all of the associated communications infrastructure, could be considered part of the IoT. The potential future deployment of devices is mindboggling—50 billion devices to be connected by 2020 with an estimated 200 devices per person being possible. One way to try to grasp the scale of the Internet of Things (IoT) is to visit the website Thingful (www.thingful.net), a search engine for the IoT.

The IoT has already established that an enormous amount of data can be generated. However, it has been estimated that only 3 percent of the generated data is analyzed, and only 15 percent is tagged and ready for analysis without manipulation. The challenge facing many service providers and potential end users is how best to use that data for decision making that realizes efficiencies and a return on investment on data collection infrastructure.

FAST FORWARD

- The Internet of Things has the potential to save costs and energy.
- Organizations must make sure that proposed solutions are mature enough to realize promised savings.
- There is significant hype surrounding digital performance management, remote monitoring and control, and smart energy consumption, but their financial efficacy has not yet been consistently demonstrated.

Industry 4.0

Originally coined in Germany, Industry 4.0 is a broad term that can be applied to several trends in manufacturing and automation. In the U.S., terms such as the Industrial Internet (of Things), advanced manufacturing, or digital manufacturing are used. The German Federal Ministry of Education and Research defines Industry 4.0 as "the flexibility that exists in value-creating networks is increased by the application of cyber-physical production systems [CPPS]. This enables machines and plants to adapt their behavior to changing orders and operating conditions through self-optimization and reconfiguration. . . Intelligent production systems and processes, as well as suitable engineering methods and tools, will be a key factor to successfully implement distributed and interconnected production facilities in future smart factories."

Although there is enough jargon in the above paragraph to be teased out over several articles, the central premise is that the IoT allows industrial processes to communicate with the outside world to manage themselves in response to changes in key production drivers, such as customer specifications or energy prices. The IoT is the central technology as the data generated by existing control systems is collated with other data to optimize the industrial process. That said, Industry 4.0 is broader than the IoT, encompassing technologies such as "big data" analytics, machine learning, and additive manufacturing (3-D printing).

Industry 4.0 can also mean very different things to different industries. According to a survey in Germany in 2015, only 10 percent of manufacturing companies have extensively adopted Industry 4.0 techniques, with more than half either not planning to implement any techniques or not giving it any consideration at all. In addition, Industry

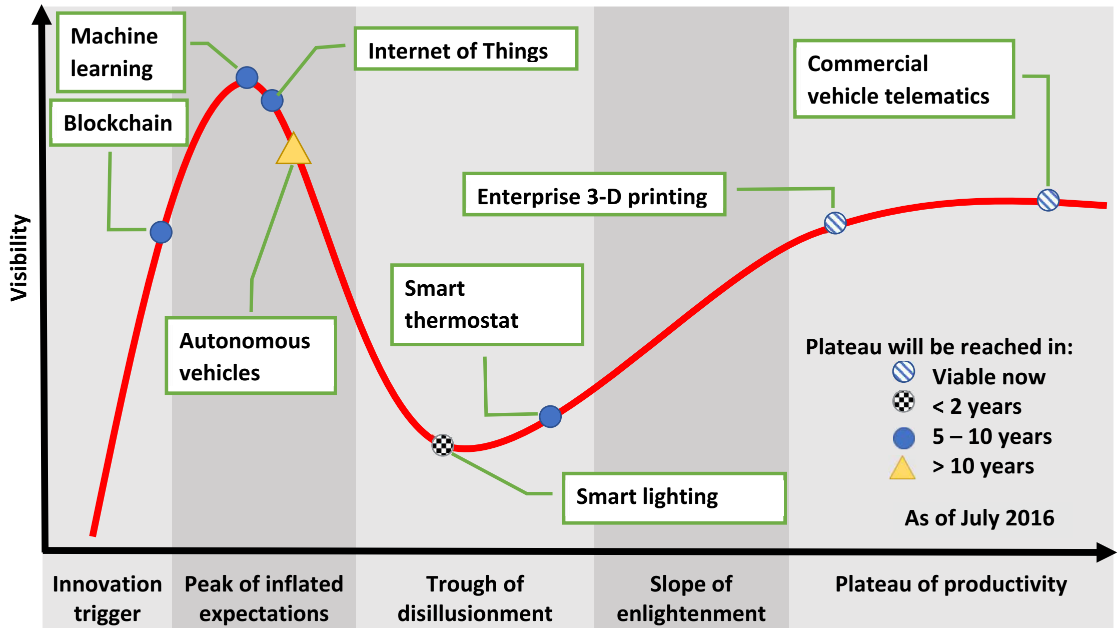


Figure 1. Hype cycle of selected Internet of Things technologies (adapted from Gartner)

4.0 may be much more important for manufacturing discrete items compared with processing bulk materials. Manufacturing can benefit from the customization of end products to individual customer needs in ways the process industry never will.

Growing pains

All these promises of efficiency and new ways of manufacturing are very exciting. But how do you tell if a technology is mature enough to deliver its promises? One method used by the consulting and market research firm Gartner is the "hype cycle" (figure 1.) Gartner uses the hype cycle to support investment decision making. The figure illustrates technologies discussed later in this article and additional "high visibility" technologies to show how the hype cycle works.

The central premise of the hype cycle is that visibility does not equate to efficacy. "Fear of missing out" can be an effective marketing tool, but it does not lend itself to reliable investment decisions. Quite often the costs of understanding how a technology is best applied and waiting for its sufficient adoption can significantly outweigh any "first mover" advantages.

Figure 1 suggests that the IoT is in its early stages and that some critical supporting technologies, such as machine learning, need further development for it to reach its potential. Savings can be achieved from the IoT now; however, organizations need to ensure that any technology chosen has a clearly defined pathway to savings. Too many interdependent technologies are likely to disappoint.

Elements of Industry 4.0, such as enterprise-level 3-D printing, have matured enough to realize some of the envisaged benefits. However, Industry 4.0 relies heavily on the integration of systems, many of which are still relatively new. As with the IoT, effective implementation should rely on clearly identified savings. Further benefits may occur, but organizations should not rely on them to develop business cases.

Beyond performance issues

Both IoT and Industry 4.0 are not without their downsides. Concerns about the security of the devices and their potential to be hijacked persist. For example, a cyberattack in October 2016, which focused on the U.S. East Coast, was blamed on IoT devices not being equipped to prevent themselves from being hijacked. Such issues are a significant barrier to the wider adoption of the IoT and Industry 4.0.

The IoT is not free either. Beside the capital cost associated with the installation of data collection devices and communications infrastructure, the International Energy Agency has estimated that by 2025 the annual standby energy consumption associated with IoT devices will be equivalent to the electricity production of Portugal.

All the above and energy efficiency

Proponents of the Internet of Things and Industry 4.0 have identified energy efficiency as a significant potential benefit. The American Council for an Energy Efficiency Economy estimated potential savings of 12 to 22 percent of all energy consumed, while the consultant McKinsey suggests 10 to 20 percent energy savings.

These are high-level estimates for potential future benefits. But what energy cost and consumption savings have existing IoT technologies achieved to date? Where is the potential, and what would be the best way to identify what is relevant to your organization now?

Looking through the lens of EN 16247:2014, efficiency opportunities can be broadly classified across building, process, and transport. Figure 2 is a summary of some deployed technologies

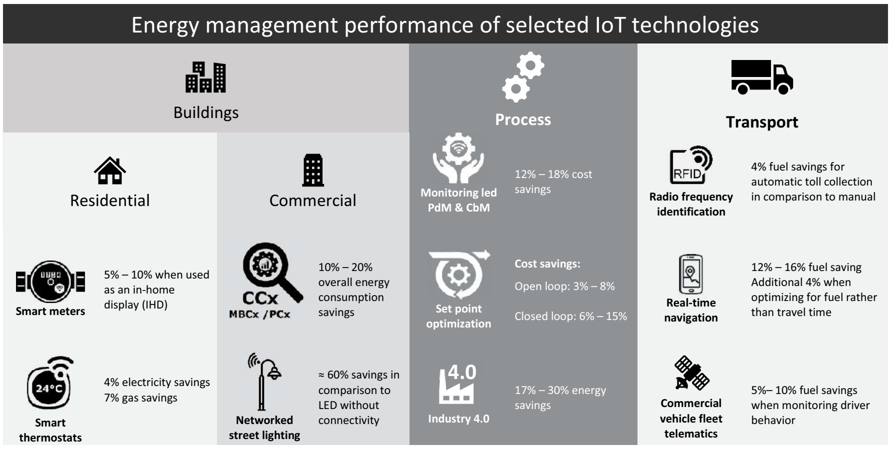


Figure 2. Selected IoT technologies from the perspective of EN 16247: 2014 (energy audits)

and their efficacy for reducing energy consumption.

Transport

The transportation and logistics sectors have been among the first to gain cost and energy consumption savings from the IoT. Radio frequency identification (RFID), introduced in the early 2000s, is finally realizing its initial potential—giving some indication of how long it takes these technologies to mature. RFID technology is used in many road toll and weigh-in-motion systems, so vehicles do not have to come to a stop and accelerate back to cruising speed, saving fuel and increasing efficiency. Fuel savings of 4 percent have been estimated for an RFID toll collection system in comparison to a manual system.

Satellite guidance with real-time correction for traffic is a form of IoT efficiency that is almost universally recognizable. Reported savings of between 12 and 16 percent have been demonstrated in independent studies, with an additional 4 percent anticipated when optimizing for fuel consumption rather than travel time. Real-time satellite tracking and telematics of commercial vehicles save between 5 and 10 percent by ensuring the monitored drives follow safe and efficient driving techniques. These savings do not include any other productivity or fleet optimization gains.

Buildings

IoT is progressing to a new type of smart building that better responds to the concerns of owners and managers about energy consumption. IoT enables operational systems that have more accurate and useful information for improving operations and saving the most energy for tenants. Focusing on heating, ventilation, and air conditioning (HVAC), lighting, and some types of electrical loads, it is reasonable to expect savings in the range of 10 to 25 percent when implementing proactive energy management programs in midsized buildings.

Residential buildings

The IoT is readily recognizable in smart utility meters, which promise to bring "time of use" billing and load shaping and which were previously reserved for large consumers, to residential customers. However, even before this promise can be realized, smart meters have been used to provide data to in-home displays, so customers can monitor energy use and receive feedback on cost. Trials conducted in various countries have demonstrated savings between 5 to 10 percent from in-home displays for residential customers.

Smart thermostats are domestic heating and cooling control systems that learn the user's pattern of behaviors to optimize energy consumption and comfort levels. Savings of approximately 4 percent in electricity and 7 percent in gas consumption have been reported from pilot studies. Additional savings are anticipated as additional connectivity (e.g., geofencing—turning climate systems on or off depending on user distance from site—and learning user patterns of occupancy) is added.

Commercial buildings

The term "commercial building" is broad and can be applied to hospitals, hotels, offices, and even public spaces. These buildings are much more energy intensive than those in the residential sector and offer greater potential for cost-effective energy savings.

To increase reliability and efficiency, and to gain other operating benefits, such as reduced maintenance and improved safety, many refineries and process plants are turning to the IoT.

The building management system (BMS) of large commercial buildings already generates significant volumes of data. However, previous generations of BMSs were not designed to use this data to optimize building energy performance.

Continuous commissioning (CCx), also known as monitoring-based commissioning (MBCx) or persistent commissioning (PCx), uses the data generated from a BMS to continuously identify potential energy-saving opportunities. Using advanced "big data" analytics, persistent commissions regularly report to the facilities manager to ensure that the elements of the site's energy-using equipment, normally HVAC equipment, are operating at optimal levels and that any deviations are investigated and acted upon.

CCx/MBCx/PCx is a well-established service in the U.S., recognized as achieving savings between 10 and 20 percent. The service is valued by energy users, as it helps to significantly reduce costs of capital and operations.

CCx/MBCx/PCx has not appeared in Gartner's hype cycle, because it was financially viable from the start at sites of sufficient size. The main advancement in the past few years is that analytics have moved to the cloud, so CCx/MBCx/PCx is viable for much smaller sites. Respectable returns on investments (less than three years) can be achieved for energy consumption of less than U.S. $0.5 million.

Networked public lighting: Lighting technology has experienced a revolution in recent years as LEDs replace traditional light sources. Although the move from sodium and mercury vapor lamps to LED has been the source of major savings, the nature of public lighting makes additional connectivity and control more financially attractive. Providing minimal light levels in unoccupied areas as well as communicating maintenance information brings savings to system operators that are not available to residential customers. An independent global trial of LED technology in 12 of the world's largest cities found that while LEDs can generate energy savings of 50 percent, these savings reached more than 80 percent when LED lighting was coupled with smart controls.

Process

Traditional industrial energy management focuses on the efficient provision and use of process energy needs, such as heating, cooling, compressed air, and electricity. The IoT has a wealth of new data streams to support energy management measures. Process industries may be slower to adopt some of these technologies than the consumer market due to a greater familiarity with the use of sensors and automation. A key driver for the digital transformation for the process industries is maintaining global competitiveness and technological advances, therefore forcing the alignment of production and wider business processes through the tools that offer new possibilities for business models.

Monitoring-led preventative maintenance, condition-based maintenance, and predictive maintenance

To increase reliability and efficiency, and to gain other operating benefits, such as reduced maintenance and improved safety, many refineries and process plants are turning to the IoT. Technologies, such as acoustic monitoring of steam traps, condition monitoring of pumps, and heat exchanger performance, all wirelessly connected to supervisory control and data acquisition and analytics systems, provide cost-effective installation and paybacks of less than six months.

"Calculations show the difference in operating costs associated with equipment reliability and energy efficiency between a well-run refinery and an average one is about $12.3 million per year for a typical 250,000 barrel-per-day facility. Assuming about 60 percent of refineries are not operating as well as they could, the overall worldwide financial impact runs to billions of dollars annually," says Deanna Johnson of Emerson Process Management.

Set point control

A new generation of software tools for energy efficiency allows two ways of energy plant management: *open loop*, where the optimal set points are indicated to the operators to manually set the optimization variables; or *closed loop*, where the set points are sent directly to each optimizable variable. These implementations can typically achieve energy-cost reductions from 3 to 8 percent for the open-loop model, and 6 to 15 percent for closed-loop applications.

Replacing gut feeling with real-time and comprehensive data leads to better decision making.

Industry 4.0

While improved energy efficiency is always welcome, it is rarely the main driver of Industry 4.0 deployments. However, energy savings have been reported by those organizations that have attempted to make Industry 4.0 a reality. For example, Daimler in Germany has reported a 30 percent improvement in energy efficiency for its robot systems that use Industry 4.0 techniques. Another example is Canadian Forest Products, which reported a 15 percent reduction in energy consumption by using real-time alerts for energy consumption outside of anticipated norms.

Making the IoT your own

The digital world delivers more actionable data than ever before. Replacing gut feeling with real-time and comprehensive data leads to better decision making. Whether this is about projects to fund, plant utilization, or sales accounts to focus on, data will be available to evaluate and select.

To gain the benefit of the IoT, though, you need to have an in-depth understanding of your processes. Which pa-

rameters are critical to the energy and productivity performance of your processes? This may seem obvious, but in our experience, many organizations have a poor understanding of the relationship of energy use to operational settings. Those who have deployed the IoT and Industry 4.0 say that the digitization of the manufacturing processes allowed them to better understand the actual energy demand of their machines.

Conducting energy audits to international standards, such as ISO 5002 or EN 16247, can provide the necessary baseline data relating energy use to production. It also provides a road map to appropriate future instrumentation. What was previously very expensive and difficult to measure may no longer be. It may not be difficult to retrofit smart meters and controllers to remote equipment.

Interpretation of data flows is a critical aspect. Information overload is an issue across all industrial sectors. When alarms are sounded, an appropriate set of options must be available to operators to gain potential savings. Impressive looking dashboards are only useful if they lead to appropriate actions. However, identifying these sets of appropriate actions is quite often excluded from data acquisition and reporting projects. Reporting often focuses on middle and senior management needs, rather than on the operators who ultimately decide if savings will be realized or not.

Finally, a comprehensive "whole of business" capital expenditure process should be used to transform sales promises into realistic business cases for the efficacy of technologies for your organization. Energy savings alone are unlikely to justify the expenditure on IoT and Industry 4.0. However, improved productivity, reduced downtime, and improved product quality can all contribute. ■

ABOUT THE AUTHORS

Brian Dwyer, C.Eng MIEI, is principal consultant – industrial, Energenz Socio Fundador – Instituto BioGesta, Argentina, with 20 years of experience in energy and resource (water and waste) efficiency. He has worked with governments and the private sector in Europe, Asia Pacific, and the Americas in the fast-moving consumer goods, resources, automotive, and commercial building sectors.

Joao Bassa, MSc (jbassa@gvmail.br), senior consultant – MAHAM Serviços de Engenharia Consultiva, Brazil, has 40 years of international industrial experience in automation and process controls. He is a professor at Mauá Technology Institute, a member of the *InTech* Editorial Advisory Board, and ISA district 4 (Brazil) Standards & Practices chairman.

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

RESOURCES

"The Internet of Things Is Totally Unregulated, and That Might Have to Change"
https://qz.com/817516/dyn-ddos-attack-the-internet-of-things-is-totally-unregulated-and-that-might-have-to-change

"Where's the Beef in Continuous Commissioning?"
http://aceee.org/files/proceedings/2012/data/papers/0193-000090.pdf

"IIoT applications enable the process world"
www.isa.org/intech/20160405

Accelerating clean energy through Industry 4.0
www.unido.org/sites/default/files/2017-08/REPORT_Accelerating_clean_energy_through_Industry_4.0.Final_0.pdf

Alarm management life cycle

By Bridget Fitzpatrick

Leveraging classes

Alarm systems are critical for facilitating process safety, ensuring efficient operations, and maintaining quality. Alarm management has been broadly implemented in the process industries over the past 20 to 30 years. If your facility has not embraced this fundamental aspect of automation and control, time is wasting! For sites that started in the early days with the ASM Consortium™ work of the 1990s, or later with the publication of ISA-18.2 in 2009, alarm management concepts are likely well integrated or even commonplace.

One of the common phenomena of alarm management is an initial gain in performance, followed by a gradual erosion of benefits. A major root cause of this variation is that most processes continually change—perhaps more often than we think. Changes to raw materials and product specifications, debottlenecking, new environmental regulations, and plant trials may affect alarm management. It is important to understand that alarm management is a never-ending effort. Managing the life-cycle aspects is as critical as getting the correct initial design or rationalization. One concept that can help manage the work process is alarm class or classification.

What is an "alarm class"?

As stated in ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*, an alarm class is a "group of alarms with a common set of alarm management requirements (e.g., testing, training, monitoring, and audit requirements)." One type of alarm class is a safety critical alarm, which, according to ANSI/ISA-18.2-2016, is defined as "an alarm that is classified as critical to process safety for the protection of human life or the environment."

An alarm may belong to more than one class. The alarm philosophy is *required* to provide a definition for alarm classes. However, like requirements in many standards, the specific definition and requirements of alarm classes are left to the owner to define. The recommendation is to embrace the alarm class as a tool in site alarm management work processes to help ensure effective requirement management of special types of alarms. In setting requirements for alarm classes, it can be effective to review the components of the ANSI/ISA-18.2 life cycle (figure 1).

Per ANSI/ISA-18.2-2016, specific alarm management considerations should include:

- alarm prioritization
- alarm documentation
- human-machine interface design
- operating procedures associated with these alarms
- operator training and training documentation
- alarm maintenance
- alarm testing
- alarm monitoring and assessment
- alarm management of change
- alarm history retention
- alarm auditing

When alarm management software is actively used to manage the alarm system, an alarm class can be a very effective cross-reference tool. The classification can help manage and record compliance with requirements and help prevent inadvertent deletion of, or changes to, important alarms.

Common types of classes

Alarms can come from a variety of sources. The most common classes of alarms are related to personnel protection, safety, product quality, environmental issues, and company or site policies.

Assigning classes of alarms by only the source may seem attractive; however, the alarm source can have a wide variety of alarm management requirements. All functional safety alarms, for example, can have different requirements for training, testing, auditing, or documentation. Class assignment depends on the requirements of the grouped alarms.

Highly managed alarms

ANSI/ISA-18.2 introduced the concept of the highly managed alarm (HMA). HMAs by definition require more administration and documentation. If HMA classes are used, the alarm philosophy requires the organization to define the criteria for assigning alarms to HMA classes. The designation of alarm classes as highly managed should be based on essentials, including alarms for:

- process safety that is critical to protecting human life (e.g., safety alarms)
- personnel safety or protection
- environmental protection
- current good manufacturing practice

FAST FORWARD

- Alarm management concepts are likely well integrated at sites that started with the ASM Consortium work in the 1990s or later with the publication of ISA-18.2 in 2009.
- A common phenomenon of alarm management is an initial gain in performance, followed by a gradual erosion of benefits caused by many variations in operations.
- Life-cycle management is critical for effective long-term operation, and the concept of alarm class helps manage the work process.

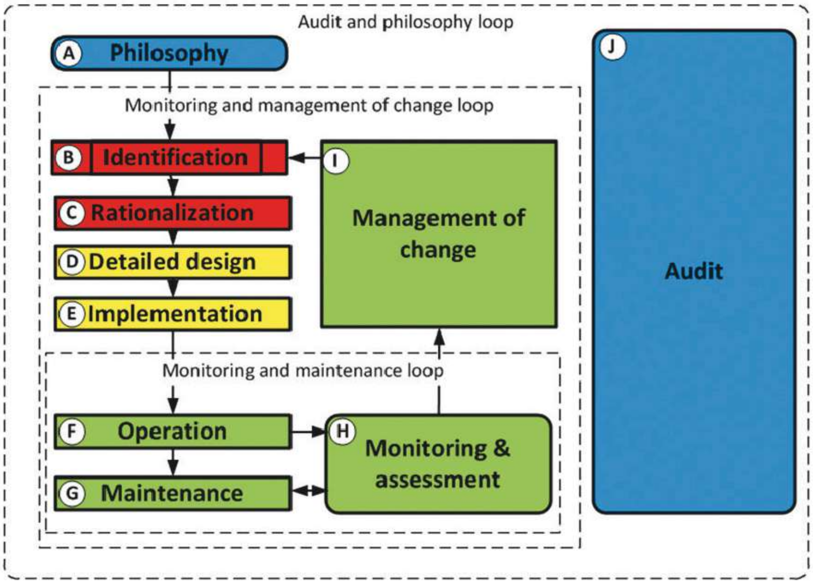


Figure 1. ANSI/ISA-18.2 alarm management life cycle

- commercial loss
- product quality
- process licensor requirements
- company policy

Although this may seem to add paperwork and complexity for limited or no gain, experience has shown it is an effective best practice for managing the requirements.

Example alarm class: H2S toxic gas

The detection of hydrogen sulfide gas (H2S) will likely have defined action and danger levels for different physical areas. Managing these alarms as a class defines these settings, special handling based on mode of operation, the human-machine interface (HMI) presentation, operator response, frequency of testing, training for staff, metrics for monitoring and reporting, and audit requirements.

A problematic H2S monitor that routinely alarms might have its alarm set point raised to not report the "nuisance" spike. Masking that spike might hide a safety concern related to a routine spike of detected H2S during a sampling procedure. A managed H2S class alarm will detect that change during an audit, recognize the sampling procedure issues, and result in a safer condition.

Steps for an effective alarm system

Falling back on the old adage that you cannot improve what you do not measure, monitoring, assessment, and audit activities are arguably the most important for long-term success. By undertaking monitoring and assessment, actual performance is measured and available for improvement. Similarly, audits of the work processes highlight any behavior that does not follow the alarm philosophy.

Note: The ISA technical report on this topic (ISA-TR18.2.5-2012, *Alarm System Monitoring, Assessment, and Auditing*) is a good reference for methods, metrics, and work practices.

The three loops shown in the ISA life cycle (figure 1) highlight areas for focused activity: audit and philosophy, monitoring and management of change, and monitoring and maintenance.

- An audit is conducted to ensure that the alarm management work processes are sound and aligned with the philosophy. As alarm management work processes mature, it is important to make sure that the philosophy is updated to reflect changes in practice. Philosophy documents that remain out of sync will fall increasingly out of use.
- In monitoring performance, issues related to following management of change procedures will become apparent. To effectively manage alarm systems, it is common to develop "fast track" or simplified processes. Allowing changes to occur without following a formal management of change process will make it difficult to achieve system integrity.
- Similarly, allowing the maintenance function to transfer alarms in and out of service without structured expectations and schedules can cause less effective systems.

Manage the work processes

Alarm class can help manage each stage of the life cycle:

Philosophy: In the philosophy process, operational definitions or terms and work processes are set. Alarm classes are listed and defined. This establishes clear expectations about alarm classes and how their related requirements are managed throughout the life cycle.

Identification: In a similar manner, clear alarm class ground rules set in the work practices related to identification help manage consistency.

Rationalization: Guidelines related to different classes of alarms help streamline and manage the rationalization process. Classes are assigned during rationalization.

Detailed design: Alarm classes may have specific requirements for setting the alarm design basis. This may be related to things such as the alarm limit or priority, implementation details, the general presentation on the HMI, or the need for specific online help information.

Implementation: When implementing certain alarm classes, specific requirements for testing and training may be required.

Operation: When certain alarm classes are in operation, they require refresher training.

Maintenance: Taking certain alarm classes out of operation and placing them into the maintenance stage of the life cycle may require specific remediation plans. Additional monitoring requirements, altered modes of operation, or specific testing requirements might be needed before returning to service.

Monitoring and assessment: An emerging concept requires the alarm system as a whole to meet certain performance levels to continue to take credit for independent protection layer (IPL) alarms.

Example alarm class: IPL alarms

IPL

A layer of protection analysis may identify alarms that provide risk reduction. These are generally known as independent protection layer alarms. Such alarms may have additional requirements for monitoring, including frequency, time in alarm, time shelved, time out of service, average alarm rate when active, and percent of time participating in an alarm flood.

"High frequency" may indicate time durations higher than estimated during the functional safety studies. "Time in alarm" may reflect exposure time to the underlying hazard. "Shelved" and "out of service time" may reflect time not available as a layer of protection. Review of these time frames in an audit may reflect the need for recognition of different modes of operation, addition of alternate alarms, and related recordkeeping

Management of change: Alarms generated from engineering studies or functional safety may require different levels of approval for changes.

Audit: Certain classes of alarms may require specific audit periods or level of detail on audits to meet compliance requirements.

Right size the effort

Adding alarm classes may seem daunting at first. However, managing the requirements is much easier to implement if you recognize that some alarm types have different life-cycle requirements. Segregate those alarms into classes as a first phase. To "right size" the effort, use an initial approach of generating a set of alarm classes that splits out the key "special" or HMA alarms and leaves the rest as a general class. It is important to approach the process by finding the important alarms with special requirements, rather than considering the need to discuss and classify every alarm. ■

ABOUT THE AUTHOR

Bridget Fitzpatrick (Bridget.Fitzpatrick@woodplc.com), an ISA Fellow, is disciple technical authority for HMI, abnormal condition management and human factors, for the automation and control organization within Wood. Wood provides project, engineering, and technical services for energy and industrial markets. Fitzpatrick has an MBA in technology management from the University of Phoenix and a SB in chemical engineering from the Massachusetts Institute of Technology. She sits on the ISA Standards and Practices Board and is managing director of the ISA18 (Alarm Management) committee.

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

Welcome to Industry 5.0

The "human touch" revolution is now under way

By Esben H. Østergaard, PhD

At HANNOVER MESSE 2017, like most industrial trade shows, the predominant theme was Industry 4.0. Although Industry 4.0 still has not scaled up to cover a significant percentage of manufacturing setups, its vision of near-total automation—and the resulting cost savings—has clearly captured the industry's imagination.

More importantly, even though the "lights-out" factory is still a rare phenomenon, the connected automation technologies that form the backbone of Industry 4.0 are being widely and increasingly deployed. They are making important differences in the manufacture of many types of products and, in industries like health-care, even the provision of services.

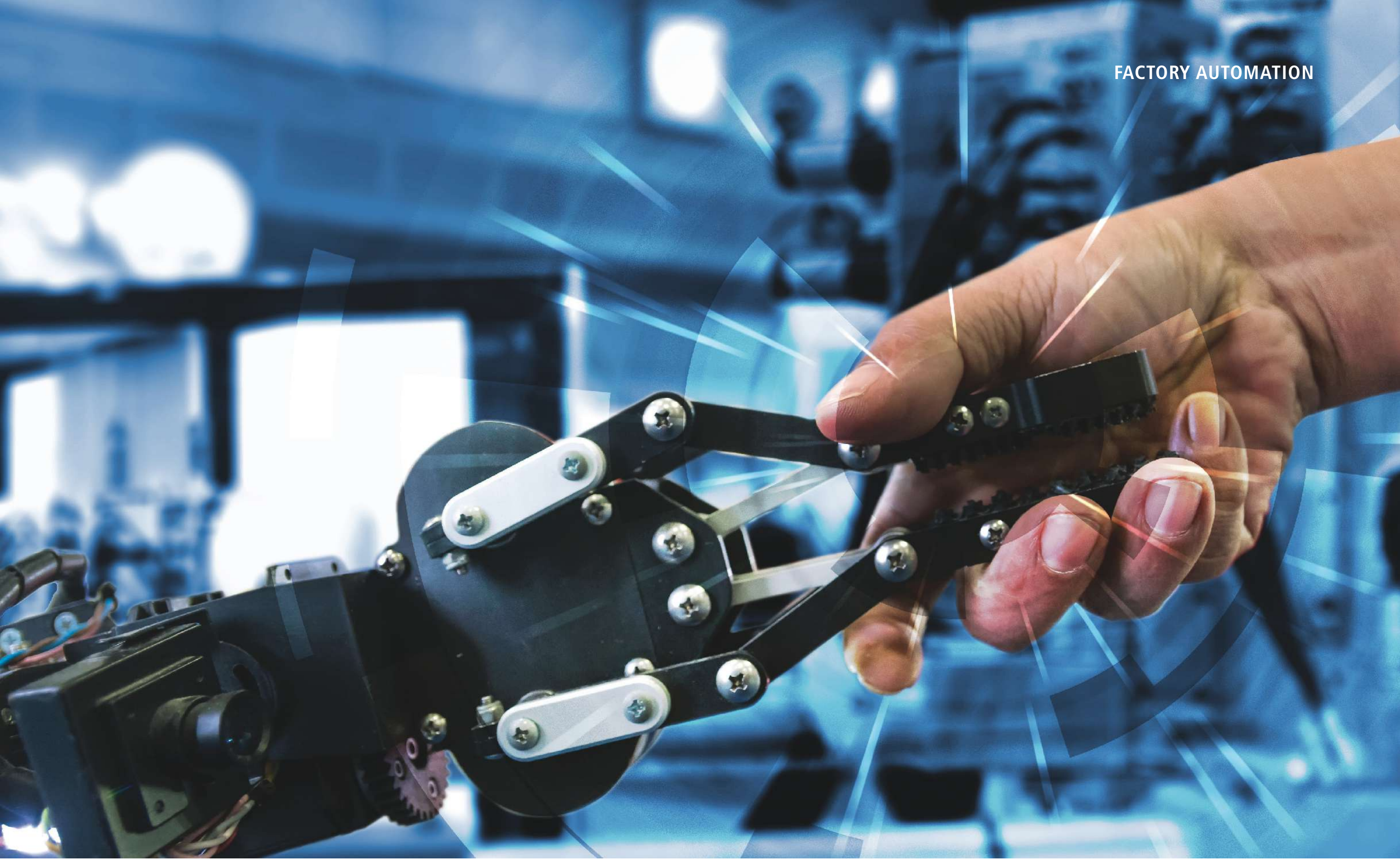
Role of robots

The use of robots in manufacturing has been on the rise since the 1960s, when they were first introduced as part of what technologists call Industry 3.0 (defined by programmable logic and advanced manufacturing). Robots grew up in the car industry, where they were used primarily to weld car bodies together. As technologies matured, companies began using robots in other areas, such as logistics and the medical and food industries. Starting in 2006, more robots were used outside the automotive industry than inside it.

The main driver behind the rise of industrial robots was a desire to reduce or eliminate the "three Ds"—dull, dangerous, and dirty jobs. But other important drivers included the need for consistency of quality and consistency of flow in manufacturing.

Today, robots are used not just in huge manufacturing and logistics facilities, but—thanks to the advent of smaller, more affordable, and easy-to-use collaborative robots ("cobots")—in small and medium-sized businesses too. The benefits of robotic automation include:

- Robots improve the consistency of product quality and production line flow, meeting demand for high-quality products at lower cost.
- They save workers from having to perform repetitive, tedious, and dangerous tasks.
- Today's connected, or Industry 4.0, robots are able to consistently generate data on parts flow and process quality—data that artificial intelligence or old-school data analysis can use to optimize both a factory and manufacturing processes.
- Thanks to greater inherent flexibility than special machines or other hard automation, robots enable greater product variation on a single line and—when integrated with logistics systems in Industry 4.0 setups—enable factories to produce variants based on the customer's choice of preconfigured options



(often referred to as "mass customization").

- Because robots cost almost the same everywhere in the world, they can help companies reshore manufacturing jobs that were transferred to low-cost labor countries and generally level the playing field.

Mass production to mass personalization

The fourth point above—that connected Industry 4.0 technologies, including robots, let manufacturers mass customize their products like never before—is worth looking at in detail. Let's take buying a car as an example: Many readers of this article grew up under Industry 3.0, which accompanied the rise of computing in business.

Buying a car in the 1970s, 1980s, and 1990s usually involved selecting a make and model at a car dealership, or—if nothing in the showroom quite fit the bill—perhaps ordering a car in a particular color and with certain extras, like air conditioning. Granted, that was a lot of choice compared to what Henry "as long as it's black" Ford had to offer (i.e., Industry 2.0). But it was nothing like "configuring" a car online today.

Car buyers now have so many options to choose from that any given customer has a good chance of ending up with a car that at least appears to be one of a kind. Now, if you are the owner of this car and live in a city of, say, half-a-million people, and if nobody else has a car that is exactly like yours, then you are driving a car that, to all appearances, was designed uniquely for you. Even if you are not a millionaire. Even if it is not a particularly expensive car.

Driven by a desire to make affordable, high-quality products that at least give the appearance of uniqueness, today's mass customization is largely enabled by Industry 4.0 technologies—including Internet connections between dealership ordering systems, supply chain systems, and even the robots on the car factory floor.

The customer makes choices from a growing list of options. This set of choices is configured and packed in just the right order. The truck arrives at the car factory at just the right minute. And the forklifts deliver the parts straight to the assembly line station where the customer's "unique" car appears.

This is Industry 4.0, and I believe it is the future

FAST FORWARD

- Collaborative robotics innovator introduces the next industrial revolution: Industry 5.0
- Industry 4.0 offers mass production with little or no human involvement; Industry 5.0 brings personalization and the human touch back to manufacturing.
- Collaborative robots are well positioned to become Industry 5.0 tools, helping humans create the personalized products demanded by consumers.

By placing humans back at the center of industrial production, Industry 5.0 gives consumers the products they want and gives workers jobs that are more meaningful.

of at least a large segment of consumer goods manufacturing. But it is not perfect. For producers, "lights-out" manufacturing provides few opportunities for adding value. It is all about lowering costs while ensuring product differentiation. For workers, it is even worse. Those who are employed in Industry 4.0 setups are expected to work like machines, "programmed" by management to perform an exact number of tasks every hour. It is work for robots, performed by humans only until technology advances far enough to replace the humans altogether. And it would not surprise me if a lean analysis of this type of factory found that it wastes human problem-solving skills, value-adding human creativity, and the critical and exclusively human ability to deeply understand customers.

Most importantly, the mass customization described above and enabled by Industry 4.0 is not enough. Because consumers want more. They want mass personalization, which can only be had when the human touch returns to manufacturing. This is what I call Industry 5.0.

Psychology trumps technology

In the 1960s, as Industry 3.0 was starting to make waves in society, the Canadian media theory guru Marshall McLuhan proclaimed that "the medium is the message"—that new technologies determine changes in patterns of human thought and behavior. Technologists like me might wish that were the case—i.e., that we are the ones who decide how people act. But I do not believe that McLuhan was right. Human psychology trumps technology and puts it to its own uses.

People want to stand out, to be seen as unique, to express themselves through their choices—including their purchasing choices. Now, for the first time since the dawn of the Industrial Age, technologies are available that let people express themselves as individuals through personalized products. Not just low-tech products, but any product that can send the right signals. And not just products that only the super-rich can afford, but products within reach for people with modest incomes.

This desire for mass personalization forms the psychological and cultural driver behind Industry 5.0—which involves using technology to return value added by humans to manufacturing. Before we examine that in more detail, note that the desire for mass personalization also calls another Industry 3.0 assumption into question. The American futurist Alvin Toffler's influential 1970s work *Future Shock* saw too many choices as a *problem* for consumers, who would need to band together into groups to deal with choice overload. Yet in place of Toffler's "shock," we see consumers reveling in choice—with one person expressing herself by playing music from an infinite number of options online and another spinning vinyl on a Shinola turntable, handmade in Detroit.

The mass personalization and related trends also question common Industry 4.0 assumptions—especially the oft-expressed but wrong-headed claim that robots are "taking over" and "stealing our jobs." We have found that companies that deploy collaborative robots end up employing more people, not fewer, than they did before they went robotic. Instead of replacing workers, the cobots have helped grow these companies' businesses. We expect that, just as with Industry 1.0, Industry 2.0, and Industry 3.0, this latest wave of industrial automation will result in net job growth, not loss.

To be clear, there are huge swaths of product types that nobody wants personalized and for which Industry 4.0 setups, with their traditional industrial robots, are perfect. Nobody wants a personalized drywall anchor, engine block, or lawnmower blade. If these products can be made at a minimal cost in a lights-out factory, it benefits everyone.

Industry 5.0 products, on the other hand, empower people to realize the basic human urge to express themselves—even if they have to pay a premium price. Making these products requires what we call the human touch.

Return of the human touch

The personalized products consumers will demand most and pay most for are products with the distinctive mark of human care and craftsmanship. Fine watches, craft beers, designer items of every kind, and even (I saw it in the supermarket recently) black salt from Iceland, hand dyed with local coal.

Products like these can only be made through human involvement—human engagement. This human touch, above all, is what consumers seek to express their identity through the products they buy. These consumers accept technology—they do not mind if automation, for example, is a part of the manufacturing process. But they crave the personal imprint of human designers and craftspeople, who produce something special and unique through their personal effort. This is personalization. This is the feeling of luxury. This is the future.

This Industry 5.0 trend is more anti-industrial than industrial. It is a return to something earlier, to a time before industrialization, when a gift, for example, was something someone you knew spent months knitting or carving or creating by hand. It was just for you, because the person who made the gift knew you personally and thus knew how to make a gift for you and no one else.

But how do the human designers and craftspeople of today make products that live up to the quality standards people expect? How do they make products at a price people can afford? Collaborative robots are a big part of the answer.

High mix/low volume is part of the fifth industrial revolution that brings smaller, more personalized batches of products to market, aided by cobots. Add a welding torch at the end of the arm tooling and you have a welding robot; the next day you can add a camera for quality inspection or a pneumatic suction cup for pick and place on the same cobot arm.

Enter collaborative robots

Collaborative robots are exactly the tools companies need to produce the personalized products consumers demand today. Cobots bring the human touch to the masses.

Far from fenced-off industrial robots that replace human workers with automated processes, collaborative robots enhance human craftsmanship with the speed, accuracy, and precision required to make modern products with a human touch. Although consumers might want to express themselves through market-square baskets and hand-painted flowerpots, they also want to do it with their smartphones, luxury headsets, and "personalized" car designs.

Collaborative robots are essentially power tools that give craftspeople—operators—superhuman powers in terms of speed and accuracy. That is what it takes to make industrially manufactured products with a human touch.

Broader implications

As briefly mentioned earlier, what I am calling Industry 5.0 is in fact not an incremental development from Industry 4.0. It is not just more ramped up automation. It is, in an important sense, the end of automation—but an "end" that is enabled at least in part by robotic automation. That is the great irony in the latest leap forward in automation—whether or not you call it Industry 5.0. It is a return to what in many respects resembles a preindustrial form of goods production, but one that is enabled by the most advanced industrial automation technologies, starting with collaborative robots.

Our company does not wax too philosophical. But I suggest that what I am referring to as Industry 5.0 addresses—at least in some small way—what Marx called *alienation*, the idea that, through modern industrial production, workers lose control over their lives by losing control over their work.

They become automatons, who only go through the motions of human labor, without contributing to or benefiting from it in any meaningful way. By putting human beings back at the center of industrial production—aided by tools such as cobots—Industry 5.0 not only gives consumers the products they want today, but it gives workers jobs that are more meaningful than factory jobs have been in well over a century. ■

ABOUT THE AUTHOR

Esben H. Østergaard, PhD (esben@universal-robots.com), is chief technology officer at Universal Robots and is responsible for the enhancement of existing UR cobots and the development of new products. Østergaard is one of the inventors of UR cobots. During his years as researcher and assistant professor in robotics and user interfaces at the University of Southern Denmark, he created the foundation for a reinvention of the industrial robot. He also worked as a research scientist at USC Robotics Labs in Southern California and at AIST in Tokyo as a visiting researcher.

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

Swinging for the fence with wireless technology

ISA100 Wireless community experience

By Andre Ristaino

End-user surveys conducted over the past five years have listed reliability and security as the two most important factors inhibiting adoption of wireless technology in manufacturing. During this time, many end-user companies performed structured studies to learn for themselves what is real and what is wireless marketing hype, and the ISA100 Wireless Compliance Institute published some of these independent studies and their findings. Here are two studies showing positive findings for wireless technology.

2014 Nippon Steel & Sumikin Engineering

This project studied the reliability of ISA100 Wireless communications and multivendor interoperability in a steel plant. The study concluded that the reliability as measured by packet error rates was more than sufficient and recommended moving forward with wireless technology. It also concluded that mixed vendor configurations demonstrated seamless interoperability.

2015 Petronas

This project studied the reliability of native ISA100 Wireless communications between two floating offshore oil platforms performing remote gas monitoring for a safety application. They were 5 km apart in the South Pacific Ocean during monsoon season. The study showed that zero packets were lost in the wireless transmission between the two platforms, concluding that ISA100 Wireless was reliable in this case.

Getting to the bottom of it

However, not everyone is convinced, causing us to look a little deeper. Surveys conducted during 2017 Wireless Compliance Institute (WCI) end-user events repeated the same set of questions to gauge what, if anything, regarding end-user adoption of wireless technology has changed in the past five years.

This time, survey results were aggregated into two groups: end users who have *not* implemented wireless technology and end users who *have* implemented wireless technology. We asked, "What are the key factors inhibiting adoption of wireless technology in manufacturing?" Response from end users who *have not implemented* wireless technology:

1. reliability
2. security

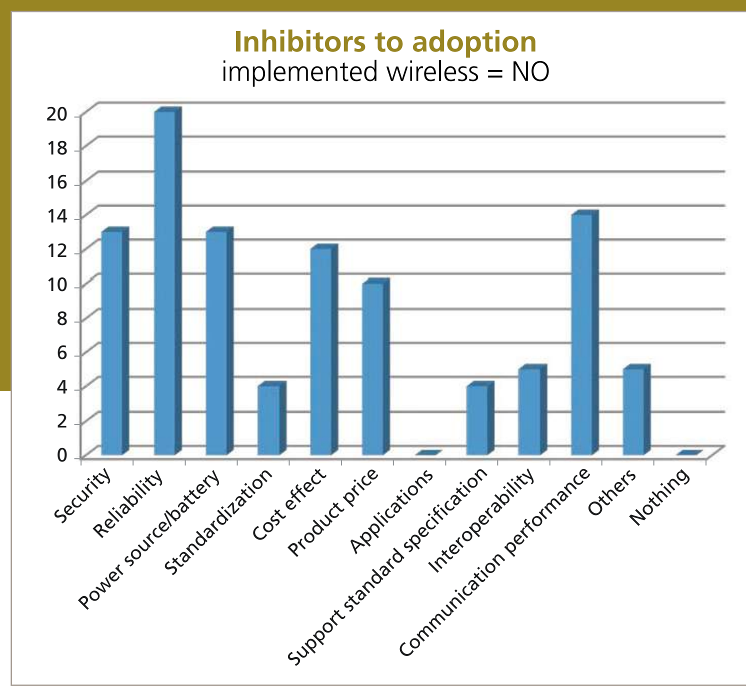
Response from end users *who have implemented* wireless technology:

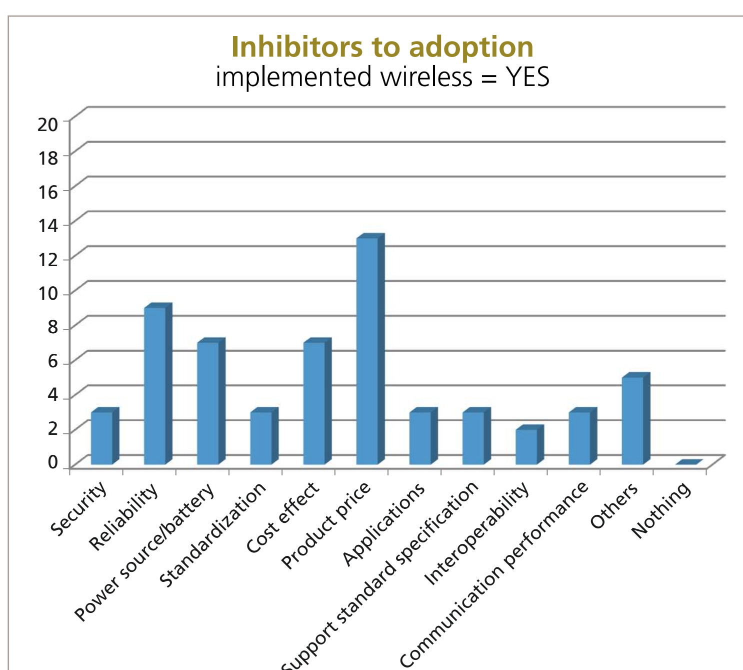
1. cost
2. availability of new applications

Wireless

FAST FORWARD

- Independent studies indicate positive findings for wireless technology applications.
- End users who do not have real-world experience with wireless technology express fear of the unknown.
- End users applying wireless want to do more with wireless and want it cheaper.

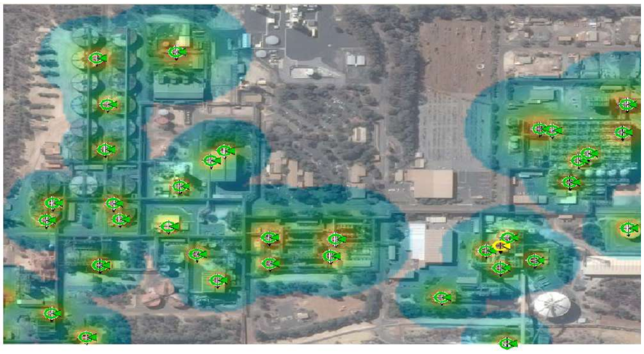




The two themes here are *fear of the unknown* for end users who have no real-world experience with wireless technology; and *I want to do more with wireless and now want it cheaper* for those who do have real-world experience with wireless technology.

Most of the companies with wireless application experience started small with noncritical applications, such as asset monitoring, during

Andre Ristaino (right), managing director, ISA100 Wireless Compliance Institute, presents the 2017 ISA100 Wireless Excellence in Automation Award to Chester Davidson, global services manager, Alcoa, at the February 2018 ARC Industry Forum in Orlando.



"Heat map" showing typical Alcoa operating area coverage using wireless technology.

the early phases. They gained confidence as they became familiar with the technology. Experienced end users have now expanded into safety and reliability applications.

Interestingly, at ISA100 wireless standards committee meetings between 2007–2009, the then ISA100 committee co-chairman Wayne Manges, PhD, from Oak Ridge National Laboratory repeatedly predicted that the future of wireless was low-cost "lick and stick" sensors. Manges saw a future of ubiquitous low-cost sensing/instrumentation, Internet of Things (IoT), and useful, not-yet-invented applications fueled by wireless enablement.

This year, the ISA100 Wireless Compliance Institute awarded its Excellence in Automation Award to Alcoa, whose application of wireless technology seems to bear out many predictions made by Manges, including ubiquitous wireless connectivity, lower-cost sensors, and wireless closed-loop control.

Alcoa was recognized for its visionary work with wireless technology. In 2014, Alcoa made ISA100 Wireless technology its global standard across refinery operations. The company established engineering standards, installed wireless infrastructure and monitoring equipment, and developed wireless training modules and support processes.

In 2015 Alcoa formed a wireless advisory board to provide corporate governance for wireless technology implementation and developed instrumentation selection criteria.

From 2016 to 2018, it has worked with its vendor to develop new ISA100 Wireless instruments for its specific needs, including a lower-cost, lightweight wireless pressure transmitter; a wireless safety shower panic button; a multiuse wireless push button; and an ISA100 Wireless serial interface for use on in-house specialty analyzers. Additionally, the company enabled Wi-Fi in the process area, supporting a global, connected worker initiative. Alcoa's objectives in selecting ISA100 Wireless as an enabling technology were to:

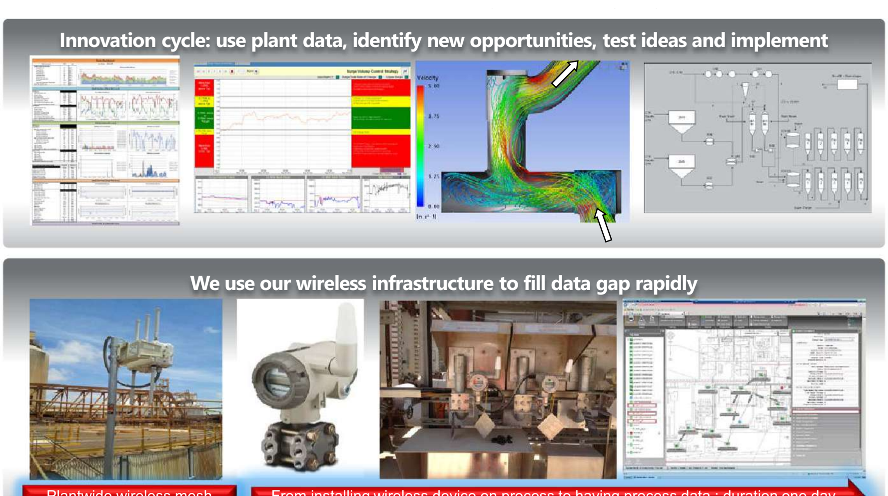
- provide an engineered, secured, managed, and integrated wireless network in alumina refinery process areas
- support mobile operators using handheld devices
- allow wireless connectivity of process control system or EHM equipment that is either remote or mobile
- enable IIoT and IoT in the future

The adoption and implementation of ISA100 Wireless has reduced capital expenditure related to installation of process/condition monitoring instruments, increased deployment speeds, facilitated troubleshooting via mobile and temporary sensors, and extended monitoring applications to moving equipment. The complete presentation of Alcoa's work is on the WCI website (https://isa100wci.org/en-US/Learning-Center/Presentations).

With 100 percent wireless coverage at operating sites, Alcoa has reduced the time to instrument a process from 3–6 months using wired sensors to three days or less using wireless sensors. This capability provides a huge return on investment (ROI), especially for quickly analyzing processes for optimization or temporarily troubleshooting an asset or process.

Based upon ISA100 Wireless, Alcoa is now learning to apply wireless to closed-loop control in a noncritical application for water tower level management. Over time, Alcoa expects to expand wireless into more critical process control applications.

Wireless has been making big inroads in safety applications. The Draeger GS01 wireless gas sensor was implemented in a SIL-2 certified safety loop (the full loop is SIL-2, not just the gas sensor), and end users are finding wireless to be extremely useful for alarm monitoring. Alcoa has added wireless alarms to all safety washdown stations, notifying the safety staff of the location of any wash station that was triggered. ISA100 Wireless technology conferences during 2017 focused on wireless for reliability and safety applications. Presentations from the October 2017 Taipei event contain descriptions of ISA100 Wireless applications supporting safety and improved reliability for plant operations.



Summary of Alcoa wireless results

The next chapter in the wireless story is scale. The deployment of ISA100 Wireless for 100 percent site coverage at Alcoa is a large-scale wireless infrastructure deployment and sets the stage for ubiquitous sensing.

In another use case, hundreds and thousands of steam trap monitors are currently being deployed at hydrocarbon processing sites using ISA100 Wireless networks. Steam trap monitors offer huge ROI, with typical payback in 12 months or less due to device efficiency improvements and reductions in device maintenance costs. We expect to have a real-world story describing lessons learned and benefits realized by this time next year.

Quietly growing

The 2017 ON World Market Report on industrial wireless sensor networks and the Industrial Internet of Things (IIoT) said that ISA100 Wireless is the fastest growing industrial wireless mesh standard, with adoption increasing at 2.5 times the pace of its leading competitor. ISA100 Wireless adoption increased 67 percent over the past two years. Major factors driving ISA100 Wireless adoption over its competition include:

- flexible time scheduling
- software and protocol tunneling
- support for flexible topologies, such as star and mesh

These features are especially important for growing wireless applications, such as gas detection, steam trap monitoring, and oil and gas well site remote monitoring.

Suppliers had reduced cost and faster time to market for wireless product offerings using ISA100 Wireless. Complex products with proprietary protocols can be converted economically with the protocol tunneling and object technology features of ISA100 Wireless. For example, the GE Bentley Nevada vibration monitoring application was implemented using protocol tunneling, and the host applications remained unchanged. Further, the ISA100 Wireless network capabilities allow the large wave form data sets to be transmitted through native ISA100 Wireless networks. Enraf radar level gauges were similarly converted; these instruments also use large wave form data sets.

Novel uses of ISA100 Wireless include a specialized ISA100 Wireless network and wireless handheld control for loading crane applications at shipping ports, as well as use of ISA100 Wireless networks onboard communication satellites. Native IPv6 to the device provides the advanced features of the updated IP protocol as well as future-proofing device addressing. Further, recent engineering graduates are typically familiar with open standards-based IP addressing schemes, making the technology uptake easier.

Staying relevant for process industry

Although ISA100 Wireless is useful outside of the traditional process industry, Wireless Compliance Institute members remain focused on their process industry roots. Through an agreement with Fieldbus Foundation (now FCG), WCI standardized on device description (DD) specifications based on the Fieldbus Foundation specifications, thus ensuring device compatibility with host control systems.

WCI formed a collaboration agreement with FDT, and in 2014 jointly announced availability of an ISA100 Wireless annex to make FDT device type managers useable by ISA100 Wireless devices. Through collaboration with FCG, WCI developed an ISA100 Wireless annex for the FDI platform, an important process industry initiative. WCI customers can now generate FDI DD specifications through the ISA100 Wireless FDI annex or through FDT technology, whichever they prefer.

What is next?

ISA100 WCI suppliers continue to expand the portfolio of ISA100 Wireless products and applications that support traditional process industry needs. However, there is also expansion into new applications that require high reliability and the advanced features of ISA100 Wireless. While still robust, sensors and gateways are appearing in smaller, less expensive packaging and moving into adjacent industry verticals. Shoebox-sized gateways are now appearing in packaging the size of a deck of cards.

WCI is investing in improvements to the ISA100 Wireless implementation specification, third-party technology offerings, and the supporting technology ecosystem to benefit existing and new suppliers. In midyear 2018, WCI will announce the availability date of an offering that significantly reduces the cost and time to convert wired devices to wireless.

Open standards and multivendor interoperability continue to be the foundation of ISA100 Wireless. In addition to standardized device testing and certification, WCI conducts interoperability trials one or two times per year to ensure that the ISA100 Wireless brand promise of interoperability works in the real world. These are fun events (see the 2017 Taipei summary on the website) that generate goodwill among members and provide opportunities for business networking. WCI gains valuable feedback from ISA100 Wireless suppliers at these events, which helps to guide the WCI technology road map. ■

Open standards and multivendor interoperability continue to be the foundation of ISA100 Wireless.

ABOUT THE AUTHOR

Andre Ristaino (aristaino@isa.org) is managing director of the ISA Automation Standards Compliance Institute in Research Triangle Park, N.C. He provides staff leadership for ISA's conformance certification programs, including the ISA100 Wireless conformity assessment scheme operated by the ISA100 Wireless Compliance Institute. Ristaino is an international presenter on the IEC 62443 standards and control systems certification and the ISA100 Wireless (IEC 62734 standard) technology. Ristaino earned a BS in business management from the University of Maryland, College Park, and an MS in computer systems applications from the American University in Washington D.C. Ristaino holds an APICS CPIM certification.

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

EdgeX Foundry

IoT, IIoT, and Industry 4.0 unifying architecture

By John D. H. Hose

The Linux Foundation EdgeX Foundry project is focused on creating a unifying open architecture for network edge devices to support the vision and goals of the Internet of Things (IoT), Industrial Internet of Things (IIoT), and Industry 4.0. EdgeX Foundry is a vendor-neutral, open-source software framework platform built for the edge of the network. It interacts with the physical, everyday working world of enabling devices, sensors, actuators, and other IoT end points and components to connect securely and operate efficiently. The intent is to build a common framework for IIoT edge computing. The EdgeX Foundry community encourages a rapidly growing number of IoT solution providers to work together in an ecosystem of interoperable components to reduce uncertainty, accelerate time to market, and facilitate scale.

By bringing this much needed interoperability, EdgeX Foundry makes it easier to monitor real-world sensors and actuators, send instructions to them, collect data from them, and move the data across the fog up to the cloud, where it may be stored, aggregated, analyzed, and turned into information. With EdgeX, data travels toward the cloud and laterally to other gateways, or back to devices, sensors, and actuators.

The initiative is aligned around a common goal: simplifying and standardizing the foundation for tiered edge computing architectures in the industrial IoT market while still supporting the ecosystem to provide significant value-added differentiation.

EDGEX FOUNDRY™

Founding members include Advanced Micro Devices (AMD), Alleantia, Analog Devices, Bayshore Networks, Beechwoods Software, Canonical, ClearBlade, CloudPlugs, Cloud of Things, Cumulocity, Davra Networks, Dell, Device Authority, Eigen Innovations, EpiSensor, FogHorn Systems, ForgeRock, Great Bay Software, IMS Evolve, IOTech, IoTium, KMC Controls, Kodaro, Linaro, MachineShop, Mobiliya, Mocana, Modius, NetFoundry, Neustar, Opto 22, relayr, RevTwo, RFMicron, Sight Machine, SoloInsight, Striim, Switch Automation, Two Bulls, V5 Systems, Vantiq, VMware, and ZingBox. Industry affiliate members include Cloud Foundry Foundation, EnOcean Alliance, Mainflux, Object Management Group, Project Haystack, and ULE Alliance.

"South side" and "north side"

EdgeX Foundry–based edge devices unify physical sensing and control devices with networks and systems.

South side: All IoT objects within the physical realm and the edge of the network that communicates directly with those devices, sensors, actuators, and other IoT objects—and collects the data from them—is known collectively as the "south side."

North side: The cloud (or enterprise system) where data is collected, stored, aggregated, analyzed, and turned into information and the part of the network that communicates with the cloud is referred to as the "north side" of the network.

The EdgeX architecture enables data to be sent "north," "south," or laterally in peer-to-peer architecture as required by applications.

EdgeX Foundry architectural tenets

EdgeX Foundry was conceived with the following tenets guiding the overall architecture:

- EdgeX Foundry must be platform agnostic with regard to:
  - Hardware
  - Operating system (e.g., Linux, Windows)
  - Distribution: It must allow the distribution of functionality through microservices at the edge, on a gateway, in the fog, on the cloud, etc.
  - Protocol and sensor

FAST FORWARD

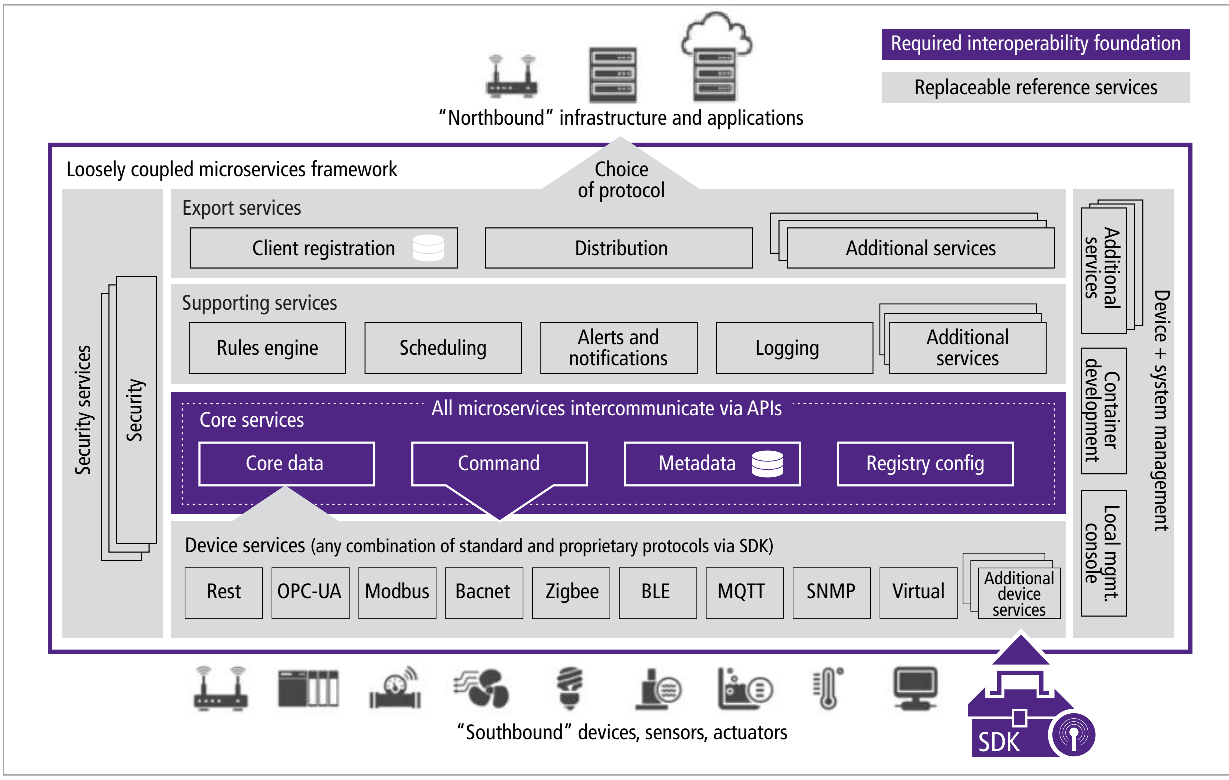
- **The Linux Foundation EdgeX Foundry project is focused on creating an open architecture to achieve the vision and goals of the IoT, IIoT, and Industry 4.0 with a framework that simplifies interoperability and accelerates large deployments.**
- **EdgeX Foundry is a vendor-neutral, open-source software framework built for the edge of the network, so devices, sensors, actuators, and other IoT end points and components can connect securely and operate efficiently.**
- **EdgeX Foundry is fostering an ecosystem of innovative developers of the building blocks of edge devices.**

- EdgeX Foundry must be extremely flexible:
  - Any part of the platform may be upgraded, replaced, or augmented by other microservices or software components.
  - It must allow services to scale up and down based on device capability and use case.
  - It should provide "reference implementation" services but encourages best-of-breed solutions.
- EdgeX Foundry must have store and forward capability (to support disconnected/remote edge systems).
- EdgeX Foundry must support and facilitate "intelligence" moving closer to the edge in order to address:
  - Actuation latency concerns
  - Bandwidth and storage concerns
  - Remote operation concerns
- EdgeX Foundry must support brown and green device or sensor field deployments.
- EdgeX Foundry must be secure and easily managed.

Service layers

EdgeX Foundry is a collection of open-source microservices. Microservices are a new, architecture style of building systems using simple, lightweight, and loosely coupled services that can be developed and released independently of each other. Developers describe the term "loosely coupled" as a way to build code without a tight dependency on other code by developing an application as a suite of small services, each running in its own process and communicating with lightweight mechanisms. They may be written in different programming languages and use different data storage technologies.

These microservices are organized into four service layers and two underlying augmenting system services. The service layers traverse from the edge of the physical realm from the device services layer, to the edge of the information realm of the export services layer, with the core services layer at the center. The four



service layers of EdgeX Foundry are:

- core services layer
- supporting services layer
- export services layer
- device services layer

The two underlying system services of EdgeX Foundry are:

- security
- system management

Core services layer

The core services (CS) layer separates the north side and south side layers at the edge. Core services include the following components:

- Core data: a persistence repository and associated management service for data collected from the south side objects.
- Command: a service that facilitates and controls actuation requests from the north side to the south side.
- Metadata: a repository and associated management service of metadata about the objects that are connected to EdgeX Foundry. It has the capability to provision new devices and pair them with their owning device services.
- Registry and configuration: provides other EdgeX Foundry microservices with information about associated services within EdgeX Foundry and microservices configuration properties (i.e., a repository of initialization values).

Supporting services layer

The supporting services (SS) layer encompasses a wide range of microservices that provide the edge analytics and intelligence and provide service to EdgeX Foundry itself. Normal software application duties, such as logging, scheduling, and data clean up (scrubbing), are performed by microservices in the SS layer.

The rules engines and alerting and notification microservices are within the SS layer, because they operate on top of the core services layer. The local analytics capability (implemented today as a simple rules engine) is also located in this layer. At this time, the EdgeX Foundry supporting services layer includes the following microservices:

- architecture – supporting services – alerts and notifications
- architecture – supporting services – logging
- architecture – supporting services – scheduling
- architecture – supporting services – rules engine

Export services layer

EdgeX Foundry operates independently of other systems when necessary. Gateways often operate in isolated and sometimes disconnected environments and monitor and manage a collection of sensors and devices that have little or no outside monitoring or control. Therefore, EdgeX Foundry can operate and sustain itself over long periods without connection to the "north side" systems. The data and intelligence that is created at the edge should be collected often and transported to enterprise (cloud) systems. The transporting is done by the export services (ES) layer. The ES layer has a set of microservices that performs the following activities:

- enables off-gateway clients to register for data that interests them, coming from the south side objects
- informs where and when the data is to be delivered
- informs the format and shape in which that data is to be delivered

For example, the "where and when" could be sending temperature data to a REST address every hour, and the format and shape could be to supply JSON data in compressed form.

At this time, the export services layer

includes the following microservices:

- architecture – export services – client registration
- architecture – export services – distribution
- export services – Google IoT core

Device services layer

The device services layer interacts with device services. Device services (DS) are the edge connectors interacting with the devices or IoT objects (the "things") that include, but are not limited to, alarm systems, heating and air conditioning systems in homes and office buildings, lights, machines in any industry, irrigation systems, drones, currently automated transit (i.e., some rail systems), currently automated factories, and appliances in homes. In the future, this may include driverless cars and trucks, traffic signals, fully automated fast food facilities, fully automated self-serve grocery stores, and devices taking medical readings from patients.

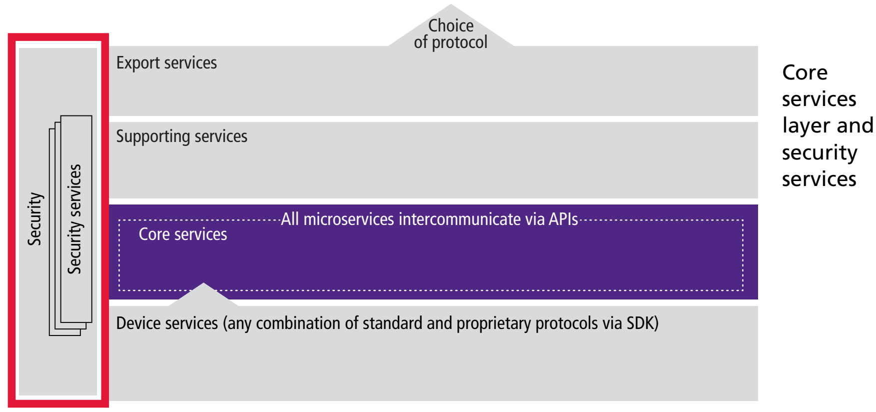
Device services may service one or a number of devices (i.e., sensor, actuator) at one time. A "device" that a DS manages could be something other than a single physical device. It could be another gateway (and all of that gateway's devices); a device manager; or a device aggregator that acts as a device, or collection of devices, to EdgeX Foundry.

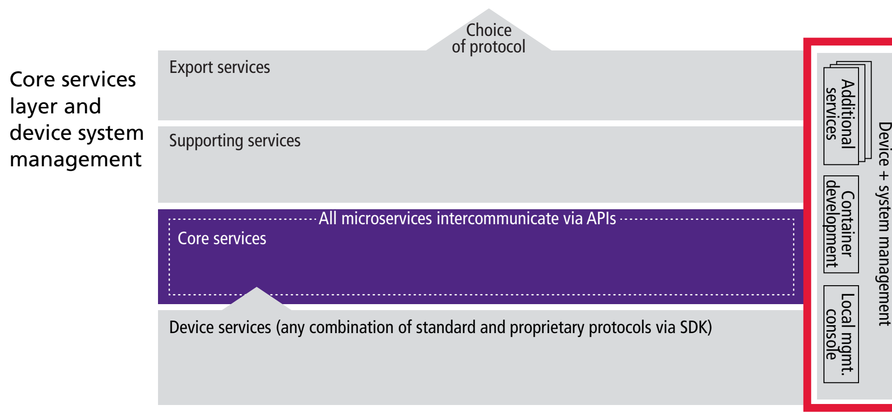
The DS layer's microservices communicate with the devices, sensors, actuators, and other IoT objects through protocols native to each IoT object. The DS layer converts the data produced and communicated by the IoT object into a common EdgeX Foundry data structure, and sends that converted data into the core services layer, and to other microservices in other layers of EdgeX Foundry.

EdgeX Foundry provides a device service software developer kit (SDK) for generating the shell of a device service. It makes the creation of new device services easier and provides connector code to the core services layer. At this time, the EdgeX Foundry DS layer includes the following microservice: architecture – device services – virtual device.

Examples of device services

- A BACNet DS converts the BACNet device-supplied temperature and humidity readings into a common EdgeX Foundry object data structure.
- A DS receives and translates commands from other EdgeX Foundry services or enterprise systems and communicates those requests to the devices for actuation in a programming language that the device understands.
- A DS receives a request to turn off a Modbus PLC-controlled motor. The DS translates the generic EdgeX Foundry "shutoff" request into a Modbus serial command that the PLC-controlled motor understands for actuation.





Security elements both inside and outside of EdgeX Foundry protect the data and command of devices, sensors, and other IoT objects managed by EdgeX Foundry.

System management

System management facilities provide the installation, upgrade, start, stop, and monitoring of EdgeX Foundry microservices and BIOS firmware, operating system, and other gateway-related software. They can also support these functions from off-box, enterprise-based systems.

Ecosystems and flexibility

EdgeX Foundry enables the development of edge devices in an open architecture, multivendor, interoperable environment in the open-source technology community. This fosters an ecosystem of creative and innovative developers building the components for the realization of the IoT, IIoT, and Industry 4.0. ■

ABOUT THE AUTHOR

John D. H. Hose is a consultant for IoT companies entering new markets and building value through strategic partnerships. Hose was a senior manager of IT service strategy at EMC Corporation and Dell Technologies. He has driven the development and deployment of demand management and service portfolio management processes following ITIL and ITSM best practices. Hose started his career providing IT business partner and business relationship manager support in higher education at MIT and Brandeis University. He holds an MBA from Babson College in global management and a BA from Brandeis University.

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

Career opportunity knocks

Will you answer?

Perspectives from the president

By Brian Curtis,
2018 ISA president

I am proud to be the 2018 ISA president and to participate in the advancement of the automation profession. As someone who has been highly engaged for many years in my local (Ireland) ISA section, I am very aware of the personal and professional career rewards that come with active ISA membership involvement. Career development is a significant part of human development and spans an individual's entire life. It includes learning, work, leisure, and transitions to achieve a personally determined and evolving future. ISA is the best organization for career development in the automation profession, and, as many of us have learned, the more you contribute to the organization, the more value you receive.

ISA is continually advancing automation by providing opportunities for automation professionals to learn more, develop their careers, and help form the future of automation. This is accomplished in many ways, including opportunities to improve knowledge, skills, problem solving, leadership development, and friendship. Members develop and contribute through collaboration, mentorship, volunteerism, sponsorship, and student scholarships. I and many others have learned that contributing time, knowledge, and talents enhances our understanding and insights in unexpected ways.

ISA ecosystem

"Ecosystem" is a hot buzzword in business circles today, and the ISA organization is an ecosystem available to automation professionals, as ISA members, to advance their careers and the profession. I challenge you to be a member and make the most of, capitalize on, and benefit from the ISA ecosystem. In nature, an ecosystem is a community of living organisms interacting as a system in conjunction with the nonliving components of their environment (things like air, water, and mineral soil). ISA is an ecosystem of people focused on common goals and visions with a wide range of automation and control backgrounds, experience, and expertise. ISA provides a broad platform where members gain information and skills to improve operations, quality, and productivity, which are critical for manufacturers to compete.

The ISA ecosystem of automation profession members is a culture that helps members increase their knowledge, grow in their careers, and drive positive industry change. Leveraging what they learn, members can contribute entirely new value to their employers' operations, making them more successful. The ISA ecosystem resources include the ISA.org website, *InTech* magazine, Automation.com, books, standards, technical papers, webinars, ISA Interchange, training, and events. The most important part of the ISA ecosystem is ISA members who have a wealth of knowledge and experience.

ISA conferences and symposiums are a great example of bringing people together around topics that create focused ecosystems. ISA conferences and symposiums include the ISA Analysis Division Symposium (AD), Foundations of Alarm Management, ISA LDAR Fugitive Emissions Symposium, International Instrumentation Symposium (IIS), ISA POWID-EPRI Symposium, and ISA Water/Wastewater and Automatic Controls Symposium.

Symposiums and other events have great content value, but the interactions among people who share the same interests, challenges, and problems also bring an abundance of knowledge. I believe there is great value at these events where people interact formally and informally in conversations, creating lasting connections, and, in many cases, long-term friendships. In Judith E. Glaser's book, *Conversational Intelligence*, she talks about how conversations actually rewire our DNA and brain chemistry for mutual success. Over the years, these personal connections from events become your own specialized ecosystem of people with common interests and a storehouse of knowledge. In my experience, asking people in my ecosystem for ideas and thoughts proved invaluable for solving automation control problems and improving operations. Today, it is much easier to continually stay in touch and share with people you have met using email and the ISA LinkedIn group, which has more than 45,000 members.

Young and experienced benefit

Whether you are a young person just entering the workforce, new to the industry, or an experienced veteran, the ISA ecosystem can help you navigate industrial automation challenges and new technology. ISA continues to create opportunities for a younger generation of bright new minds to grow and meet the challenges of the future. ISA members and leadership continue to make decisions based on our future—not what we have done in the past. We cannot constrain ourselves to our past behavior and practices. Attracting new and younger leaders to the Society is important, because they bring new thinking and fresh perspectives that in an open environment, when combined with experienced leaders, create a much stronger organization and more value.

FAST FORWARD

- ISA gives automation professionals opportunities to learn more and develop their careers.
- It takes committed and passionate members in a network of peers to apply their talents and knowledge to assist others.
- You can get involved by being an ISA volunteer, contributing to the automation profession and your own development.

Diversity of thought

The automation industry is faced with rapid change and challenges, and the diversity of ISA members throughout industry is a great resource of experience, ideas, and know-how to deal with these changes in the automation industry. The broader ISA ecosystem outside of your organization is important for protecting against the dangers of a company becoming inwardly focused and not changing with the times. Companies that are completely inwardly focused run the risk of missing new opportunities for improvements and being blindsided by changes in the external reality.

Focused on the future

Clearly, ISA is an organization that is proud of its past but is firmly focused on the future. In setting the standard for automation and control, we are determined to constantly raise the bar. Evidence of new Society growth and new opportunities for all of us to learn, participate, and help shape the future of our profession and industry are all around us. The world of the automation professional is changing daily, affected by evolving and emerging new technologies and solutions that need to be applied in creative new ways. ISA is committed to adapting in this changing environment.

ISA continues to create opportunities for a younger generation of bright new minds to grow and meet the challenges of the future.

The roots of ISA are in the process industries, mainly petrochemical, pharmaceutical, and food and beverage. This is an important strength, and now other industry sectors are recognizing they benefit from leveraging and applying our expertise. There are many opportunities to make our intellectual property (IP) available to other segments of the economy involved in automation. In doing so, we can contribute to the improvement of other industries and make their services and solutions more valuable to their customers and end users. There are many opportunities to secure new members and customers by explaining and demonstrating value.

Members are at the heart of ISA. They truly "make" ISA possible. Without the members, we would not possess the IP that is so valuable to those in the automation profession. It takes committed and passionate members—working within a network of peers—to volunteer and apply their talents and knowledge to assist others.

We have so many strengths and so much knowledge that can benefit the world, to make it a better and safer place. So, why not do it?

We have so many strengths and so much knowledge that can benefit the world, to make it a better and safer place. So, why not do it? In the process, we will expand our membership base, add new customers, and grow. Building automation is an area that has expressed interest in our cybersecurity standards. By leading with our expertise in cybersecurity, we can explore other ways of providing service and value.

Given that there are so many new opportunities, we have to think a bit differently, modify what we do and how we do things, and accept change. We are not going to move away from our core strengths—in standards, training, publications, certificate and certification programs, and events—but we need to introduce new business models and delivery formats to meet the demands of an evolving world.

ISA sets the standard for automation by enabling automation professionals across the world to work for the benefit of all. The ISA Board knows with great staff, great volunteer leaders, members, customers, partners, and member support and commitment to ISA, we all can make a difference each day in improving ISA and shaping the future of the automation profession. Sometimes that difference begins with just a conversation with our peers and colleagues.

The advent of a new year is the ideal time to take a fresh look at all the different ways ISA members can get involved in ISA sections and divisions and support the organization's vision and mission.

ISA vision

ISA sets the standard for automation by enabling automation professionals across the world to work for the benefit of all.

ISA published mission

ISA's mission is to enable our members, including worldwide subject-matter experts, automation suppliers, and end users, to work together to develop and deliver the highest quality, unbiased automation information, including standards, training, publications, and certifications.

Will you answer?

Career growth comes from action. Your opportunity is to get involved by being a member and ISA volunteer contributing to the automation profession and your own development. ■

ABOUT THE AUTHOR

Brian Curtis (President@isa.org), the 2018 ISA president, is the operations manager for Veolia Energy Ireland, providing services to Novartis Ringaskiddy Ltd. in Cork, Ireland. He has more than 35 years of experience in the petrochemical, biotechnology, and bulk pharmaceutical industries, specializing in design, construction management, and commissioning of electrical, instrumentation, and automation control systems. He has managed complex engineering projects in Ireland, England, Belgium, the Netherlands, Italy, and Germany.

A long-time ISA member, Curtis has served on the ISA Executive Board since 2013, as well as the Geographic Assembly Board (2012–2015) and the Finance Committee (2013–2017). He was Ireland section president and vice president of District 12. Curtis has also been active on several Society task forces, including cybersecurity, governance, and globalization-related committees. He received the ISA Distinguished Society Service Award in 2010.

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


Endress+Hauser
We offer process application expertise through our products, solutions and services.
SUPPORT
+ SUCCESS
You optimize your process for maximum safety, reliability and efficiency, with minimum impact on the environment.

Why automation slept

By Paul J. Galeski, PE, CAP

ABOUT THE AUTHOR

Paul J. Galeski, PE, CAP (paul.galeski@mavtechglobal.com), is the president and founder of MAVERICK Technologies, LLC. The company specializes in high-level operational consulting and the development of automation strategy and implementation for automation technology. He is a contributing author to Aspatore Books' *Inside the Minds*, a series that examines C-level business intelligence. Galeski is currently vice president and general manager of global solutions and services with Rockwell Automation.

Process manufacturing has come a long way since the days of pneumatic and mechanical controls. Over the past several decades, firms have updated their equipment and operations, increasing capacity and improving quality by varying degrees. Typically, however, process plants and facilities have not been early adopters, and are reluctant to embrace state-of-the-art automation technology and methodologies. This slow-to-adopt approach has driven many of them to a critical crossroads: modernize or face inevitable decline.

As legacy systems age and supplier support for older equipment wanes, it is increasingly difficult to keep facilities up and running. In most cases, rip and replace is not a viable approach for manufacturers struggling to get or keep their competitive edge. With Industry 4.0 upon us and with Industrial Internet of Things, the cloud, mobility, open architecture, and advanced data analytics swiftly driving change, legacy factories are finding it more and more challenging to stay competitive.

Add to this the impact of the impending shortage of skilled workers in the engineering disciplines. As companies lose their long-term employees who have specialized operational knowledge, they will need to attract and retain top new talent to survive. Process operations, however, tend to maintain the status quo, hoping the workforce issue will just go away.

Millennials and the incoming workforce expect to work with smart, open, and flexible systems. They want a modern workplace they can intuitively understand, and they do not want to deal with archaic human-machine interfaces nor with other obsolete, complicated legacy systems.

Why do process facilities remain sleeping giants while technology takes quantum leaps forward? Simply stated: Risk avoidance and fear of change.

Long-term employees feel comfortable with their current systems; they understand how they work and how to troubleshoot them. The prevailing culture is to keep production going, using quick fixes to patch problems. While some users are interested in trying new technologies, many hesitate to take responsibility and the perceived risk of implementing something new.

For example, wireless technology is a game-changing innovation that industrial users have largely not adopted. Most consider wireless to be unreliable amid concerns about bandwidth, standards, integration, security, and overall performance. Today, wireless connections are still not commonly used in the industrial control environment but are widely accepted in many other applications.

How do we prevent the impending obsolescence of those plants, mills, and process facilities still operating on legacy systems?

Rather than bolting on "technology just for the sake of technology," process firms must now actively seek and implement the right solutions and work to overcome any internal cultural factors impeding modernization and forward progress.

For example, consider the benefits of adopting plug-and-play solutions to replace less efficient ways of accomplishing critical tasks. New data analytics solutions replace time-consuming spreadsheets used for analyzing big data. These browser-based solutions deliver better information faster and can be implemented quickly. Users can interact directly with the data and create visual representations, greatly increasing personal productivity and improving plant operations.

Look again at wireless as a quick and inexpensive way to add new points of measurement for less cost and in less time than with traditional wired solutions. These new measurement points automatically join self-configuring wireless mesh networks, sending data to control and monitoring systems that use the data to improve operations. Wireless technology can now be used for monitoring as well as for real-time control.

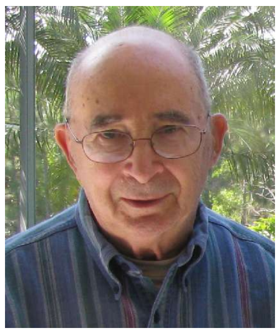
Even when the decision is made to improve and update operations through wireless or other new technologies, sorting through numerous supplier offerings and arriving at a fit-for-purpose solution within budget is time consuming and can be overwhelming. Partnering with a solutions provider who has domain experience and who fully understands modern automation solutions can make the difference between the business stalling out or moving forward.

The automation solutions provider must have the knowledge base and perspective to help evaluate each unique process and recommend appropriate improvements to develop a long-term modernization plan. It should have expertise on multiple platforms and in critical areas like migration, cybersecurity, and data analytics.

The technologies and consulting expertise are available to help our sleeping giants unleash their untapped production potential. The time is now for process industries to get more competitive, stay agile, and ensure their sustainability. But the clock is ticking, faster and faster. ■

Stanley Weiner – Humorist, author, and mentor

By Greg McMillan



I lost my best friend, co-author, and inspiration. Industry lost a "one of a kind" leader in the effective use of instrumentation in the process industry. **Stanley Weiner** passed away recently from Parkinson's disease complications.

Stan gave practical guidance by instruction and example and was a great advocate of using the best instrumentation despite potential budget limitations. He showed us how to do project estimates that could provide the best without being questioned.

He also introduced me to humor, making the whole experience fun. We shared insightful humor in a half dozen ISA books that opened minds and detailed lessons learned in the design, commissioning, and startup of decades of automation systems. We enlisted the help of plant and corporate engineers to write the humorous stories in *How to Become an Instrument Engineer – Part 1.523,* showing that humor can be contagious.

Along the way, we discovered the talented illustrator Ted Williams, who had a great sense of humor in his cartoons and creative touches. Ted created the cartoons for all of our books and our "Control Talk" column. The humor made learning necessary knowledge enjoyable and memorable—rather than challenging and tiring. Even spouses of automation engineers have been seen reading the books and smiling; they were gaining some understanding of what an instrument engineer is and does.

I hope, but do not expect, there will be more humorous books written by and for practitioners on the front lines in our profession. But there will never be another Stanley Weiner.

Editor's note:

ISA Fellow Stanley Weiner, a retired chemical engineer who worked at Monsanto, died on 16 February 2018 in Naples, Fla. In 1987, ISA made Weiner a Fellow for his outstanding contribution to the profession.

A collection of all six cartoon books by Weiner and McMillan is available on CD-ROM: *The Funny and Not So Funny Side of Life as an Automation Engineer.* The CD includes several recorded commentaries by McMillan and McMillan's out-of-print classic, *A Funny Thing Happened on the Way to the Control Room.* For more information, visit www.isa.org/cartoonCD.

CD titles *The Life and Times of an Automation Professional: An Illustrated Guide* (www.isa.org/autolife) and *The Funnier Side of Retirement for Engineers and People of the Technical Persuasion* (www.isa.org/retirement) are also available in print. Available in print (but not on the CD) is *101 Tips for a Successful Automation Career* (www.isa.org/101Tips). ■

New CAPs and CCSTs

Qualifying for and passing one of ISA's certification exams is a noteworthy accomplishment. The exams are rigorous and require a solid command of various disciplines in automation and control. On page 40 is a list of individuals who have recently passed either our Certified Automation Professional (CAP) or one of the three levels of our Certified Control System Technician (CCST) exam. Congratulations to our new certification holders! For more information about the ISA CAP and CCST certification programs, please visit www.isa.org/training-and-certifications/isa-certification.

ISA CERTIFIED AUTOMATION PROFESSIONAL®

CERTIFIED CONTROL SYSTEMS TECHNICIAN® ISA

In memoriam

ISA Fellow **Vincent Cushing, PhD,** passed away 1 February 2018 in Annapolis, Md. In 1983 Cushing received the Albert F. Sperry award for his "pioneering work in the theory, design, and application of electromagnetic flowmeters and in non-contact flowmetering." This ISA award recognized an outstanding technical, educational, or philosophical contribution to the science and technology of instrumentation, systems, and automation.

Cushing earned degrees in physics and mathematics from the University of Notre Dame and a doctorate in physics from the Illinois Institute of Technology. Early in his career he was a rocket scientist at Armour Research Foundation, where he developed and analyzed atomic weapons and high-altitude radiation measurements. He later founded the Engineering Physics Company, where he invented an insertable electromagnetic flowmeter and related technologies.

He was awarded 28 patents, presented technical papers at conferences around the world, oversaw installations of his instruments on ships, in pipes, over streams, and under Arctic ice, and established himself as the world's foremost authority on applications of magnetic induction.

Cushing saw the world through science and applied his engineering skills to solve any problem. His home is filled with inventions. Donations may be made to the Vincent and Marie Cushing Scholarship Fund at the University of Notre Dame. ■

Certified Control System Technicians

Level 1

Gregory T. Glover
U.S.

Matthew L. Jones
U.S.

Eric D. Moore
U.S.

Larry Presley
U.S.

Kenneth L. Woods
U.S.

Matthew C. Boros
U.S.

Kenneth A. Hutton
U.S.

Stephen G. LaGrange
U.S.

Michael J. McGarry
U.S.

Bradley J. Mentzer
U.S.

Cameron W. McGuire
Holly Frontier Refinery
U.S.

Brandon J. Summers
Turnkey Instrument Solutions
U.S.

Joshua A. Vaneck
U.S.

Jeffrey C. Diersing
U.S.

Gary L. Carr
Greater Cincinnati Water Works
U.S.

Nicholas R. Hughes
U.S.

Lenny R. Matthews
U.S.

Ethan A. Haas
U.S.

Aaron M. Maki
Regeneron Pharmaceuticals
U.S.

Steven A. Culver
U.S.

Shawn C. Riper
U.S.

Aaron R. Eakin
U.S.

Todd N. Ellis
U.S.

Duston R. Marsh
U.S.

Phillip J. Steinhiser
U.S.

Richard Dean West
U.S.

James Lamont Taylor
BP Husky Refining, LLC
U.S.

Jeffrey Ray Anderson
Micron Technology Inc.
U.S.

Michael L. Balls
Micron Technology Inc.
U.S.

Timothy H. Olando
Process Control Services
U.S.

Marco A. Albor
U.S.

Jonathan M. Mungcal
U.S.

Roel B. Ponlaroche
U.S.

Barry A. Miller
U.S.

Adam J. Allfree
Kansas City Board of Public Utilities
U.S.

Lyle D. Hermreck
Kansas City Board of Public Utilities
U.S.

Christopher M. Hosbach
General Control Systems
U.S.

Carter S. Long
U.S.

Toby L. Short
C&W Services
U.S.

Brett E. Birchmier
U.S.

Anthony G. Gilland
U.S.

Matthew A. Poe
U.S.

Bryan R. Ewing
U.S.

Brian Contino
MarkWest
U.S.

Christopher L. Harkleroad
U.S.

Jacob W. Henke
U.S.

Charles J. Kammerdiener
U.S.

Jerad E. Louzy
U.S.

David Stanley Atkisson
Upper Occoquan Service Authority
U.S.

Steven R. Mongeon
U.S.

Benjamin R. Hinojosa
U.S.

Michael J. Roach
U.S.

Steve F. Cooley
California Motor Controls
U.S.

Zachary T. Chamelin
Dominion Energy
U.S.

Lonnie J. Stephenson
U.S.

Michael William Corey Pritt
U.S.

Haley A. Parker
City of San Luis Obispo
U.S.

Bryan M. Scott
U.S.

Hatim Abdelaal Ahmed
DC Pro Engineering
U.A.E.

Isaac Gonzalez
Regeneron Pharmaceutical
U.S.

Chad Paxson
Cobb County Water System
U.S.

Chad C. Friesenhahn
Williams Midstream
U.S.

Neil Hedderson
Ushitau
Canada

Benjamin J. Smith
U.S.

Brad R. Hendrickson
Nestle Gerber
U.S.

Steve L. Mullennix
U.S.

Zachariah Lee Christoffersen
U.S.

James Marshall
U.S.

Robert J. Meyer
U.S.

Robert T. Radomski
U.S.

Ronald L. Temple
U.S.

Nabta Kamal Mohammed Elmoubark
DC Pro Engineering
U.A.E.

Blaine G. Joiner
U.S.

Jeffrey W. Motta
U.S.

Mitchell Higdon
U.S.

Level 2

Sean C. O'Connor
DC Water
U.S.

Clinton W. Poca
U.S.

Dean R. Prentice
U.S.

Joseph John Andrew
U.S.

Daniel J. Randall
U.S.

Jeremy S. Kibler
U.S.

Christopher J. Bubon
Ingredion
U.S.

Ellery B. Raitt
Lonza Biologics
U.S.

Micah J. M. Dudley
UTC Aerospace System
U.S.

Chad N. Allen
U.S.

Roman A. Rangel
Metro Water Waste Reclamation District
U.S.

Nicholas Korzie
U.S.

Daniel W. Mos
Epcor Water Services
Canada

Chad W. Bonnett
U.S.

Level 3

Willie A. Williams
U.S.

Philip J. Hart
West-Ward Pharmaceuticals
U.S.

Joshua R. Bean
Linde
U.S.

Mark J. Pyle
Flint Hills Resources
U.S.

Burt C. Jagdeo
U.S.

Mark V. Sturgell
Metro Waste Water Reclamation District
U.S.

Ryan E. Robinson
MWRD
U.S.

Patrick D. Pittman
Flint Hill Resources
U.S.

Erik Stephens Jurgens
U.S.

Certified Automation Professionals

Fabio de Oliveira Alves
Brazil

Derek T. Norton
U.S.

Hani Joudah
Saudi Arabia

Jarid J. Orgeron
U.S.

Dave G. Meyer
Canada

Christopher T. Simmers
American Water
U.S.

Cody P. Bennett
U.S.

Mohamed A. Alemam
Novatech
U.S.

Jose Raymundo B. Jojie Lopez
U.S.

Abdulrhman Alwhibi
SWCC
Saudi Arabia

Hock-Chee Lee
The Dow Co.
U.S.

Stephen Goodwin
Canada

Michael S. Brown
Williams
U.S.

Vijaykumar M. Prajapati
Saudi Aramco
Saudi Arabia

Ahmed Mohamed Salih Osman
Malaysia

Domenic C. Palazzolo
Palazzolo Industrial Control LLC
U.S.

Rohitkumar R. Sidpara
Qatar Fertiliser Co.
Qatar

ISA Certified Automation Professional (CAP) program

CAP question

How are the maintainability and maintenance of automation systems related?

A. Maintainability is a front-end, design outcome; maintenance is related to ongoing system availability.
B. Maintainability is related to system availability; maintenance is related to traceability and warranties.
C. Maintainability is a front-end engineering function; maintenance is an ongoing engineering function.
D. Maintainability is related to malfunctions; maintenance is related to service quality.

CAP answer

The correct answer is *A*, "Maintainability is a front-end, design outcome; maintenance is related to ongoing system availability." Maintainability is the probability that a device will be restored to an operating condition within a specified period when maintenance is done with prescribed resources and procedures. It can also refer to the inherent characteristic of a design or installation that determines the ease, economy, safety, and accuracy with which maintenance actions can be performed on it.

As such, maintainability should be addressed during the front-end engineering and design phase of a project, so these characteristics are built in to the process. This includes addressing items like accessibility for removing pumps, piping, and instruments; complete documentation and procedures; availability of spare parts; personnel training and qualification; and suitability for purpose.

Maintenance is what is performed on a system to ensure that it remains in good working condition, but also, if a failure should occur, maintenance is the mechanism used to return the system to the previous working condition.

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

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

ISA Certified Control Systems Technician (CCST) program

CCST question

When using the parity system to detect transmission errors, the parity bit is set to a "1" or a "0" based on the content of the:

A. bits in the data word
B. start bit and bits in the data word
C. bits in the data word, including parity
D. bits in the data word, parity, and the stop bit

CCST answer

The correct answer is *A*, "bits in the data word." Parity is a simple method using a binary code ("1" or "0") to detect data transmission errors by making the sum of the "1" bits in the source data either an odd or an even number. The calculated parity bit is then appended to the end of the data stream.

For example, if the following data word is to have "even parity," the parity bit would be set to "1" in order for there to be an overall "even number" of bits set to "1":

1 1 0 1 1 0 1 parity bit = 1

The resulting data, with the parity bit, would be: 1 1 0 1 1 0 1 1 (total of six "1" bits).

The receiving device strips off the parity bit, recalculates the parity, and compares the result to the parity bit received. If it matches, it is assumed that the received data and the sent data match. If not, an error (parity error) is flagged. For communication to occur, both the sender and receiver must be configured for the same sense of parity (both odd or both even).

Since there are five "1" bits in the original word, the parity bit for "odd parity" is a "0."

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

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.

Closed-loop control troubleshooting

By Jacques Smuts, PhD, PE

Every plant in the process industry most likely has several control loops that do not perform well. Although there are many factors that may negatively affect control loop performance, a few of these factors are most common. With some skill and knowledge, it is reasonably easy to identify which of these common factors is the root cause of poor control loop performance.

With closed-loop control, poor performance typically manifests itself as deviations from set point. By analyzing these deviations, one can determine if they are caused by suboptimal controller tuning settings, a poorly performing control valve, insufficient filtering of the measurement signal, or simply process disturbances where the frequency and magnitude exceed the regulatory capabilities of a control loop. The diagram (figure 1) can be used as a troubleshooting tool to help determine the root cause of poor control loop performance.

Much of the troubleshooting that follows requires looking at process trends. Normally these are time trends of the process variable (PV), set point (SP), and controller output (CO). The time span of the trends depends on the dynamic nature of the process—fast-responding processes, such as flow and liquid pressure, require only a few minutes of data for proper analysis, while slow-responding processes may require data spanning several hours. Control systems have built-in or add-on process historians that can be used for viewing process trends.

Oscillations

The first step in troubleshooting poor control is to determine if the deviations of the PV from its SP are random or cyclical in nature. With cyclical deviations, or oscillations, the PV peaks at fairly regular intervals. Random deviations do not have this regularity (figure 2). A visual inspection of the PV trend is all that is required to make this determination.

Once it has been determined that the control loop is oscillating, one should determine the origin of the oscillation. A control loop can be causing its own oscillation, or it could be affected by an interacting oscillation somewhere else in the process. A simple way to determine if the origin of the oscillation lies within the control loop or has an external source is to put the control loop in manual to see if the oscillation stops or continues. If the oscillation continues, it is likely caused by an external source. The exception here is if the control valve's positioner oscillates by itself. This can be determined by leaving the controller in manual mode, going out to the valve in the field, and seeing if the valve stem is oscillating.

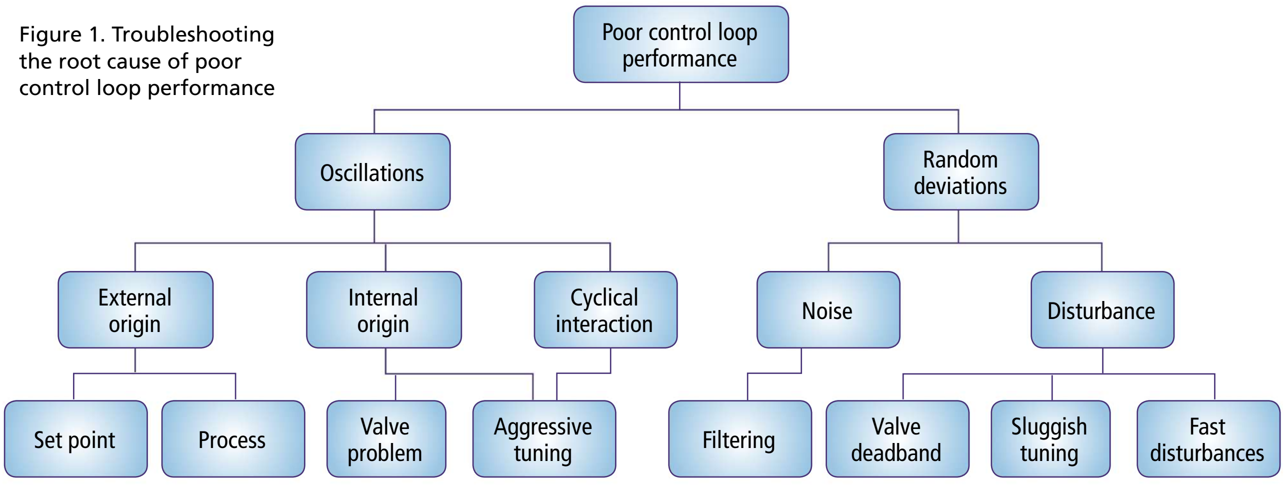


Figure 1. Troubleshooting the root cause of poor control loop performance

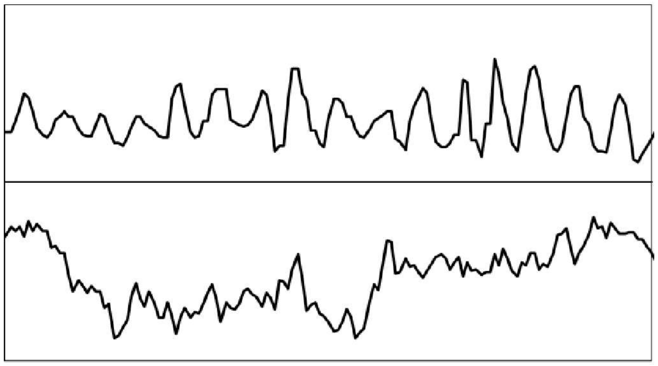


Figure 2. Oscillations (top trend) versus random deviations (bottom trend)

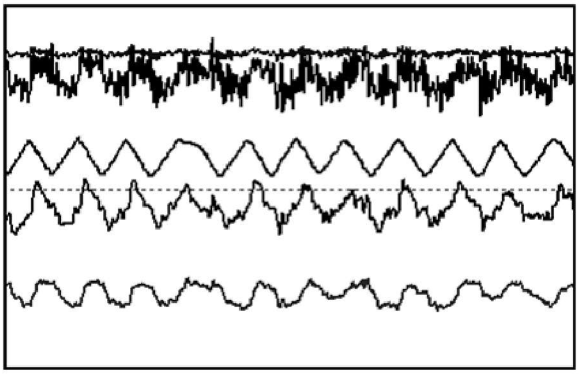


Figure 3. The triangular wave (middle trend) leads the other oscillations and has the least distortion.

An external source of oscillation could affect a control loop through the process or via the SP (if the latter is generated by another controller). This determination can be made by looking at a trend of the SP. It should be easy to see if the SP oscillates. If the SP is oscillating, the control loop generating the set point should be checked, as described later.

If the oscillation is coming from the process, a bit more detective work is needed. Trends of all the possible interacting process variables need to be inspected. With highly interactive processes, several control loops may be oscillating at the same frequency. The root cause of multiple oscillations can normally be found by looking at the trends to see which one of them peaks first. This can also be combined with looking at which signal has the least distortion (the crispest or cleanest oscillation, such as the triangular wave in figure 3). The oscillation leading the others and having the least distortion is most likely the cause of all the other oscillations. One can then troubleshoot the source of oscillation further, as described below.

Once the exact loop causing the oscillation has been identified, the root cause can be determined through a few simple steps. The oscillation can have one of two causes: incorrect tuning or a control valve problem. If the control loop is oscillating because of tuning, trends of the PV and CO are normally smooth sine waves (except if the CO runs into upper or lower limits). If a control valve problem is causing the oscillation, a trend of the CO more closely resembles a triangular wave, while the PV more closely resembles a square wave (figure 4). Control valve stiction is a common cause of control loop oscillations, and being a valve problem, it needs to be addressed through control valve maintenance or positioner tuning. When incorrect tuning settings cause a control loop to oscillate, the PID controller needs to be tuned again, preferably by using a scientific tuning method, not trial and error.

Another scenario to consider is when two or more closely coupled control loops cause each other to oscillate. For example, if a pressure-reducing control loop is closely followed in the process by a flow control loop, the two control loops can appear to be fighting each other, causing both loops to oscillate. If either one of the controllers is put in manual, both control loops cease to oscillate. In this case, the most important control loop needs to be tuned for a fast response, and the other loop tuned to respond three to five times slower. The lambda tuning method lends itself well to tuning the second loop for a slow response.

Random deviations

Now on to the case in which the PV deviates from its SP in a random (nonoscillatory) fashion. If the deviations occur very rapidly, much faster than the control loop can respond, the deviations can be considered to be noise. The best solution for PV noise is to apply a small filter, such as a first-order lag filter, to the signal. Note that a filter changes the dynamics of the control loop, and consequently the controller has to be tuned again.

If the deviations are too slow in nature to be considered noise, a filter should not be applied. Because the PV deviates relatively slowly from its SP, the controller may seem to respond to it too slowly, allowing large deviations before gaining control over the process. This is likely a result of sluggish tuning, which calls for the controller to be tuned again for a faster response if possible (as explained later).

Note that deadband in the control valve may create the appearance of the controller responding sluggishly. It takes a while for the controller to traverse the deadband before the control valve actually starts responding and affecting the process. In this case, controller tuning is not the right solution for the problem, since deadband is a mechanical issue with the control valve. The presence of deadband in a control valve can be determined by putting the controller in manual mode and making two CO changes in one direction, and a third change in the opposite direction. Make the second and final steps equal in size and wait for the PV to settle out after every step. If, after the final step, the PV does not return to the same value as after the first step, deadband exists in the control valve (figure 5).

Also realize that every control loop has a limit on its speed of response. If this limit is exceeded by tuning the controller for too fast of a response, the control loop will become unstable and oscillate. Best practices for controller tuning recommends leaving a healthy margin away from the stability limit. If a controller has been tuned properly, and deviations of PV from the SP are still excessive, it may be the result of the disturbances being too severe to be handled solely by feedback control. Depending on the cause of the disturbance, adding cascade, feedforward, or ratio control to the control design could make a significant improvement. ■

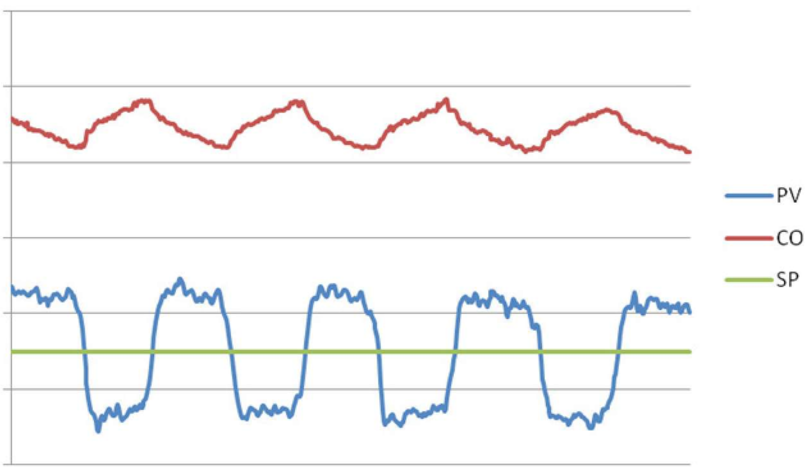


Figure 4. Control loop oscillation caused by stiction

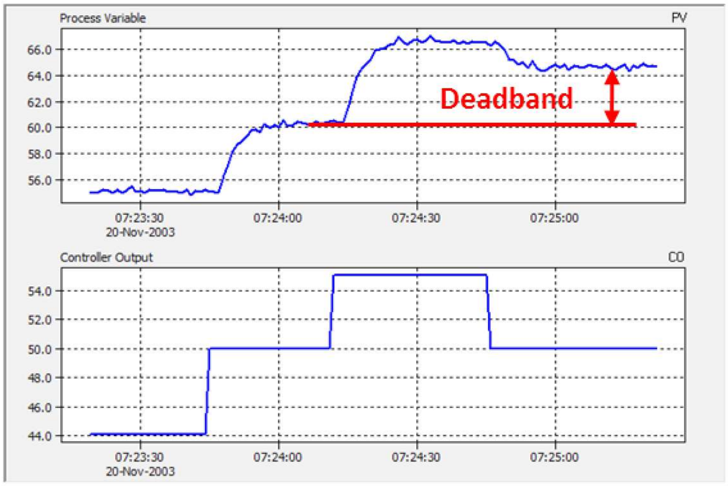


Figure 5. Control valve deadband test

ABOUT THE AUTHOR

Jacques Smuts, PhD, PE (jsmuts@opticontrols.com), is the founder and principal consultant of OptiControls, Inc. He has more than 25 years of experience in process control and is the author of the book *Process Control for Practitioners*.

So many security breaches! Are we focusing on the wrong things?

By Paul Rostick

We obsess over tools and technologies when we should be focused on culture and commitment. In the recent Equifax breach, which affected more than 143 million people, a routine security patch was not applied to a critical server. In the Target breach, which cost that company over $200 million dollars, a vendor's remote access was not properly managed, and the information technology (IT) department ignored clear signs that the network was compromised. The Russian hackers who shut down the Ukrainian electric grid, affecting more than 80,000 customers, used phishing emails to trick users and steal their network accounts. And in what may be one of the scariest industrial security incidents so far, unknown hackers who compromised a Schneider Electric Triconex safety controller in Saudi Arabia reached their target because an engineering workstation was not properly isolated and secured.

Organizational failure

What these breaches, and thousands of others, have in common is this: They were not caused by a failure of technology—they were caused by a failure of the organization. You can be certain that all of these companies had some kind of cybersecurity policy, yet at the moment of greatest need they were unable to defend themselves. We see this pattern again and again—without a foundational security culture mandated by a clear executive commitment, cybersecurity efforts continue to fail, often miserably, and at great cost. This should be unacceptable.

Why do we obsess over security controls and not over security culture? Because controls are easy, and culture is hard. Anyone can write policies; you can find free templates on the Internet. Buying tools is fun, and any competent technician can install them. We get a sense of accomplishing something.

Changing an organization's culture requires far more effort to accomplish and far more energy to sustain. Culture cannot be delegated to technicians—it is the responsibility of the C-suite. The irony is that we already learned this lesson from safety. We know that people will not necessarily behave safely. Left to human nature and the pressures of deadlines and costs, people, including management, take shortcuts, and soon people get hurt—or worse. As a result, we do not just buy hardhats, we *instill* culture. "Do it safely, brother. Everyone goes home."

Because safety and security are two sides of the same coin, one would think we would pick up on this correlation more clearly. Though we earnestly write policies, install tools, do assessments, and try to implement controls—we see from these breaches that without the sustaining culture, these efforts will unravel, just like safety unravels without its sustaining culture. If you are responsible for security, you cannot be everywhere reviewing every design and counseling every technician, every integrator, every engineer, and every operator on the myriad security implications of every action. The culture itself must do this. Security awareness and knowledge and skills and commitment must pervade the very fabric of the organization—just like safety. As the saying goes, *if it isn't secure, it isn't safe.*

And what about new projects? When you raise a warning about a potentially insecure design, will anyone hear you over the din of the project deadline? The safety guy can throw the red flag—can you? Not without a security culture.

Culture and commitment

As someone who built an industrial cybersecurity program from scratch, I have these lessons burned into my brain. You cannot truly fix a problem if you treat symptoms. Only correcting the root cause will fix the problem permanently. The root cause failure that led to all those breaches, and all the breaches yet to come, is the lack of a security culture and a corresponding executive commitment to make security a core competency. For security to be an organization's core competency, you need an executive sponsor and a champion (preferably the CEO) who will advocate for the appropriate governance, funding, staffing, and training to create a real security program alongside your real safety program. If your executive has not made a clear commitment to a security culture, then at the worst moment, the organization will likely fail as have so many others. No one should be surprised when that happens. In any complex endeavor, without the necessary foundations of success, failure is practically preordained. Security is no exception.

I am not arguing against security controls, or tools or technologies, or policies or procedures or practices. They are necessary and critical—but they are not sufficient. They are not foundational. Security is not a thing; it is a management outcome, and there is no magic here: Culture and Commitment = Outcome. ■

ABOUT THE AUTHOR

Paul Rostick (paul.rostick@aesolns.com) is the chief information security officer and industrial cybersecurity advisor for aeSolutions (www.aesolns.com), a member of Control System Integrators Association (CSIA) (www.controlsys.org). In this dual role he advises both his own executives and customer executives on establishing strategic IT/OT cybersecurity programs.

New ISA99 standard on developing products that are cybersecure by design

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), is designed to provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

A newly published standard in the series, ISA-62443-4-1, *Security for Industrial Automation and Control Systems Part 4-1: Product Security Development Life-Cycle Requirements*, specifies process requirements for the secure development of products used in an IACS. It defines a secure development life cycle for developing and maintaining secure products. The life cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management, and product end-of-life.

These requirements can be applied to new or existing processes for developing, maintaining, and retiring hardware, software, or firmware. The requirements apply to the developer and maintainer of a product, but not to the integrator or user of the product.

"Designing security into products from the beginning of the development life cycle is critical, because it can help eliminate vulnerabilities from products before they ever reach the field," emphasizes Michael Medoff of exida, who led the ISA99 development group for the standard. "We all know how difficult and expensive it can be to constantly have to patch software in the field. The new standard gives us a real opportunity to break the cycle of frequent security patches and to produce products that are secure by design."

Also coming in 2018

Two additional standards in the ISA 62443 series are expected to be published in the coming months. The first, ISA/IEC 62443-3-2: *Security Risk Assessment, System Partitioning and Security Levels*, is based on the understanding that IACS security is a matter of risk management. Each IACS presents a different risk to an organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. Further, each organization that owns and operates an IACS has a different tolerance for risk.

For these reasons, ISA/IEC 62443-3-2 will define a set of engineering measures to guide an organization through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels. A key concept is the application of IACS security zones and conduits, which were introduced in ISA/IEC 62443-1-1: *Concepts and Models*. The new standard is a basis for specifying security countermeasures by aligning the identified target security level with the required security level capabilities specified in ISA/IEC 62443-3-3: *System Security Requirements and Security Levels*.

The second standard, ISA-62443-4-2: *Technical Security Requirements for IACS Components*, will provide the cybersecurity technical requirements for the components that make up an IACS, specifically the embedded devices, network components, host components, and software applications. This document, which derives its requirements from the IACS security requirements of ISA/IEC 62443-3-3, will specify security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.

In addition, ISA99 has begun working on converting ISA-TR62443-2-3, *Patch Management in the IACS Environment*, into a standard by adding normative language. The current technical report addresses the installation of patches, also called software updates, software upgrades, firmware upgrades, service packs, hotfixes, basic input/output system updates, and other digital electronic program updates that resolve bug fixes, operability, reliability, and cybersecurity vulnerabilities. It covers many of the problems and industry concerns associated with IACS patch management for asset owners and IACS product suppliers. It also describes the effects poor patch management can have on the reliability and operability of an IACS.

The technical report provides a defined format for the exchange of information about security patches from asset owners to IACS product suppliers, and definitions of activities associated with the development of the patch information by IACS product suppliers and deployment of the patches by asset owners. The exchange format and activities are defined for use in security-related patches, but may also be applicable to other types of patches or updates.

For information on viewing or obtaining any of the ISA/IEC 62443 standards, visit www.isa.org/findstandards. For information on ISA99 and the ISA/IEC 62443 series of cybersecurity standards, contact Eliana Brazda, ISA Standards, ebrazda@isa.org or +1-919-990-9200. ■

Edge programmable controller

The "groov" EPIC system combines I/O, control, data processing, and visualization into one secure, maintainable, edge-of-network industrial system. Combining intelligent I/O with an embedded Linux real-time controller, gateway functions, and an integrated display, the device will be of particular interest for process control, machine control, original equipment manufacturers, manufacturing, SCADA/RTU, building and facilities, and IIoT applications. Commercial, retail, warehousing, and distribution customers will also find that the system opens a variety of options for tracking, storing, and visualizing data.

Optional access to the Linux operating system through secure shell (SSH) is available. This access, along with toolchains and interpreters for Java, C/C++, Python, and JavaScript/Node.js, allows OEM developers to execute custom-developed applications on this edge processing control system.

The system is also approved for UL hazardous locations, is ATEX compliant, and has an integrated color touchscreen with HDMI output for an optional external monitor. It has an integrated power supply and dead-front design. There is onboard system configuration, commissioning, and troubleshooting and remote configuration and troubleshooting from any Web browser on any device.

Opto 22
www.opto22.com

Industrial controller

The IC-3173 industrial controller is the company's first IP67-rated controller and is suited to act as an IIoT edge node in harsh locations, including spray down manufacturing environments, test cells, and outdoor locations without the need for a protective enclosure. These controllers have up to a 2.2-GHz Intel Core i7 dual-core processor, 8-GB DDR3 RAM, 64-GB storage, four Power over Ethernet (PoE) GigE ports, two USB 3.0 ports, and two display ports in a design with no moving parts. Industrial controllers also include a user-programmable Xilinx Kintex-7 FPGA, which improves system performance with custom I/O timing, synchronization, control, and image coprocessing capabilities.

National Instruments
www.ni.com

Dual-redundancy controller

The PACSystems RX3i CPE400 has dual redundancy and can function in high temperatures. The CPE400 is suitable for applications in oil and gas, water and wastewater, and other infrastructure industries with assets requiring smaller footprints. The CPE400 is also effective in applications requiring rugged controls; it operates in a temperature range from –40°C to +70°C and supports a conformal coated option for corrosive environments. The redundancy is powered by the PACSystems High Availability solution over Profinet and uses embedded Ethernet technology. The controller also provides a secure, authenticated data transfer from the industrial asset to the cloud over encrypted channels. It is differentiated by not only its processing capability, but also by a control dual-redundancy solution that makes it possible to perform maintenance and application updates while the application is running.

GE
www.geautomation.com

Programmable logic controller

The MicroSmart FC6A Plus is a PLC with up to 2,060 local I/O. With its expanded I/O capacity, the FC6A Plus can control and monitor machines or small-scale manufacturing facilities. It can execute basic instructions in 21 nanoseconds, and program memory is 800 kB (100 K steps), so the FC6A Plus can handle large programs with complex control requirements, such as PID, flow totalization, and recipes.

Two models are available, each with 24 VDC input power. The 16 I/O model has eight inputs and eight relay or transistor outputs. The 32 I/O model has 16 inputs and 16 transistor outputs. Each model also includes an integral 0–10 VDC analog input with 12-bit resolution and can accommodate up to three plug-in discrete, analog, serial communication, or Bluetooth cartridges. Each discrete cartridge has four discrete I/O points, either four inputs or four outputs. Each analog cartridge has two analog I/O points, either two inputs or two outputs.

IDEC Corporation
www.idec.com

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.

USB HART MODEM

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

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

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

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.

IT industrial controls engineer

Denver Water: Under general supervision, the IT industrial controls engineer performs technical engineering-related duties to maintain, design, and commission the hardware, software, and communication systems for Denver Water's industrial control systems. He or she will modify drawings and associated software documentation to accurately represent existing controls systems and coordinate with operations to ensure successful acceptance and use of control system solutions. The position requires a bachelor's degree in engineering, computer science, or a related field; at least four years of related work experience; or an equivalent combination of training, education, and experience that provides the required skills and knowledge . . . see more at Jobs.isa.org.

Plant engineer

JM Huber: The plant engineer in Fairmont, Ga., leads the maintenance department, supports plant operations, directly manages the maintenance supervisor, identifies and evaluates process improvements and new technologies, and implements projects to improve production. The position requires approximately 10 percent travel. A four-year engineering degree with at least five years of experience in manufacturing is required. Experience in mineral processing or the chemical process industries is strongly preferred and experience in unit operations, such as particle size reduction, classification, bulk material handling, pneumatic conveying, and powder drying and processing, is preferred . . . see more at Jobs.isa.org.

Mechanical engineer

Auburn University: The individual in this position in Auburn, Ala., provides mechanical engineering services and review of work, as well as troubleshooting existing mechanical systems to resolve problems. The engineer reviews and manages moderate to complex designs and technical drawings created by outside consultants, provides mechanical engineering support for construction and maintenance projects on campus buildings and systems, and designs and fabricates experimental apparatus in support of research projects. The position requires a bachelor's degree in mechanical engineering, four years of professional experience, and a valid driver's license . . . see more at Jobs.isa.org.

Software engineer intern

Hewlett Packard Enterprise: Internship positions are available in test automation, cloud automation, wireless/AP, and other types of engineering. Applicants must be actively pursuing a BS or MS in computer science, computer engineering, or a related degree program and must be at least a junior. Programming coursework must have included one or more of the following: C, C++, Java, JavaScript, Python, and the student must have a GPA of 3.5 or higher. Knowledge of servers, IoT products, software development methodologies, and version control software is a plus . . . see more at Jobs.isa.org.

Securing the IIoT: Collaboration can win the day

By Chris Lyden

ABOUT THE AUTHOR
Chris Lyden (americas.marketing@schneider-electric.com) is senior vice president, strategy, for Schneider Electric's Process Automation business. He is responsible for the business unit's strategic planning process; product and technology road map and vision; mergers and acquisitions pipeline; and industry applications consulting.

Just as new innovations and technology have helped industrial manufacturers improve operations, advancements in technology have emboldened a new generation of malicious actors to attempt far more innovative, aggressive, and dangerous cybersecurity attacks.

Not long ago, industrial information technology (IT) and operational technology (OT) were isolated. The hardware and software systems that monitor and control physical equipment were independent from the computers, systems, and applications that process and store operating and business data.

But now the IIoT is transforming how manufacturing and process plants control and manage operations. Connectivity, networking, big data, predictive analytics, cloud computing, edge computing, and the like are gaining acceptance. The line between IT and OT is blurring, so connectivity has become both inescapable and necessary. Yet it also widens access points for hackers. Cybersecurity threats come from every direction. Operations networks not built for connectivity are being connected, and security protocols are ignored for the benefit of data access. The threat vector now extends even to base-level assets. Attackers can target anything from a connected toaster to a wireless field device. It is a new type of cyberattack for industrial control systems (ICSs), which are increasingly accessible over the Internet.

The actors have also changed. Attackers are becoming more sophisticated. Attack techniques are readily available on the dark web, so low-level cybercriminals can access the necessary information for level-4 attacks. Motivations have changed, too; it is not always about money. Notoriety is also prized. And then there are nation-state perpetrators, who have emerged as our most dangerous threat.

We are facing a geopolitical climate where malicious actors have unlimited resources to carry out cyberattacks. That means industry players need to come together to improve our overall cybersecurity culture and hygiene. But where do we begin?

Multipronged approach

As an industry, we must take a multipronged approach to security threats. First, vendors have to reinforce their commitments to making products stronger and to educating end users on inherent product cybersecurity features. Organizations need to adhere to security best practices, identify threats, and respond accordingly. They should strengthen their own site security protocols, while maintaining the documented procedures from systems, solutions, and software suppliers.

Cybersecurity is a journey, not a destination. More than just technology, it must be accompanied by regular employee training, ongoing risk and threat assessments, firmware updates, maintenance of software and hardware, and procedure and change control. The old adage "an ounce of protection is worth a pound of cure" could not be more true in preventing cyberattacks. Unfortunately, cybersecurity funding and resources often become available only after an attack. Instead, to address continuous threats, the industry needs to invest now in our people, with better training and education, and in our ICS technologies.

Second, we all—suppliers, end users, third-party providers, integrators, standards bodies, and other industry organizations and government agencies—have to come together to put into place stronger unifying standards and practices. From there, we have to be aware of these standards and implement and always adhere to them, regardless of industry or type of facility. Lax adherence to cybersecurity protocols is widespread. Everyone must implement tighter basic cybersecurity controls and practices, but there is also a deeper need for more robust security reviews within all ICS and embedded device systems.

Third, we need new levels of collaboration and openness. For true change, industry leaders must commit to transparency that promotes openness across competitive lines. Cybersecurity is not limited to a single company, industry, or region. It is an international threat to public safety that can only be addressed and resolved through collaboration.

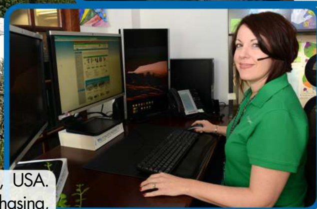
In the face of increasingly bold attacks perpetrated by malicious actors with unlimited time and resources, everyone must participate in open conversations and drive new approaches that allow installed and new technology to combat the highest-level cyberattacks.

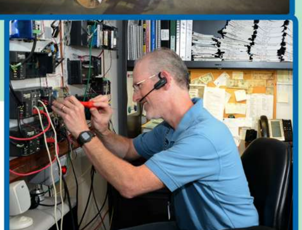
We must not be paralyzed by fear, but we must not be complacent, either. The time for an industrywide initiative to address highest-level attacks is now. The entire industry must collaborate openly to educate and train our workforce, strengthen our technology, and install and adhere to stronger unifying standards. This is the clearest path toward ensuring the safety and security of the world's infrastructure and the long-term protection of the people, communities, and environment we serve. ■

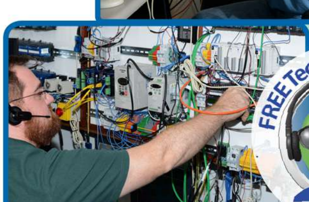

GET MORE THAN
YOU PAY FOR ...
Order Today, Ships Today
FREE shipping - orders over $49
2-day Shipping
FREE Technical Support
Located in USA
Voted Best in Service - 15 years straight
VOTED Best in SERVICE 15 YEARS
FREE software and manuals
30-day Money-Back Guarantee
30 day
from AUTOMATIONDIRECT.com
The common sense way to buy industrial controls.

and Warehouses

es north of Atlanta, GA, USA.
nical support teams, purchasing,
houses and speedy logistics team.







service

ent!

aced us at
one, we've been
rs in a row.

information
lecision.
ndreds

online.

ng our products after
esn't make sense.

quickly
ct you're
w.

C and HMI
for intuitive

we try to
mber of our most
ries controllers,
to deal with,

EE CAD

Direct.com

This ".com" is powered by ".awesomepeople"!

For over twenty years our sole focus has been customer service. That takes many forms: great prices, fast delivery, and quality products. But regardless of our product selection and other tangibles like pricing, the intangible value of customer service is something that cannot be faked, automated or glossed over.

Our team members here at AutomationDirect.com approach every day with this one goal in mind - serve the customer. It's a simple philosophy that many companies forget or make too complex and fail at. If the answer to any decision is **"Yes, this is good for our customers"**, then we do it.

It's common sense.

"Should we have real upfront pricing online and realtime stock availability?
Yes, this is good for our customers."

"Should we have FREE tech support before, during, and after any sale instead of charging yearly fees for tech support?
Yes, this is good for our customers."

"Should we offer FREE software on many products instead of charging licensing fees?
Yes, this is good for our customers."

"Should we have all our documentation online for FREE so people can access anytime, even before they choose to purchase?
Yes, this is good for our customers."

"Should we offer more selection by consistently introducing more new quality products with great prices monthly, sometimes weekly?
Yes, this is good for our customers."

"Should we offer FREE shipping for orders over $49?
Yes, this is good for our customers."

"Should we be fiscally responsible and run an efficient business so customers can rely on us decade after decade after decade?
Yes, this is good for our customers."

All these are discussions we've had internally and all have had certain aspects of "can we do that?", "that will be hard to accomplish", "no one else is doing that, how can we?". But if you bring it back to the simple answer, "Yes, this is good for our customers", then the perceived obstacles really don't matter.

Our company has evolved dramatically since 1994 and it's this type of decision making by all our team members over the years that keeps our customers coming back and new customers checking us out daily.

If you're a current customer, we sincerely thank you for your business. We wouldn't be here if it wasn't for you and promise to do our best for you every day. If you're new and checking us out for the first time, we hope you give us an opportunity to serve you.

AUTOMATIONDIRECT.com