August 2021

InTech

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

Machine modularity for mass customization

Alarm management program upgrade

Power quality measurement

Homebrew automation

Digital Twins Enable the Autonomous Paper Mill

www.isa.org/intech

InTech

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.

ISSN 0192-303X

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

Volume 68, Issue 4

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

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

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

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

Printed in the U.S.A.

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

To order reprints of *InTech* print or digital articles, contact Jill Kaletha at 1 800 428 3340 x149 or jkaletha@mossbergco.com.

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

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.

From Industrial Automation to Industrial Autonomy

By Renee Bassett, *InTech* Chief Editor

"As they digitally transform, many plants are in the early stages of the journey from industrial automation to industrial autonomy," says Kevin McMillen, president and CEO of Yokogawa Corporation of America. "The move to industrial autonomy has gained momentum due to the impact of COVID-19 and is at the forefront of efforts to improve worker productivity, quality, and safety."

McMillen says the results of digital transformation will "range from a connected, empowered workforce to highly agile operations that can rapidly adapt and respond to market dynamics." And he's not alone.

In the AUTOMATION 2021 Special Report released this month, Automation.com's Bill Lydon identifies the "digitalization dozen—12 trends manifesting the manufacturing digital revolution." From edge computing to modular machine design to 5G wireless communications and more, these trends are shaping industrial systems in profound ways. "The changes being enabled by both new technologies from outside the realm of traditional automation solutions, as well as by proven tools and techniques expanded into new areas, will have impacts as transformational as the introduction of programmable logic controllers and distributed control systems a generation ago," says Lydon.

This second annual *Automation & Control Trends Analysis* ebook, produced by Automation.com and sponsored this year by Yokogawa, reveals a future leading to autonomous operations, such as those described in this month's cover story ("Digital Twins Enable the Autonomous Paper Mill"). McMillen says that, according to Yokogawa's global process industry survey, "64% of end users expect to establish autonomous operations over the next decade." He also agrees that the time is right for accelerated adoption of other technologies, such as open architecture, artificial intelligence and machine learning, cloud computing, the Industrial Internet of Things, and robotics.

Digital transformation requires the low-cost implementation of change, such as the ability to make rapid, iterative, and data-driven innovations in plant operations. That might be best served by the quickly evolving "outcome-as-a-service" business model. "Although complete outsourcing of the operations and maintenance of an entire facility—such as process-plant-as-a-service—is further in the future," McMillen says, "smaller-scale initiatives such as equipment-, process unit-, feedstock-, or catalyst-performance-as-a-service are emerging."

The changes being enabled will have impacts as transformational as the introduction of PLCs and DCSs a generation ago.

The COVID-19 pandemic has clearly helped the idea of industrial autonomy gain momentum as companies seek to improve worker productivity, quality, and safety, adds McMillen. "Outcomes will range from a connected, empowered workforce to highly agile operations that can rapidly adapt and respond to market dynamics. Plants that make these changes now will be ready for the next big disruption when it arises," he says.

Sign up to receive the AUTOMATION 2021 Special Report by visiting Automation.com/Trends2021 and let me know which of the Digitalization Dozen your organization is tasking you to apply and why. I want to know where you are on the journey from industrial automation to industrial autonomy. ■

ISA *INTECH* STAFF

CHIEF EDITOR
Renee Bassett
rbassett@isa.org

CONTRIBUTING EDITOR
Bill Lydon
blydon@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Lisa Starck
lstarck@isa.org

GRAPHIC DESIGNER
Bonnie Walker
bwalker@isa.org

ISA PRESIDENT
Steve Mustard

PUBLICATIONS VICE PRESIDENT
Joao Miguel Bassa

ADVERTISING & SPONSORSHIP
https://tinyurl.com/ISA-InTechMediakit2021

Open Integration, 'Digital Chain' May Solve IIoT Device Management Challenges

Users understand the need to apply intelligent field devices to achieve efficiencies and remain competitive. Users also require more efficient ways to deal with the reality of multivendor systems and Industrial Internet of Things (IIoT) devices. Suppliers with a strong commitment to serving customers are embracing open concepts to meet those customer needs.

The Open Integration Partner program, initiated by Endress+Hauser and now including 35 participating companies, seeks to improve the quality and efficiency of device integration and life-cycle maintenance of control and automation systems by focusing on simple, fast, and manufacturer-independent integration of components and devices into automation systems. The group held its first physical meeting in June 2019 at Endress+Hauser facilities in Reinach, Switzerland, then took a year off during the pandemic.

The Open Integration Partner Meeting occurred again—virtually this time—on 17 June 2021. The virtual event was an impressive follow-up to the first meeting, during which users made it clear that process control industry users want open, interoperable systems instead of proprietary solutions. The cooperation partners this year included Auma Riester, Bürkert, Festo, Flowserve, Hima Paul Hildebrandt, Honeywell Process Solutions, Mitsubishi Electric, Pepperl+Fuchs, Phoenix Contact, Rockwell Automation, Schneider Electric, Softing Industrial Automation, and Turck.

Vendors have their own data models for intelligent devices, asset management systems, and other software. The Open Integration initiative is focused on creating standard data models for devices to give users greater efficiency and productivity. This is analogous to what happened in the computer-aided design (CAD) market years ago, when each supplier had its own platform and data models for creating CAD drawings: Major users, particularly in the automotive industry, demanded standardization of the models. Eventually this drove the industry to open standards.

The meeting included a presentation by BASF on leveraging DIN SPEC 91406, the standard for automatic identification of physical objects and information on physical objects in information technology (IT) systems, particularly in IoT systems. DIN, the German Institute for Standardization, wrangles a consortium of asset owners and operators working on DIN SPEC 91406. Their goal is standardized identification of physical objects using 2D codes, such as QR codes, that mobile devices can read and that can be used to retrieve all relative information about a field device.

All information relating to the physical object can be identified in various IT systems, including assembly, maintenance, inspection, repair, and disassembly. Original equipment manufacturers (OEMs) can link all information, such as drawings, operating instructions, and spare parts lists to this ID, so users can quickly access all relevant information. Test, calibration, certification, and other documentation can also be electronically linked to digital records for each device.

Using these IDs, everyone can exchange information about a physical device throughout its life cycle, creating a digital chain of secure electronic access. This one-to-one ID is therefore the prerequisite for accessing and maintaining information in the physical object's digital twin throughout its life cycle. This is particularly important for physical objects embedded in IIoT systems.

Industrial use cases for a digital chain of secure data can include on-site access to installation information or safety instructions for construction and operations and maintenance personnel, and access to repair instructions or spare parts lists for maintenance. Engineering can use digital chains to secure research of technical specifications on existing equipment, comparisons of OEM offerings, or downloads of 3D equipment surface models. ■ *—By Bill Lydon*

ServiceNow Enters Industrial Sector with Digital Workflows

ServiceNow, a company that streamlines work processes with modern digital workflows, recently debuted its first product for the manufacturing and industrial sectors. The company's workflow automation platform enables an enterprise to optimize business processes in any area, including logistics, customer service, employee hiring, or scientific discovery.

The company says customers have been asking for help to secure critical infrastructure. Abhijit Mitra, vice president and GM of industry products, said, "We are taking the IT expertise we have gained over the years and applying it to the manufacturing sector. We are applying our workflow platform [to] operational tech management."

For its first product designed for the manufacturing sector, ServiceNow is partnering with Siemens Energy to help energy companies monitor, identify, and respond to cyberthreats. The solution combines AI-based software from Siemens' Managed Detection and Response service with ServiceNow's Operational Technology Management software to detect cyber anomalies and create a workflow to streamline their mitigation. ■ *—By Melissa Landon*

Ethernet-APL is Closing the Industrial Digitalization Gap

Industrial networks have been using Ethernet for years. Now, work on the Advanced Physical Layer of Ethernet (Ethernet-APL) is accomplishing the goals of Industry 4.0 and industrial digitalization by closing the lingering communications gap between sensors/edge devices and business operations systems. The Ethernet-APL organization demonstrated the capabilities at the ACHEMA Pulse "Live Days" event in June. Organization members, including FieldComm Group, OPC Foundation, ODVA, and Profibus & Profinet International, showcased "IT-centric instrumentation" for process control, including hazardous areas.

The Ethernet-APL strategy achieves a common sensor and instrument physical and transport but does not converge and harmonize communication protocols, which remain separate and unique. Using universally accepted IT and IoT methods and frameworks, Ethernet-APL is connecting sensors to business systems in process plants using standard IEEE 802.3cg communications managed with IP—achieving high-speed, uniform, sensor information transfer via Ethernet.

The initiative uses the work of the IEEE 802.3cg task force, including amendments to the IEEE 802.3 Ethernet standard for an Ethernet physical layer operating at 10 Mb/s over single-pair cable with power delivery. Current and voltage will be limited to have an intrinsically safe solution for zones 0 & 1/ Division 1. The APL project team has also cooperated with semiconductor manufacturers, who will offer 10BASE-T1L Phys for Ethernet-APL, enabling sensor manufacturers to support the standard. Just like standard Ethernet, this is a common transport for multiple protocol and messaging types.

The ACHEMA demonstration included 12 different field instruments and devices.

The multivendor demonstration during ACHEMA Pulse illustrated interaction across different product vendors and networks, highlighting the multiple options and interoperability that Ethernet-APL will offer end users. The ACHEMA Working Ethernet-APL demonstration included: Rockwell, Siemens, and Emerson process controllers; ABB industrial PLCs; and ABB, Emerson, Endress+Hauser, and Siemens asset management software. The demonstration included 12 field instruments and devices from ABB, Emerson, Anderson Hauser, Krohne, Pepperl+Fuchs, Phoenix contact, Rockwell Automation, Sampson, Siemens, Stahl, Vega, and Yokogawa.

Ethernet-APL is the physical layer. Each individual standards organization will be responsible for its own conformance tests and Ethernet-APL certifications for devices supporting the protocol. Some of these registrations are expected to be defined and available by the end of the year. ■ *—By Bill Lydon*

ISAGCA: Secure PLC Coding Best Practices Released

The ISA Global Cybersecurity Alliance (ISAGCA), along with admeritia GmbH, announced that it is a contributing organization for the release of the "Top 20 Secure PLC Coding Practices." This public-sourced document is the result of a grass-roots initiative to provide guidelines to control engineers for improving the security posture of industrial control systems (ICSs).

ISAGCA members and others from around the world contributed to the document, which encompasses advice covering the four primary programmable logic controller (PLC) programming languages: Ladder Diagrams (LD), Function Block Diagrams (FBD), Structured Text (ST), and Instruction List (IL).

The "Top 20 PLC Coding Practices" document began with Jake Brodsky's S4x20 session on tips and tricks he had learned in his long career with a water utility to improve the resiliency, maintenance, and security of programmable logic controllers and the underlying physical processes. PLCs, which were insecure when first designed, have been better secured over the years through the development of secure protocols, encrypted communications, network segmentation, and more. However, there has not been a focus on using the characteristic features in PLCs, supervisory control and data acquisition systems, or distributed control systems (DCS) for security, or much instruction on how to program PLCs with security in mind, he said.

Dale Peterson—ICS security consultant, speaker, podcaster, and founder of S4 Events—said Brodsky called out the fact that people programming and configuring PLCs are not being taught security practices. "It's gratifying that the community, including organizations like ISAGCA, came together to fill this gap by creating and making freely available the 'Top 20 PLC Secure Coding Practices,' " he said.

Two of the project leaders, Sarah Fluchs and Vivek Ponnada, joined Dale Peterson on his podcast and webcast to discuss the list and how it can be used. Source: plc-security.com

Little to no additional software tools or hardware are needed to implement these practices. Download the document and find links to informative videos at www.plc-security.com. ■ *—By Renee Bassett*

PureCycle Plastics Recycling Plants Will Be 'Born Digital'

PureCycle Technologies is planning a network of global facilities to enable large-scale recycling of a common but rarely recycled plastic. It is being supported by advanced digital technologies and automation from Emerson Automation Solutions. Emerson's Plantweb digital ecosystem was chosen for the breadth of digital solutions, including intelligent sensors and control valves, advanced operations software and systems, cloud data management, and analytics.

"Unlike traditional manufacturing facilities coping with transforming legacy platforms to digital, PureCycle's progressive approach will enable all future facilities to be born digital," said Dustin Olson, chief manufacturing officer of PureCycle Technologies. "With Emerson's help, each PureCycle facility is expected to start up with the most advanced digital automation technologies available, allowing for faster project completion, fully integrated systems, and world-class operating performance."

Polypropylene, identified as resin recycling code #5, is one of the world's most versatile plastics produced. It is widely used around the world for food and cosmetics packaging, toys, automobile parts, and more. Despite more than 170 billion pounds being produced each year, less than 1 percent is reclaimed annually for recycling and reuse.

"PureCycle's first-of-its-kind technology purifies waste plastic to remove color, odor, and other contaminants to create a near-virgin ultrapure recycled polypropylene suitable for nearly any application," Olson said.

PureCycle Technologies holds a global license to commercialize the only patented solvent-based purification recycling technology, developed by The Procter & Gamble Company. Early last year, machine builder Koch Modular was awarded the design and construction contract for the new plastics recycling plant. Koch Modular had been working with PureCycle for more than three years on the development of the technology. Koch Modular designed and constructed the predecessor Phase I Feedstock Evaluation Unit, which delivered successful production at scale in 2019. Koch's contract included the supply of a complete raw-material-in-finished-product-out process system, modularly constructed, in a controlled indoor environment, that was then shipped to the plant site via roadway. ■ *—By Renee Bassett*

New Group to Further AI for Industrial Automation

The Association for Advancing Automation (A3) has created a new artificial intelligence (AI) Technology Strategy Board of leading AI experts. It is part of a major initiative to promote education and adoption of the applications of artificial intelligence in automation industries. This new board places AI leadership at the same level as A3's existing technology groups: robotics, vision & imaging, and motion control & motors.

Artificial intelligence is layering atop robotics, vision, motion control, and other automation technologies to create new solutions, great flexibility, and expanding opportunities. Big tech companies—once focused more on phones than factory floors—now view manufacturing, robotics, and industrial automation as key segments of their businesses.

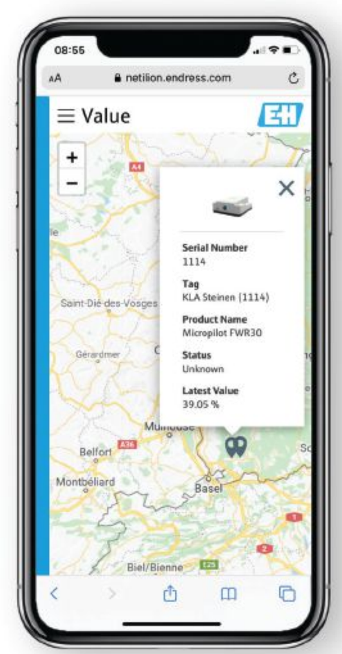
The AI Technology Strategy Board will comprise senior executives from leading AI and technology companies. This is the first time the global trade association has added a technology group to its leadership since adding motion control in 2006. A3 represents 1,100 companies from across the automation industry. Companies such as Amazon, GE, Google, Intel, Microsoft, NVIDIA, and Siemens have helped guide A3's initiatives. ■

Endress+Hauser Unveils IIoT, Edge Innovations

In a world of increasing interest in open systems, Endress+Hauser showed its technological innovation in the areas of sensors, edge devices, and smart instrumentation. In May the company announced its Netilion IIoT solution platform, which combines digital services and hardware components that improve the management, maintenance, and support of process control instruments and analyzers. Netilion helps users keep track of their installed base of instrumentation, including the instruments' performance and health status.

A free smartphone app guides the user in capturing field instrument asset data using QR codes or RFID tags, storing images and instrument locations/accessibility, and saving other quality-relevant data. Netilion Analytics can be used to create a digital twin of the system, while Netilion Health tracks the condition of the instrument so that maintenance optimization measures can be initiated.

Netilion securely connects field devices, such as the new FieldEdge SGC500 gateway to the Internet, supporting HART, WirelessHART, and Profibus communication standards in combination with EtherNet/IP. The connection can be used to securely upload installed-base information and create lists of the instruments without requiring interaction with control systems. HTTPS data transfer with end-to-end encryption and authentication according to the OAuth 2.0 standard guarantees a highly secure connection, and data can only flow in one direction—from the field device to the Internet. ■



The Netilion IIoT solution platform includes a smartphone app.

Cybersecurity Preparedness Depends on Procedures and Infrastructure

By Achilli Sfizzo Neto

Ransomware and malware are increasingly targeting industrial operational technology (OT) networks and applications, forcing OT to play catch up with information technology (IT) by defining and following strategies for defense in depth.

Every member of an organization in the OT space, from its frontline workers to executives, must change daily procedures to incorporate cybersecure best practices to keep production and data uncompromised. While there has been a substantial increase in vulnerability assessments—efforts surveying networks, applications, and organizational practices for weak points where bad actors can gain access to sensitive information—the patches being implemented remain subpar in many instances.

Controllers and smart devices are being created with cybersecurity in mind, but these products do not compensate for underlying infrastructure vulnerabilities.

You know you have a problem, but how do you fix it? It is one thing to be aware of your vulnerabilities, and another to deal with them effectively.

Part of the issue began 20 years ago. As technology was rapidly evolving and OT began connecting isolated subsystems, many companies never stepped back to confirm infrastructure was ready. Today, many manufacturers are creating controllers and smart devices with cybersecurity in mind, but installing these products in a facility does not compensate for underlying infrastructure vulnerabilities.

With so much to be done, planning and prioritizing is critical. Efforts should focus on network infrastructure and core components. Many modern OT network security strategies rely on IT departments to air gap the automation system, with a single point or two for external access. But if the safeguard is breached from the outside or compromised by a user on the inside, the automation system must depend on its own set of protections. These include:

- network separation and segmentation
- protection against unauthorized access, or log in
- protection against unauthorized modification and manipulation
- authentication support
- audit and security event reporting
- intrusion detection and alerting.

Intrusion detection is of particular interest. A 2018 study by Mandiant revealed the average containment time of cybersecurity crises in 2017 was five days after detection. However, the average time for intrusion detection was a staggering 66 days. Although cybercriminality is very much a developing practice, the good news is there are parallels among many incidents.

Hacking does not occur in one fell swoop. It typically involves days, weeks, or months of bad actors snooping around the network and making a battle plan, be it a coordinated multi-actor effort or a lone wolf attack. By giving organizations the tools to detect unauthorized access and activity, smart automation systems can shut down these intrusions long before they turn into frontpage headlines.

This is accomplished by threat detection devices—which funnel all data to and from an OT network—working in concert with programmable logic controllers and other controllers. Artificial intelligence and machine learning algorithms can perform tasks such as cutting power in strategic locations, turning off device communications, initiating secure firewalls, identifying and quarantining affected devices, and denying external access to the network during cyberevents. Before unauthorized access can grow into a highly consequential attack, these quick intrusion detection and defense-in-depth strategies can be used to drastically reduce the risk of disruptive incidents.

Managers and leaders must support modern infrastructure improvements and champion safe practices in their companies. Cyberevent prevention begins with a culture of awareness and is carried forward by appropriate investments in people, procedures, and products.

This is more important than ever because global supply chains carry the potential for chaotic disruption with widespread impact, sometimes triggered by exploiting a single vulnerability. For this reason, there is no room for downtime when cybercriminals strike. With cyberattacks, it is not a question of if, but of when they will impact your organization. By taking proactive steps, companies can significantly reduce their impact. ■

ABOUT THE AUTHOR

Achilli Sfizzo Neto is the head of the factory automation business for Siemens Digital Industries, U.S. He was previously CEO for Chemtech – A Siemens Business; business unit head for Process Industries and Drives and Process Solutions; and division head for Building Technologies in Brazil. He also brings sales, service, and operations experience from Avaya and Nokia.

IIoT Platforms: Vendor Confusion Requires User Caution

By Michael Risse

ABOUT THE AUTHOR

Michael Risse is the CMO and vice president at Seeq Corporation, a company building advanced analytics applications for engineers and subject-matter experts. He was formerly a consultant with big data platform and application companies, and prior to that worked with Microsoft for 20 years.

Industry analyst LNS just released its *Solution Selection Matrix for Industrial Transformation (IX) Platforms,* a comprehensive guide intended to help process manufacturers develop, evaluate, and even select from a short list of IX platform vendors. LNS joins a crowded set of offerings including Gartner's *Magic Quadrant for Industrial IoT Platforms* (October 2020), the Forrester *Wave for Industrial IoT Platforms* (Q4 2019), and IDC's *MarketScape for Worldwide Industrial IoT Platforms in Manufacturing* (June 2019). This does not count other unranked vendor lists from ARC Advisory Group or ABI Research (Q4 2019). And apologies in advance for all the analyst lists and quadrants and comparisons that I failed to include.

Taken together, these comparisons list more than two dozen Internet of Things (IoT) platforms, with no two analyst lists having the exact same companies. There is some consistency among the top-ranked vendors—congratulations to PTC/ThingWorx and Hitachi Lumada—but the various scoring models, and in particular the diversity of vendors, is a source of concern for end users.

Why? Because this is not the industrial automation market, where the top 10 vendors can survive and compete, divided by vertical industry focus, geography, and a history of proprietary, vertically integrated offerings.

Instead, the IoT (or IIoT) platforms market is the software world, and what happens in software markets is that offerings consolidate: Good luck finding two or three vendors, much less six in some software segments. Cloud computing? The majority of the market is just two vendors, Microsoft Azure and Amazon Web Services (AWS). Enterprise resource planning applications have one vendor, SAP, and maybe Oracle. The network effect, economies of scale, and relatively low switching costs add up to size being an advantage. To the victor go the spoils.

Which is why the analysts are so engaged in the IoT platform discussion now—because most of the 24+ vendors in the market will not survive the natural attrition common to software markets. They will be acquired or consolidated, and a few of the niche vendors will go out of business. This is happening already with Cumulocity being acquired by Software AG, ThingWorx by PTC, and Carriots by Altair. Thus, vendor viability is a real and appropriate consideration for end users.

A second concern is the public cloud players, called "hyperscalers" by some analysts. Azure and AWS do not, as of today, have as many of the capabilities as the specialized IoT vendors, and the public cloud rankings in the comparisons confirm this. But Azure and AWS can buy electricity at the lowest rates, and they can afford the capital expense of putting data centers in any country close to customers and power supplies. So, while Azure and AWS get mixed IoT platform scores today, they play the long game and should not be discounted.

Beyond viability and the looming interests of Azure and AWS in the IoT market, there is a final consideration for investing in IoT platforms. Given the risks of a decision and the challenges of investing in a platform or DIY stack of solution components to deliver data securely to the cloud, will it be worthwhile from a return-on-investment perspective?

Many of the platforms, for example, claim to support analytics but are behind the market in terms of contextualization, self-service, integrated machine learning, and other features. This means the last mile, the true value of insights to improve business outcomes, are still out of reach after the creation, collection, and storage of the data. Data is good, but it is outcomes that matter.

The IoT platforms market, as all the analyst reports demonstrate, is at the height of its confusion before a period of consolidation, standardization, and simplicity for users. In the meantime, *caveat emptor.* ■

Figure courtesy of Seeq

Digital Twins Enable the Autonomous Paper Mill

Robust and well-maintained control system optimization, advanced process control, and model-based predictive control can increase production, decrease costs, and autonomously operate the mill of the future.

FAST FORWARD
- The digital twin is a virtual plant—a dynamic model containing the process, mechanical, and electrical/control design information in one place.
- Model predictive control provides an additional tool to improve the control of critical processes where PID or rule-based expert control is not well suited.
- With the digital twin and the process model, coupled with the DCS and the control model, the behavior of the autonomous mill can be analyzed over a range of production rates, operational settings, and constraints.

By Brad S. Carlberg, PE

An autonomous mill runs itself with little or no human intervention using a digital twin. Smart sensors and instruments collect data, and secure and robust communications move the data from the mill floor to a control computer and back. Software and human expertise combine equipment data with data pulled from a process computer or distributed control system (DCS) and data mined from the mill's enterprise resource planning system to navigate the best path for production and profits.

A digital twin is a digital representation of a real-world entity or system. The implementation of a digital twin is an encapsulated software object or model that mirrors a unique physical object, process, organization, or other abstraction, according to Gartner. Within the context of a pulp and paper plant, it is a virtual plant, a dynamic model containing the process, mechanical, and electrical/control design information in one place. Design deficiencies can be corrected using this dynamic process model. Difficulties of traditional proportional, integral, derivative (PID) control are overcome by similar use of a model predictive controller. Characteristics of a digital twin include:

- the ability to create and embed knowledge into precompiled objects that represent common equipment
- the ability to have design decisions communicated to all engineering disciplines through a database
- the ability to communicate via OPC to any control system.

Model-based predictive control (MPC) is an additional tool to improve the control of critical processes where PID or rule-based expert control is not well suited to the application. MPC can often reduce process variability beyond the best performance that could be obtained with PID or expert system control methods. MPC can manage applications where there are delays in the process response to actuator changes or multiple interactions between process variables.

The virtual plant concept unites the engineering disciplines and enables process and control designs to be tested before startup. MPC can provide additional production and improved operability.

Creating dynamic process models

Creating dynamic process models for individual areas of a world-class kraft pulp mill can be challenging. The ability to import and export the actual control system configuration to and from the digital twin allows not only a comprehensive checkout of the process models, but also verification of the process control strategy and the application programming composed to implement it.

The operator's workstation uses the same operator interface graphics as those in the real plant. At the workstation, the operator has full use of the same screens used in the real plant. The digital twin software and hardware emulate the DCS configuration and the control models exactly as they will be run in the field. The virtual signals upon which the emulated DCS configuration code acts are generated by the process models.

The digital twin uses first principles equations to calculate mass, energy, and momentum balances across multicomponent systems. Appropriately programmed, models can predict the operating characteristics of the process and track variables of interest. A valuable feature of the modeling software is its ability to interface directly with most DCS.

Once the dynamic process model, or virtual process plant, is built in the digital twin software, the planned process plant behavior is analyzed

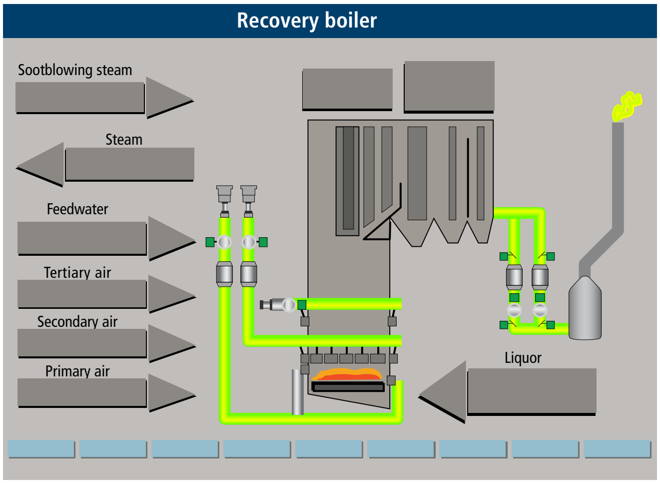


Figure 1. Recovery boiler DCS operator graphic

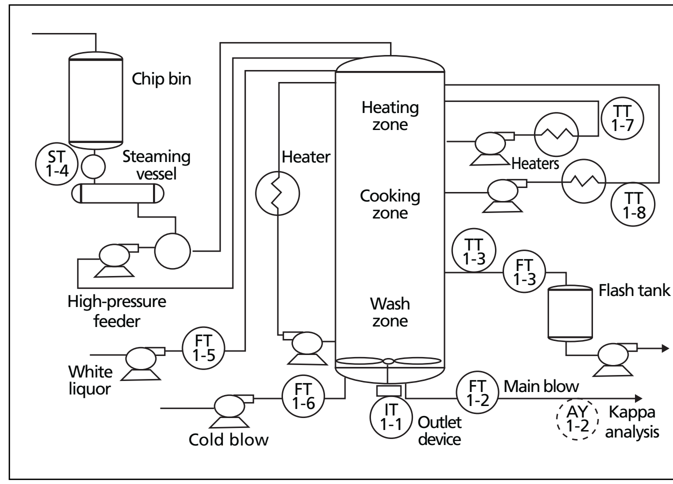


Figure 2. Digester process

Source: Terence Blevins, Willy K. Wojsznis, and Mark Nixon

over a range of pulp quality parameters, production rates, and operational settings and constraints. The virtual process plant helps discover dynamic system behavior problems, including process control issues. The next step is to run the digital twin, just as a real plant can be run, through startup sequences, production rate changes, ore changes, etc., to determine how the plant will behave during such changes.

With the digital twin and the process model, coupled with the DCS and the control model, the behavior of the autonomous mill can be analyzed over a range of production rates, operational settings, and constraints. Key process design assumptions and decisions could be made clear, and the autonomous mill can be optimized.

Mill optimization opportunities

Multitudes of careers have been spent understanding and refining the pulp and paper industry, and textbooks and technical papers too numerous to list have been written about the various processes and equipment in a pulp and paper mill. Many opportunities for process optimization involve energy savings, chemical saving, or increases in production rate. An autonomous plant can improve operations in more than the 10 process areas represented here.

1. Recovery boiler automation.
The recovery boiler can be optimized to adjust for the continual variability in black liquor British thermal unit (BTU) value and compensate for changes in boiler load (figure 1). When the effects of liquor BTU and boiler load variations are eliminated, all parameters associated with the recovery process become more stable and the boiler can typically be operated with a higher throughput, better efficiency, improved green liquor reduction, minimized fouling, and reduced emissions.

When compared to a traditional control strategy, this system can provide the following benefits to mill recovery operations:

- five to 15 percent increase in black liquor throughput
- one to 2 percent increase in thermal efficiency
- improved reduction efficiency
- reduced water wash frequency
- improved environmental compliance
- reduced variability in all process parameters

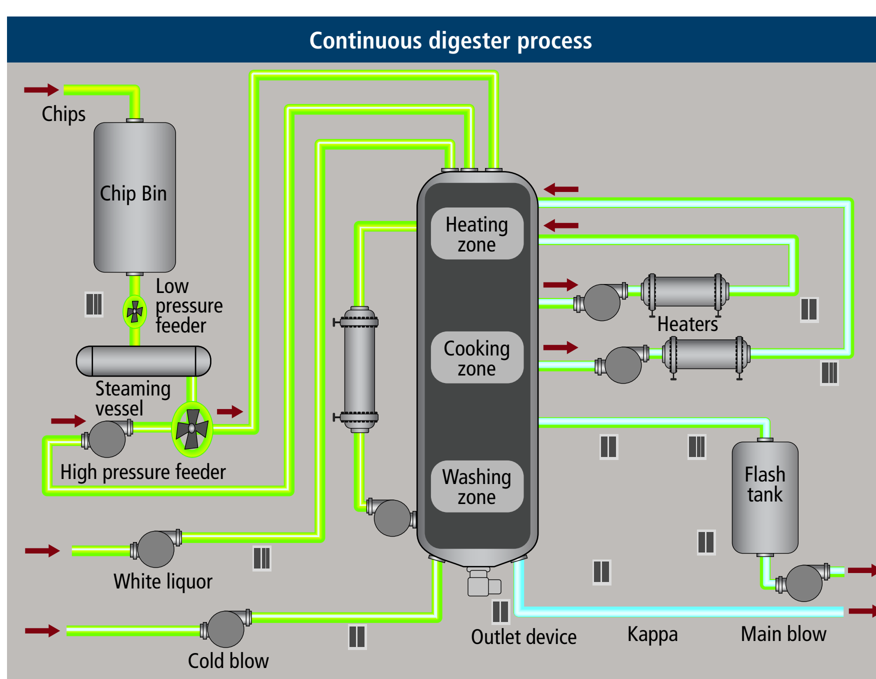


Figure 3. Continuous digester DCS operator graphic

Source: Terence Blevins, Willy K. Wojsznis, and Mark Nixon

- automatic control virtually at all times
- consistent boiler operation throughout all shifts

The kraft recovery boiler uses steam sootblowers (usually around 50 per boiler) to blow fly ash in the combustion gases off the boiler tubes. Without the sootblowers, particulate would build up on the tubes, effectively insulating them and preventing heat transfer to the water. This thereby reduces the steam output from the boiler and lowers the boiler efficiency. To level the steam usage to the boiler, the individual sootblowers are scheduled so that they operate in a predefined sequence.

Optimization of these sequences can involve using "smart sootblowing" based on furnace draft pressures and temperatures, which signal when to blow certain regions of the tubes. For example, if the temperature rises in a particular region, that condition indicates the tubes are becoming covered with soot and the sootblowers in that region would be operated. Typical sootblowers use high-pressure steam to blow soot off boiler tubes to improve heat transfer between furnace gases and boiler water. You can also sequence individual sootblower operations for optimal steam usage; low temperature and high differential pressure signal which sections to operate.

2. Black liquor evaporators.
Black liquor evaporators concentrate the weak black liquor from the pulp washing process at around 15 percent solids to around 60 percent solids, so they will burn effectively in the recovery boiler. The process can be optimized by using the pressure and temperature differential to signal tube fouling that would cause a decreased heat transfer rate and a lower vacuum, and automatically start a boil-out of the evaporators to clean the fouling.

3. Recausticizing.
In the causticizing area of the pulp mill, green liquor is reacted with lime to form the white liquor used in the wood chip digesting (cooking) process. Traditionally, conductivity was used as a variable to measure the reaction completeness. With new nuclear instruments, the exact chemical composition in the white liquor can be determined to better gauge the reaction completeness. Since the causticizing process has a long lag time and is not a good candidate for traditional PID control, a new optimization technique using MPC can tune the process more tightly, which yields a more consistent white liquor product.

4. Batch and continuous digesters.
The pulp digesting (cooking) process uses either batch or continuous digesters (figure 2). Either way, the principle is the same: The wood chips and the cooking chemicals are added to the digester under pressure and at an elevated temperature from the steam addition, and the wood chips are cooked

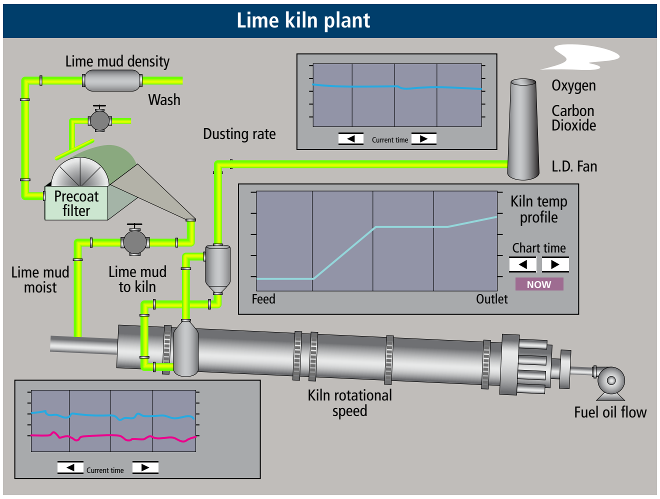


Figure 4. Lime kiln DCS operator graphic

for 60 to 90 minutes. The pulp stock slurry exits the digester at a consistency of 6 percent, and the resulting pulp fibers are close to the state required to make paper. Optimization can involve energy savings by increasing throughput and scheduling the batches, so steam consumption is leveled, and the spikes cause fluctuations in boiler demand. Also, online freeness (a measure of the cooking completeness) analyzers can close the control loop to more accurately determine when the cook is complete (figure 3).

5. Screening and refining.
Screening and refining are used to get uniform pulp stock. The screen lets the optimally sized pulp fibers pass through but centrifugally removes knots, uncooked or undercooked fiber bundles that can be recycled back to the digester for additional cooking. The refiner, which is a piece of equipment with two rotating, rough-surfaced plates, is used to cut or defibrillate the wood fibers resulting in more uniform pulp stock.

6. Washing.
The digested, screened, and refined pulp stock, although uniform in fiber size, is still dirty with all the organic and inorganic by-products from the digesting process, known as weak black liquor at around 15 percent solids. The dark color comes primarily from the lignin, which is the "glue" that binds the wood fibers and gives the wood its strength and rigidity. There are also a lot of residual cooking of inorganic chemicals that can be reused in the digesting process.

The brown stock washers usually consist of three, countercurrent (the pulp stock comes from one direction and clean wash water comes from the opposite direction) stages. Fresh make-up wash water is added on the cleanest pulp at the latter stages to wash the pulp stock, but the recycled weak liquor wash water is added on the dirtiest pulp at the earlier stages. A common optimization technique is to use dilution factor washing based on pounds of wash water to pounds of wood fiber (the optimal ratio is about 1.0) to minimize overwashing that would use water that would subsequently have to be evaporated to get the black liquor to the magic number of 65 percent for burning in the recovery boiler.

7. Bleaching.
The decision whether to bleach the pulp is based on the final product of the paper mill. If the product is cardboard or paper sacks, bleaching is probably unnecessary. But if the product is writing paper, paper towels, tissue, diapers, etc., the pulp must be bleached. The bleach plant usually consists of multiple (three to five) stage washers interspersed between bleach towers. Typically, bleaching chemicals are liquid or gaseous chlorine, chlorine dioxide, sodium hydroxide, sodium hypochlorite, hydrogen peroxide, liquid or gaseous oxygen, and liquid or gaseous ozone. These bleaching towers allow the resident time (usually one to three hours per tower) for the bleaching chemicals to brighten and whiten the pulp.

The predominant area for savings in the bleach plant is to optimize the chemical usage by using techniques like kappa factor bleaching and stock tracking throughout the bleaching stages to apply bleaching chemicals based on a precise ratio of pounds of effective chlorine to the pounds of fiber.

As with the causticizer, the bleaching process has a long lag time and is not a good candidate for traditional PID control. A new optimization technique involving the use of MPC can tune the process more tightly, which yields a more consistently bleached pulp.

8. Lime kiln.
The lime kiln is a large (15 ft. diameter by 200 ft. long), rotating cylinder used to calcinate the by-product of the causticizing process—the lime mud—to convert it back to the lime that can be added in the causticizer. The predominant area for savings is energy (gas burned in the lime kiln) by optimizing the lime mud moisture content and the temperature of the calcined lime exiting the kiln.

As with the causticizer and bleach plant, the lime kiln process has a long lag time and is not a good candidate for traditional PID control. A new optimization technique involving the use of MPC can tune the process more tightly, which yields a more efficient combustion process (figure 4).

9. Pulp stock preparation, cleaning, refining, and blending.
This is the area where the pulping ends and the papermaking begins. The "art of papermaking" is in the final cleaning to remove any remaining contaminants, in the tickle refining to brush the fibers to optimize fiber bonding in the paper sheet, in the blending of different pulp species (hardwood and softwood), filler, additives, to achieve the optimal paper optical, physiochemical, strength, structural, and surface properties.

10. Papermaking, pressing, and drying sections of the paper mill.
After preparation, the pulp is stored in the machine chest. From there, the fan pump pumps the pulp stock to the headbox from which the pulp stock slurry is laid down on the fourdrinier

wire along the entire width (sometimes more than 300 in.) of the machine via the slice out of the headbox. The primary control variables in papermaking are weight, moisture, and caliper (thickness).

A typical paper machine can be as long as a football field. As in the pulp mill where most of the processes remove the pulping by-products, most of the paper machine removes the water from the paper. This happens in first the forming section, followed by the press section, and, finally, the dryer section.

The main areas for savings are energy savings in the dryer. Steam is used there to heat the dryer cans that heat the paper sheet as it passes over them on its way to the dry end of the paper machine.

- Paper sheet rolls over the steam-heated dryer cylinders to evaporate moisture.
- Optimize steam usage to save energy costs.

Recently, video cameras placed at strategic points along the paper machine have been used effectively to alert the operators of events that can cause a paper sheet break. With this information, the operator can avoid an actual sheet significantly decreasing production downtime.

Using cascaded and coupled variable frequency drives (VFDs) to control the various rollers in the fourdrinier wire, press, and dryer sections can more tightly regulate the tension (rush and drag) of the paper sheet, mitigating undue stresses that could cause a paper sheet break. Using production rate control will enable the autonomous mill to achieve optimal performance.

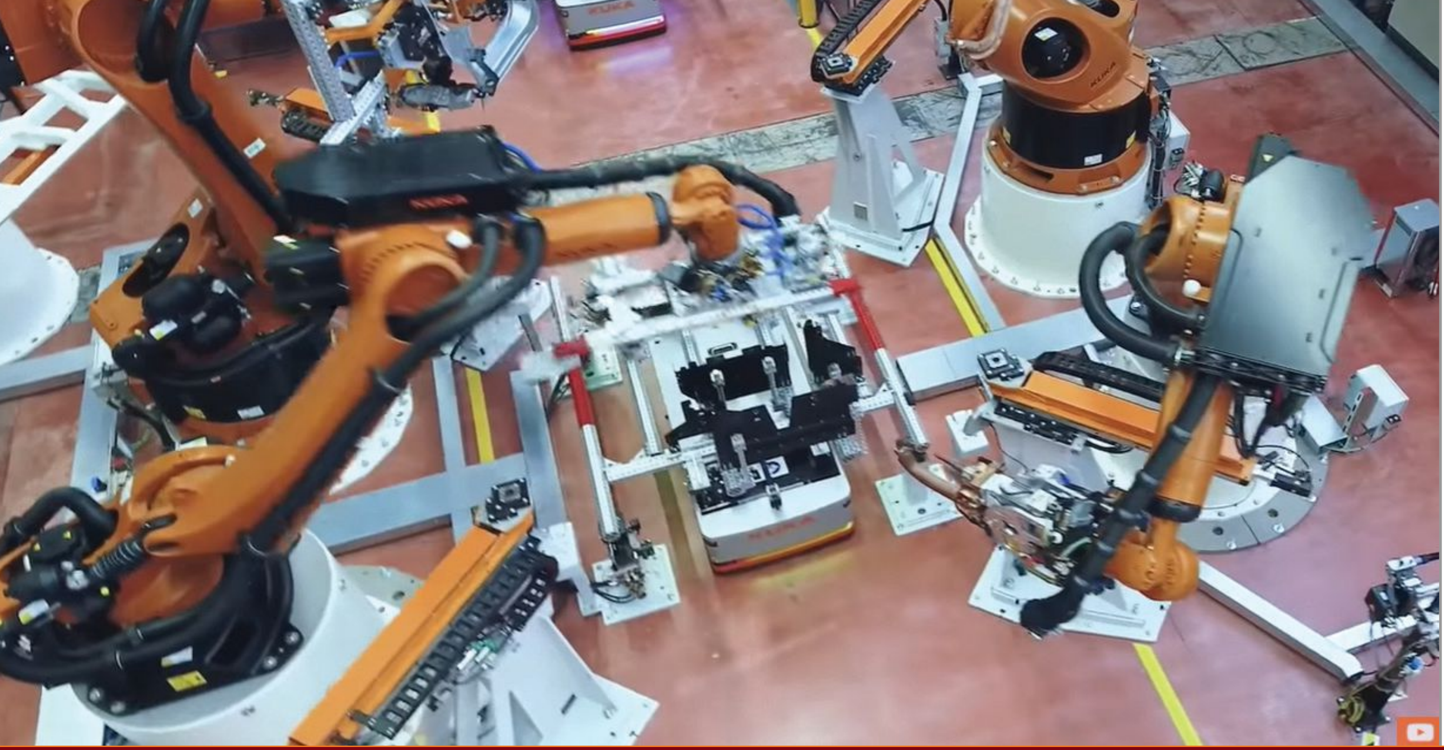
Final thoughts

The same way pilots can rely on automatic control of aircraft, once continuous and error-free automation is achieved for one mill area, and eventually multiple mill areas, operators will be freed to observe more and intervene less. For the foreseeable future, there will need to be operators in pulp and paper mills. But by utilizing advanced control coupled with digital twin technology, mill operators will trend toward less direct intervention and move toward a more supervisory role as trust is gained in the ability of the mill to become more autonomous. ■

This article was adapted from a paper presented at the 66th Annual Pulp and Paper Industries Virtual Conference, held 21–24 June 2021 in conjunction with the ISA Pulp & Paper Industry Division (PUPID).

ABOUT THE AUTHOR

Brad S. Carlberg, PE (brad.carlberg@bsc-engineering.com), is a senior control systems engineer at BSC Engineering. He has more than 37 years of experience in process engineering and process control, specifically with distributed control systems and programmable logic controllers.



Machine Modularity Addresses Mass Customization

Interfaces are a vital component of modularization. But do machine builders have to adhere to specific standards?

By Jakob Dück

One of the most significant challenges manufacturers face is: *How do I serve the very special and unusual wishes of consumers?* As things stand today, this would appear to apply only to makers of consumer packaged goods and other consumer products, such as automobiles and appliances. But the current trend toward factoring in individual customer wishes has consequences that extend deep into production technology choices. Original equipment manufacturers (OEMs) and *their* suppliers must consider the trend of mass customization.

The scope and degree of individualization as it is currently strived for can no longer be achieved with the tool kit of conventional mass production, but calls for a completely different design of production processes, including machines and systems. The individualization of mass production is one of the core aspects of Industry 4.0. The resulting challenge for the manufacturers of production systems is as follows: How should the necessary equipment and processes for "individualized production" be shaped and designed so that the costs will not explode and the resources required will not rise sky high?

KUKA, a robot manufacturer, has formulated an answer: "The key [to mass customization] lies in a high degree of standardization and automation, which at the same time affords scope for variations of customer-relevant product features. What is more, the concept of modularization, which provides customers specific, tailored product configurations based on a modular building block system, is a cost-effective way to meet individual customer needs." This results in three central perspectives for OEMs:

- the shift toward individualized serial customization
- modularization as the key, in combination with automation and standardization
- preservation of latitudes for the variation of customer-specific product features

This perfectly describes the conflicting demands made on OEMs in the mechanical and plant engineering sector. The dilemma is very reminiscent of the statement ascribed to the philosopher Hegel, "Freedom is the insight of necessity."

Importance of interfaces

Interfaces are a vital component of modularization. But do they always have to adhere to certain standards? The increasing automation and modularization of production systems has technical and business advantages for both OEMs and end users. As the degree of automation rises and modularization deepens, however, it is precisely the interfaces that play an increasingly decisive role as the link between the elements or modules. This is because the following holds true: The interfaces do not determine the entire modularity, but, without interfaces, the modules will never become a whole.

This will be further differentiated, because in some instances standardized interfaces will be more advantageous and in others "individualized" interfaces will be more advantageous. The importance of customer-specific product definitions for OEMs in the mechanical and plant engineering sector can be well illustrated, as shown in the left side of the figure 1 diagram. The possible degree of product individualization by the end user is related to the life cycle of production systems. The further the cycle progresses, the smaller the remaining scope for individualization is (transition from "hard" to "soft customization").

For OEMs to determine the right degree of individualization for their machines and to bring them into line with the different automation and modularization requirements along the life cycle, it is expedient to think in terms of different "clusters" or functional groups, such as sensor technology and drive technology.

Sensor and actuator technology. The development of electronic components has enabled a tremendous compression of functions. Higher energy efficiency and greater packing densities go hand in hand with these ongoing developments. The technology boost in this cluster is encountered in many places in the production system: in the process-integrated acquisition of input parameters and signals, in the on-site preprocessing of this input data,

FAST FORWARD

- The scope and degree of individualization as currently strived for can no longer be achieved with the tool kit of conventional mass production.
- To determine the right degree of individualization for their machines, OEMs should think in terms of different "clusters" or functional groups.
- Some OEMs have deliberately opted for nonstandard interfaces on their technology units, modules, and machines.

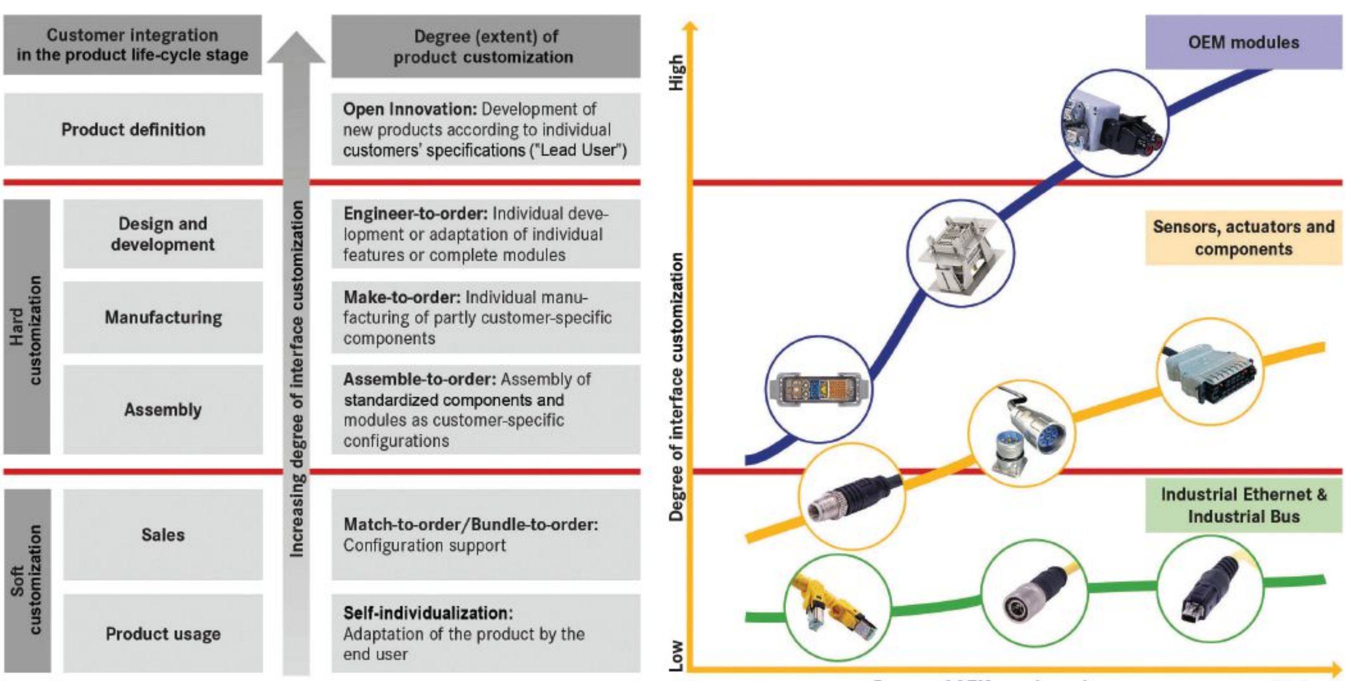


Figure 1. OEM individualization concepts according to time of customer integration (left side), and typical design for individualized interfaces according to functional groups (right side). Source: HARTING

in the energy-efficient triggering and control of actuators, in brilliant image processing and reproduction, as well as in the touch functionalities of the operating units.

On one hand, this technological progress facilitates the decentralization, modularization, and scaling of machines. On the other hand, thinking in terms of ever more compact building blocks and elementary functions is becoming necessary, and the initial input and efforts required to develop such systems is on the rise.

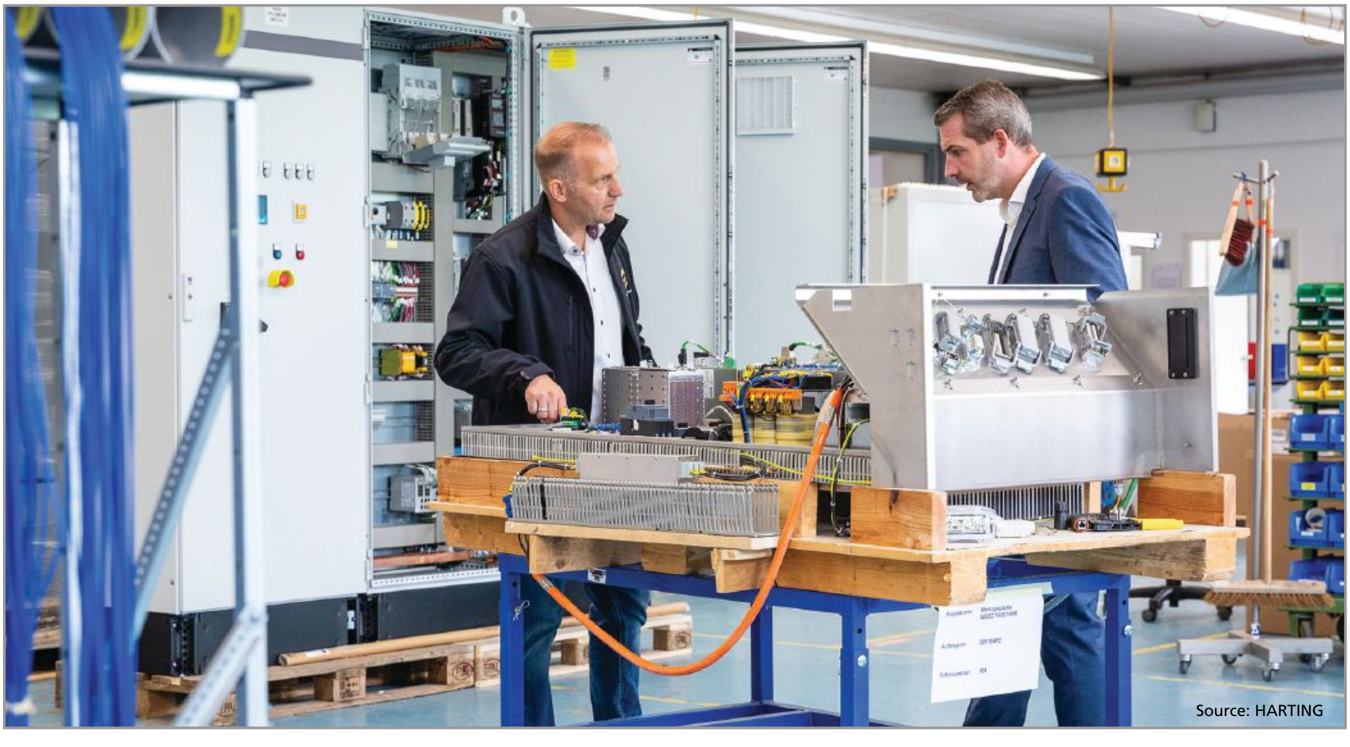
Despite these partially negative implications, the advantages of customer-oriented individualization of the product range in mechanical engineering outweigh the disadvantages. This is because the appropriate overall arrangement of sensors, actuators, and other machine control components, as well as the interconnection of the functions and processes based on them, are absolute OEM domains. They alone hold comprehensive system competence here. These are the key assets they can leverage to their advantage.

Drive technology. There are similar significant and far-reaching shifts here. Although know-how was at the core of mechanical development in the past, in recent decades it has migrated almost entirely to software departments or electrical design. Due to the enormous increase in performance of the technologies for electronic drive controls, matched with decreasing prices at the same time, entirely new concepts for machine and production plants have emerged. The function group for the complex control of the motion sequences and related processes also forms a central competence of machine manufacturers.

Specialized technology units. It is noticeable that the manufacturers of manufacturing systems are increasingly concentrating on a few technologies in their development activities. The generalist perspective remains with the overall system suppliers, whose know-how resides precisely in the application and connection of technologies. With regard to the question of the right interfaces, however, it is the highly specialized technology units that are of interest. A common, defining aspect of these functional groups is the fact that they are deployed as finished units or aggregates with firmly circumscribed physical and technical functions and precisely defined interfaces. The linking of the units represents the central OEM know-how, not the components used themselves.

Digitalization. The term "digitalization" is omnipresent in today's technical literature and other media and comprises many aspects. Applied to interfaces in mechanical engineering, it refers to data transmission technologies. Data transmission in the form of industrial bus systems—including Industrial Ethernet—has long been shaped and used by manufacturing technologists. The possibilities of cost-effective data connection to higher-level systems up to the cloud, with ever greater data throughput and real-time capabilities, are genuinely revolutionary in technology terms. These technologies would enable OEMs active in the mechanical and plant engineering sector to reshape their entire business approaches.

Different manifestations of these changes are described and designed under the heading of Industrial Internet of Things (IoT). All data transmission aspects, including industrial buses and industrial Ethernet, are considered here from the perspective of interfaces as a functional group or functional layer.



Some OEMs have deliberately opted for nonstandard interfaces on their technology units and machines. A control cabinet, for example, might require customer-specific interface solutions.

While the solutions in this area are not part of the OEM's core competence, they hold the greatest potential for change in today's manufacturing systems.

Deciding on individual interfaces

My company provides solutions for all electromechanical interfaces required in modern control, drive, human-machine interface, and communication technology for production systems at work in all branches of industry. Analyzing current customer applications, we have come up with the following advice for the individualization of interfaces based on the above-described function groups (right side of figure 1):

1. Generally speaking, it makes sense to use individualized or customer-specific electromechanical interfaces for the functional groups, which largely represent the core OEM know-how.
2. Customer-specific, tailored interfaces are most often used for those modules and aggregates that are developed or manufactured directly by the respective manufacturer. This applies to all degrees of product individualization in mechanical engineering, from "soft customization" through the various stages of "hard customization," to one-of-a-kind productions.
3. With regard to sensors and actuators, the typical interfaces for the respective industry sector are usually chosen. Trendsetters and innovators, however, do try to set themselves apart from the market by deploying specific, tailored interfaces.
4. When it comes to data interfaces, machine manufacturers rely entirely on standardized solutions. This applies both to the industrial bus and Ethernet connections employed and to all other forms of digital data transmission.

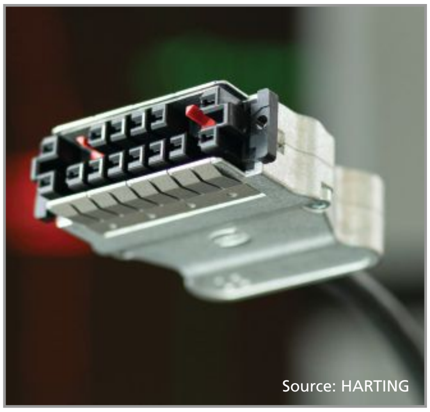
What are the main reasons behind the design of the interfaces? In terms of data transmission, it is evident that both Industrial Ethernet and bus systems in the manufacturing area and the higher-level data interfaces are subject to tremendous change. The technologies deployed are largely determined by the suppliers of the control components. Therefore, the recommendations for production-system OEMs are twofold:

- As far as possible, these interfaces should follow the latest standards of the control technology employed and ensure the modularity and scalability of the machines and systems.
- With regard to interfaces beyond the machine edge, such as those for connection to higher-level systems, the interfaces should always represent the advanced state of the art.

Consequently, as an OEM, an economically and technically optimally designed system for current requirements is in place; it is a system that is at least in part capable of meeting future (yet unknown) requirements. Moreover, a company would then also be ideally equipped for the continuous expansion of after-sales and service activities based on digital services.

With regard to other functional groups, the advantages and disadvantages of individualized interfaces should be systematically weighed and listed individually. What are the arguments in favor of customized interfaces and what are the arguments against them? There are OEMs that have deliberately opted for nonstandard interfaces on their technology units, modules, and machines. Here are the key reasons:

- End user requirements for companies that operate specific production lines and want to consciously differentiate themselves from individual suppliers or focus on them.
- Differentiation vis-à-vis competitors in the expansion of business models to offer after-sales, service, and similar services aimed at a long overall life cycle of production systems. Individualized interfaces allow these services to be controlled and expanded in a user-friendly manner.
- Intentionally nonstandard design of machine interfaces or equipping technology with specific interfaces in order to stand out from the competition. In particular, OEMs that perceive themselves as technology leaders, innovators, or trendsetters are taking advantage of these opportunities.
- Use of sensors, actuators, or their combination developed according to specific specifications of individual manufacturers. In these instances, too, the protection of one's own know-how is the strongest motive for leveraging individualized interfaces.



Interfaces should follow the latest standards of the control technology employed and ensure the modularity and scalability of the machines and systems. These Har-motion connectors were developed to customer specifications.

Customizing electromechanical interfaces to meet even the most unusual OEM requests is increasingly possible. Depending on the degree of individualization required, modular design principles applied to connector products can provide convenient scalability and minimal customization. At the highest level of "hard customization," however, customer-specific interfaces can be developed to meet individual customer requirements. This range allows OEMs to cost effectively meet even the most unusual customer wishes in mechanical and plant engineering. ■

ABOUT THE AUTHOR

Jakob Dück is global industry segment manager, mechanical engineering for HARTING Electric. After a control and measurement technology apprenticeship, Dück graduated with a diploma in electrical engineering from the Polytechnic State University in Odessa, Ukraine. He worked in R&D for an international machine manufacturer for more than 13 years before joining HARTING Technology Group in 2001.

Reduce Energy Costs by Measuring Power Quality

By Frank Healy

Once you have optimized energy use through common methods, consider where energy waste arises.

In 1954, U.S. Atomic Energy Commission chairman Lewis Strauss predicted that one day electrical energy would become "too cheap to meter." People jumped on the idea with relish. What most did not realize, however, was that Strauss was making the prediction based on advances in fusion power, not on the nuclear fission power we still use today. For fusion to occur, you need to harness the mechanisms of the sun on earth and generate a temperature of at least 100,000,000 degrees Celsius. Nuclear fission energy creates its own types of problems—the biggest being nuclear waste and safety. Consequently, saving energy and minimizing energy waste became the most important aspects of energy usage.

Through the 1950s and 1960s, energy reduction programs flourished and, in the 1970s, became even more important as oil prices rose. It is ironic that, worldwide, politicians argue that users should not have to worry about such matters, but every year energy costs increase. New sources are identified to reduce costs for a while, but energy use expands. The market does its

job of increasing the price in line with scarcity.

Sometime in the 1980s, as a young hospital engineer, I was tasked with implementing an energy savings program in a 1,000-bed general hospital. There were a wide range of properties in the complex, from those that were not more than one year old to those over 100 years old. As you can imagine, the challenge was interesting.

The site was going to be completely rebuilt over the next two to five years, so a priority system was developed to work on buildings that were not going away soon. Fortunately, it seemed that most of the oldest properties would be decommissioned in two to three years, and many temporary buildings would also disappear. I built my plan accordingly. (Although I left the hospital and the area many years ago, Google Maps shows that many of the buildings expected to be decommissioned are still in use—even the temporary ones!)

Benchmarking electrical energy consumption

The first step in developing the energy program was benchmarking electrical energy consumption across the property. The first targets were areas where energy could be controlled relatively easily, such as buildings with departments that would typically close on the weekend and not allow public access.

Through an initial survey, we soon discovered that these departments used a significant amount of energy during times when they were closed. Contributing to the energy usage was supplementary electrical heating, lighting, and computers not switched off. The supplementary electrical heating had been installed when the normal building heating had been faulty or was being refurbished—no one could quite remember why. It was no longer needed, so it was disconnected. Policies were implemented to ensure all lighting and computers were switched off in the evenings and on weekends.

The survey was extended for some weeks to make sure this was happening; the policy was quickly accepted without complaint.

After identifying areas that could provide quick wins, more detailed studies were performed in more contentious areas. The first was in operating rooms (ORs).The hospital at that time primarily carried out nonemergency surgery; a second hospital in the group contained the emergency OR. However, the general hospital did have an intensive care unit, and the surgical staff insisted that it had to be ready and working 24 hours a day, seven days a week.

Of the five ORs, two were specifically designed for orthopedic surgery and had laminar flow air systems, which are designed to minimize the possibility of cross-infection. Surgeries were always planned many weeks in advance, and these ORs were always scheduled to operate during weekdays, from early morning into the evening and sometimes on Saturday mornings.

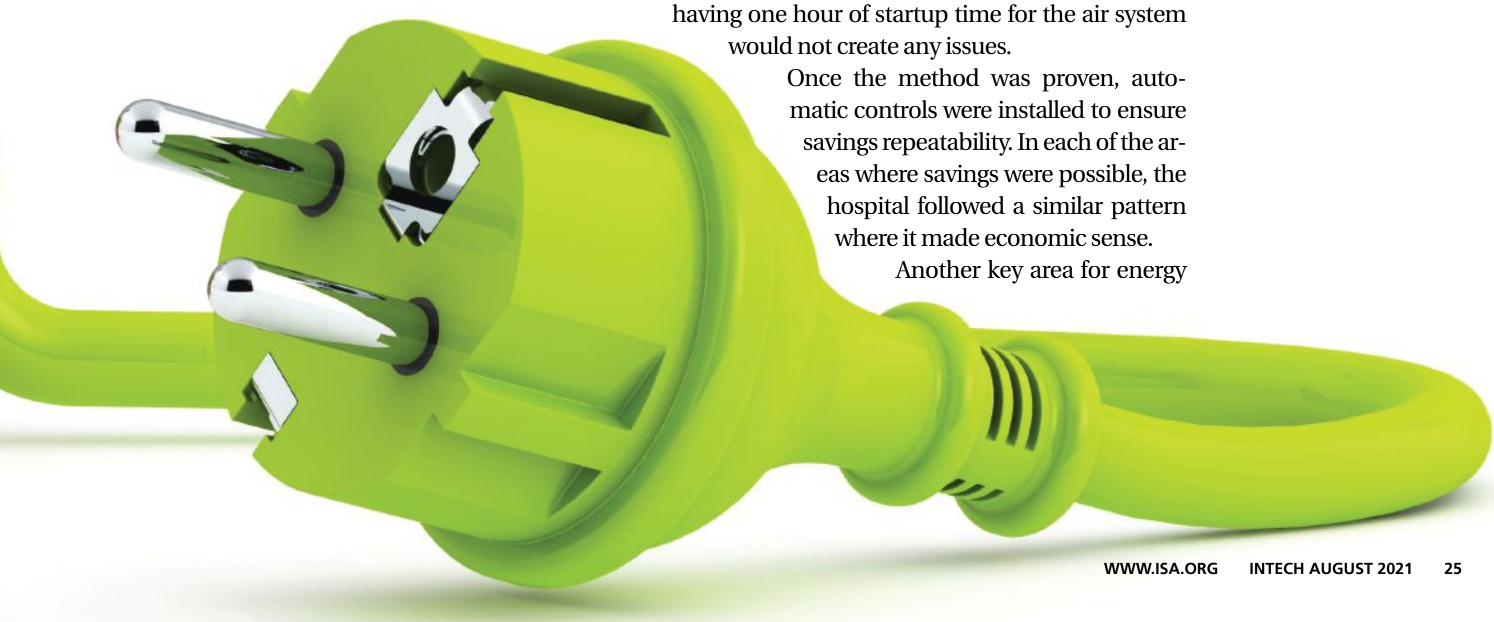
Operating the laminar flow ventilation was very expensive due to the electrical loads needed to move huge volumes of air through resistant HEPA filters. Measurements showed significant energy-saving opportunities from switching off these systems during the night and during nonoperating times. But surgeons were very resistant to switching these off. To convince them, we worked on a plan that included junior surgical staff who were responsible for setup prior to surgery. They were able to show that setup could be done in less than one hour, during the time the surgeon would be driving to the hospital. The cross-contamination expert in the hospital shared studies showing only having one hour of startup time for the air system would not create any issues.

Once the method was proven, automatic controls were installed to ensure savings repeatability. In each of the areas where savings were possible, the hospital followed a similar pattern where it made economic sense.

Another key area for energy

FAST FORWARD

- The first step in developing the energy program was "benchmarking" electrical energy consumption across the property.
- As current flows through conductors, some energy will inevitably become waste as heat.
- The person performing energy savings studies must be a cross between an energy engineer and a politician.



waste reduction is improving the power factor for the larger loads. Much has been covered on power factor correction elsewhere, but here is the key takeaway:

- When you monitor larger loads and check the power factor, if it is less than 0.9, then it is a strong candidate for correction. A power factor equipment supplier will help you chose the best solution based on the power rating of the system and the optimal power factor, considering the cost of the equipment.

These examples reveal that energy savings are not as simple as turning off the lights. Saving energy requires cooperation with the tenants and operators of the properties affected. It requires the person performing the studies to be a cross between an energy engineer and a politician.

Advanced power quality considerations

Once you have reduced energy consumption through the common method of turning off stuff that is not in use, turn to a more advanced approach: Consider where energy waste arises. One area is through losses in conductors. As current flows through conductors, some energy will inevitably be generated that becomes wasted as heat (figure 1).

Remember the fundamental I^2R equation, which indicates the power delivered, described as Joule losses? What can you do about those? Reduce the current flow (*I*) so the power is less, or reduce the resistance (*R*). Both present a problem. If you deliver lower current, the load will not operate correctly. The cost of reducing the resistance is high, as it requires the installation of more copper or aluminum conductors. So what do you do?

First, consider the optimal conductor sizing. The National Electric Code (NFPA 70 or NEC 100) provides a lot of help to correctly size a conductor. This document is one of a group of documents that describes the ideal conductor sizes for almost every circumstance. For example, the situation in a residential property in the southern U.S. is very different from operating inside a substation in a remote pumping station in the Canadian Northern Territories in the middle of winter, where thousands of amperes may be flowing. The NFPA 70 provides guidance for both situations.

The main consideration for conductor sizing is to ensure safe operation of the conductors by having the correctly sized conductor with the most appropriate insulation. The correct size will be dependent on the length, the cross-sectional area, and the anticipated current rating required, which provides minimized Joule losses and acceptable voltage drop in the conductor. Typically, the Joule losses will be 2 percent or less.

You may now be thinking, if I design to code then my energy waste will be minimized. In an ideal world that would be correct. But once the installation of the cabling is completed and the loads are installed, the situation can change. It may be that when the first equipment is installed, everything works just fine, but over time things change as additions, moves, and changes take place. It may be that new equipment is required for processes that were not considered during the original installation. Perhaps the location of equipment does not make sense once it is being integrated into a larger process, or upgrading to new equipment is required that on paper can save energy or result in higher efficiency. These additions, moves, and especially changes can have a significant effect on the installation in terms of waste energy. Key areas in which energy waste may occur are related to voltage regulation, harmonics, heating, and unbalanced loads.

Voltage regulation. As more efficient loads are installed, the voltage in the system may rise or not be correctly controlled at the transformer. Voltage regulation or optimization works like a control valve to reduce energy consumption in voltage-dependent loads by reducing or controlling voltage levels to within the equipment manufacturer's specified voltage limits to return an energy saving.

As for voltage optimization, it is not widely accepted as practical in the U.S., as it requires very specific use cases to be successful. The upfront cost of the equipment is a significant barrier to adoption too. Most of the material explaining voltage optimization appears to be marketing material, although the American National Standards Institute does have some recommendations for very specific use cases.

Harmonics. Harmonics distort the voltage and current so that the ideal sine wave for voltage is not maintained. This results in overheating in phase and neutral conductors. These are known as "triplen harmonics" as they typically affect third, ninth, 15th, 21st, etc., sine waves. These are additive and will flow in the neutral, causing additional Joule losses (wasted energy) and risk of failure due to overheating. This heating can take place in cable runs, or in motor windings and transformers. The latter two are very prone to overheating, as the lengths of the conductors in the windings are of significant length. Ultimately, overheating can cause significant damage or complete failure (which could be massively expensive and disruptive for larger motors and transformers).

Unbalance. As loads are added, the unbalanced voltage between phases can change. This may be from installing multiple single-phase loads on the same

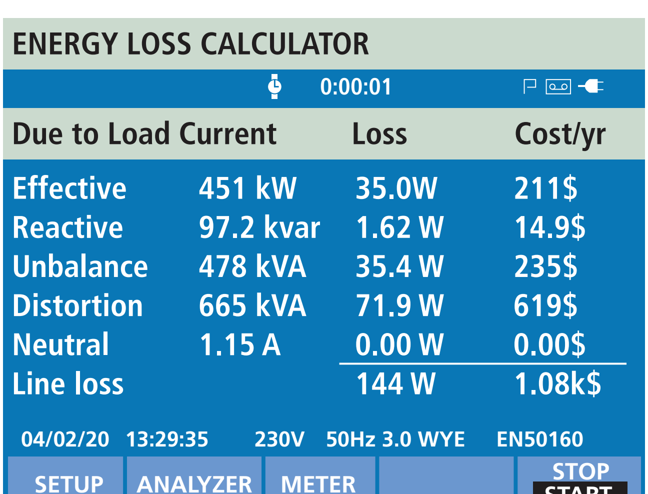


Figure 1. As current flows through conductors, some energy will inevitably be generated that becomes wasted as heat.
Source: Fluke

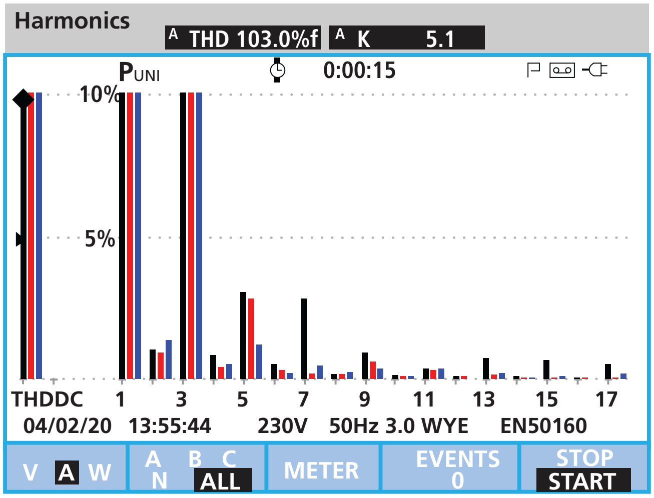


Figure 2. Power quality studies can reveal areas where energy is being wasted due the effects of harmonics and unbalance.
Source: Fluke

phase or may be from three-phase loads that are not balanced. For example:

- Motors with unbalanced mechanical loading can affect the voltage and current.
- Transformers receiving unbalanced voltage can overheat and potentially fail.
- Electric vehicle charging points can be unbalanced.

Benefits of power quality studies

Many users are dismissive of power quality studies because they think there is nothing that can be done to reduce Joule losses. The fact is that much can be done to save energy through power quality monitoring. Also, many happy users have discovered other important findings by performing power quality surveys:

- They discovered potential failure points in key equipment, such as large motors and power transformers. These would be very expensive if they failed and caused major disruption.
- They found equipment malfunctions in systems.
- They came across breakers prone to accidental tripping due to improper setup.

Once power quality studies reveal areas where energy is being wasted due the effects of harmonics and unbalance (figure 2), steps can be taken to fix the problems:

1. Install a range of harmonic filters on loads that are contributing to harmonic distortion. Some of these might be at the main service entrance. Some might be at specific pieces of equipment such as drives.
2. Consider the sources of unbalance. Often these are large motors that also have mechanical unbalance issues that have not been addressed.
3. Some unbalance mitigation is simple: Single-phase loads can be more equally distributed across the phases. Some installers have considered the problem and avoided adding all the loads to phase A/1, but then added them all to phase B/2 instead.
4. Redistributing and reconnecting single-phase loads can reduce voltage unbalance caused by unequal load distribution across the phases. The most prevalent culprits among heavy, single-phase loads are lighting equipment and occasionally welders. A blown fuse on a bank of three-phase power factor improvement capacitors could also cause the problem; simply replacing the fuse can resolve a major unbalance.

Best way to reduce energy costs

There are many technical ways to reduce energy costs: benchmarking through energy surveys, installation of mitigation equipment for harmonic voltage distortion, reduction of unbalance, etc. But the best place to start is with your electricity bill from your utility. This is often the single most effective way to reduce energy cost.

First, discover who is responsible for the bill if it is not you. It may be that your organization has an individual who is solely responsible for the bill. If it is an energy manager, that is a good thing, as he or she will be aware of at least some of the issues. Or it may be a financial administration manager, which might not be so good. We have discovered during many exercises we have done that many financial administration managers adopt a standard procedure of paying suppliers based on the company's terms, not the supplier's terms. Consequently, the supplier has been applying a late payment penalty over every billing period that has not been questioned by any administrator. In some cases, we found that an excess of 10 to 15 percent was being paid on bills totaling hundreds of thousands of dollars per billing period. The result was a huge waste that could be fixed in seconds.

Consider also the tariff being applied. Industrial electricity bills often include a demand charge, which is an agreed cost of energy for peak times and off-peak times. The tariff often includes a maximum available demand, which is the maximum amount of power that may be drawn during a defined period, typically 15 or 20 minutes. If the user exceeds the specified amount, the user will pay a penalty, and this penalty might not just be for that period. It can be across the whole billing period, which can get very expensive.

Ensure that the maximum demand you use is close to the demand you are paying for, otherwise you may be paying too much. Also, ensure that you are not too close to the peak demand, otherwise you may find you exceed the demand frequently. This adds to your bills, and may make your supplier very unhappy as it tries to optimize its network energy for all users to provide a reliable service at the best cost.

Finally, have a discussion with your supplier about your bill to find out if they can offer you better products that will save you money and enable them to improve the network stability. Electricity suppliers are generally very helpful in reducing your bill, as it also helps them. ■

ABOUT THE AUTHOR

Frank Healy is a power quality application specialist for Fluke. Located in Cheshire, England, U.K., he is an expert in power quality measurement and applications, with nearly 32 years of experience in the industry and more than 16 years at Fluke.

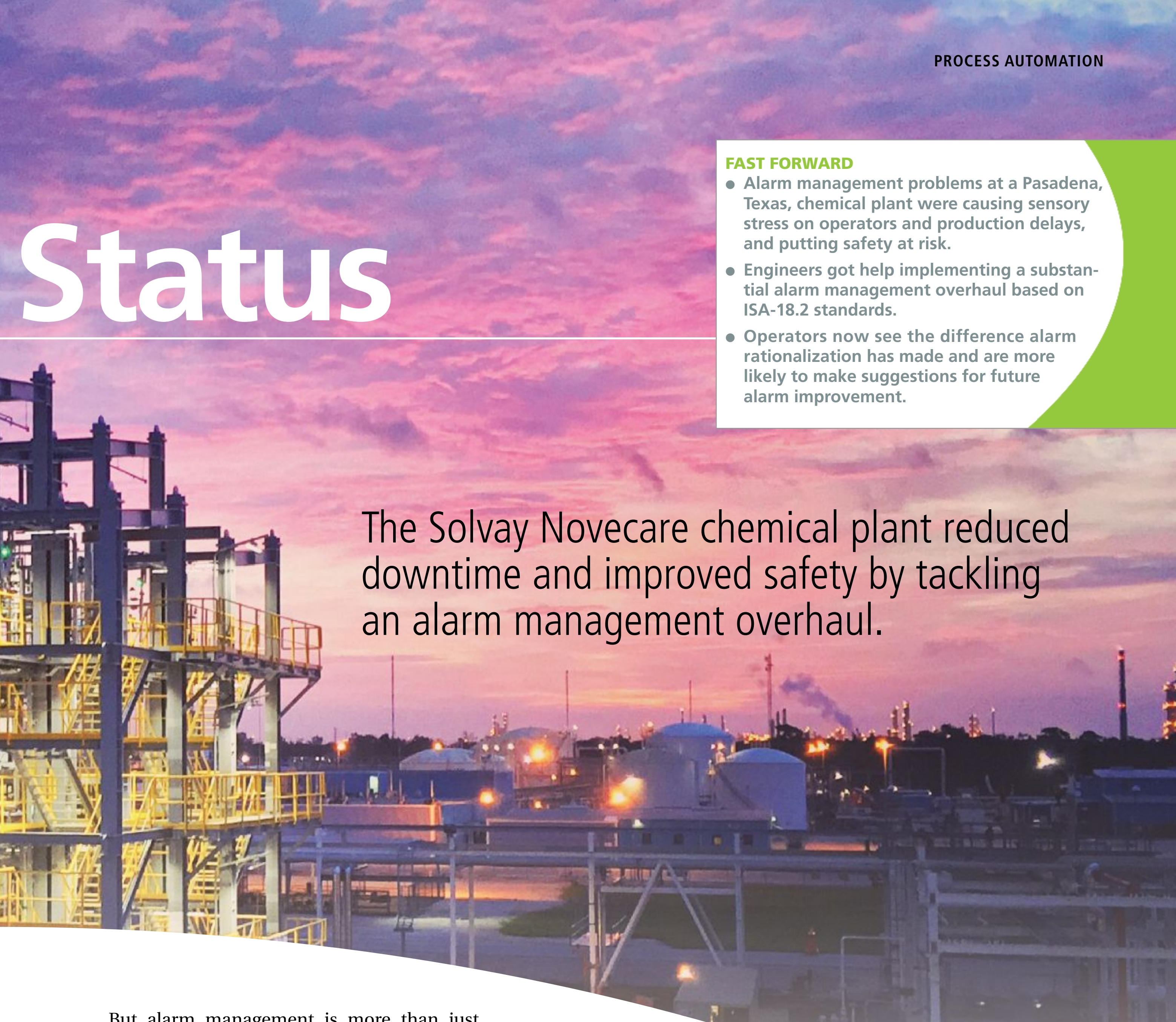
From Alarm Floods to 'Highly Protected'

By Ryan Scofield, CAP, Tracy Blauvelt-Heilaman, and Susan Chambers

The Solvay Novecare chemical plant in Pasadena, Texas suffered from nuisance alarms, "critical" alarms that were not critical, and production delays due to alarms being missed. It needed a stronger alarm management program to create a safer and more productive plant. So Solvay engineers sought help to create and execute a program that would relieve the sensory stress on their operators, eliminate production delays, and improve overall plant safety. Other goals of the alarm management program transformation were to achieve the highest level of underwriting and lowest premium for industrial insurance, and to establish baseline alarm management practices that could be rolled out to other sites.

The Pasadena plant, which opened in November 2015, operates a large-scale, "on pipe" alkoxylation unit as part of a batch process. Alkoxylates are used as emulsifiers, detergents, and wetting agents and are the chemical foundation for a wide range of Solvay Novecare specialty surfactants. Situated in the integrated industrial campus of LyondellBasell's Equistar Chemicals affiliate, the plant is supplied with its key raw material, ethylene oxide, via pipeline, which enhances the sustainability and surety of supply.

Alarm management problems were affecting operations directly and indirectly. Operators were overloaded with nuisance alarms, oftentimes filling three to four pages of the alarm summary with stale alarms. This caused the operators to ignore alarms, which reduced their situation awareness and made it hard to notice new alarms.



Status

The Solvay Novecare chemical plant reduced downtime and improved safety by tackling an alarm management overhaul.

FAST FORWARD

- Alarm management problems at a Pasadena, Texas, chemical plant were causing sensory stress on operators and production delays, and putting safety at risk.
- Engineers got help implementing a substantial alarm management overhaul based on ISA-18.2 standards.
- Operators now see the difference alarm rationalization has made and are more likely to make suggestions for future alarm improvement.

But alarm management is more than just getting the alarm rate below one to two alarms every 10 minutes. It is not just quantity that is important. It is also quality. If you focus on quality—ensuring each individual alarm meets the definition criteria—then the quantity issue takes care of itself.

For example, because of the flood of nuisance alarms, the alarm horn had been left disabled after commissioning. That meant no audible notification was generated for alarms or for batch recipe prompts. This lack of audible notification made it more challenging for the operators to stay on top of the process and to know when new alarms came in. Occasionally, this led to production interruptions when key utility equipment shut down and went unnoticed.

Another problem was that a large percentage of alarms were given the highest priority, "critical," by default. This made it hard for operators to distinguish importance. It was also misleading, because many of the alarms were not critical. If everything is critical, then nothing is critical. This puts extra burden and stress on the operator. There was also no training for engineers about basic alarm management principles, so even they overlooked the lurking alarm problem in favor of troubleshooting the day's production problems.

Partners in transformation

Solvay engineers knew they could use some partners to help them with such a substantial alarm management overhaul. They chose to work with Emerson Automation Solutions, exida, and Puffer-Sweiven. The product certification and knowledge company exida specializes in automation system safety, alarm management, cybersecurity, and availability. Its SILAlarm tool and alarm management professionals brought the Solvay team step by step through the alarm rationalization process. Puffer-Sweiven is an Emerson Impact Partner, which means it is a local point of contact for sales, service, and applied engineering for Emerson Automation Solutions in Central Texas and the Texas Gulf Coast.

Solvay contracted with exida to implement a holistic alarm management approach, starting with the Pasadena plant, that would be intentionally designed as a baseline for other Solvay Novecare sites. Applying the ISA-18.2 standard, which is a recognized and generally accepted good engineering practice (RAGAGEP) by OSHA, was key to developing a successful alarm management program and is the basis of exida's recommendations.

ISA-18.2 defines a recommended workflow, called the alarm management life cycle, which Solvay embraced as its foundation for success. Most companies jump into alarm remediation (bad actor knockdown) without first establishing guidelines or setting goals. For this project, the company wanted to discuss existing alarms, as well as find missing ones. The life-cycle approach defined in ISA-18.2 is the right way to achieve that. A step-by-step process brought Solvay the results it needed from its alarm management overall.

Step 1: Benchmark performance

One of the initial steps was to benchmark the performance of the alarm system. Benchmarking identifies systematic issues and sets the baseline for judging performance improvement. ISA-18.2 defines recommended key performance indicators (KPIs), such as the average number of alarms per day, alarm priority distribution, and number of stale alarms. So, with the help of Emerson's DeltaV Analyze, the Pasadena site compared actual to recommended performance.

Step 2: Develop an alarm philosophy document

With the benchmarking step complete, the team moved on to developing an alarm philosophy document (APD) as the foundation of its alarm management program. The process started with exida leading a one-day training session for the site alarm management team, a cross-functional representation from operations, engineering, and maintenance. With training, the team members aligned their scattered ideas with the actual RAGAGEP practices found in ISA-18.2. The training also reviewed the alarm management functionality available directly in the DeltaV control system and how it could be used to improve performance of operator response to alarms.

Following training, exida led a two-day workshop with the team to develop the APD. The exida APD template is comprehensive; it addresses the entire life cycle to ensure that the necessary work practices are in place to drive performance improvement and to sustain it over time. Getting started is the hardest part, and operations groups at every site wanted a specific starting point, so that they did not have to reinvent the wheel. The APD was written with the understanding that it could be tweaked for each site with minor effort.

Operators got a better understanding of the process, pay more attention to the alarms they do get, and are more likely to make suggestions for future alarm improvement.

Establishing a consistent and objective methodology for alarm prioritization was an important goal for the alarm philosophy. Solvay aligned its alarm priority matrix with its existing corporate risk management documents, including consideration for risks to people, environment, assets, quality, and productivity. This ensures a common approach to consequence evaluation is used for process hazard analysis and alarm rationalization.

The alarm philosophy document is truly the core of Solvay's program. Developing it forced the company to think about purposeful alarm management. What alarms are actually significant? What is in the way of recognizing them now? How can we provide clear information for the very human operator? How do we resist the next urge to add yet another brighter light or louder horn to bother the operator about the latest perceived imperative? Without the structure of the APD, the company would just be playing "Whac-A-Mole" forever.

				Access			
List Name	Description	Priorities	Areas	Banner	Main toolbar	Dashboard	Overview
Alarm List	All alarms with a corrective action required	8-15	All except Maintenancxe	Y	Y	N	Y
SIS Interlocks	SIS interlock trips, bypasses, and forces	All	Interlocks_SIS	Y	Y	Y	Y
Suppressed	Suppressed alarms	All	All		Y	N	Y
DCS Interlocks	DCS interlock trips, bypasses, and forces	All	Interlocks_DCS			Y	Y
Maintenance	PV_BAD, HART alarms, hardware diagnostics, etc.	All	Maintenance				Y
Bypasses	Bypasses for SIS and DCS interlock plus EMs and phases	BYPASS	All			Y	Y
Simulation	IGN_PV, simulated inputs, and forces	Simulate	All				Y
Prompts	All EM/Phase prompts	7-8	All			MEC Bottom Right	Y

Figure 1. A dedicated summary display for the different categories of alarms gives operator access as appropriate from the banner, main toolbar, dashboard, and overview display.

Source: Solvay

Step 3: Identify and rationalize alarms

Having a solid alarm philosophy in place, the team was ready for rationalization. Solvay selected the SILAlarm tool, a DeltaV Alliance Program product for alarm management by exida, to be its master alarm database (MADB). SILAlarm was seeded with Solvay-specific details defined in the APD, such as the priority matrix, the DeltaV color scheme, and the urgency matrix. All DeltaV–configured alarms were also imported directly into SILAlarm.

With initial coaching from exida, Solvay used the SILAlarm MADB-guided tools to rationalize and document each alarm. The purpose of rationalization is to ensure that all alarms presented to the operator are (a) actionable, (b) represent an unexpected situation, and (c) are prioritized to indicate their relative importance and urgency. Rationalization is a systematic, bottoms-up approach that ensures alarm management fundamentals are met; "bad actor knockdown" is a reactive process.

The Solvay team knew that following the APD and implementing alarm rationalization represented a paradigm shift for operations. To sow the seeds of success, the team made sure that operations was heavily involved in rationalization with participation from all shifts. Direct involvement in the improvement process increased enthusiasm amongst all plant personnel. Operators gained a new perspective on their role and a better appreciation for engineering. Operators and engineering are collaborators now. As a result, operators are more likely to raise concerns and potential issues to the alarm team. This also enabled transition out of "project" mode and into ongoing continuous improvement mode, which is the essence of the lifecycle approach.

An important part of the rationalization process is to document in the MADB the likely cause, consequence, corrective action, and allowable time to respond for each alarm. The senior operators had a great deal of insight, effectively transforming rationalization into a knowledge capture process. They identified redundant alarms, which alarms would come first in a sequence, and causal events and patterns. Junior operators grew from the experience (what does it mean when I get this alarm?) and thought about things differently the next time they were back at the human-machine interface console.

Rationalization takes effort and requires patience. The Solvay team rationalized approximately 9,000 alarms over a six-month timeframe. To prevent burnout, meetings were held twice monthly for no more than 5.5 hours at a time. As a parallel benefit, the rationalization exercise even uncovered maintenance issues such as transmitter problems, equipment problems, and process problems.

Step 4: Leverage DeltaV alarm system

SILAlarm allows all the rationalization results in the MADB to be imported directly into DeltaV, automatically updating alarm configuration and DeltaV Alarm Help. This saved significant time and prevented errors from manual entry. Now, when a new alarm occurs, the operators can quickly call up Alarm Help to review the cause, consequence, corrective action, and time-to-respond information for that alarm as it was captured during rationalization.

One of the outcomes of the APD was defining how to best leverage the alarm management functionality of the control system to better support operations. The team tailored the alarm priority system to differentiate and segregate alarms from batch prompts (with audible annunciation and without), bypasses (interlocks, equipment modules, and phases), indication of simulated/forced variables, and reports (situations that do not require a timely response or require no response at all).

The team at Puffer Sweiven created a dedicated summary display for the different categories with operator access as appropriate from the banner, main toolbar, dashboard, and overview display (figure 1). These displays are a way to improve the operator's situation awareness while also improving their ability to focus on alarms and batch status (now that non-alarms are no longer mixed in). The APD defined a consistent approach to audible annunciation (alarm horns) for the control room and in the field, which was implemented accordingly in DeltaV.

The Puffer Sweiven team also was an instrumental resource in implement-

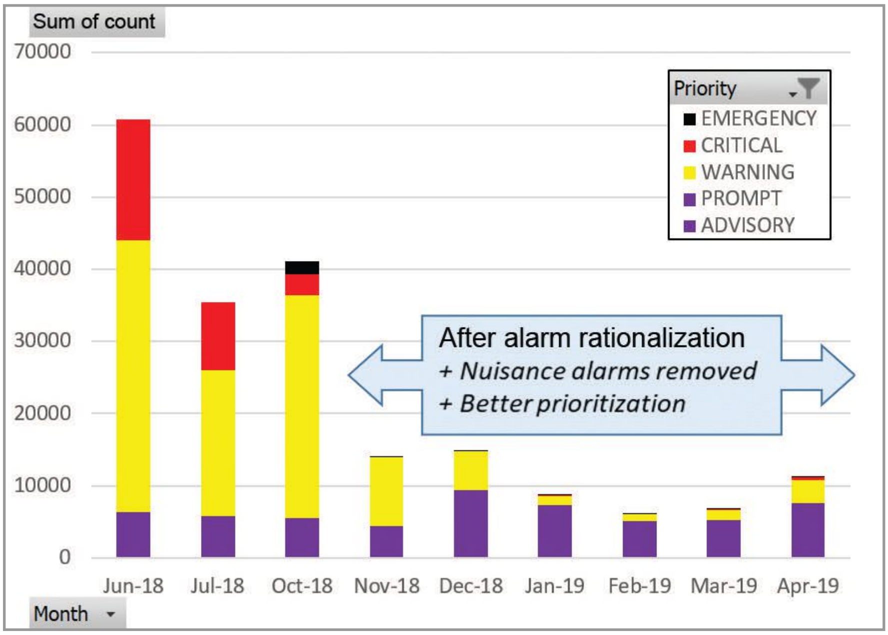


Figure 2. After rationalization, alarms were reduced and reprioritized based on importance, with the distribution of alarm priorities brought in line with ISA-18.2 recommendations.

Source: Solvay

ing conditional alarms and other advanced logic to make the alarms most useful for the operators. Conditional alarming allows an alarm to be dynamically enabled or disabled based on a status or indication. For example, a low discharge pressure alarm on the outlet of a pump can reference the pump RUN status, in addition to the pressure value, when determining whether to annunciate. That means what was once a common nuisance alarm—the low discharge pressure alarm being triggered just by the pump being turned off—can be eliminated.

Results: Better operator understanding

When critical alarms are rare, they really get the operator's attention when they do occur. ISA-18.2 recommends that the distribution of alarm priorities be about 5 percent high priority, about 15 percent medium priority, and about 80 percent low priority. By following the standard's alarm priority matrix during rationalization, Solvay's alarms were reduced and reprioritized based on importance (figure 2). Previously, a majority of alarms were default categorized as critical, making it impossible for operators to distinguish their true importance. Now operators have a clearer understanding of what is important.

More Information on the ISA 18.2 Standard

Sovay's alarm reduction and reprioritization followed recommendations found in ISA-18.2, *Management of Alarm Systems for the Process Industries.* First published in 2009, this standard is managed by the ISA18, Instrument Signals and Alarms committee, chaired by Donald G. Dunn and Nicholas P. Sands. The committee "establishes terminology and practices for alarm systems, including the definition, design, installation, operation, maintenance and modification, and work processes recommended to effectively maintain an alarm system over time."

Current ISA18 standards and technical reports include:

- ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*
- ISA-TR18.2.1-2018, *Alarm Philosophy*
- ISA-TR18.2.2-2016, *Alarm Identification and Rationalization*
- ISA-TR18.2.3-2015, *Basic Alarm Design*
- ISA-TR18.2.4-2012, *Enhanced and Advanced Alarm Methods*
- ISA-TR18.2.5-2012, *Alarm System Monitoring, Assessment, and Auditing*
- ISA-TR18.2.6-2012, *Alarm Systems for Batch and Discrete Processes*
- ISA-TR18.2.7-2017, *Alarm Management When Utilizing Packaged Systems*
- ISA-18.1-1979 (R2004), *Annunciator Sequences and Specifications*

More information is available online at www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa18.

Alarm rationalization successfully eliminated nuisance alarms and reduced alarm load by 84 percent. The three to four pages of standing alarms were reduced to only 10 to 12 alarms active at any one time. The alarm horn was turned on. Now if utility upsets occur, the operator quickly notices and can investigate or call for maintenance to resolve the issue before there is a production delay.

Operator involvement was key to the success of implementing SILAlarm. Operators got a better understanding of the process and the initiative and gave alarm-help suggestions relevant to the work they do. They see the difference alarm rationalization has made, pay more attention to the alarms they do get, and are more likely to make suggestions for future alarm improvement.

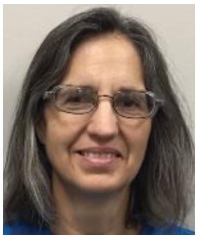
One of the most notable benefits of the alarm management program was achieving Highly Protected Risk (HPR) status from Solvay's insurance underwriter. The HPR designation reduced the plant's insurance premium and means that the Pasadena facility meets the highest industry standards for property protection and risk management. Only 6 percent of the insurer's customers reach this status. The Pasadena plant was only the eighth Solvay plant in the world to reach that status.

Solvay made substantial improvements to Pasadena's alarm program, relieving sensory stress for the Pasadena operators and allowing them to focus on the important information. There is still work to do, but that is the nature of a life-cycle approach. The support of exida's alarm management professionals and SILAlarm tool, along with the alarm tools in DeltaV, have facilitated the company's success. Going forward Solvay wants to multiply the accomplishments from Pasadena by applying them at other facilities. ■

ABOUT THE AUTHORS

Ryan Scofield, CAP, is global automation manager at Solvay Novecare. For more than 20 years, Scofield has provided hands-on training in the field and at seminars and shared expertise in capital project execution, instrumentation, batch automation, and manufacturing execution systems.

Tracy Blauvelt-Heilaman is an automation engineer at Solvay with more than 20 years of experience in specialty chemical manufacturing environments. Blauvelt-Heilaman helps teams establish and maintain high work standards for robust and safe operations.



Susan Chambers is a Solvay Pasadena automation engineer. Her duties include instrument and electrical support on projects and alarm rationalization.

Choked Flow in Control Valves

Choked flow is a poorly understood phenomenon that can affect control valve sizing, along with trim and material specification.

By Katherine Bartels and Adam Harmon

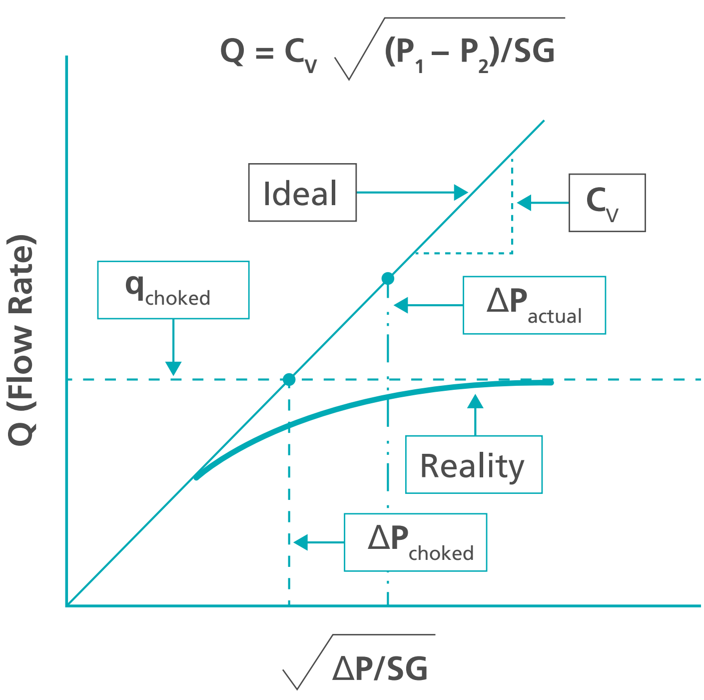


Figure 1. In an ideal world, flow rate through a valve rises as the pressure drop across the valve increases. In reality, the maximum flow will be limited due to choked flow conditions.

Choked flow in control valves is a subject of serious concern for industrial users. The term is usually associated with destructive process conditions that can damage valve internals or expose operators to noise levels well above OSHA limits. Although choked flow is not always the cause of these conditions, it may indicate when they occur.

This article describes the phenomenon of choked flow and shows why it occurs and how it can be predicted. It also explains when choked flow conditions are damaging and how this damage can be reduced or avoided.

What is choked flow?

If the inlet pressure (P_1) and valve flow area are fixed, the flow through a valve will normally rise as the downstream pressure (P_2) is reduced. The "Ideal" line in figure 1 illustrates this point, showing how liquid flow rises linearly when charted against the square root of the differential pressure across the valve divided by specific gravity.

In actuality, the maximum liquid flow through the valve can never exceed a choked flow limit, and at this point flow will increase no further, no matter how low the P_2 pressure is reduced.

A similar phenomenon occurs with valves in gas service. If the P_1 pressure and flow area remain fixed, flow through the valve will rise as P_2 is reduced, but at some point, choking will begin to

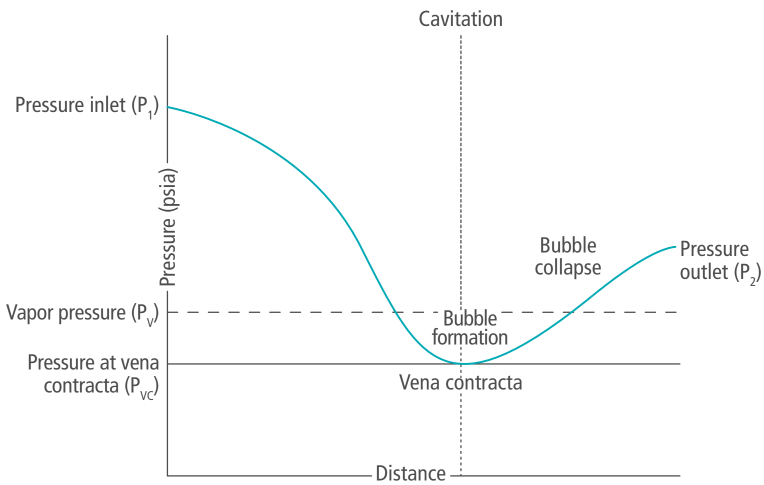


Figure 2. This graph shows a typical pressure curve of a cavitating liquid passing through a control valve. If P_2 is reduced still further, the expanding vapor will create an increasing pressure drop and eventually limit flow.

occur and the flow will rise no higher, regardless of the value of P_2.

Why does choked flow occur?

In liquid applications, choking is a result of the reduction in pressure through the control elements. Figure 2 shows the instantaneous pressure as liquid moves through a control valve. The inlet and outlet cross-sectional areas of a valve are much larger than the control area, such as the cage or the area around the plug and seat. Because the total flow at any location in the valve is the same, the liquid velocity in the reduced area (vena contracta) must be much higher to pass the same flow.

By Bernoulli's law, the total energy at every point in the flow stream is constant, so if velocity is increased, pressure must fall. As the fluid passes through the restriction, it speeds up, lowering the pressure at that point. Once the liquid enters the much larger outlet piping, the flow rate slows, and some pressure is recovered. This pronounced pressure dip becomes more dramatic as flows are increased.

If the instantaneous pressure in the vena contracta falls below the vapor pressure, then vapor bubbles will begin to form as the liquid begins to boil. The conversion to vapor increases the volume of the fluid and begins to restrict flow. If the downstream pressure is lowered still further, the vapor volume will increase to the point that flow throughput can increase no further, regardless of how low the downstream pressure is reduced. This condition is called choked flow.

In gas applications, the vapor velocity through the valve will increase until the vapor reaches sonic velocity. At this point, the vapor can go no faster because a standing shock wave forms and limits flow. Further reduction of the downstream pressure will have no effect on flow through the valve.

Choked vapor flow conditions are very common in relief valves and control valves with very high flows, but can also occur in high velocity flare headers at piping transitions. Choked flow is also common in vacuum systems, because the low air pressures found in these systems greatly reduce the speed of sound, increasing the likelihood of standing shock waves.

Choked flow misconceptions and issues

Choked flow by itself does not generally damage a valve, but there are flow conditions commonly associated with choked flow that can create problems, including:

Noise levels: Choked flow does not directly create noise, but high noise can result from process phenomena normally associated with choked flow. In liquid systems, cavitation can be present during choked flow, which creates noise and can ultimately damage the valve. As downstream pressure is reduced, cavitation transitions to flashing. While cavitation can have a high sound pressure level due to the implosion of the collapsing vapor bubbles from micro-jets and shock waves, flashing will have reduced noise due to the resulting two-phase flow.

In vapor flow, noise will rise significantly as the velocity turns sonic. As the downstream pressure is reduced, the extra energy is converted to sound energy. Valves with excessive pressure drop can generate sound levels greater than 100 dB.

With either liquid or vapor flows, the overall level of noise is usually related to the differential pressure across the valve. When choking first appears, noise will be present but may not be excessive. As the downstream pressure falls, noise will increase dramatically and can damage valve internals and subject operators to unsafe sound levels.

Flashing and cavitation: A common misconception is that choked flow conditions require flashing conditions, but choked flow can occur under cavitating conditions as well. As shown in figure 2, cavitation will result when the P_2 pressure rises

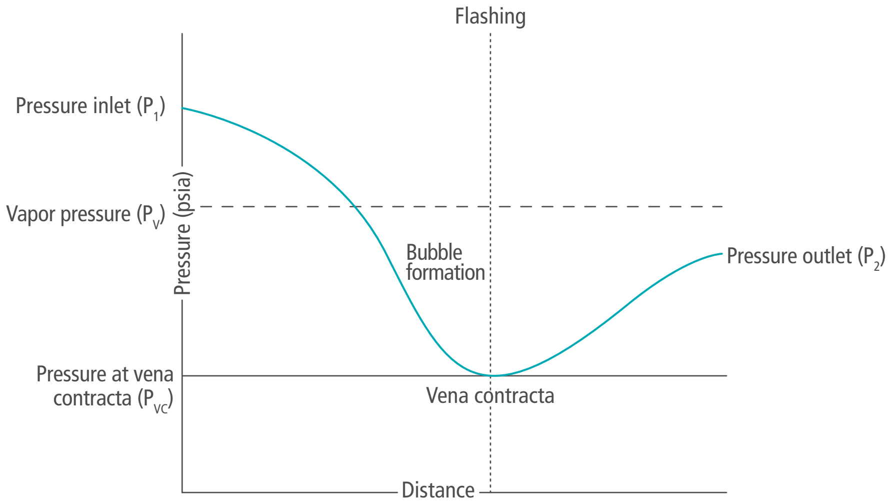


Figure 3. This graph shows a typical pressure curve of a flashing liquid passing through a control valve. Fluid enters the valve as a liquid and exits as a vapor.

above the vapor pressure of the liquid. When this occurs, the bubbles collapse and turn back into liquid. If the P_2 pressure remains below the vapor pressure, the liquid will boil and flash to vapor as it passes through the valve and remain a vapor as it exits (figure 3).

Incipient cavitation will not usually result in fully choked flow. However, as cavitation becomes more pronounced, the flow will begin to choke, and the overall flow will deviate from the ideal flow curve as shown in figure 1. The level of cavitation (and extent of choking) is dependent on the properties of the liquid; the process pressure, temperature, and flow; the inlet and outlet piping; and the specific construction and parameters associated with the valve itself.

Flashing may or may not indicate choked flow. If the valve differential pressure is high, the P_2 pressure is well below the vapor pressure, and the flow is low, the flow through a valve could be flashing but not choked.

Valve damage due to choking: Users often assume choked flow conditions will damage the valve. However, there are times when a valve is choked and the damage is minimal, and there are times when the valve is not choked and the rate of damage is significant.

Cavitation can ultimately damage a valve. As the bubbles collapse, they form microjets and create localized shock waves that erode valve internals and downstream piping. As discussed above, cavitation can occur without necessarily fully choking the valve flow.

Flashing conditions can create valve damage as well, but this is typically less pronounced than cavitation damage, and is usually worse at very low valve openings when the valve flow is probably not choked. As the valve opens further, the flow may become choked, but the valve damage will likely be reduced as the plug moves away from the seat.

Excessive noise can also damage the valve due to high vibration and metal fatigue. As discussed earlier, the amount of noise generated varies significantly based on process conditions, so the noise may not be directly associated with flow choking. Cavitation, flashing, and noise damage can be alleviated and even eliminated by specifying appropriate valve body designs, special valve trims, and materials of construction (figures 4 and 5).

Low recovery valves (such as globe valves) generate a much less pronounced pressure dip as the flow passes through, so cavitation is reduced. Special anticavitation trims (figure 5) can reduce the risk of cavitation damage even more by either further minimizing the pressure dip, or by directing the cavitating liquid into the center of the flow passage to minimize damage to the valve internals and walls.

Hardened alloys can be used for critical valve internal components to reduce damage caused by flashing or cavitation. Noise can be significantly reduced by using low noise trims, inlet and outlet noise attenuators, or downstream modal noise attenuators.

Valve sizing: Calculating a choked flow scenario is based upon process conditions and flowing media parameters for a given valve position. The fact that a valve is choked for a unique combination of parameters does not mean it cannot pass more

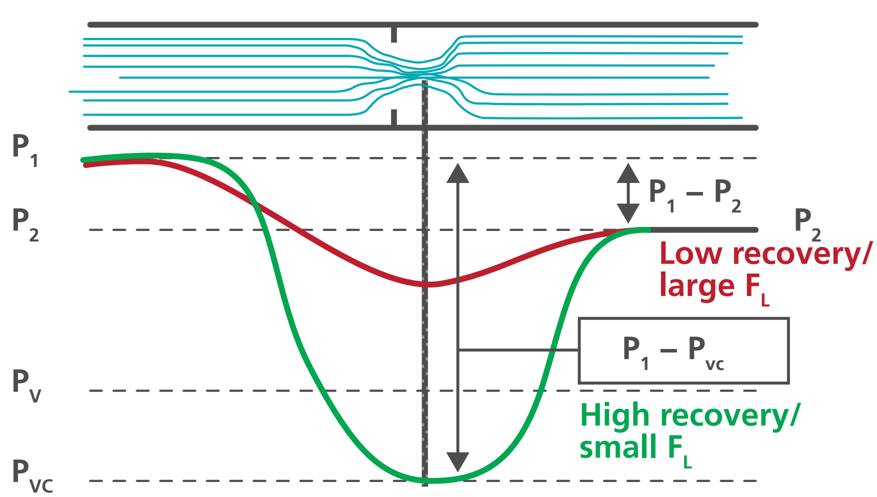


Figure 4. This graph compares the vena contracta pressures of a high recovery (ball, butterfly) valve versus a low recovery (globe) valve for the same process conditions. A high recovery valve creates significantly lower internal pressures, increasing the likelihood of cavitation.

flow, as an increase in flow can often be obtained by increasing the Cv of the valve. Software programs are available to predict choked flow conditions and estimate the maximum flow, as described in the subsequent section.

Predicting choked flow

Many valve vendors have control valve sizing programs that can predict choked flow conditions and help users size the valve correctly. However, these programs are only as accurate as the input data, so the correct process and valve information must be entered.

The presence and extent of flow choking depends on many process conditions, including the physical properties of the fluid involved, flow rates, upstream and downstream pressures, process temperature, and inlet and outlet piping configurations—as well as a number of details associated with the control valve itself. Special parameters, such as pressure drop ratio, pressure recovery factor, and cavitation index, help predict exactly when cavitation or choking will occur, and how much flow a valve will pass. Because the parameters for each body style and trim are different, each option must be evaluated individually to determine the actual flow that can be safely passed under a specific set of process conditions.

Such sizing calculations can become complicated, especially when several trim options are available, so it is wise to consult your valve vendor to help evaluate options and determine the best solution for your application.

Valve selection

Choked flow, in and of itself, is not a cause for concern. The confusion stems from the association of choked flow with many negative phenomena that can affect and damage control valves. When faced with the possibility of choked flow, or if there are concerns or questions about how to proceed with valve sizing or selection, contact valve vendors for technical support. They can usually provide valve sizing programs that predict when choking will occur and its impact on valve sizing and selection. They can also help users choose the best combination of materials and trim designs to alleviate damaging conditions. ■

Figure 5. Special valve trims, such as the Emerson Fisher Whisper III trim, can be employed to attenuate noise, reduce cavitation, or direct cavitating liquids away from valve components—all of which minimize damage to the valve.

Figures all courtesy of Emerson

ABOUT THE AUTHORS

Katherine Bartels is a design engineer at Emerson Automation Solutions, with a focus on custom anticavitation valves. She graduated with a BS in mechanical engineering from Iowa State University and has been with Emerson for six years.

Adam Harmon is a senior design engineer at Emerson Automation Solutions, with a focus on valves in steam conditioning applications. He has a BS in mechanical engineering from Iowa State University and has been with Emerson for 11 years.

Meet 2020 ISA Fellow Donald Dunn

Early in his career in 1998, Donald Dunn worked with Lion Dale Chemicals. As part of his role, he performed incident investigations and noticed that one of the root causes of many incident investigations was a causal factor of operators not responding to alarms. "Alarm floods was the biggest problem," he explained. "They'd get so many alarms that they didn't know what to respond to. That experience is what drove me to get involved in alarm management, industry safety, and ultimately ISA18."

Now, as an ISA Fellow, Dunn is being honored for many years of work on the education and standardization of terminology, as well as requirements and guidance related to alarm management and process industry safety. Currently, Dunn works as a senior consultant with WS Nelson in New Orleans, though he lives in Houston. He is also a senior member of the Institute of Electrical and Electronics Engineers (IEEE).

"Within the automation realm, my most significant accomplishment is the effort that Nick Sands and I put forth to cochair ISA-18.2, the standard for alarm management," Dunn said. "It was the first global standard for alarm management. The standard uses a life-cycle approach, following an alarm from cradle to grave. It covers a multitude of topics, such as implementation, operation, and maintenance."

When Dunn first joined ISA and started working on updating and developing other standards ahead of the development of ISA-18.2, he went to an ISA show in Houston in 2003. There, he went to a meeting with a managing director who was seeking someone to chair the committee and develop a standard. The managing director asked Dunn to co-chair the committee because Dunn had been involved in the development of similar standards for many years. Dunn happened to be sitting next to Nick Sands, whom he had just met. "I said, 'I will happily co-chair if this guy right here would co-chair it with me,'" Dunn explained. The two ended up working together until 2009 to put together and finally publish the ISA-18.2 standard.

"Learn your craft and get involved in organizations like ISA and IEEE."
—Donald Dunn

Sands recruited Dunn to run for vice president of the ISA Standards and Practices Development Board. He was elected in 2009. During his time on the board, Dunn discovered that ISA was not charging for its standards, which are intellectual property. "I spent three years discovering why that was the case and developing a consensus to change it," he said. "We were running on a deficit within the standards and practice portfolio. I worked very hard to change that." And he did; the standards portfolio now turns a profit for ISA.

Dunn says ISA membership has both helped broaden his knowledge base and expanded his number of industry contacts. "Engineers have worked on a lot of problems in the past, and if you encounter a problem and reach out to others for help, you might be surprised how many are willing to assist," he said.

During his career, Dunn noticed that lots of young engineers want to be managers, but he advises them to step back and ensure they know the field. "My number one piece of advice is to learn your craft," he said. "Number two is to get involved in organizations like ISA and IEEE. That will help you learn the technical side of your craft and develop your network. Those are the things I've tried to preach during my whole career." ■ *—By Melissa Landon*

ISA, MBI Answer Need for Industrial Cybersecurity Training in Germany

ISA and Maschinenbau-Institut GmbH (MBI), a service company of the German mechanical engineering industry association, or VDMA, are joining forces to offer a unique cybersecurity training program for German speakers. The first offering will be a Cybersecurity Fundamentals course for VDMA members located on the group's Fraunhofer site in Karlsruhe, Germany. With more than 3,300 members, the VDMA is the largest network organization and is an important voice for mechanical engineering in Germany and Europe.

Forged in response to the changing industrial security landscape and growing cyberthreats to automation networks and systems, the collaboration focuses specifically on training VDMA members in operational technology (OT) security standards. Both organizations will share training expertise based on the ISA/IEC 62443 set of cybersecurity standards.

"Cybersecurity needs to be addressed by our members, as recent global ransomware attacks have demonstrated their potential impact," said managing director Catherine John of MBI, which is the education academy of VDMA. "Our members need to adequately manage the associated cyberrisk stemming from the vulnerabilities of OT technology, coupled with the increased connectivity in our digital era."

"ISA is committed to providing high-quality technical resources that cover all areas of cybersecurity," said ISA European director Pieter van der Klooster. "We have covered the entire spectrum of cybersecurity education and advocacy, from the development of the world's only consensus industrial cybersecurity standard, to critical education, to compliance programs helping companies certify products and systems." ■

Bartusiak Helps Further Open Process Automation Systems

ISA executive board member Don Bartusiak, who has previously served as ExxonMobil's chief engineer for process control, has become known as a significant champion of Open Process Automation. During a presentation at the 2017 ARC Forum in Orlando, Fla., he announced ExxonMobil's next-generation multivendor automation architecture initiative and described how industry had had enough of closed, proprietary automation systems. The future, he said, was multivendor, interoperable, standards-based, open, and secure.

The future is here with the late June launch of the Coalition for Open Process Automation (COPA) QuickStart system, which is aligned with The Open Group O-PAS Standard, a "standards of standards" for industrial process automation developed by the Open Process Automation™ Forum (OPAF). Bartusiak's company, Collaborative Systems Integration, is the systems integrator for the COPA QuickStart offering.

Bartusiak said, "Industrial manufacturers have repeatedly told me that if O-PAS Standard–aligned systems were available, they would buy them. The COPA QuickStart system is our answer to that challenge."

COPA is applying years of research, collaboration, and investment by members of OPAF to bring to market industrial control systems (ICSs) that are built on industry standards for open, secure, and interoperable architectures. The COPA partner companies have engineered COPA QuickStart to incorporate components and technologies from multiple vendors into a single, advanced, and cohesive industrial control system. It is said to provide the critical first step in helping industrial manufacturers start learning, proving, and adopting open architecture ICS solutions into their operations.

"The move is analogous to the shifts that occurred when PC technology displaced minicomputers and mainframes," says Automation.com's Bill Lydon. "That extraordinarily successful trend accelerated efficiency and profitability for companies of all sizes."

Find out more at https://copacontrol.org or at www.opengroup.org/forum/open-process-automation-forum. ■

In Memoriam: Harold L. Wade

Harold L. Wade, PhD, PE—ISA Fellow, Life Member of IEEE, book author, and all-around Renaissance man—died on 24 May 2021. He was 91. Wade possessed more than 50 years of experience designing, applying, and installing process control systems in such industries as petroleum refining, chemical processing, textiles, and water treatment. He was the author of ISA's best-selling book, *Basic and Advanced Regulatory Control: System Design and Application, Third Edition*, which explains the application of basic and advanced regulatory control strategies. He also developed the process control training program, PC-ControLAB.

Wade received a BS in mechanical engineering from Oklahoma State University and earned both master's and doctorate degrees in systems engineering from Case Western Reserve University. Wade held technical positions at Honeywell, Foxboro, and his own consulting engineering firm, Wade Associates, Inc. in Houston, Texas.

Wade was a course instructor, a Donald P. Eckman award recipient for 2008, a long-time member of ISA's Automation Controls and Robotics Division (ACARD), and a member of the American Theatre Organ Society. ISA member Brad Carlberg called him "ISA ACARD's Renaissance Man" and noted, "We lost a truly great man with his passing." On ISA Connect, Carlberg shared a YouTube link to Wade's 2020 Christmas piano program, as well as a story in Wade's own words:

My first year in college I was a music major at Texas Christian University, Ft. Worth. Toward the end of the year, I decided I'm not going to make it as a professional musician, so I should change to my other choice, engineering. So, I transferred to Oklahoma A & M (now Oklahoma State University) as a mechanical engineering major.

At that time, few engineering students graduated in four years, but I felt bad that I had wasted my parents' money on a now-useless first year of college, so I was anxious to graduate as quickly as possible. After three years I only needed 24 semester hours of classes to graduate, so I signed up for all 24.

At the end of the previous semester, one of the instructors had asked me to be his teaching assistant in the hydraulics lab. Should provide a little bit of $$, I thought, so I accepted. (His assistant? I never saw him. I was the lab instructor, teaching my fellow students.)

This was the days of the "big bands" and fraternity and sorority dances every Friday and Saturday night. There were two dance bands on campus, and at the start of my final semester, the leader of the "excellent" band said, "Harold, we just lost our piano player. Could you play the piano for us?" That was a dream come true for me, so I said yes. Now I had 24 semester hours of coursework and two part-time jobs. My grade-point average took somewhat of a nose-dive, but I paid all of my college expenses for the semester and still had a few $$ left over. ■

Cybersecurity First Responder Credentialing Program Debuts

The ISA Global Cybersecurity Alliance (ISAGCA) and the Incident Command System for Industrial Control Systems (ICS4ICS) have announced the release of a cybersecurity first-responder credentialing program. The ISAGCA joined forces with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and cybersecurity response teams from more than 50 participating companies to adopt the Federal Emergency Management Agency's Incident Command System framework for response structure, roles, and interoperability. This is the framework used by first responders globally when responding to hurricanes, floods, earthquakes, industrial accidents, and other high impact situations.

Incident Command Systems have been tested during more than 30 years of emergency and nonemergency applications, throughout all levels of government and within the private sector. The approach guides companies, organizations, and municipalities in identifying an incident, assessing damage, addressing immediate challenges, communicating with the right agencies and stakeholders, and resuming day-to-day operations. The ICS4ICS framework applies traditional Incident Command Systems best practices to cybersecurity incidents, ensuring common terminology and enabling diverse incident management and support entities to work together.

ICS4ICS provides clearly defined command structures, including standard roles needed in a response, and the framework can scale to support small or extremely largescale incidents that affect many organizations. "For many years, we've needed ICS4ICS, to enable collectively organized cyber and physical responses in a unified way," said ISAGCA advisory board chairperson and ICS4ICS leader Megan Samford. "Credentialing cybersecurity first responders is an important milestone in this valuable public-private partnership."

ISAGCA has developed an adjudication process and certified its first four responders. "I'm proud to be one of them and stand ready to help companies recover from cyberincidents," said Samford, who is also VP and chief product security officer of Schneider Electric's energy management business.

The adjudication process, managed by a formal committee within ICS4ICS, consists of an application process and panel of incident command system subject-matter experts who evaluate the candidate's submittal. The inaugural round of credentialing recognized these cybersecurity experts:

- Mark Bristow, branch chief of cyber defense coordination at CISA, whose 15-year career with U.S. government cybersecurity agencies includes responses to incidents ranging from Ukraine cyberattacks to attempts by Russian government hackers to intrude on energy equities
- Neal Gay, senior manager of managed defense/industrial control systems at FireEye
- Megan Samford, ISAGCA chairperson; VP and chief product security officer of Schneider Electric's energy management business
- Brian Wisniewski, U.S. Army Reserve.

Find out more at www.isa.org/isagca or https://tinyurl.com/y75m5dyy. ■

ISAGCA Releases Cybersecurity Whitepaper

A new document from the ISA Global Cybersecurity Alliance organization provides an overview of ISA 62443-3-2, *Security Risk Assessment for Design,* as well as a summary of methodologies that can be used to execute an industrial automation control system (IACS) cybersecurity risk assessment. The included risk assessment work process is applicable to many sectors, including process industries, building automation, medical device manufacturing, power generation, water/wastewater treatment, and transportation. Download it for free from www.isa.org/ISAGCA. ■

New ISA Initiatives Support Being a Lifelong Learner

Steve Mustard, PE, C.Eng., CAP, GICSP

I took my Professional Engineer exams almost 30 years after graduating from university. I do not recommend doing this. Taking the Fundamentals of Engineering exam while you still remember all your engineering math from university is likely the better way to go. I also advocate taking your Principles and Practice of Engineering exam as soon as possible in your career.

Having said that, I will say that there is a sense of satisfaction when all the studying pays off and you achieve a certification or accreditation. I have also taken the Certified Automation Professional (CAP) exam. I did not do any of this because someone asked me to. Rather, I wanted to test my knowledge, challenge myself, and keep getting better at what I do.

There are other ways to show commitment as a lifelong learner than taking exams and achieving more letters behind your name. I have been involved in an ISA initiative to develop an exam for the Certified Mission Critical Professional qualification. As part of this, I was asked to write the study guide, *Mission Critical Operations Primer.* I am also a certified ISA trainer in cybersecurity and teach the IC31 and IC32 classes. There is always something new to learn, even from a class you are teaching. The questions from the students in these classes have given me new perspectives.

Since I immigrated to the U.S., the common element in my learning journey has been ISA. Gerald Wilbanks, former ISA President, was a key contributor to my PE study. I purchased the *Automation Body of Knowledge* (AutoBok) and CAP study guide to prepare for the CAP exam. I studied the ISA/IEC 62443 standard to prepare for teaching cybersecurity classes.

One of the things I am most proud to have been involved with is the Automation Competency Model. While this was developed for the U.S. Department of Labor and leveraged much of the work already done by ISA in the Certified Control Systems Technician (CCST), Certified Automation Professional (CAP) certifications, and the AutoBok, this model is applicable to the global automation profession.

And now, as president, I have had the great privilege to watch ISA embark on new learning initiatives in continued support of our automation profession. These new programs (coming out very soon) build on the traditional skills and knowledge required for automation professionals, adding further opportunities to develop. The first is an automation project management certificate, which will allow professionals to demonstrate their competence in managing complex automation projects. The other is the automation digital skills program, which is designed to provide automation professionals with the knowledge they need to work in the Industry 4.0 world and beyond.

With all of this, there is no better time for you to commit (or recommit) yourself to lifelong learning. I encourage you to get more involved with ISA, and in doing so, join a workgroup, become an ISA instructor, write a blog or a book, or see how many ISA certificates or certifications you can achieve. You are never too old to learn something new. Trust me—I am living proof! ■ *—By Steve Mustard*

ISA Certified Automation Professional (CAP)

Certified Automation Professionals (CAPs) are responsible for the direction, design, and deployment of systems and equipment for manufacturing and control systems. For more information, visit www.isa.org/training-and-certification/isa-certification/cap.

CAP review question

Which item below covers all aspects of electronic records including signatures, integrity and authenticity, record creation, audit trails, and archiving?

A. 21 CFR Part 12
B. 12 CFR Part 14
C. 21 CFR Part 11
D. 21 CFR Part 21

CAP answer

The answer is *C*, "21 CFR Part 11." Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the U.S. Food and Drug Administration regulations on electronic records and electronic signatures. It defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

References: Sands, Nicholas P. & Verhappen, Ian, *A Guide to the Automation Body of Knowledge, Third Edition*, ISA Press, 2019.

"Title 21 CFR Part 11" (https://www.ecfr.gov/cgi-bin/ECFR)

ISA Certified Control Systems Technician (CCST)

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. For more information, visit www.isa.org/training-and-certification/isa-certification/ccst.

CCST review question

An instrument location plan shows the __________ of each instrument:

A. location and wiring plan
B. location, elevation, and tag number
C. specification number and tag number
D. location, specification number, and elevation

CCST answer

The answer is *B*, "location, elevation, and tag number." Instrument location plans are valuable drawings when installing new systems. They show important physical characteristics about the instrument so that they can be installed easily and efficiently. The tag number identifies the instrument to be installed. Along with the location and elevation, the installer will know exactly where the instrument should be located, even before going to the specific location.

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

ISAGCA Responds to NIST Call for Standards to Fulfill Executive Order 14028

By Renee Bassett

ABOUT THE AUTHOR

Renee Bassett (rbassett@isa.org) is editor in chief for *InTech* magazine, *InTech Focus* ebooks, and Automation.com publications and ebooks. She is a journalist and project manager for print and digital publications with 20+ years' experience writing about industrial automation, IT/software systems, machine building, and related technology.

International Society of Automation Global Cybersecurity Alliance (ISAGCA) filed comments in response to a virtual workshop hosted by the National Institute of Standards and Technology (NIST) on 2–3 June 2021. The purpose of the workshop was to enhance the security of the software supply chain and to fulfill President Biden's Executive Order 14028, "Improving the Nation's Cybersecurity," issued on 12 May 2021.

Among other things, section 4 of that executive order (EO) directs the U.S. Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders in identifying standards, tools, best practices, and other guidelines to enhance software supply chain security. Those standards and guidelines will be used by other agencies to direct the federal government's procurement of software. The workshop focused on assignments in section 4 of the EO.

The goals of the workshop were to: share NIST's plans to develop software-related standards and guidelines called for by the executive order; and receive and discuss information and ideas about the approach and content NIST should consider in developing those standards and guidelines.

ISAGCA asked that several additions be considered, such as referencing selected parts of the ISA/IEC 62443 standard when defining critical software, product security development life-cycle requirements, and technical security requirements.

NIST requested position statements in five areas:

1. Criteria for designating "critical software."
2. Initial list of secure software development life-cycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.
3. Guidelines outlining security measures to be applied to the federal government's use of critical software.
4. Initial minimum requirements for testing software source code.
5. Guidelines for software integrity chains and provenance.

"ISAGCA member companies have a long history of adopting a standards-based approach for securing automation products and operating sites based on the ISA/IEC 62443 series of international cybersecurity standards. The scope of ISA/IEC 62443 standards applies to critical software in all phases of the automation solution life cycle," said Andre Ristaino, managing director of ISAGCA. The NIST Cybersecurity Framework (CSF) includes several key standards as informative references. Table 1 shows where the ISA/IEC 62443 standards align with the NIST CSF requirements.

In its response to NIST, ISAGCA asked that several additions be considered, such as referencing selected parts of the ISA/IEC 62443 standard when defining "critical software to the executive order," "product security development life-cycle requirements," and "technical security requirements" for automation components as standards to secure software for operational technologies (OT).

ISAGCA justified the "critical software" request stating the standard proposes "to define commands and essential functions, including parameters and associated data that must be properly protected either by built-in technical capabilities (ISA/IEC 62443-4-2), integrated system capabilities (ISA/IEC 62443-3-3), and/or procedural/organizational capabilities."

ISAGCA further requested that ISA/IEC 62443 4-1: *Product Security Development Life-Cycle Requirements* be referenced as a standard to secure the software development life cycle for OT.

To comply with NIST's security measures request, ISAGCA requested that ISA/IEC 62443 4-2: *Technical Security Requirements for Automation Components* be referenced as a standard to ensure software security capabilities for OT components.

ISAGCA requested ISA/IEC 62443 4-1: *Product Security Development Life-Cycle Requirements* (Section 9) be referenced to define the minimum requirements for testing software source code. ISA/IEC 62443 4-1, *Security Requirements for Externally Provided Components* requires software product development organizations to have a process to identify and manage security risks of these components used within the product.

ISA and its members have been ardent supporters of the NIST cybersecurity framework and contributed to the development of both NIST CSF in 2014 and the ISA/IEC 62443 standard.

Product suppliers have been developing automation products using ISA/IEC 62443 security lifecycle practices in their development processes since 2010.

Companies are having their development processes and products independently audited and certified to conform to ISA/IEC 62443 via accredited certification bodies in the U.S. and around the globe. Company examples include ABB, Aveva, Azbil, Bayshore Networks, Carrier Corp., CISCO, Eaton, Emerson Automation Solutions, Emerson Power & Water Solutions, GE Power Conversion, Hima, Hitachi, Honeywell, Johnson Controls, Nexus Controls, Rockwell Automation, Schneider Electric, Siemens, Toshiba, Yokogawa, Valmet, and Wartsila. ■

Function identifier	Function	Category identifier	NIST CSF category	IEC 62443
ID	Identify	ID.AM	Asset management	:2-4–SP.06.02/SP.01x
		ID.BE	Business environment	:2-4–SP.01x
		ID.GV	Governance	:2-4–SP.01x :2-1–ORG-02
		ID.RA	Risk assessment	:2-4–SP.02.01
		ID.RM	Risk management strategy	:2-1/2-4/3-3/4-1
		ID.SC	Supply chain risk management	IEC 62443-2-4
PR	Protect	PR.AC	Identity management and access control	:3-3–SR02.04/SR.02.07/SR.03.08x :2-4–SP.08x
		PR.AT	Awareness and training	:2-4–SP.01
		PR.DS	Data security	:2-1–DATA01-04/CRYPT-01-03 :2-4–SP.05.09x/SP.03.10x :3-3–SR.03.01RE(1) /SR.04.03
		PR.IP	Information protection processes and procedures	:2-1:ORG-02/NET-12 :2-4:SP.03.08x :3-3-SR7.6
		PR.MA	Maintenance	:2-4(complete) :3-3-SR.04.02
		PR.PT	Protective technology	:2-4-SP.08x :3-3-SR01.01–SR.02.07
DE	Detect	DE.AE	Anomalies and events	:2-4–SP.08x
		DE.CM	Security continuous monitoring	:3-3-SR02.08-SR02.12/SR03.09 /SR.06.01/SR.06.02 :2-4–SP.08x
		DE.DP	Detection processes	:2-4–SP.07.x/SF.06x
RS	Respond	RS.RP	Response planning	:2-4-SP.02.x/SP.12.x :2-4-ORG-08/10/02
		RS.CO	Communications	:2-4-SP.02.x/SP.12.x :2-1-ORG-x
		RS.AN	Analysis	:2-4-SP.02.x/SP.12.x :2-1-ORG-x
		RS.MI	Mitigation	:2-4-SP.02.x/SP.12.x :2-1-ORG-x
		RS.IM	Improvements	:2-4-SP.02.x/SP.12.x :2-1-ORG-x
RC	Recover	RS.RP	Recovery planning	:2-4-SP.12.x :2-1-ORG-x
		RC.IM	Improvements	:2-4-SP.12.x :2-1-ORG-x
		RC.CO	Communications	:2-4-SP.12.x :2-1-ORG-x

Table 1. Map of ISA 62443 to NIST CSF

Hopped-up Homebrew Automation

By Jason Wilson

When this homebrewer wanted to take his craft to the next level, he found that industrial controllers and valves were fermentation friendly.

After attending a local beer brewery tour several years back, I became fascinated by the detailed science and math underlying the production process. It did not take long for me to become a homebrew enthusiast, and in 2012 my wife and I fermented our first beer batches using a commercial kit of the type used by thousands. I would label these first three attempts as "not so good," but I was intrigued by the concept and kept improving my skills.

With a day job completely unrelated to the beer brewing field, it was necessary to learn more by reading books and gathering information on the topic. As time passed, I upgraded equipment and improved my skills, so I could have progressively better results. Realizing that progressing would demand careful control of the brewing process, it became important to research how to automate the system.

Recipe for success

The basic recipe for beer has been around for a very long time. Barley grain is malted, which means it is soaked in water and allowed to germinate, then dried and sometimes roasted, or kilned. At the brewery, this grain is crushed and introduced into hot water, creating the mash, and the heat converts the grain starches into sugars. The mash is boiled with hops to create unfermented beer, or wort. The wort is cooled, and then the yeast is introduced to perform the fermentation process of converting sugars into alcohol. Temperature control figures prominently at every step.

For instance, during the mashing process there are various enzymes that are activated once the temperature rises to a certain point, and then denatured once the temperature moves a little higher. One enzyme might be activated at 149°F and denatured at 152°, while other enzymes have varying and sometimes overlapping temperature ranges. The resulting final product's flavor is affected by which enzymes are active for how long, so the brewer needs to control the mash accurately to a target temperature profile for a specific time to take advantage of various flavor-impacting enzymes during the process. Even with a mechanical or digital thermometer, this is exceedingly hard to do by hand, and even in the best case requires constant manual attention and intervention.

Most homebrewers start with small kettles, burners, a cooler, and some other accessories—all of which they work manually. Results can be quite good, but obviously the manual steps can introduce a lot of variability and are time consuming. As homebrewers become more proficient, they recognize the need to gain better control of the process to make consistent and improved batches and confidently track improvements (figure 1).

Gearing up

With upgraded small-batch kettles and burners at hand, the next step was to reach out for inspiration from an acquaintance who teaches automation at a nearby technical college. Without any specific training in electrical, instrumentation, or controls programming, the complexity and expense of automation systems seemed a little intimidating. Hopefully, my hands-on handyman experience would be enough.

A key outcome of this connection was becoming introduced to the AutomationDirect website, where it quickly became clear how the company's solenoid valves, sensors, industrial controllers, and other associated items could help to automate a brew system. The parts were economical, and there was plenty of support information available to help build confidence. Also, it was quick and easy to obtain additional pieces and parts as the project developed.

Even without a programming background, it was easy for this first-time hobbyist to learn about and use the software (figure 2). The AutomationDirect website offered many helpful technical support documents and videos, and when it became necessary to reach out for phone support to get past a minor snag, their experts were very knowledgeable and helpful.

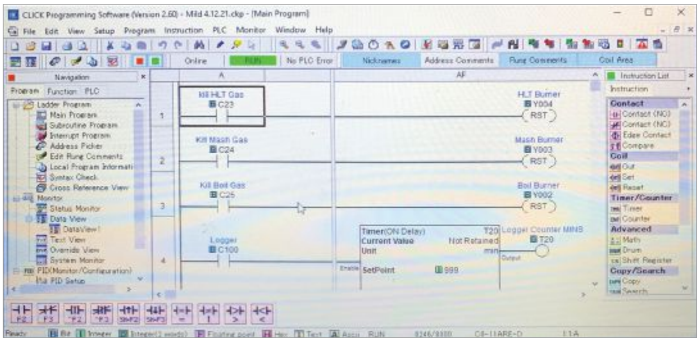
The first task was to automate the monitoring and control of temperature. The solution was to use an AutomationDirect CLICK programmable logic controller (PLC), with thermocouples wired to inputs using thermocouple extension wire, and the outputs connected to solenoids regulating gas flows. The burner was controlled to maintain temperature using on/off logic, and multi-event recipes allowed detailed configuration of time and temperature set points for each step (figure 3).

Another next step was to automate some of the brute-force tasks, such as filling and emptying the kettles. With a little plumbing, and some float level sensors and solenoid valves wired to the PLC, it was possible to control each of these steps accurately (figure 4). Almost all these products were stainless steel or food-grade components sourced from the AutomationDirect website.

With the basics well in hand, the project was soon moving into more advanced capabilities. After learning how to use a smartphone as a mobile human-machine interface (HMI), various HMI displays were configured to monitor the brewing status and change set points. The PLC was configured to perform some data logging to create a record of each batch, helping to replicate the best batches in the future, and enabling decisions to be made about

Figure 1. This homebrew rig started as a completely manual operation but is now monitored and controlled by an AutomationDirect CLICK PLC, level sensors, solenoids, and more. Its operation can be viewed and controlled remotely with a smartphone.

Figure 2. The CLICK programming software is free, easy enough for beginners to use, and includes enough functionality even for advanced applications.



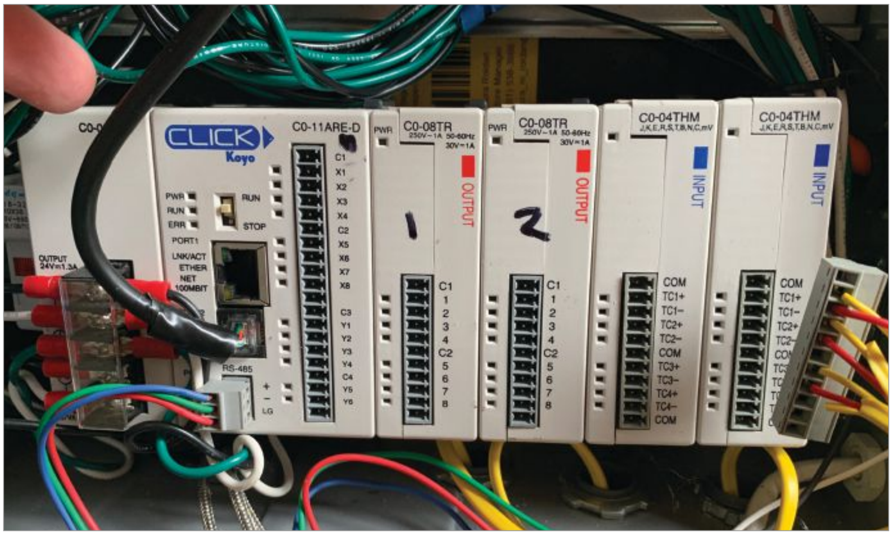


Figure 3. Input/output signals wired to various CLICK I/O modules from thermocouples for temperature, from level switches, and to solenoid valves enabled brewing temperatures and levels to be controlled.

Figure 4. Stainless-steel and food-grade float sensors and solenoid valves were used to automate the filling and discharging processes.

how and where to improve the recipe. With mobile/remote monitoring capability, it is now possible to confidently go jogging or do anything else while brewing beer, instead of hovering over the system like a mad scientist.

Brewing into the future

Bill Owens, who founded America's first brew pub in 1983, once said "Give a man a beer and waste an hour. Teach a man to brew and waste a lifetime." Many would say the word "waste" is a bit strong when describing a beverage that is among the most-consumed worldwide and is found in almost every culture, but one can see how it is easy to get excited about this hobby.

Today, the homebrew system is still under development, but none of the time spent so far has been a waste. On the contrary, it has been fun refining the brewing process and improving recipes. The experience with AutomationDirect products and the system built using them has delivered a lot of flexibility to experiment, and one day may enable the operation to be scaled up to a commercial level. ■

Figures courtesy of Jason Wilson

ABOUT THE AUTHOR

Jason Wilson works as an operations coordinator at SGS, which performs quality inspection services for goods around the world. He resides in Houston and uses a portion of his spare time to pursue his beer homebrewing hobby.

SUBMIT YOUR STORY

InTech magazine's Digitalization Diaries section is a showcase for case studies and first-person essays created in conjunction with Automation.com, a subsidiary of ISA. Digitalization Diaries seeks to capture and convey the real-world challenges and successes of digital transformation being experienced by members of ISA and the larger industrial automation community. Take notes and pictures during your next professional project and submit your story to content@automation.com with "Digitalization Diaries" in the subject line. Submit your success story to content@automation.com.

AUTOMATION.COM

ISA18 Update: Management of Alarms

ANSI/ISA-18.2, *Management of Alarm Systems for the Process Industries*, has found wide use and success in improving the development, design, installation, and management of alarm systems across the process industry sectors. The first edition, published in 2009, changed the world of alarm management with the introduction of activities grouped into the alarm management life cycle. A subsequent IEC version, IEC 62682, published in late 2014 and led by ISA18 co-chairs Donald Dunn and Nicholas Sands, added improvements, such as the elimination of country-centric criteria. The ISA18 committee then used the IEC version as a starting point for preparing the current 2016 ANSI/ISA version of the standard.

The ISA18 committee plans to begin working on the next revision of the standard in 2022. In the meantime, the committee has been busy with several projects—including one looking to the future of alarm management through the creation of a new working group 9 on the digitalization of alarm management activities. The scope of WG9, currently being developed, could include topics ranging from digital design to artificial intelligence for improved alarm system performance.

A new technical report being developed by ISA18 working group 8, led by Dale Reed of Rockwell Automation, is focused on alerts, events, prompts, and other notifications. The intent is to help users manage the notifications between the control system and operator that are not alarms, and other notifications not intended for the operator. The technical report is expected to be completed in mid-2022.

At the same time, ISA18 working groups are engaged in updating the following technical reports:

- ISA–TR18.2.3, *Basic Alarm Design*, which provides guidance on implementing the practices set forth in ISA-18.2. Following the life-cycle model of ISA-18.2, the document assumes that alarms to be addressed in basic alarm design have completed rationalization where attributes such as alarm set point and priority have been defined.
- ISA-TR18.2.5, *Alarm System Monitoring, Assessment, and Auditing*, which provides guidance on the use of alarm system analysis for both ongoing monitoring and periodic performance assessment. Monitoring, assessment, and audit are essential to achieving and maintaining the performance objectives of the alarm system. These activities can identify improvement opportunities in the other life-cycle stages, such as philosophy, rationalization, detailed design, implementation, operation, maintenance, and management of change.

ISA18 is also working on an update of ISA-18.1 (reaffirmed in 2004), *Annunciator Sequences and Specifications*. The purpose of the standard is to establish uniform annunciator terminology, sequence designations, and sequence presentation and to assist in the preparation of annunciator specifications and documentation. The standard is primarily for use with electrical annunciators that call attention to abnormal process conditions by the use of individual illuminated visual displays and audible devices. Annunciators can range from a single annunciator cabinet to complex annunciator systems with many lamp cabinets and remote logic cabinets. The sequence designations provided can be used to describe basic annunciator sequences and also many sequence variations. The standard lists types of information that should be included in annunciator specifications and types of documents that should be provided by manufacturers.

For information about ISA18 and its published standards and technical reports, please visit www.isa.org/isa18. ■

ISA18 Expert Receives Purdue Engineering Award

Joseph S. Alford, PhD, an ISA Fellow and long-time contributing expert on ISA18, has been honored with a 2021 Distinguished Alumnus Award from Purdue University's College of Engineering, Davidson School of Chemical Engineering. The award was given in recognition of his accomplishments over a 35-year career at Eli Lilly and Company "for his championing of key technical and auditing practices in the bio-pharma industry leading to the in-house design, development, validation, implementation, and application of computer-based process automation and data historian systems."

Alford has been an active participant and leader in ISA throughout his career, serving as a key contributor to ISA18 and as a member of the *InTech* Editorial Advisory Board. He received ISA's 2001 Douglas H. Annin Award in recognition of "outstanding achievement in the design, application, or development of the components in an automatic control system from the input measurement through the final control element." He is a Fellow and Life Member of ISA and the American Institute of Chemical Engineers. For more information, please visit: https://engineering.purdue.edu/Engr/People/Awards/Institutional/DEA/DEA_2021/Awardees/alford. ■

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.

Senior commissioning engineer

McDonough Bolyard Peck: Project assignments for this position in Fairfax, Va., include leading the review of the basis of design of the owner's project requirements, developing Cx specifications, HVAC plan reviews, concurrent reviews of submittals, on-site representation, project documentation of Cx issues, TAB verification and functional performance testing procedures, and the final Cx report. The commissioning engineer will represent the company in analytical and field assignments and will troubleshoot existing HVAC and temperature control problems and offer input for saving energy. The position requires significant experience with commercial HVAC systems. Experience should include three or more of the following: design, construction, installation, maintenance, testing and balancing, building automation temperature control systems, and troubleshooting operational issues. The engineer must have completed a minimum of eight projects . . . see more at Jobs.isa.org.

Manufacturing engineer

Aji Bio-Pharma Services: The company in San Diego is seeking a manufacturing engineer who will maintain and provide input to manufacturing equipment that supports biopharmaceutical manufacturing, including aseptic filling. The engineer will support end users in specifying, diagnosing, repairing, and upgrading manufacturing systems, including the completion of GMP-related documentation. A bachelor's degree in bioengineering, ChE, EE, IE, ME, or a similar field is preferred. Requirements also include a minimum of two to five years of relevant experience, at least two years of cGMP experience, a broad understanding of facility and utility systems, well-developed hands-on experience with manufacturing equipment, and an understanding of manufacturing systems and GMP requirements . . . see more at Jobs.isa.org.

Controls specialist manager

Southeast Louisiana Flood Protection Authority: The Operations Department oversees the staffing, operation, and maintenance of three permanent canal closure and pump station facilities along Lake Pontchartrain. All operations department staff are considered essential and expected to work on site for the duration of storm events. Job responsibilities are 50 percent operations and maintenance, including professional recommendations and design to repair or replace damaged electrical equipment, directing the outsourcing of specialized services, and providing periodic inspection reports; 30 percent technical functions, including operation and repair of pump stations' SCADA and troubleshooting Allen Bradley Ethernet/IP control systems; and 20 percent administrative, including cost estimates, schedules, budgets, and reports. Qualifications include the ability to develop and troubleshoot detailed PLC for code using the ControlLogix platform, the ability to develop large-scale HMI applications in the FactoryTalk environment with global objects, and proficiency as a systems integrator to connect multiple third-party systems together . . . see more at Jobs.isa.org.

Manufacturing engineer

Stryker: The company, in Cary, Ill., offers products and services in orthopedics, medical and surgical, and neurotechnology and spine to help improve patient outcomes. The manufacturing engineer is responsible for engineering support to manufacturing processes and projects. The successful candidate will use manufacturing data to implement continuous improvement and cost reduction of equipment and processes and support new product launches. Additional responsibilities include using Lean principles to simplify processes and workflows, troubleshooting equipment and determining root cause solutions, investigating product quality nonconformances, performing equipment validation, training technical and operations personnel, and collaborating with cross-functional teams to increase productivity, reduce costs and maintain regulatory compliance. The manufacturing engineer will also lead capital projects. The position requires a BS in engineering and one or more years of related work experience. Experience working in medical device, pharmaceutical, or other highly regulated industries (aerospace or automotive) is preferred . . . see more at Jobs.isa.org.

Senior Platform Electrical Engineer

Trane Technologies: The senior platform electrical engineer will work in Minneapolis to research, design, and maintain products for the Thermo King North America Trailer business. The position will collaborate cross-functionally across multiple regions and have frequent interaction with the company's global manufacturing facilities, dealerships, and customers as well as be responsible for delivering major new product development programs that meet specific performance and quality/cost/delivery goals. The senior platform electrical engineer will also provide technical support to Q&R and other functions, including product management, manufacturing, and field service. The minimum requirement for the position is a BS in electrical engineering and at least five years of engineering experience. Key competencies include experience with vehicle electrical system design and harness/interconnection systems; experience with electric machines, power electronics, and automotive networks; proficiency using electrical tools and instruments to perform tests, troubleshoot, and gather data; and proficiency with Pro/Engineer or Creo Schematic . . . see more at Jobs.isa.org.

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.

datafiles

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

USB HART MODEM

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

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

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

INDUSTRIAL CYBERSECURITY QUICK START GUIDE

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

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

Cybersecurity Investment Tax Credits

By Bill Lydon

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

Cyberattacks continue to grow worldwide, which has increased awareness and concern about utilities, industries, and personal risk. There is a universal understanding that this is a national security threat. In the U.S., I suggest the government consider creating cybersecurity investment tax credits for industry to stimulate more protection.

There have been many incidents that prove cyberattacks can bring down businesses and infrastructure. Most recently, the Colonial Pipeline ransomware attack shut down the largest gasoline pipeline in the U.S., which carries 2.5 million barrels per day of gasoline and other refined fuels.

This cyberattack had the biggest impact on physical operations of critical infrastructure in U.S. history. Some reports attribute the attack to a criminal group called "DarkSide," known for ransomware attacks. A recent report by Cyberreason estimates that the group has targeted well over 40 victims, with ransom demands ranging from $200,000 to $2 million USD per incident.

On 28 May 2021, Reuters reported that U.S. energy companies are scrambling to buy more cybersecurity insurance after the attack on Colonial Pipeline disrupted the U.S. fuel supply, but they can expect to pay more as cyber insurers plan to hike rates following a slew of ransomware attacks. Fundamentally these companies are trying to hedge risk rather than mitigate root causes.

Ransomware attack lesson

The lesson from ransomware attacks is clear: national security is at high risk in any country. Cyberattacks, including those targeting automation and control systems, are increasing significantly. My view is the "big game" has not yet started. Winners of classic military battles generally get good reconnaissance and probe at their opponents' defenses before launching major attacks. Carrying the war analogy further, there are typically campaigns with many battles. "Even as we speak, there are thousands of attacks on all aspects of the energy sector and the private sector generally. . . . it's happening all the time," U.S. Energy Secretary Jennifer Granholm told Jake Tapper on CNN's "State of the Union" cable show 7 June 2021.

Cybersecurity tax credit

A cybersecurity investment tax credit would work like tax credits for energy conservation that have been around for many years. Energy conservation tax credits had a major goal of achieving energy independence, which was viewed as a national security issue. More recent tax credits include those for installation of alternative energy generation, particularly solar and wind.

There is nothing wrong with awareness, but we need action.

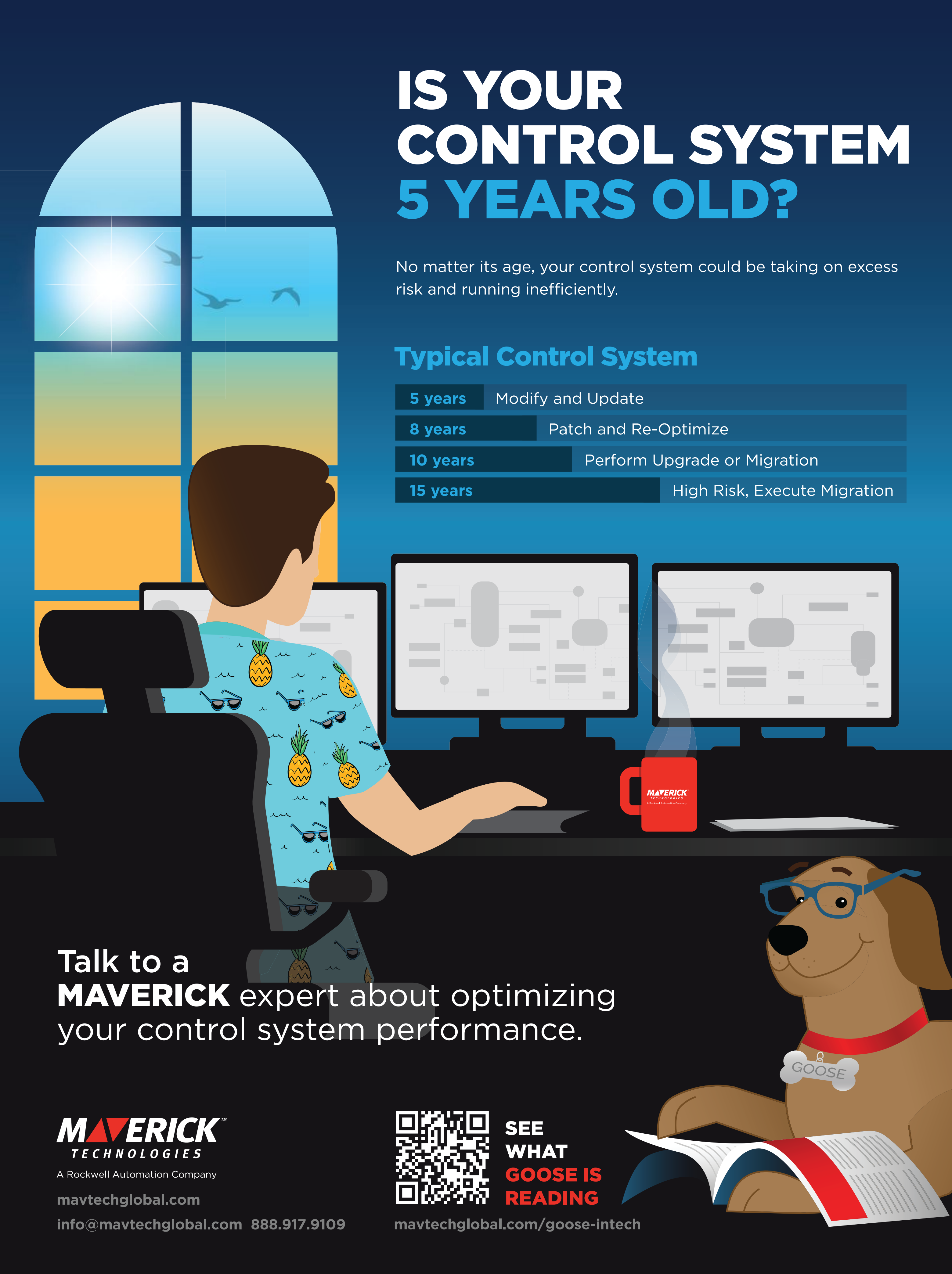
A bipartisan group of U.S. House of Representatives members recently introduced legislation to step up cybersecurity literacy and increase awareness among the American public amid the spike in cyberthreats against critical infrastructure. The American Cybersecurity Literacy Act would require the National Telecommunications and Information Administration (NTIA) to establish a cyber literacy campaign to help promote understanding of how to stay safe online and prevent successful cyberattacks.

Action is needed

Cybersecurity tax credits incentivize companies to invest in personnel education and technologies to protect operations and strengthen national security by selecting an appropriate solution for their businesses. As with energy conservation, there are existing standards, product solutions, and guidelines, including ISA/IEC 62443, that need to be applied based on the specific use case.

In the June 2021 issue of *InTech*, Eric Cosman provided guidance in his article, "Automation Systems Cybersecurity: From Standards to Practices." It is interesting that companies can take a tax deduction for insurance premiums that only provide a level of financial protection.

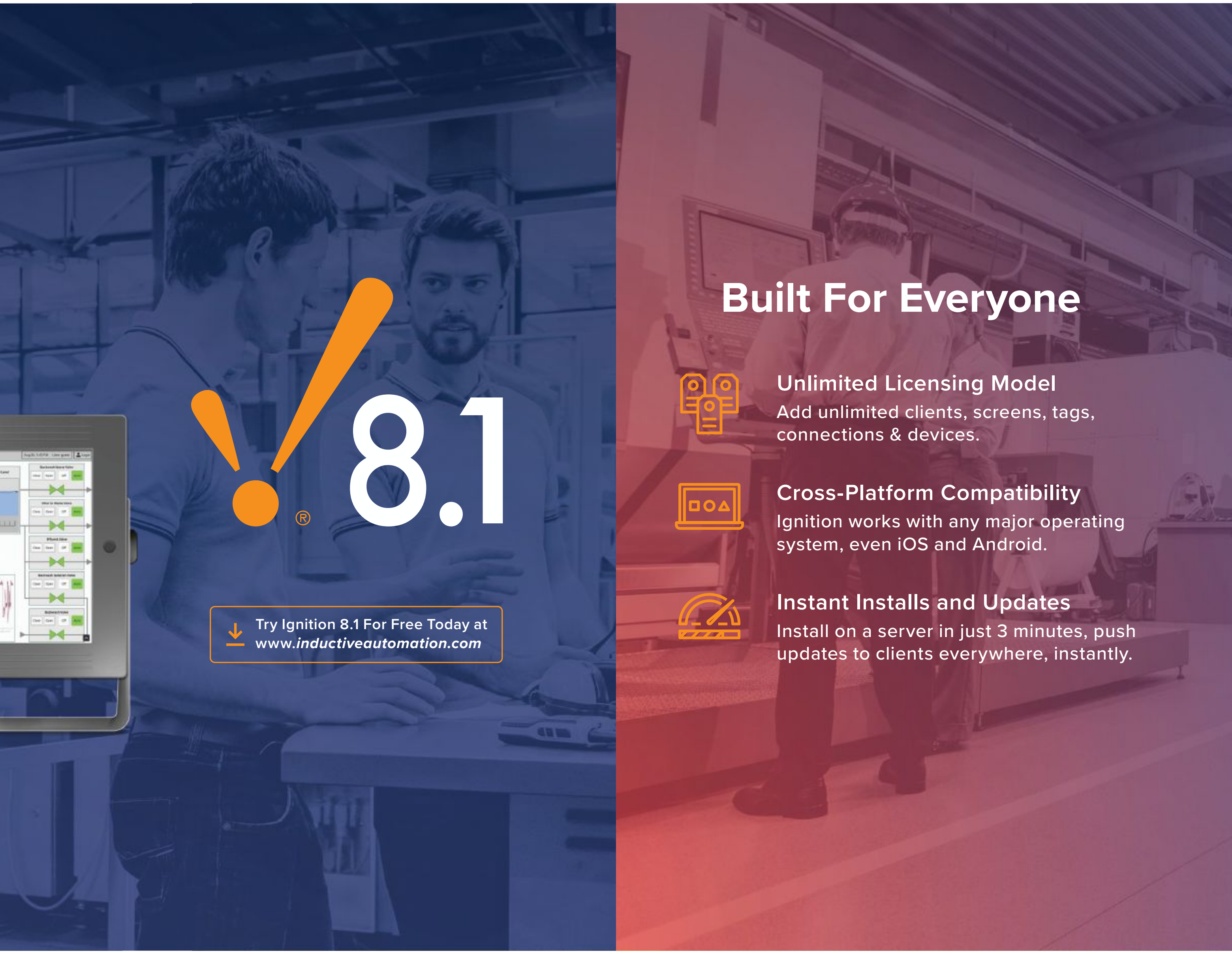
I spent a number of years in the energy conservation area and realized the value of investment tax credits to achieve results and stimulate the development of superior solutions. The time is now for action on this topic. ■


IS YOUR
CONTROL SYSTEM
5 YEARS OLD?
No matter its age, your control system could be taking on excess risk and running inefficiently.
Typical Control System
5 years Modify and Update
8 years Patch and Re-Optimize
10 years Perform Upgrade or Migration
15 years High Risk, Execute Migration
GOOSE
Talk to a
MAVERICK expert about optimizing
your control system performance.
MAVERICK TECHNOLOGIES
A Rockwell Automation Company
mavtechglobal.com
info@mavtechglobal.com 888.917.9109
SEE
WHAT
GOOSE IS
READING
mavtechglobal.com/goose-intech

Ignition 8.1
by inductive automation

Built For The Plant Floor

Build Mobile-Responsive HTML5 Applications
That Run Natively on Any Screen


8.1
Try Ignition 8.1 For Free Today at
www.inductiveautomation.com
Built For Everyone
Unlimited Licensing Model
Add unlimited clients, screens, tags, connections & devices.
Cross-Platform Compatibility
Ignition works with any major operating system, even iOS and Android.
Instant Installs and Updates
Install on a server in just 3 minutes, push updates to clients everywhere, instantly.