March/April 2020

InTech

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

1945 ISA 2020

Remote monitoring for maintenance

Industrial cloud computing

Alarm management

Functional safety

Data center security

Blurring the boundaries

Virtual commissioning and digital twins blur the boundaries between design and automation

www.isa.org/intech

Make any device an edge device

with low-cost cloud solutions from AutomationDirect

Stride pocket portal™

Now with FREE cloud data logging!

STRIDE Pocket Portal's FREE cloud subscription allows you to log up to 5,000 data points per month. Additional paid subscriptions are available for cloud notifications and scheduled email reporting.

WiFi

Analog, Discrete or Modbus RTU

INDUSTRY IIoT 4.0

IoT BRIDGE
PRICED AT
$99.00
(SE-PB100)

- Wireless Industrial IoT end-to-end solution to log your data in the cloud
- Faster Monitoring: Unmonitored assets can get connected and become monitored assets in minutes
- Remote Control: Write to Modbus coils, registers, or discrete outputs using the mobile app
- Reduce Costs: Enterprises can implement IoT capabilities without needing technical expertise and without modifying equipment
- Retrofit Solution: Industrial controls, commercial buildings, retail spaces, or factories can be entirely retrofitted with IoT capabilities in days instead of months
- Work Smarter: Continuously monitor and optimize asset performance

STRIDE Pocket Portal / IoT Bridge

The STRIDE Pocket Portal is a simple, low-cost cloud data logging and storage solution that will gather and store data directly to the cloud from any device including sensors, actuators, and Modbus RTU-capable controllers.

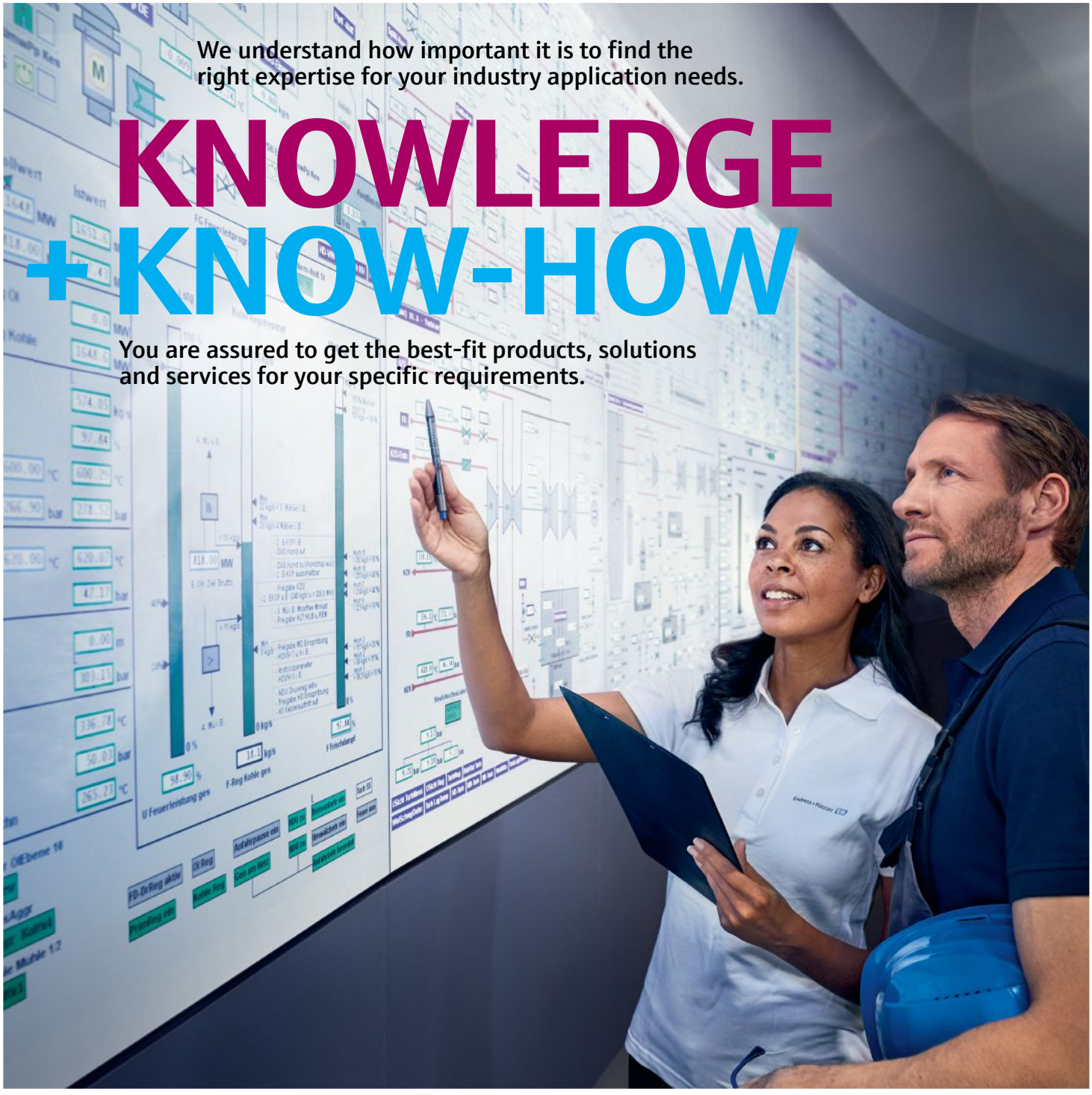
The extremely compact size allows the Pocket Portal to fit anywhere and with WiFi capability, network connections are established without any extra network cabling. The STRIDE Pocket Portal is perfect for anyone needing a small DIY cloud-based data solution that won't break the bank!

Research, price, buy at: *www.automationdirect.com/stride*

Order Today, Ships Today!

VOTED Best in SERVICE 15 YEARS

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



We understand how important it is to find the right expertise for your industry application needs.

KNOWLEDGE + KNOW-HOW

You are assured to get the best-fit products, solutions and services for your specific requirements.

Customers around the world trust us when it comes to process automation. Our shared goal is plant safety, availability and efficiency. We are with you every day, everywhere.

People for Process Automation

Do you want to learn more?
www.us.endress.com

Endress+Hauser

March/April 2020 | Volume 67, Issue 2

www.isa.org

InTech

COVER STORY

12

Blurring the boundaries between design and automation

By Noam Ribon and Colm Gavin

The design and deployment of projects, including machines and production lines, can be dramatically improved by applying virtual commissioning and digital twins. Mechanical design, electrical design, and automation can be performed interactively, increasing efficiency and lowering project time.

ONLINE EXTRA:

ISA launches 75th Anniversary website

www.isa.org/75in2020

www.isa.org/InTech

DEPARTMENTS

COLUMNS

RESOURCES

InTech FOCUS is ISA's six-times-per-year digital magazine (or ebook) that delivers long-form educational articles on automation and instrumentation fundamentals from a variety of industry experts. Single-issue topics include Flow & Level, Temperature & Pressure, Controls, Process Safety, and Final Control Elements.

InTech Plus is ISA's twice-monthly digital newsletter, providing news, technical content, and professional development tools and resources. Both *InTech FOCUS* and *InTech Plus* are powered by Automation.com, global publisher of automation content and a subsidiary of the International Society of Automation. Subscribe to *InTech FOCUS, InTech Plus*, and more at www.automation.com/subscribe.

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

ISSN 0192-303X

***InTech,* 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 67, Issue 2.**

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

Subscriptions: For ISA members, 8.65% of annual membership dues is the nondeductible portion allocated to the *InTech* subscription. Other subscribers: $175 in North America; $235 outside North America. Multi-year rates available on request. Single copy and back issues: $20 + shipping.

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

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

Printed in the U.S.A.

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

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

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

InTech magazine incorporates *Industrial Computing*® magazine.

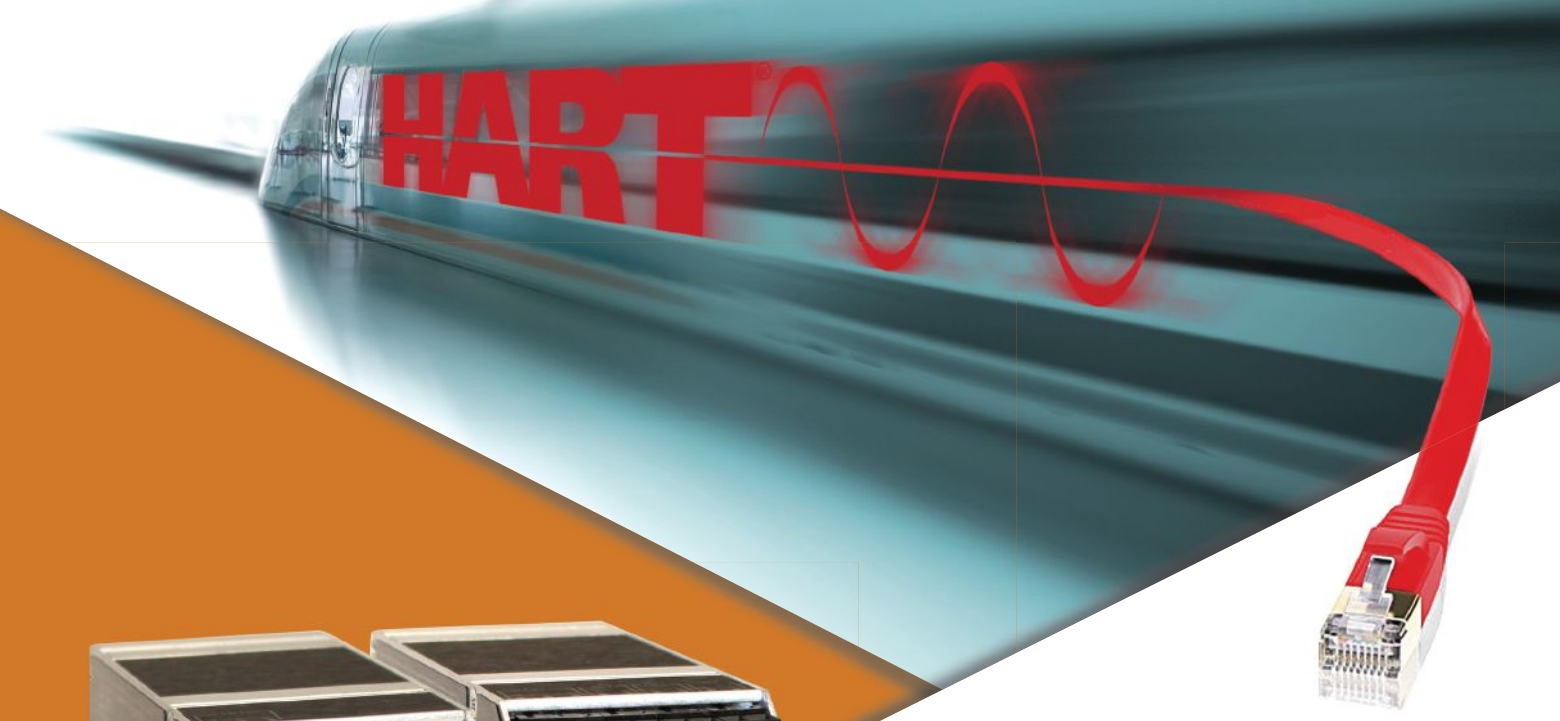
PRINTED WITH SOY INK

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

MOORE INDUSTRIES WORLDWIDE
Demand Moore Reliability

50 Years of Reliabilty
1968 - 2018

Accelerate Your HART Data at the Speed of Ethernet



Get the process detail you need from your Smart HART devices to MODBUS/TCP and HART-IP based monitoring and control systems at the speed of Ethernet with the **HES HART to Ethernet Gateway System**.

Connect up to 64 Smart HART devices and collect the Dynamic and Device Variables, along with diagnostics, from each device that delivers critical information needed to address process and device problems before they turn into unplanned downtime. Plus, the built-in web server lets you easily monitor all HART device data via any web browser.

To learn more about the Moore Industries
HES HART to Ethernet Gateway System
Call **800-999-2900**
or visit **www.miinet.com/HES**

Predicting the future . . . day by day

By Renee Bassett, *InTech* Chief Editor

I am writing this on 24 March. By the time you are reading it in April or later, world events will have changed again in response to the coronavirus pandemic.

Today, major U.S. airlines are drafting plans for a voluntary shutdown of all U.S. flights. A growing number of U.S. states and cities, and countries around the world, are urging lockdowns of "non-essential" businesses as cases of the virus top 43,000 in the U.S. and 381,000 globally. Everything from social interaction to industrial operations are being disrupted in unprecedented ways, and whatever is happening today is unlikely to be the same next week or next month.

Already, dozens of spring and summer events—everything from ISA's annual Analysis Division Symposium to the Tokyo Summer Olympics—have been cancelled or postponed as congregating in groups larger than 10 (U.S.) or two (U.K.) has been banned. Tens of thousands of people are learning to work from home or learning what it means to not work at all for an indefinite period. Predictions about what this all means for industrial automation and control professionals vary widely.

Some automation providers are reporting that they are officially deemed "essential businesses," because they support so many customers in the essential areas of food/beverage, pharmaceuticals, chemicals, oil/gas, and logistics. That means they have to continue to operate at regular levels to support those customers, even if/when a shelter-in-place order is issued. Others contend that the coronavirus outbreak reveals the weakest links in the industrial supply chain to be the suppliers' suppliers, and managers should plan accordingly.

"Industry 4.0 has received much attention; however, the focus has been on the activities inside the factory gates. But investments in robotics or IoT sensors and the like assume that assembly lines receive a steady flow of raw materials," explains Michael Larner, principal analyst at ABI Research. "Initially, plant managers and factory owners will be looking to secure supplies and be getting an appreciation of constraints further up the supply chain plus how much influence they have on their suppliers. In the longer term, manufacturers will need to conduct extensive due diligence to understand their risk exposure."

To mitigate supply chain risks, Larner says, manufacturers should not only source components from multiple suppliers but also find suppliers in multiple locations.

Some predict that, in the long term, the coronavirus pandemic could be a boon to automation and digitalization efforts. "Before COVID-19 struck, industrial automation was slowed by flat capital expenditure and declining industrial production," says David Bicknell, principal analyst with GlobalData. "The virus has exposed the fact that despite the hype, advanced factory automation has not substituted human workers at scale. Technologies such as blockchain for inventory management and logistics, and cloud-orchestrated AI [artificial intelligence] for assembly line robotics have either been insufficiently developed or too difficult to use." Had industry implemented them sooner, "it would now be in a different place," he adds.

Bicknell contends that, "the virus may now focus organizations' minds on the need to automate faster in the medium term and will accelerate an investment in factory automation when the global economy eventually rebounds." But, he admits, "that will take a while."

What do you think? Talk to me about how the coronavirus pandemic is affecting you, and how you predict it will affect industry. Reach me at rbassett@automation.com, rbassett@isa.org, or www.linkedIn.com/in/rrbassett. ■

Solving big data problems with a little data approach

By Derek Thomas

ABOUT THE AUTHOR

Derek Thomas is the vice president of sales and marketing for Emerson's Machine Automation Solutions business, responsible for global sales, strategy, marketing and product management. He has an MBA from Washington University in St. Louis and a BS in mechanical engineering from Purdue University.

Nearly every industrial facility has an opportunity to create value from collected and stored big data by implementing Industrial Internet of Things (IIoT) and other operational improvement initiatives. In the process industries, this data often resides in centralized control systems and historians, while in discrete part manufacturing, the data is more likely to be dispersed across the plant or trapped within machines. But no matter where the data is collected or stored, the best approach to creating value is often to start small, with a "little data" approach.

McKinsey & Company gives some insight into the scale of data analysis opportunities. "Most data generated by existing IoT sensors is ignored. In the oil-drilling industry, an early adopter, we found that only 1 percent of the data from the 30,000 sensors on a typical oil rig is used, and even this small fraction of data is not used for optimization, prediction, and data-driven decision making."

Many big data projects fail because a "boil the ocean" approach is pursued, whereby substantial time and capital are committed upfront in the hope of analyzing all the stored and incoming data to derive insights. These types of approaches usually begin with discussions of what technologies should be used, particularly the cloud and other IT-related infrastructures, and often end with frustration and unsatisfactory results, even after months or even years of effort.

A better and more practical way is to start at the machine or production-line level by defining specific problems that are solvable with better use of little data. Focusing the field of view to a specific, defined asset reduces complexity and simplifies the search for a solution. This simplification is crucial, because the people implementing a little data project should be the personnel most familiar with operations.

Another advantage of the little data approach is it quickly yields tangible improvements by empowering users to find, solve, improve, and move on to the next opportunity. This creates positive momentum within a company, and as experience and comfort increases, it becomes easier to scale efforts to larger data sets using the lessons learned.

For these and other reasons, a little data approach is the most practical path for IIoT projects at many industrial plants, but it requires different technologies than the IT-centric methodology used in many big data projects. The plant personnel most familiar with operations are generally also very competent when it comes to real-time control systems. This is by necessity; these systems keep plants running smoothly, and adjustments to these systems are often required to improve operations. Unfortunately, most real-time controllers do not have the required capability to analyze data produced by field devices to generate insight, a requirement for little data projects.

This type of edge processing has traditionally required a separate industrial computing device and software solution to store and process data. Integrating these elements with the existing controller and network was often problematic due to: the complexity of setting up, programming, and managing in two different environments; synchronization; lag/latency; and other issues. A little data project using two separate devices could thus become quite complex and unreliable, slowing implementation and driving up costs.

A modern class of edge controller addresses these issues by combining two functions into a single device. The first function is real-time control, much like what was done by a traditional programmable logic controller. The second set of functions is performed by a computing platform with a processor capable of data storage, analysis, and a wide range of other tasks—similar to what could be done with an industrial PC. Because both functions are performed in one device, there is no additional effort required to integrate two components—data is simply passed between the two functional areas safely and securely.

Once the edge controller stores and processes the data already being collected for real-time control, results are readily transmitted to enterprise platforms, such as manufacturing execution systems, enterprise resource planning, maintenance management, and other analytics systems—both on premises and cloud-based—through the typical industrial or Ethernet protocols. These higher-level platforms thus have the information required to improve operations.

Big data projects seem to call for big and complex solutions, but a large-scale approach often fails due to high costs and excessive implementation time. A better way is to begin with targeted efforts for analyzing little data to create insights, creating value and building momentum. ■

IIoT devices run longer on Tadiran batteries.

PROVEN

40

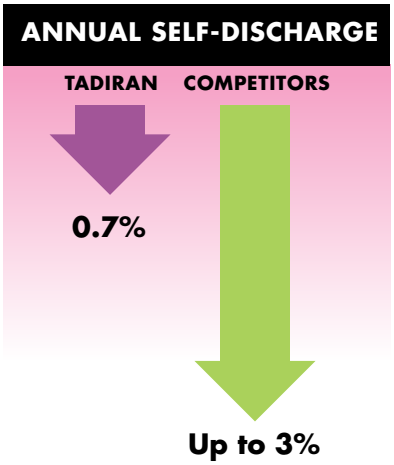
YEAR

OPERATING

LIFE*

Remote wireless devices connected to the Industrial Internet of Things (IIoT) run on Tadiran bobbin-type $LiSOCl_2$ batteries.

Our batteries offer a winning combination: a patented hybrid layer capacitor (HLC) that delivers the high pulses required for two-way wireless communications; the widest temperature range of all; and the lowest self-discharge rate (0.7% per year), enabling our cells to last up to 4 times longer than the competition.



Looking to have your remote wireless device complete a 40-year marathon? Then team up with Tadiran batteries that last a lifetime.

TADIRAN BATTERIES

* Tadiran $LiSOCl_2$ batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.

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

www.tadiranbat.com

From COVID-19 to cybersecurity: A tale of toilet paper and risk

I never thought that I'd be comparing toilet-roll purchasing habits with cybersecurity risk management, but here I am in the midst of the COVID-19 pandemic seeing some interesting parallels. As an industrial automation consultant and subject-matter expert for ISA, I travel the world talking to organizations about managing their cybersecurity risk. Common themes have emerged. I realize that both COVID-19 and industrial cybersecurity discussions provoke similar reactions—and behind both is the psychology of how people interpret and respond to risk. Here's some examples:

Some organizations ask for advice from experts, then promptly ignore that advice because it is inconvenient to them.

- There are organizations that deny the abundance of data and insist that they are not at risk. These are COVID-19 deniers, watching the reports of the exponential spread of the virus but claiming that there is really nothing to worry about. Scottish author Hunter Davies recently tweeted that "I'm 84. I survived rationing. I'm not scared of the coronavirus," which would be like an organization claiming: "We've been around for 84 years. We survived a hurricane, so we'll survive a cyberattack."
- There are organizations that ask for advice from cybersecurity experts, then promptly ignore that advice because it is inconvenient to them. When epidemiologists recommend taking extreme action and shutting down public events, they base this on their specialist knowledge and experience. While there may be initial resistance to such recommendations, it is almost always necessary to follow the guidance of experts. After all, expert comes from the Latin *expertus*, meaning tested or proved.
- There are organizations that follow others and undertake costly but ultimately ineffective or misguided responses to cybersecurity risk. A typical case is deploying expensive cybersecurity software solutions without establishing good basic cybersecurity hygiene practices. Often the software is purchased because others have done the same, so it must be the right thing to do. But there are more important steps to take. This is the equivalent to the panic buying of toilet paper rolls that we are seeing today. While stocking up on toilet paper might seem like a sensible contingency plan, there are other factors to consider—not least is exposure to the virus in the supermarket itself.

Psychologist Paul Slovic's review article, "Perception of risk," published in *Science* in 1987, gives some insight into why this happens. Slovic's analysis compared the difference in perception of the risks of nuclear energy versus driving automobiles. He concluded that because there are so many automobile accidents, the risk is knowable. There is also a limited media coverage of automobile accidents, with no speculation of unknown events. Unlike automobile accidents, nuclear energy represents an unknown risk with a relative lack of data. Nuclear accidents get widespread media coverage resulting in speculation about future possible disasters. The result is that the lower risk scenario (nuclear energy) induces more fear than a higher risk activity (driving an automobile).

In the toilet paper versus community spread scenarios, the fear of running out of toilet paper is knowable, whereas there is still much uncertainty about the likelihood of contracting COVID-19, so once again people are failing to accurately measure risk. But the more you know about your risk, the less there is to fear. ■

—Steve Mustard, ISA subject-matter expert. Visit https://isa.org to find out what ISA does to provide training to properly understand cybersecurity risks and to create experts through its cybersecurity certificate program.

ARC 2020 Conference: IT/OT combine for digitalization

The increasing speed of integration of business, engineering, and manufacturing systems was evident at the 2020 ARC Orlando Forum. Focused on the theme "Driving Digital Transformation in Industry and Cities," the 3–6 February event boasted more than 800 attendees representing more than 300 companies from 20 countries.

Multiple tracks and sessions comprised over 200 industry presenters and panel participants sharing their insights, experiences, and concerns. Reflecting the increasing integration of information technology (IT) and operational technology (OT) disciplines, this year's conference had more IT people attending than ever before, and the vendor showcase featured more IT companies than OT. Many of the presentations illustrated that there are big advantages when companies operate in new, collaborative ways across the whole of the enterprise in order to create flexible and synchronized manufacturing. Read this article at Automation.com to find out more, including:

- How successful digitalization requires alignment starting at the top of the organization.
- How traditionally siloed organizations are now working collaboratively across departments, including engineering, IT, OT, purchasing, and manufacturing operations.
- Details of the Dow Corporation digitalization journey as presented by Melanie Kalmar, Dow Corporate VP, chief information officer and chief digital officer, and Peter Holicki, Dow senior vice president of operations for manufacturing and engineering. Holicki and Kalmar described their efforts to create a culture that leveraged what they had in common to build trust, so teams would be willing to try new things together, and even make mistakes. ■

—Bill Lydon, Automation.com contributing editor

In memoriam: Richard "Rich" Merritt, 1943–2020

Rich Merritt was born at a very young age, on 8 November 1943 in Hackensack, N.J. He was the son of Harold and Florence (Bahr) Merritt, an avid sports car/race car driver and racing fan, and a devoted husband, father, and grandfather. He was also a giant of industrial automation and control technical communications, serving countless publications and clients over his long career, including Automation.com and ISA's *InTech* magazine. Alas, Richard "Rich" Jesse Merritt died Saturday, 8 February 2020, at his home in Cedar Rapids. He was 76.

In agreement with his wishes, Merritt was cremated, and no services were held. Then came the coronavirus restrictions, and the family's planned celebration of life was delayed. So, here is a little about the man who touched so many lives through his spoken and written words.

On his LinkedIn page, Merritt wrote: "Almost all my life has been in automation and process control—including developing automation systems, writing about them as an editor, and marketing them to customers. I know products and technologies, and I know how to write about them in a clear, concise way that gets the attention of magazine editors and their readers."

"I have always been amazed at the way Rich can call upon his vast industry experience and technical knowledge to write on any subject involving process control and automation," said Dan Hebert, PE and principal of Controls PR. "He writes like he's 'been there, done that' and his writing is typically crystal clear. He also has a knack for interviewing people, from machine builders to systems integrators to control engineers, and manages to wrest gems of knowledge from them."

Merritt was a storyteller and a technologist who wrote a lot of automation-related copy over the years. "Rich was one of our most valued writers from 2009 to 2019," said Hebert, "creating hundreds of beautifully crafted articles, press releases, and whitepapers."

Merritt was a guy many considered a friend. David Sear, editor for *Valve World* magazine, said "Rich and I knew each other and developed a friendship without every really becoming acquainted. That may sound strange, but it will probably strike a chord with many who work in the wonderful yet transient world of PR, editing, and journalism."

Sear said those exchanges would prompt a spate of emails during which he knew he could trust Merritt's professionality but also got to know a little of his unique nature. "Seeing Rich's name pop up on my PC always added a little sunshine to the cloudiest of days," said Sear. "And even in passing, Merritt still managed to make me smile."

Merritt wrote news, articles, products, and a column for *Control* magazine in the late 1990s and early aughts. As senior technical editor, he said, "My writing helped take *Control* from third place to the Number 1 magazine in its field. I won 10 ASBPE writing awards in four years, including Best Column three years in a row, and Best Technical article four times."

Paul Studebaker, editor in chief of *Control* magazine and ControlGlobal.com at the time, said Merritt never shied away from taking controversial positions on topics, such as "manufacturing execution systems, or MES, (bad!) to climate change (good!)."

"Rich also made me jealous with extended trips to Hawaii and his excellent motor racing skills," Studebaker added. "He linked me to videos so I could ride along, and I watched his humble BMW eat Vettes and Vipers." He said you could always tell you were reading one of Rich's pieces because, eventually, you'd encounter an "alas" Even today, a search for "alas" on ControlGlobal.com brings up tons of vintage Rich:

- "Alas, I rarely see anyone who actually might know what is going on inside the company . . . ."
- "Alas, most HMI vendors appear to be dragging their feet . . . ."

Alas, Rich Merritt is gone. According to his daughter, Cathi, he planned to write his own obituary but ran out of time. But, she said, there was one line that he was absolutely adamant about including at the start: "I was born at a very young age . . . ."

Rich, you will be missed. ■

—Renee Bassett, chief editor, Automation.com and InTech

MITRE Framework tracks cyber-attacks on industrial control systems

MITRE has released a new tool for industrial control system (ICS) cybersecurity based on its globally accessible, freely available MITRE ATT&CK knowledge base for critical infrastructure. It focuses on the unique threat behaviors leveraged by adversaries targeting ICS environments, and creates a forum for establishing how ICS intrusions are different from enterprise IT intrusions to help ICS operations and security teams better protect their mission-critical systems.

ATT&CK for ICS is a knowledge base for describing the actions an adversary may take while operating within an ICS network. Quint Wysor, senior manager of cybersecurity at Duke Energy, says "the introduction of the new industrial control systems–focused version will enhance the work that industries with critical infrastructure, including the utility sector, have already done to protect their information and infrastructure."

The knowledge base can play several key roles for defenders, including helping establish a standard language for security practitioners to use as they report incidents. It can help with the development of incident response playbooks, prioritizing defenses as well as finding gaps, reporting threat intelligence, training analysts, and emulating adversaries during exercises. It adds the behavior that adversaries use within ICS environments. ■

Blurring the boundaries between design and automation

How virtual commissioning and digital twins reduce time to market and minimize risk

By Noam Ribon and Colm Gavin

Machine, station, line, and system development is usually sequential: Mechanical design, electrical design, and automation are performed one after the other. If a mistake is made anywhere in the development process and is not detected, the error costs grow substantially over the phase of development. Undetected errors can be expensive during commissioning.

Virtual commissioning is essential to minimize, if not eliminate, those costs. Though virtual commissioning is not a new concept, the now ubiquitous digital twin that is sufficiently accurate, combined with vendor multidisciplined expertise, is allowing leading-edge companies to use it. For these companies, virtual commissioning is another added benefit of their investment in simulation, or digital twins, extending value in the manufacturing of lines, production cells, machines, and even systems. For example, in bids for delivery of turnkey production cells and lines, some automotive companies require an accompanying simulation that confirms the performance of the proposed solution.

This demand is causing machine builders, for example, to modernize and transition traditional systems for the benefit of their customers and the longevity of their brand and services.

What is driving the success of virtual commissioning? Let's explore this technology in more detail and discover the properties catapulting its popularity.

Definition, benefits, differentiators

Virtual commissioning allows developers to debug automation control logic and programmable logic controller (PLC) code in a virtual environment before downloading it to physical equipment. Simulating and validating the automation equipment virtually confirms it will work as expected, thus substantially reducing system installation cost and startup time.

An overall driver in virtual commissioning is the widespread availability of the digital twin, which is a virtual representation of a physical product, process, or system used to understand and predict the physical counterpart's performance characteristics. Using digital twins can lead to:

Compressing time: Customers are continually changing their tastes, very quickly, driving a reciprocal need to respond quickly.

Saving costs: Less time is required to physically debug design and its associated controls. Costs eliminated are travel and time and material costs associated with the physical presence of a team on site, and in some cases, rebuilding the physical twin that was damaged by running incorrect controls logic. In this case, delays from waiting for a new prototype may prove to be the costliest. Customers with long startup times due to machine issues are affected financially.

Minimizing risk: All testing can be done virtually, so transitions result in only minimal issues, with no PLC program problems. Knowing that issues will be ironed out virtually increases the confidence of an on-time, on-budget delivery, for example, when shipping a machine and starting it at a new facility. This process that once took a week is now complete in a weekend—two work shifts.

When the virtual commissioning or digital twin is linked to the actual PLC program of its physical counterpart, it makes validation of the overall automation system possible. On one end, the PLC program is tested by observing how the physical system would behave, and on the other, with an actual controls program running the operation of the physical system so it can be better anticipated. Siemens provides a virtual PLC for some of its hardware PLCs, making virtual commissioning completely virtual, sometimes referred to as *software in the loop (SIL)*.

All insights obtained and errors discovered can be used for optimization purposes before real production begins. Virtual commissioning significantly empowers a company to move toward *availability, accuracy, and vendor multidiscipline expertise.*

FAST FORWARD

- Transitioning to virtual commissioning is an easy one. Start ramping up by learning the tools, and go from there.
- Commissioning a new production machine, station, line, or system is a crucial phase of a project. It demonstrates whether the overall system will operate as planned.
- Unplanned behavior can quickly lead to delays and high costs. Virtual commissioning can greatly reduce this risk.

Improved communication

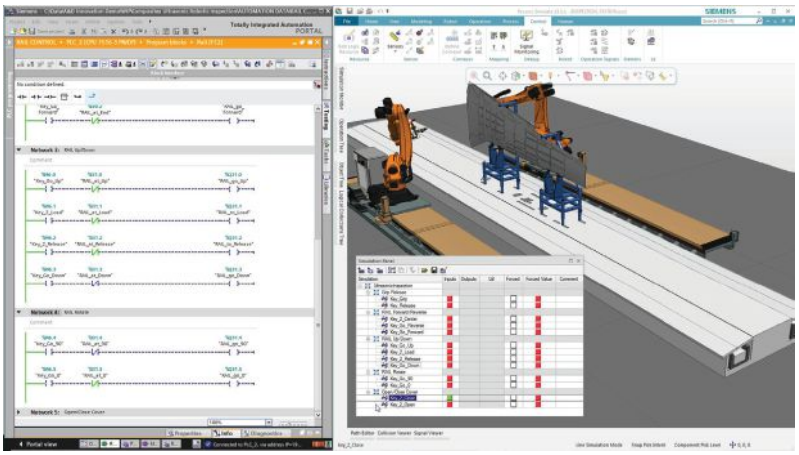
Two all-encompassing benefits of virtual commissioning are parallel work and improved communication between the designer and automation engineer. These aspects bring effective results, including:

Verifying sequence of operations: A virtual human-machine interface (HMI) and PLC allow you to debug your code. Very early in the design process, design engineers can experience the intent of the automation engineers. Automation engineers can better relate to what their design engineer counterparts had in mind, arriving at an all-around better multidisciplinary outcome.

Training: With a virtual HMI and model running, you can provide comprehensive training for operators to become familiar with the machine before interacting physically, reducing the operator turnover rate.

Promotion: With simulation, you demonstrate how the machine will work for a customer in its unique environment and validate precisely what the machine does before using it.

One example is the design of a new machine. Design software and automation unite to provide value for simulating the kinematics, behavioral physics (gravity, friction, and torque), electrical architecture, and even hydraulics via a digital model. Knowing how a machine, for



Robotic ultrasonic inspection of a composite wing, driven by PLC code, emulates the system's behavior.

Virtual commissioning based on simulation is used to understand operations and, when linked to the actual PLC counterpart, makes validating the entire automation system possible.

example, will perform in conjunction with the automation code saves time, allowing automation personnel to collaborate sooner with the mechanical engineer. Thus, the physical machine can be fabricated on the factory floor before finishing the code.

Fewer errors

Virtual commissioning eliminates errors early in the development process. The Six Sigma model describes the importance of detecting possible errors at an early stage. It helps calculate the error quotas that occur during a business process: The rule of tens says that error-related costs for an unidentified error increase by a factor of 10 from one value-added level to the next. The earlier an error is identified and corrected, the cheaper this is for the organization.

Error identification early in the product life cycle results in a quality engineering project. Therefore, finding errors in the *planning phase* versus the development lab (reworking parts), startup (machine on the factory floor), or operation (the machine is shipped to end customer) is ideal and economical.

Tronrud Engineering, a Norwegian machine builder, developed an innovative machine prototype that could pack 300 pillow bags per minute into boxes while maintaining the same footprint—twice the speed of traditional machines. During development, the project team created three-dimensional models of the machine and its parts to simulate its behavior. This virtual image of the machine—the digital twin—enabled parallel work on design, mechanics, and programming.

As a result, Tronrud reduced the design phase by 10 percent and commissioning time by 25 percent, significantly reducing the time to market. Reducing time on the shop floor makes it possible to produce more machines.

"Digitalization is a huge opportunity. It's a matter of not being afraid of the challenges but rather take the benefit that helps us to create more value," said Olav Tronrud, CEO, Forecasting.

Acceptance testing

End customers of systems, lines, production cells, or machine vendors are starting to demand virtual factory acceptance testing. A digital twin is essential to performing this task. Companies that use a digital twin put themselves at a competitive advantage to addressing these demands and winning that business. We can already see discussions and predict a new trend in the automation industry. As described above, companies are already significantly reducing their time to market, but also the time to commission systems once delivered. Commissioning time used to be non-elastic. It takes what it takes, and surprises are addressed by pouring more resources in, at significant costs. Using the digital twin for virtual commissioning, vendors can now offer their customers a share of those savings, otherwise accounted for as profits. With virtual commissioning it is now a win-win situation, that in turn has the potential to drive more business to the vendor.

Eisenmann builds facilities for surface finishing technology, material flow automation, environmental technology and ceramics firing lines, as well as special facilities for energy recovery, coating, thermal processing, and recycling.

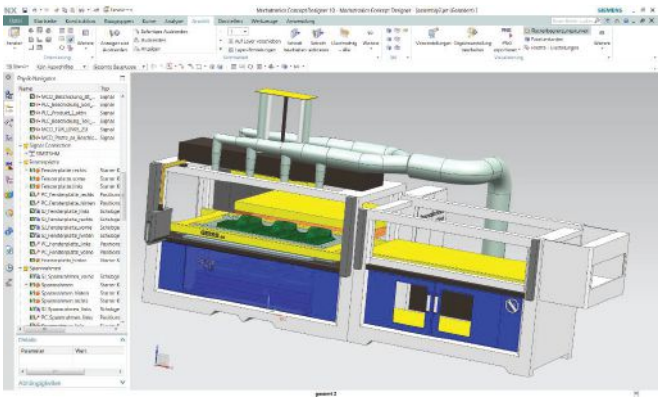
As a future hub of international air traffic, the New Doha International Airport (NDIA) in Qatar set out to create a smoothly functioning, reliable logistics system. NDIA selected Eisenmann to install an electric monorail system.

Eisenmann started with the two-dimensional layout of the catering building and built a simulation model that runs an animated simulation of this layout. For the quotation phase, peak scenarios were simulated. In this project, Eisenmann practiced for the first time with a virtual commissioning concept, by connecting the material flow computer to the simulation model, and thus could identify and resolve most of the problems in the program.

"You can actually visualize any improper material flow in the virtual simulation model. I worked on this side by side with a control programmer, who developed and debugged the control programs" said Dr. Monika Schneider, simulation expert for Eisenmann.

Ralf Weiland, senior vice president of conveyor systems for Eisenmann added, "With our virtual commission-

Tronrod Engineering used virtual images of the machine and digital twin to develop an innovative machine that could pack 300 pillow bags per minute into boxes.



Working with a digital twin, automation engineers can better relate to what their design engineer counterparts had in mind.

ing capability, supported by creating realistic validations in a virtual environment . . . we believe we can shorten delivery time on every project."

Reducing risk

Transitioning to virtual commissioning is an easy one. Start ramping up by learning the tools, and go from there. Once the mechanical engineers learn the tools, they become quicker and more adept for future projects. Commissioning a new production machine, station, line, or system is a crucial phase of a project. It demonstrates whether the overall system—consisting of mechanics, electrical systems, and automation—will operate as planned. Unplanned behavior can quickly lead to delays and high costs. Virtual commissioning can greatly reduce this risk. ■

ABOUT THE AUTHORS

Noam Ribon (noam.ribon@siemens.com) is a senior business consultant with Siemens PLM Software with a specialization in digitalization of manufacturing, program, project, and IT management. He has more than 30 years of computer aided design, product life-cycle management, digital manufacturing, and digitalization (Industry 4.0) software experience across various industries. Ribon earned a BS in mechanical engineering from Technion Institute of Technology, Israel, and an MBA from the University of Phoenix.

Colm Gavin (colm.gavin@siemens.com) promotes digitalization topics with Siemens Digital Industries Software group for machine and line builders. Working for Siemens for 19 years, Colm uses his experience in discrete manufacturing to assist companies in taking advantage of new innovations with Industry 4.0. He was previously responsible for the marketing of Siemens' Totally Integrated Automation Portal software in the U.S. Gavin holds a BS in manufacturing engineering from Trinity College, Dublin, Ireland.

View the online version at www.isa.org/intech/20200401.

Alarm management questions that everyone asks

How to achieve an effective and efficient alarm management program

By Donald G. Dunn and Nicholas P. Sands, PE, CAP

Understanding and implementing effective alarm management brings many operational benefits. This article highlights common questions and answers to help you understand alarm management.

FAST FORWARD

- The article is a comprehensive overview of alarm management questions everyone asks.
- Alarm systems should provide the right indication at the right time for operators to respond and avoid undesired consequences.
- ANSI/ISA-18.2 is the authoritative standard on alarm management, supported by seven technical reports with additional guidance.

What is alarm management?

Alarm management is the taming of the alarm system, changing it from a mixed alarm and awareness notification system with almost random priorities to a true operator support tool that notifies operators to take the right action at the right time to avoid an undesired consequence.

This transformation includes applying the definition of "alarm" in a process called rationalization to remove the notifications that are not truly alarms.

Alarm (n): audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response.

Also, during rationalization, the consequences and corrective actions for each alarm are documented, so that the operators can be trained to respond. The alarm system is monitored and assessed against performance targets to understand what issues need to be fixed to keep the system working for the operator. There are many more steps in the life cycle of alarm management, but the key steps of removing things that are not really alarms, training the operators to respond, and monitoring system performance provide most of the benefits.

Which alarm management standard do I follow: ISA-18.2, IEC 62682, or EEMUA 191?

You can build a successful alarm management program with any of the three. The activities for the full alarm management life cycle (figure 1) are more clearly organized in the ISA and International Electrotechnical Commission (IEC) standards. As standards, these documents describe what should be included in an alarm management program, but not how to do those things. Engineering Equipment and Materials Users Association (EEMUA) 191, as a guideline and *not* a standard, addresses both what and how to a limited extent. The seven ISA-18.2 technical reports address the "how" in much greater detail, aligned to the ISA standard.

As far as the standards go, ANSI/ISA-18.2 and IEC 62682 are almost the same, as the IEC version was only slightly modified from the ISA version. ISA-18.2 was first published in 2009 and was designed not to conflict with the EEMUA 191 guideline and the NAMUR (the German Standardization Association for Measurement and Control in Chemical Industries) NA102 worksheet. The goal was to build a consistent set of terminology and activities for alarm management. Today, ISA-18.2 is the authoritative standard on alarm management.

Regulatory requirements can be a factor in choosing to follow the standards on alarm management.

Is an alarm management program a regulatory requirement?

Yes, alarm management can be a regulatory requirement, depending on the industry and the country. In the U.S., facilities covered by the Occupational Safety and Health Administration (OSHA) Process Safety Management (PSM) and the Environmental Protection Agency (EPA) Risk Management Plan (RMP) can meet requirements using the ISA or IEC standard as recognized and generally accepted good engineering practice (RAGAGEP). The pharmaceutical industry can meet Food and Drug Administration (FDA) Current Good Manufacturing Practice (CGMP) requirements using the standards. These OSHA, EPA, and FDA programs predate the alarm management standards, so there is not an explicit reference to alarm management, but there are references to alarms.

The pipeline industry, regulated by the Pipeline

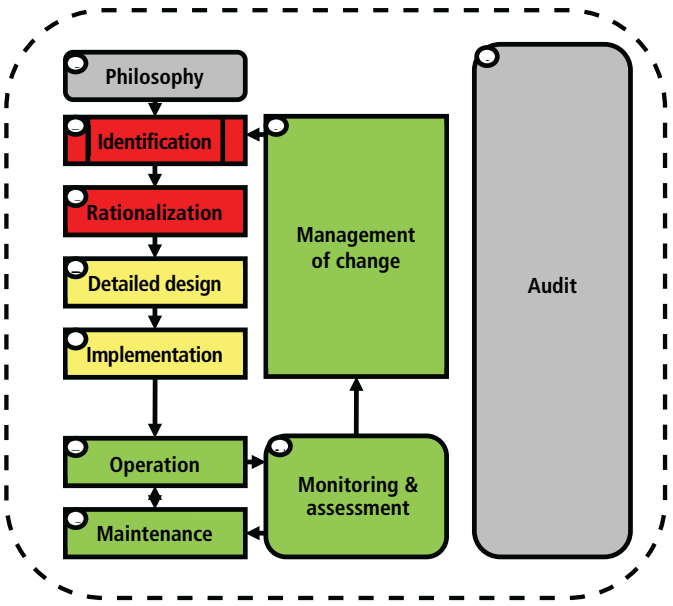


Figure 1. The alarm management life cycle.

and Hazardous Materials Safety Administration (PHMSA), specifically requires alarm management since 2012 because of incidents. The pipeline industry often uses API RP1167, which is also derived in part from ISA-18.2.

In Europe, facilities covered by the Seveso directives also have a requirement for alarm management. The ISA or IEC standard would be good guidance. In the U.K., EEMUA 191 is still often used, as the Health and Safety Executive (HSE) has not updated its 2000 information sheet on *Better Alarm Handling* to reference BS62682, the British Standards version of IEC 62682, versus the EEMUA 191 guideline.

Aside from regulatory requirements, many companies now have policies on alarm management after incidents or have requirements for alarm management from their insurance companies. So, there are several ways to have alarm management as a requirement.

How much does implementing an alarm management program cost?

There are many ways to implement an alarm management program, and the cost varies with choices. Key elements and cost factors include:

- Benchmark – number of locations
- Training – number of people, locations, duration
- Philosophy – development and complexity
- Rationalization – scope, preparation, methodology, tools, facilitation
- Implementation – scope of changes
- Monitoring – scope, software, architecture
- Continuous improvement – methodology

Consider this example: The company ACME Chemicals is planning an alarm management program.

SCOPE:

- three similar plants: one in Ohio, U.S., one in Northern Ireland (NI), one in China
- about 3,000 tags per site and about 4,500 alarms per site

TRAINING:

- Overview training (2 hours) – all operations, maintenance, and technical personnel
- Detail training (16 hours) – selected operators, automation engineers, process engineers

PHILOSOPHY:

- one development workshop (3 days) with trained representatives from each site
- template philosophy document used for all three sites, with some local modifications

RATIONALIZATION:

- export of current alarms used to build potential alarm list
- unit operation rationalization conducted at NI plant
  - two weeks facilitated rationalization
- rationalization reviewed, modified, and adopted at other sites
  - three-day review

IMPLEMENTATION:

- estimate to remove or add 50 percent, about 2,250 alarms
- estimate to modify priority or set point 80 percent , about 3,700 alarms

MONITORING:

- select software for monitoring and assessment
  - includes a master alarm database and rationalization tool
- installation on central server to compare sites

CONTINUOUS IMPROVEMENT:

- biweekly meeting of the alarm team

Based on this rough plan, the cost can be estimated. Excluding employee time and travel, this program might cost about $150K – $200K.

What is the cost benefit ratio of alarm management?

The benefits of a successful alarm management program are many, but they are also hard to quantify in dollars. The most obvious benefit is for the operator, with reduced stress from alarms and improved response to alarms since they are all meaningful. Alarm management is one of those rare improvement programs that operators actually "like," because it makes their lives better. Figure 2 is an example of one company's experience before and after implementing an alarm management program.

Most of the financial benefit comes from avoiding undesired consequences, so the benefit depends on how many avoidable events happen in the plant before implementing alarm management. Using historical data on avoidable plant shutdowns, avoidable off-quality production, and the like, estimate what the reduction in events would be if the operators had a better system to notify them to take action. Do not assume 100 percent reduction, but a reasonable target like 70 percent, and calculate the value.

Every plant is different, because of culture, products, costs, and the like. ACME used the following data:

Operator-preventable events across the three sites:

- Shutdowns: 10 at $500K average
- Off-quality production: about 200K lbs. at $5/lb.
- Incidents: four at about $100K average

The target savings is about $4.5M, giving the alarm management program a very nice return of about 20 times the external cost. How can a plant not afford to implement an alarm management program?

How do I start an alarm management program?

There are three typical ways to start an alarm management program:

1. development of an alarm management philosophy,
2. alarm system monitoring, or
3. alarm system benchmark.

The real starting point is training. Then a plan can be developed that best fits the situation. Typically, new facilities start with option 1, with a goal to develop an alarm philosophy and complete rationalization and training before startup. Many existing facilities start with option 2 or 3, which both include a quantification of the current alarm system performance. With option 2, the alarm system monitoring will show the improvement of fixing the most offensive alarms that do not require rationalization. This is sometimes called bad actor resolution.

BUT before you start an alarm management program, you need to become familiar with the road map to alarm management due to its potential regulatory requirements. Purchase ISA-18.2

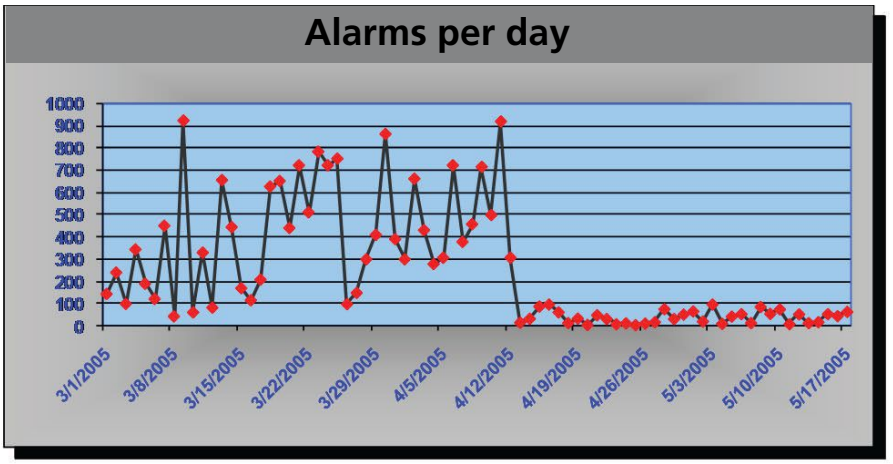


Figure 2. Before and after alarm management.

or IEC 62682. Become familiar with the alarm management life cycle and the requirements for each stage. ISA-18 has developed a number of technical reports (TRs) that go into detail describing how to implement varies stages of the alarm management life cycle. Purchasing these reports or attending an alarm management training course (by a reputable organization that has been involved with the ISA-18.2 or IEC 62682 standards development since their inception) would be beneficial. There are many organizations that can be described as late to the party who have become informational members to simply market that they are members of the standards to sell their services.

Then transition to the three entry points mentioned above. If you need to develop a business case to justify the project, perform an audit of your alarm system to determine the deficiencies and what areas need to be improved. You could also implement a benchmarking and assessment of your facility to determine if your alarm rates are acceptable (figure 3 has some of the key metrics from ISA-18.2). This will allow you to identify bad actors, which you can mitigate to develop data to help support senior leadership sponsorship for an alarm system improvement project. In addition, you can gather information, such as operator survey results, and a benchmarking and assessment report that compares your plant alarm system key performance indicators (KPIs) with ISA-18.2 and IEC 62682 requirements.

When is the alarm management program complete?

As mentioned above, alarm management is a life-cycle approach managing a work process. Asking when the alarm management program is complete is akin to asking if my safety program is complete. Once you have achieved the benefits of a well-managed alarm system, you will wonder how you ever ran the plant without it, as it is a paradigm shift within the culture for an operating plant. This fundamental shift in an organization's culture will not be easy and is rarely embraced by everyone, but this shift is required to adhere to the alarm management work processes within the standards. Everyone needs to understand that the benefits are real, quantifiable, and achievable, as there are many who have embraced this change in philosophy.

The benefit is improved plant performance through improved operational discipline, which means doing the right thing at the right time, every time. An alarm system that is well managed will notify the operator at the right time, and only the right time, for a specific action. A well-trained operator, or an operator assisted with some guidance from a well-designed alarm system, will know the right action to take in response to the alarm. An operator, not overloaded with alarms, will take the right action at the right time to correct the process condition. These imperatives are clearly and concisely stated by Campbell Brown in his famous "Horses for Courses – A Vision for Alarm Management" paper: "the fundamental goal is that Alarm Systems will be designed, procured and managed so as to deliver the right information, in the right way and at the right time for action by the Control Room Operator (where possible) to avoid, and if not, to minimise, plant upset, asset or environmental damage, and to improve safety."

M. L. Bransby and J. Jenkinson conclude in their HSE report "The Management of Alarm Systems" that "poor performance costs money in lost production and plant damage and weakens a very important line of defense against hazards to people." Therefore, improved operational discipline results in fewer incidents, increased plant reliability, reduced quality problems, and reduced environmental excursions and equipment damage. Therefore, like safety, your path to alarm management enlightenment is a continuous process.

Is alarm management really just a software application?

NO, alarm management is not just a software application. The software application is the tool utilized to monitor the alarm system. Monitoring an

Metric	Target – acceptable	Target – max manageable
Alarms per 10 min period per operating position	~1 (avg)	~2 (avg)
Max # of alarms in a 10 min period	≤10 (10 = "alarm flood")	
Percentage of 10 min periods containing > 10 alarms	~<1%	
Percentage contribution of 10 most frequent alarms	~<1% to 5%*	
Number of chattering/fleeting alarms	0*	
Number of stale alarms	< 5 on any day*	

Figure 3. Key metrics from ISA-18.2.

* Action plans required to address

alarm system is essential to ensure that the system is functioning within the defined metrics dictated by your philosophy. If the alarm system is *not* monitored, it is highly likely that it is outside of these metrics and thus not useful in allowing the operator to respond to the abnormal situation in a timely manner.

Is alarm management really just rationalization?

NO, alarm management is not really just about rationalization. Rationalization involves reviewing and justifying potential alarms to ensure that they meet the criteria for being an alarm as defined in the philosophy. It also involves defining the attributes of each alarm (such as limit, priority, classification, and type) as well as documenting the consequence, response time, and operator action. Although safety alarms generally tend to be some of the most critical in a plant, they still must go through the rationalization process. The product of rationalization is a list of configuration requirements recorded in the master alarm database (MAD). Alarm classification and prioritization are extremely important parts of rationalization. They are not mutually exclusive or redundant. Classification is a tool for managing requirements. Prioritization is exclusively for the benefit of the operator.

Alarm management is a process that involves managing alarms through the alarm management life cycle. ISA-18.2 and IEC 62682 are standards that provide a framework for the successful design, implementation, operation, and management of alarm systems in a process plant. They use a life-cycle approach consisting of distinct stages, which are similar in many respects to the life-cycle methodology of the ANSI/ISA-84 Functional Safety Standard. Although the use of life cycle is common to both standards, alarm management is a continuous activity, due to the scale and the processing of all alarms by the operator, requiring ongoing performance evaluation and adjustment. Alarm system performance evaluation or monitoring is one of the essential elements of alarm management.

Monitoring alarm system performance can be used to maintain the integrity of the safety system. In addition, the reliability of an alarm cannot be determined without an understanding of the overall performance of the alarm system. Reports can be generated that document the triggered alarms, indicating that a demand has been placed on a safety instrumented function (SIF). The frequency of layer of protection analysis (LOPA) alarms (alarms that are listed in a layer of protection analysis) can be used to evaluate and validate the assumptions of initiating event frequency. Overall performance has a direct impact on the operator's ability to successfully respond to individual alarms. An unmonitored alarm system is essentially a poorly performing alarm system that correlates to a broken alarm system.

What further information is available on alarm management?

There are dozens of well-written papers by individuals who have been active in ISA-18.2 since the 2003–2005 time frame. These individuals have been involved since the beginning of the journey to develop the first standard on alarm management. In addition, there are several books and courses available to provide further guidance on the topic.

The ISA-18.2 TRs are also a valuable resource, as they provide the guidance on how to implement alarm management. Remember, a standard communicates what you *shall* or *should* do, where a TR communicates how to do it.

The authors of this article have included a short list of published papers that provide guidance on alarm management. If you have difficulty finding additional viable resources, the authors have lists of resources we can share.

Can I get help to implement my alarm management program?

Yes, you can get help implementing an alarm management program, but as they say, be careful of what you ask, because there may be unintended consequences. Every company that has anything to do with control systems or automation services today markets themselves as "alarm management subject-matter experts." Most of these organizations have published white papers on the subject, and often this material is poor guidance at best if not completely wrong.

As with any contractor, it is important that you vet the company and individuals who are going to provide alarm management services. At a company where he worked, one of the authors of this article has seen reportable incidents due to poor alarm management rationalization. Essentially, the company, which is well known in the alarm management business, rationalized critical alarms out of existence.

There are numerous resources available, but you must review each to ensure that it will bring value to you and your organization. ■

ABOUT THE AUTHORS

Donald G. Dunn (Donald.dunn@wsnelson.com) is a senior consultant with WS Nelson, providing services to the refining, chemical, and other industries. He is currently a senior member of the IEEE and ISA and is also a member of the NFPA, API, and IEC standards development organizations. He co-chairs ISA18, chairs IEEE841 and 841.1, and is the convener of IEC 62682. Dunn served as the vice president of the ISA Standards and Practices Board in 2011–2012.

Nicholas P. Sands, PE, CAP(Nicholas.P.Sands@dupont.com), is a senior manufacturing technology fellow working in DuPont's Tyvek®, Kevlar®, and Nomex® businesses. He is the co-editor of the *Guide to the Automation Body of Knowledge, Third Edition*, an ISA Fellow, and a member of the Process Automation Hall of Fame. His work in standards includes being co-chair of ISA18, secretary of IEC 62682, and co-director of ISA84 and ISA101. His path to automation started while earning a BS in chemical engineering from Virginia Tech.

View the online version at www.isa.org/intech/20200402.

RESOURCES

ANSI/ISA-18.2-2016, *Management of Alarm Systems for the Process Industries*
www.isa.org/store/ansi/isa-182-2016,-management-of-alarm-systems-for-the-process-industries/46962374

IEC 62682-2014, *Management of Alarm Systems for the Process Industries*
https://webstore.iec.ch/publication/7363

"Horses for Courses – A Vision for Alarm Management"
IBC Alarm Systems Seminar, London, June 2002

The Management of Alarm Systems
www.hse.gov.uk/research/crr_pdf/1998/crr98166.pdf

"Alarm Management and ISA-18 – A Journey, Not a Destination"
Texas A&M Instrumentation Symposium (2010).
www.researchgate.net/publication/266096777_alarm_management_and_isa-18_-_a_journey_not_a_destination

"Get a life(cycle)! Connecting Alarm Management and Safety Instrumented Systems"
2010 ISA Safety & Security Symposium, April 29, 2010 New Orleans
https://pdfs.semanticscholar.org/9bce/de00afaeb32fb0a77e45269bbce-acc0d6c21.pdf

"Alarm systems standards important"
www.isa.org/standards-and-publications/isa-publications/intech-magazine/2005/december/safety-alarm-systems-standards-important

"ISA-SP18-Alarm Systems Management and Design Guide"
www.isa.org/link/SP18

"From Chaos to Performance: Alarm Management Using ISA 18.02"
www.isa.org/store/products/product-detail/?productId=121694

"A postcard from the promised land of alarm management"
www.isa.org/standards-and-publications/isa-publications/intech-magazine/2010/december/automation-it-a-postcard-from-the-promised-land-of-alarm-management

"When Good Alarms Go Bad"
Texas A&M 70th Instrumentation Symposium for the Process Industries, Jan. 2015.

"Diagnosing your alarm system"
www.isa.org/intech/20150805

"Good Alarms Go Bad – The Why!"
2017 Process Control & Safety Symposium & Exhibition, Houston

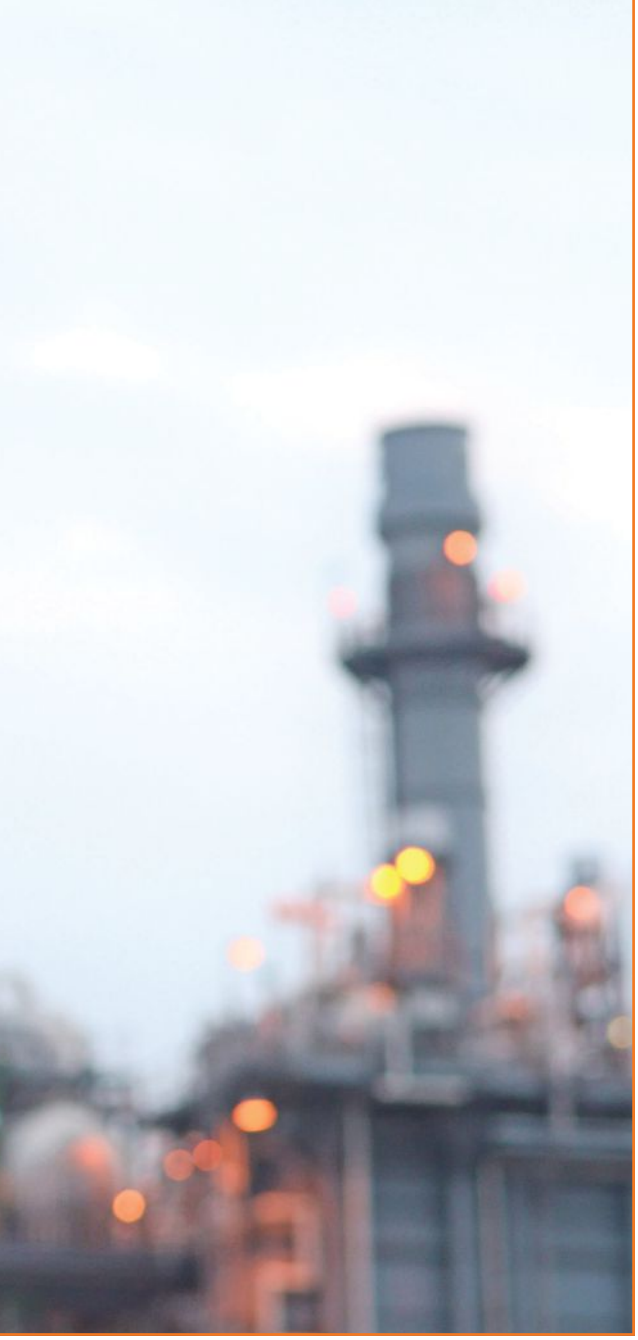
Maintenance technicians can respond faster, and even prevent problems, therefore saving money

By Bill Dehner

Add remote monitoring to increase maintenance personnel productivity

The classic tool kit for an industrial automation maintenance technician typically included assorted hand tools and a multimeter. And for many years now, the tool kit has likely included a laptop computer for the technician to interface with programmable logic controllers (PLCs), human-machine interfaces (HMIs), and other intelligent industrial devices and instruments. Another key element is likely a phone or radio, so operations personnel can contact the technician if trouble is observed. The discovery and notification of trouble is where remote monitoring can be used to improve upon existing practices, and why it should be an integral part of every technician's tool kit.

An early step for any maintenance activity is detecting the need. Some maintenance is performed on a calendar-based schedule, but many activities



FAST FORWARD

- Remote connectivity methods have steadily improved over the years and can now be readily added to existing or new systems.
- Maintenance technicians can use remote connectivity to improve their reaction time because they are proactively informed of impending problems.
- Remote connectivity and monitoring for maintenance purposes can be overlaid on existing systems without disrupting underlying operational functionality.

Figure 1. Remote monitoring is a key technology for helping maintenance personnel support multiple remote sites with many types of equipment.

are only initiated when something breaks. A range of remote monitoring technologies are helping technicians respond more quickly to failures, and to troubleshoot some problems from afar, or if this does not suffice, to arrive at the site with the right parts and tools. Remote monitoring can also guide more efficient proactive maintenance programs to address small issues before they escalate into major problems. These aspects take on even greater importance when maintenance staff must support many geographically remote sites (figure 1).

New equipment, systems, and entire manufacturing sites can be designed with built-in remote monitoring capabilities. However, there are also many options to add remote monitoring to existing operations populated with older and often standalone equipment. Making industrial systems smarter and available over the Internet in this way is often termed as an Industrial Internet of Things (IIoT) initiative, or digitalization.

This article looks at some technologies for helping end users add modern IIoT and remote monitoring options incrementally to any type of existing system. By adding a mobile device, such as a smartphone or tablet into their maintenance tool kit, technicians can provide faster and better service while cutting costs (figure 2).

But before we get into the use of modern technologies, let's look at the evolution of remote monitoring.

Connectivity over the years

Industrial automation digital technologies have certainly evolved through the decades, although to many observers the progress has often appeared to be plodding along, well behind the footprints left by consumer electronics. Reasons for this lag include the need for

Figure 2.
Maintenance personnel today are likely to include a laptop computer and smartphone as part of their tool kit.

industrial products to provide extreme operating reliability, be maintainable for years, and be robust enough to survive harsh environments.

Basic operational dependability was the foremost concern, followed somewhat by ease of configuration, and even more distantly by remote connectivity. In fact, eventually remote connectivity became a point of concern from a security standpoint, but these concerns were outweighed by its usefulness during initial installation and over the life of the automation system.

Here are some milestones of industrial digital connectivity, in roughly the order they became available:

- Originally, core PLC and HMI devices required direct local connection and specific software.
- Plant networks improved upon this situation by letting users connect from anywhere on a site.
- The first remote monitoring setups involved phone modems, direct to a target device and eventually to the plant network.
- Wi-Fi networks advanced to let users connect wirelessly.
- Internet connectivity made it possible to view HMIs and some PLCs from anywhere via web browsers.
- Now many devices have Internet/cloud connectivity, so users can use mobile devices with device-specific apps for easier access.
- IIoT-type devices can add remote monitoring without affecting existing automation systems.

Perhaps counterintuitively, the technical difficulty of remote connectivity has become generally easier as the available options improved. Early efforts required special cables, vendor-specific protocols and software, and dealing with slow and intermittent connections. As networking became a common infrastructure-like utility, and standards have streamlined the protocol options, the situation has improved greatly.

The result is that instead of remote connectivity being an esoteric option reserved for designers and engineers at the beginning of a project, it has been democratized through ease of use, so operations and maintenance personnel can take advantage of it throughout the life cycle of an automation system.

Keeping an eye on the HMI

For many troubleshooting issues, it is eventually necessary for maintenance personnel to dive into the PLC code to see what it is or is not doing. Fortunately, at many sites, the first line of defense in these situations is supported by an HMI, which can provide helpful information. Local operators can view equipment status and alarms to identify what may be causing a problem.

At the first sign of trouble, operations personnel typically contact the maintenance department. Time is saved when maintenance personnel have their own HMI station, or the ability to remotely connect to the operator's HMI, in either case so they can use the HMI's visualization to guide their maintenance efforts. Many HMIs support browser-based remote connectivity, making it possible to remotely view displays on any network-connected computer or mobile device (figure 3).

With the foreknowledge that maintenance personnel will be taking an active role in monitoring equipment and systems via HMIs, it becomes more important than ever to develop detailed diagnostic PLC code and HMI graphics for use by maintenance personnel.

Beyond troubleshooting, the integration of run-time hour timers and equipment cycle timers are the first steps toward preventative and predictive maintenance. Just like a modern car alerts the owner to an upcoming necessary oil change, based on mileage and driving conditions, any contemporary automated system or machine can and should track similar indicators. Remote connectivity makes this information readily available to the maintenance personnel who need it.

The inverse of availability in this case is security. Even within the local area network (LAN) at an operations site, it is important to allow only authorized personnel to access HMIs and PLCs. When industrial automation systems are connected through a corporate wide area network (WAN) and to the Internet, security becomes even more of a concern.

This awareness about security has led to the incorporation of IT-type technologies, such as virtual private networks (VPNs), for industrial automation networking. Users can connect with LANs/WANs from anywhere securely over VPNs, but the downside is that VPNs can be difficult to administer.

For this reason, some industrial automation suppliers have developed mission-specific VPN implementations to help end users easily benefit from VPN connectivity while requiring minimal configuration effort and no IT involvement. This type of innovation provides

Figure 3.
Industrial HMIs, like this AutomationDirect C-more, have native remote monitoring capability, for maintenance access via a laptop or mobile device.

a best-of-both-worlds solution for operational technology (OT) end users, who can best benefit from remote connectivity but may not be staffed to implement it.

The cloud changes connectivity

Before browser-based and Internet/cloud methods, remote connectivity required the design and support of specific hardware, software, and configurations. Remote connectivity innovation was not destined to end with the ubiquitous web browser, however. Interacting with web-type HMI displays over a VPN connection is workable, but sometimes can be a little inelegant. Fortunately, the rise of consumer-based smartphones and associated apps provided a new option.

The latest remote connectivity options use cloud capabilities and apps to homogenize and simplify access, so users can focus their efforts on the real issues at hand: identifying problems, often proactively, and fixing them.

Automation vendors now offer cloud services that simplify access by establishing secure VPN connectivity to any number of remote sites and systems, and serving up HMI displays and PLC data on end user computers and mobile devices (figure 4).

For a nominal monthly charge, users can deploy this functionality company-wide. The capability is scalable, so end users can grow it at their own pace. This lets them start small with a few machines as a trial, and then deploy the service to a fleet of equipment.

Mobile apps are created to be aware of the particular needs of HMI and PLC users. Therefore, these apps streamline the visualization process, and offer specific features for maintenance users, such as the ability to monitor tags directly within a PLC.

Beyond connectivity and visualization, these industrial cloud services have other advanced functions like data logging and alarm/event notification. These features are common to large supervisory control and data acquisition (SCADA) implementations. However, many end users operate dozens of standalone or lightly integrated equipment and do not have an overall SCADA system. Cloud services and remote connectivity make it easy for end users to take advantage of such functions without having to create extensive systems.

Figure 4. Cloud-based services, apps, and hardware (such as AutomationDirect StrideLinx) help users establish secure VPN connections and enable mobile app monitoring of their automation systems.

Remote connectivity is not an all-or-nothing proposition. For new projects, users can certainly select HMI and PLC platforms with these features. More likely, many users have lots of operating equipment and systems already installed, and it does not make sense to completely retrofit each with new automation. Instead, they can gain remote connectivity benefits by adding a modern PLC or HMI to existing systems, and then using these components to concentrate important information and make it available via the cloud. It this way, maintenance personnel can add the IIoT features they need to help them perform their work proactively without disrupting existing operations.

IIoT as a parallel path

As noted previously, the earliest remote monitoring systems usually required a heavy emphasis on adjusting the underlying PLC and HMI systems to provide the necessary data. Newer cloud solutions have more alternatives for improving automation systems by

Figure 5. To add IIoT capabilities without interfering with existing operations, users can install AutomationDirect Pocket Portals and access the information through an associated cloud service.

adding IIoT capabilities.

However, many users are reluctant to meddle with existing automation systems that are working just fine. Or, they may want to monitor equipment that has hardwired controls or other limitations. For these cases, a new class of lightweight, cloud-ready devices let users overlay remote monitoring functionality without disrupting existing systems (figure 5).

For applications only needing to monitor or perhaps remotely command a few discrete points, a wireless portal is an inexpensive and easy-to-install option. These portals may also support Modbus RTU communications, which is a classic but still viable industrial communications protocol supported by many types of equipment. Users can easily install one or dozens of these gateways at local equipment, and they use Wi-Fi networks that are existing or can be added quickly and inexpensively.

These portals have free cloud subscriptions with options for higher-data plans. Typical cloud features include:

- user-configurable real-time dashboards (similar to HMI displays)
- cloud storage for data logging
- ability to download data as a CSV file
- email and/or push notifications on alarms
- scheduled remote access
- mobile device monitoring

Other edge devices like MQTT gateways can integrate with typical Modbus field devices and report information up to a cloud-based broker using the MQTT protocol. This approach involves a little more user configuration than a dedicated cloud-based portal system, but it has even more flexibility for users to deploy IIoT capabilities to existing equipment.

When a maintenance group knows certain automation data could provide proactive notifications, installing a parallel system of cloud-connected edge devices can be a cost-effective way to add these IIoT features without interfering with existing functionality.

Reactive and proactive results

Maintenance operations want to use remote connectivity and monitoring to respond to problems faster, or avoid them before they happen, and therefore save money. Downtime can be costly to any manufacturer, but when dealing with a high-dollar product, like oil production, the costs of a shutdown can be astronomical. Some offshore wells can produce upwards of 34,000 barrels of oil a day, and with oil prices around $50 a barrel, just one hour of a shutdown can cost more than $70,000 in lost production.

The oil and gas industry is well aware of the costs a malfunction can have and has taken many steps to prevent these occurrences. Remotely monitoring critical assets is an important part of that prevention. Communication to these offshore platforms is well established, and many companies continuously monitor oil production components remotely.

For example, to avoid any unexpected valve failures, whenever a command to close or open is given, the automation system records the time it takes for the valve to complete its action. This information may be determined in the controller, but if it is not communicated to a higher level then it is impossible for action to be taken proactively.

By implementing remote connectivity and monitoring for crucial activities, it becomes possible to compile this data and analyze it to determine which valves are sticking or are on the way to failure. This data gives operators and technicians, both on site and off, a heads-up and allows a quick and proper response to correct the condition with scheduled maintenance.

Maintenance teams should start by addressing the most troublesome or expensive problems. As their comfort level with remote monitoring improves, it is easy to expand the types of monitoring to encompass other parts of operations.

Expand the tool kit

Today's maintenance technicians are ready to expand their tool kits by adding a mobile device for remotely monitoring equipment and systems. Remote monitoring gives these personnel the ability to respond to problems faster, and even proactively prevent them.

For users with existing systems and standalone equipment, there has not always been an easy answer for improving remote connectivity. It has been especially daunting to plan an overall platform able to connect to many different remote systems consistently. The latest cloud-based options make building-in or adding-on remote connectivity a straightforward activity, helping maintenance personnel focus their efforts on keeping their manufacturing and production plants running. ■

ABOUT THE AUTHOR

Bill Dehner (bdehner@automationdirect.com) has spent the majority of his 15-year engineering career designing and installing industrial control systems for the oil and gas, power, and package handling industries. He holds a bachelor's degree in electrical engineering with an associate's in avionics from the USAF and is currently working for AutomationDirect as a technical marketing engineer.

View the online version at www.isa.org/intech/20200403.

RESOURCES

"Remote access to automation system components"
www.isa.org/intech/20180205

"IIoT remote monitoring"
www.isa.org/intech/20190203

"HMI remote-monitoring trends"
www.isa.org/intech/20160805

The Plant Floor in Your Pocket

Get an overview of your process at a glance.
Control your SCADA with a swipe.

See the live demo now.
Scan this QR code with your phone
or visit demo.ia.io/tech

Bayesian analysis improves functional safety

By Paul Gruhn, PE, CFSE

ISA/IEC 61511 is more than statistical calculations

Functional safety engineers follow the ISA/IEC 61511 standard and perform calculations based on random hardware failures. These result in very low failure probabilities, which are then combined with similarly low failure probabilities for other safety layers, to show that the overall probability of an accident is extremely low (e.g., 1E-5/yr). Unfortunately, such numbers are based on frequentist assumptions and cannot be proven.

However, looking at actual accidents caused by control and safety system failures shows that accidents are *not* caused by random hardware failures. Accidents are typically the result of steady and slow normalization of deviation (a.k.a. drift). Although it is up to management to control these factors, Bayes' theorem can be used to update our prior belief (the initial calculated failure probability) based on observing other evidence—such as the effectiveness of the facility's process safety management process. The results can be dramatic.

Statistics

Some statistics are easy. For example, what is the probability of a fair six-sided die rolling a three?

That should not challenge anyone. The answer is based on frequentist principles and can be proven by testing or sampling.

Some seemingly simple statistical examples are not as simple as they first appear. For example, imagine there is a one-in-a-thousand chance of having a specific heart disease. There is a test to detect this disease. The test is 100 percent accurate for people who have the disease, and 95 percent accurate for those who do not. This means that 5 percent of people who do not have the disease will be incorrectly diagnosed as having it. If a randomly selected person tests positive, what is the probability that the person actually has the disease? (Stop and answer the question before proceeding. I'll talk more about it later.)

Some statistical cases are not simple at all. For example, what is the probability of *your* plant having a catastrophic process safety accident within the next year? You and others might have designed and calculated the risk to be as safe as driving a car (i.e., 1/10,000 per year), but how can you *prove* it? Frequentist-based statistics cannot be used to confirm or justify very rare events. Do you believe your plant is safer (or less safe) than any another facility you may have visited? Might there be variables, conditions, or precursors that you could *observe* that might *affect* your belief? And if so, might you be able to evaluate and *quantify* their impact on risk?

The answer is "yes." And the answer for the heart disease example above is 2 percent. (See the box at the end of this article for the solution if you did not get the correct result.)

Bayes basics: Updating prior beliefs

Past performance is *not* an indicator of future performance, especially for rare events. Past performance would *not* have indicated (at least not to those involved at the time) what would happen at Bhopal, Texas City, or any other accident site you can think of. How many managers have you heard say, "We've been running this way for 15 years without an accident; we *are* safe!"

What if you were to calculate the probability of dying in a vehicle accident? In the U.S. there are about 35,000 traffic deaths every year. Considering our population, that works out to a probability of about 1/10,000 per year. You are obviously not going to live to be 10,000 years old, so the probability of your dying in a car crash is relatively low. Yet, might there be factors that *influence* this number, ones that you might be able to observe and *control*?

Consider the following: A salesman you know—but have never met—picks you up at your office and drives you both out for lunch. What probability would you assign to being in a fatal accident? On the way to the restaurant you notice him texting while driving, speeding, and being a bit reckless. You are a bit distressed, but you know you do not have far to go, and you keep your mouth shut. At your one-hour lunch you see him consume three alcoholic beverages.

Assuming you would even be willing to get back in the car at that point (there is always Uber), what probability would you assign to being in a fatal accident *now*? (Records have shown that alcohol is involved in 40 percent of traffic fatalities, speeding 30 percent, and reckless driving 33 percent. You are 23 times more likely to crash while texting. Seatbelts reduce the risk of death by 45 percent.) This is an example of updating a prior belief based on new (even subjective) information. That is Bayes' theorem.

So one *can* observe conditions and make even subjective updates to previous predictions. People do this all the time. Even insurance companies do this when setting premiums (as premiums are not simply based on past performance).

FAST FORWARD

- Functional safety engineers who follow ISA/IEC 61511 perform calculations based on random hardware failures.
- Accidents are typically the result of steady and slow normalization of deviation, or drift.
- Using Bayes' theorem, prior belief can be updated even with subjective information.

A real example: Bhopal

Bhopal was the worst industrial disaster of all time. The facility was designed and build in the 1970s, and the accident took place in 1984. Although this was a decade before layer of protection analysis (LOPA) was introduced, this technique is useful for evaluating the original design and comparing it to the operation on the day of the event. This is *not* an attempt to explain *why* the event happened, nor should this be considered an example of 20/20 hindsight. This is simply an attempt to show how Bayes' theorem might be used in the process industry.

The facility in Bhopal was patterned after a successful and safe plant in the U.S. There were multiple independent protection layers to prevent the escalation of an event caused by the possible introduction of water into a storage tank. These are listed in table 1, along with *sample* probabilities for their failure.

Considering an initiating event frequency of perhaps 0.1/yr (a common number used in LOPA for many initiating events), the risk associated with this event would appear to be much

Description	Probability of failure
Stainless-steel construction	.01
Nitrogen purge	.1
Refrigeration system	.1
High-temperature alarm	.1
Empty reserve tank	.1
Diluting agent	.1
Vent gas scrubber and flare	.1
Rupture disk and relief valve	.1
All safety layers failing at the same time	**1E-9**

Table 1. The possible performance of safety layers at Bhopal

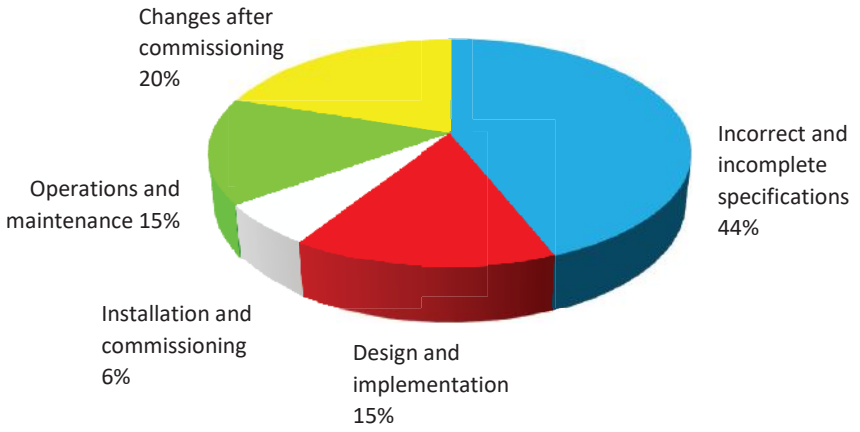


Figure 1. The causes of accidents involving control and safety systems

lower than the risk of driving a car. Yet how could this be *proven*?

In reality, *none* of the layers were effective at Bhopal, and the accident happened within the first five years of operation (i.e., within the assumed time period of practically any single initiating event). All the layers at Bhopal did not magically fail at the same time. Trevor Kletz was well known for saying, "All accidents are due to bad management." Ineffective management allowed all the layers to degrade (and there were common causes between many of them) to the point where *none* of them were available the day the event happened.

Such normalization of deviation, or drift, was not unique to Bhopal. This is a serious issue that affects many facilities even today. How might we be able to model this?

Functional safety and math

Functional safety engineers focus on the ISA/IEC 61511 standard. Following the life cycle of the standard involves determining a performance requirement for each safety instrumented function (SIF) and evaluating that the intended hardware design meets the performance requirements (and changing the design if it does not). This entails performing calculations considering the device configuration, failure rate, failure mode, diagnostic coverage, proof test interval, and much more. Yet the calculations only involve random hardware failures, and the numbers are often so low that they cannot be proven by frequentist statistics and sampling. The standard does discuss systematic failures (e.g., human errors of specification, design, operation), but *not* in a quantitative manner.

What really causes accidents involving control and safety systems? Figure 1 is well-known to all functional safety practitioners. (The results were published by the United Kingdom Health and Safety Executive more than 20 years ago, and it is unlikely that any of the values have changed since.) Few, if any, accidents have been due to a random hardware failure, yet that is what everyone is focusing on in their calculations. How might we include the management-related issues shown in figure 1 in our overall modeling? And if we were to do so, how much might it change our answer?

When deciding exactly what is a safe plant, some say, "One that has not had an accident." As discussed earlier, such thinking is flawed. Similarly, what is the definition of a safe driver? One who has not had an accident? If the salesman driver mentioned earlier tried to reassure you by saying that he drives that way all the time and he has never had an accident, would you be reassured? It should be obvious to everyone that a

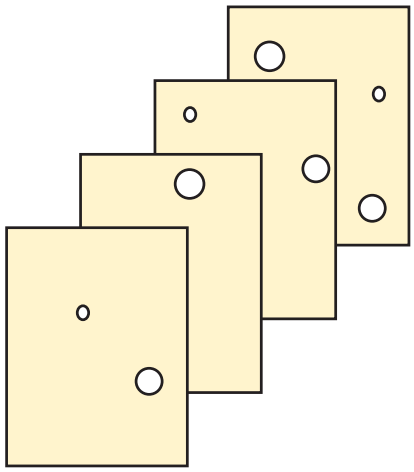


Figure 2. The swiss cheese model

safe driver is one who follows the rules and laws, does not drive under the influence of alcohol or drugs, is not distracted by texting, wears a safety belt, keeps the car in good condition, etc.

Yet does doing so *guarantee* there will not be an accident? Obviously not, but it does lower the probability. The same applies to a safe plant. And we *can* model this!

Swiss cheese model

James Reason came up with the swiss cheese model in the late 1990s (figure 2). It is a graphical representation of protection and mitigation layers. The effectiveness of each layer is represented by the size and number of holes in each layer. The holes are controlled by management; the more effective the management, the few and smaller the holes. Accidents happen when the holes line up, and a single event can proceed through each layer.

A similar concept can be represented graphically by comparing the 14 elements of the Occupational Safety and Health Administration (OSHA) process safety management (PSM) regulation to a Jenga tower (figure 3). Think of the 14 main elements as layers, and the subelements as individual pieces within each layer. An effective implementation of all the clauses in the regulation is similar to a complete Jenga tower, or a swiss cheese model with very few holes—and small ones at that.

But how many people working in process plants truly believe their facility has all the pieces in place, and that they are all 100 percent effective? Perhaps your facility is more like the tower and swiss cheese model in figure 4.

Figure 3. (Effective) process safety management, Jenga, and the swiss cheese model

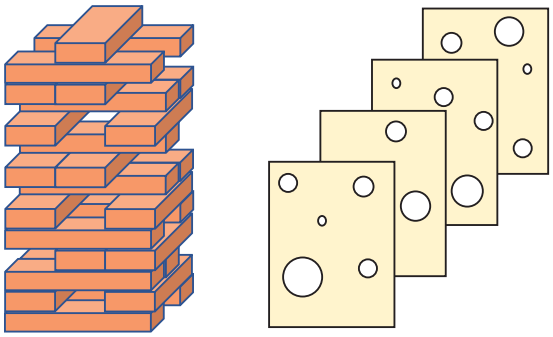


Figure 4. (Ineffective) process safety management, Jenga, and the swiss cheese model

What is deceptive is that the tower in figure 4 is still standing. Everyone then naturally assumes they must be OK. ("We've been operating this way for 15 years and have not had an accident yet; we must be safe.") Yet anyone would realize the tower is not as strong or as resilient as the one in figure 3.

Langewiesche said, "Murphy's law is wrong. Everything that can go wrong usually goes right, and then we draw the wrong conclusions." Might we be able to evaluate the completeness of the tower, or the number of holes in the swiss cheese model, and determine the impact on safety? If you knew the various layers were imperfect, might you be able to update your "prior belief" based on newly acquired information, even if that information were subjective?

Bayesian networks

Functional safety practitioners will be familiar with fault trees and event trees. What might be new to many are Bayesian networks, a simple example of which is shown in figure 5. Just as with the other modeling techniques, there is math associated with how the network diagrams interact with each other. There are also commercial programs available to solve them automatically, as diagrams can get large and complex and the math too unwieldy to solve by hand. One interesting aspect of Bayesian networks is that the math and probability tables may be based on subjective ranking (e.g., low, medium, high).

The case of interest here is to model the impact of the PSM program on the performance of a safety instrumented function (SIF). Imagine a SIF with a target of safety integrity level (SIL) 3. Imagine a fully fault-tolerant system (sensors, logic solver, and final elements) with a calculated probability of failure on demand of 0.0002. The reciprocal of this number is the risk reduction factor (RRF = 5,000), which is in the SIL 3 range, as shown in table 2.

As noted earlier, the calculations are based on frequentist statistics and cannot be proven. But as cited in the examples above, our "prior estimate" could be updated with new information, even if it were subjective. This example can be represented in the simple Bayesian network shown in figure 6.

SIL target	RRF range
4	10,000 – 100,000
3	1,000 – 10,000
2	100 – 1,000
1	10 – 100

Table 2. SIL and risk reduction factor

It is easiest to understand the solution of a Bayesian network if it can be shown graphically. This simple example can be solved with an event tree. All that is left for us to decide is what numerical values to assign to the ranking scales for the possible effectiveness of the overall PSM program. Admittedly there are many factors that could be evaluated here (e.g., competency, staffing levels, completeness of procedures, effectiveness of management of change, effectiveness of testing). The example here will simply group all these factors together. Two example ranges are shown in table 3. Before proceeding, do you think these values are reasonable?

The event tree using one value of PSM effectiveness (99 percent) is shown in figure 7, while table 4 lists the results for all the possible values.

The initial idealistic calculation (our prior belief) showed the risk reduction factor to be 5,000. Including another factor to update our belief results in a dramatic change to the number. Simply achieving SIL 2 may end up being very difficult in the real world. Admittedly, assigning numbers to the qualitative rankings of the PSM program will be a point of contention. Before showing these results to your subject-matter expert (SME) team members, ask them one simple question: What do they think is the overall effectiveness of the PSM program at their facility? Then show them the results.

In conclusion, being a safe driver is accomplished by following all the rules that are known to help avoid accidents. Similarly, operating a safe plant is accomplished by following all the rules and regulations effectively. Yet it is easy for functional safety engineers to focus instead on math and hardware calculations. The frequentist-based statistical calculations result in extremely small numbers that cannot be proven.

However, the prior belief probability can

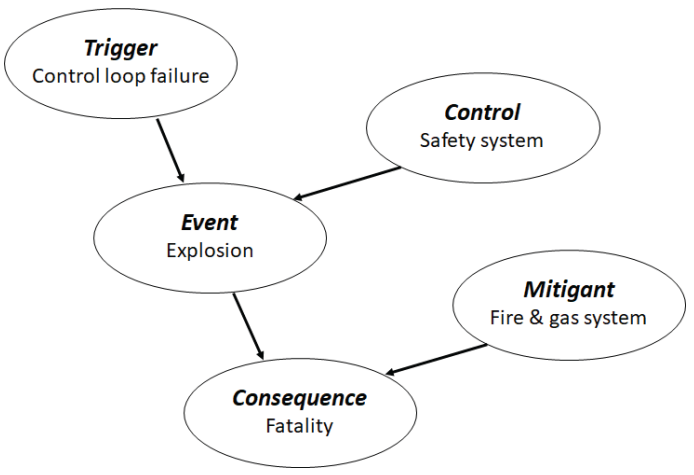


Figure 5. Sample Bayesian network

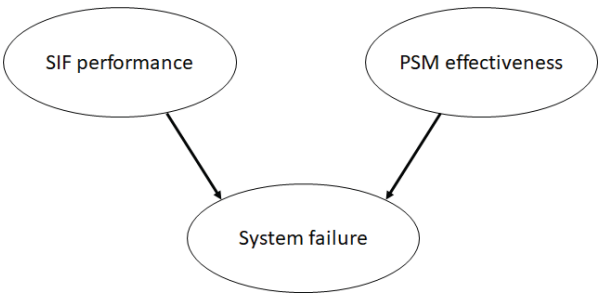


Figure 6. Bayesian network including a subjective factor

be updated with even subjective information. Doing so can change the answer by orders of magnitude. The key takeaway is that the focus of functional safety should be on effectively following all the steps in the ISA/IEC 61511 safety life cycle and the requirements of the OSHA PSM regulation, not the math (or certification of devices). Both documents were essentially written in blood through lessons learned the hard way by many organizations. ■

ABOUT THE AUTHOR

Paul Gruhn, PE, CFSE (Paul.Gruhn@aesolns.com), is principal of aeSolutions and the outgoing (2019) president of ISA. He is an ISA Life Fellow, co-chair and 25+ year member of the ISA84 standard committee, developer and instructor of ISA safety systems courses, author of several ISA textbooks, and developer of the first commercial safety system software modeling program. Gruhn is both a certified functional safety expert and an ISA84 safety instrumented systems expert.

View the online version at www.isa.org/intech/20200204.

Understanding statistics: The heart disease problem

The problem: Imagine there is a one in a thousand chance of having a specific heart disease and that there is a test to detect this disease. The test is 100 percent accurate for people who have the disease, and 95 percent accurate for those who do not. This means that 5 percent of people who do not have the disease will be incorrectly diagnosed as having it. If a randomly selected person tests positive, what is the probability that the person actually has the disease?

The solution: Just under 2 percent.

The reasoning: Only one person out of 1,000 has the disease, but if 5 percent of the people test as false positives, that would be 50 people out of 1,000 who are diagnosed, but do not actually have the disease. So, the probability of having the disease based on test results is one out of 51 people (the 50 false positives, plus the one who actually has the disease), which is just under 2 percent.

Every medical test results in false positives, so do not be misled by your medical practitioner who may not have a full understanding of the statistics. ■

Ranked scale	Optimistic value	Pessimistic value
Very high	99.99%	99%
High	99.9%	90%
Medium	99%	80%
Low	90%	60%
Very low	< 90%	< 60%

Table 3. Possible ranking for the effectiveness of a PSM program

Ranked scale	Optimistic value	SIF RRF	Pessimistic value	SIF RRF
Very high	99.99%	3,300	99%	98
High	99.9%	833	90%	10
Medium	99%	98	80%	5
Low	90%	10	60%	3
Very low	< 90%	<10	< 60%	<3

Table 4. SIF performance based on PSM effectiveness

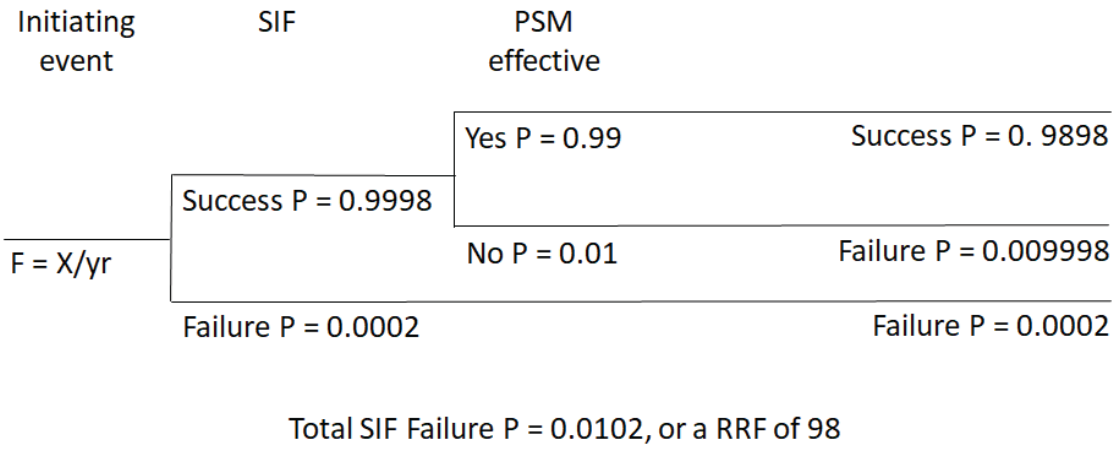


Figure 7. An event tree using one value of PSM effectiveness (99 percent)

At your service: Industrial ops in the cloud

By Matthew Littlefield

Understanding commercial cloud providers is crucial. Start with Microsoft Azure, Amazon AWS, and HPE

FAST FORWARD

- Industrial companies need to know how to choose a cloud provider for industrial operations.
- AWS has had tremendous success partnering with SaaS providers in the industrial space.
- Microsoft did an admirable job of extending its many existing partners to Azure.

Given the ease of installation and updates, single version of the truth, multisite scalability, and other benefits of cloud computing and software as a service (SaaS) applications, industrial operations are finally embracing industrial transformation (what we call "IX") in a big way. Discussions have changed from "Will we do cloud computing or make use of Industrial Internet of Things technology?" to "How will we implement cloud computing and IIoT?"

On-premises installations of cloud-computing servers give industrial operations directors more control, but also a lot of do-it-yourself responsibility. Off-prem cloud service providers have sprung up to help, but while five years ago there were still 10 or more vendors that had a credible chance of becoming the cloud leader for industrial operations, the race has come down to two front-runners: Microsoft Azure and Amazon Web Services (AWS). Here is a look at how the environment for industrial operations has evolved and what the front-runners have to offer.

Industrial transformation relies on the digitalization of processes and a variety of Industry 4.0 technologies, including cloud computing. Last year we were already seeing clear signs that 2020 will be the biggest year yet for IX. The Hannover Messe 2019 tradeshow in Germany revealed five big IX trends that got us where we are today.

1. **Industry embraces hyper-scale clouds.** Both BMW (with Microsoft) and Volkswagen (VW) (with Amazon Web Services and Siemens MindSphere) announced enterprise commitments to the cloud and IIoT for industrial operations at Hannover. The goals and expected benefits for each were driving a single version of the truth, flexibility, and improved performance. In the case of VW, its cloud/IIoT commitment encompassed 122 manufacturing sites and about 1,500 suppliers.
2. **IIoT platforms consolidate.** The world does not need 600 IIoT platforms—it does not even need 10—and last year we saw the market consolidate to a few focused on specific ecosystems or industries. The companies that had momentum include Siemens MindSphere, PTC ThingWorx with Rockwell Automation, ABB Ability, and Schneider Electric EcoStruxure. All have deep experience and credibility in operational technology (OT).
3. **Edge computing momentum continues.** Even now in the industrial sector, we are still a long way from the "cloud first" mentality that the cloud hyper-scalers would all like us to adopt. For this, and many other reasons, the focus on edge computing has grown among many industrial companies. HP Enterprise (HPE) showcased new hardware and software in 2019 with the HPE Edgeline OT Link (see sidebar), which promised scalable industrial compute capabilities coupled with industrial edge data management and intelligence. Cisco, no longer being distracted with analytics or IoT platforms, had a much more focused message about edge data management, industrial networking, industrial edge computing, and industrial cybersecurity.
4. **Companies shift to solutions and multivendor environments.** As cloud and IIoT platform consolidation continues, many industrial software vendors are showcasing their ability to orchestrate end-to-end solutions and help customers avoid platform vendor lock-in. SAP and IBM, for example, have long been the market-share leaders for enterprise asset management, but they now compete in this full solution area that we refer to as APM 4.0. This includes condition-based maintenance, reliability-centered maintenance, asset life-cycle management, and predictive analytics. Providers here include Uptake, C3AI, GE Digital, and AspenTech, among many others.

SAP has done an admirable job of bringing operationally focused solutions, with 3D visualizations and machine integrations, out of the back office and down to the shop floor,

The 10 or more vendors vying to become the cloud leader for industrial operations 10 years ago have been winnowed down.

extending across product engineering, manufacturing, and the supply chain. The combination of financial, business process, and operations is powerful. Although IBM continues to lead with IBM Cloud and IBM IoT in other industries and use cases, it is clear IBM is moving toward a solutions-based approach for industrial applications. In 2019, hardly a product was mentioned in the IBM booth, with the highlight being solutions focused on delivering value to customers quickly by improving the performance of manufacturing and assets. Behind the scenes, these solutions are delivered by taking a modular and micro-services-based approach.

Over the past five years, Oracle also has invested heavily in cloud computing services and is rebuilding value chain applications like enterprise quality management software, product life-cycle management (PLM), manufacturing operations management (MOM), and supply chain management (SCM). More recently, the company has been investing in manufacturing-specific solutions, including the launch of five IoT applications focused on areas like productivity, asset performance, workers, and fleet. Coupled with their investments in IoT and artificial intelligence (AI) embedded in enterprise software, the end-to-end solutions showcased by Oracle in 2019 were compelling.

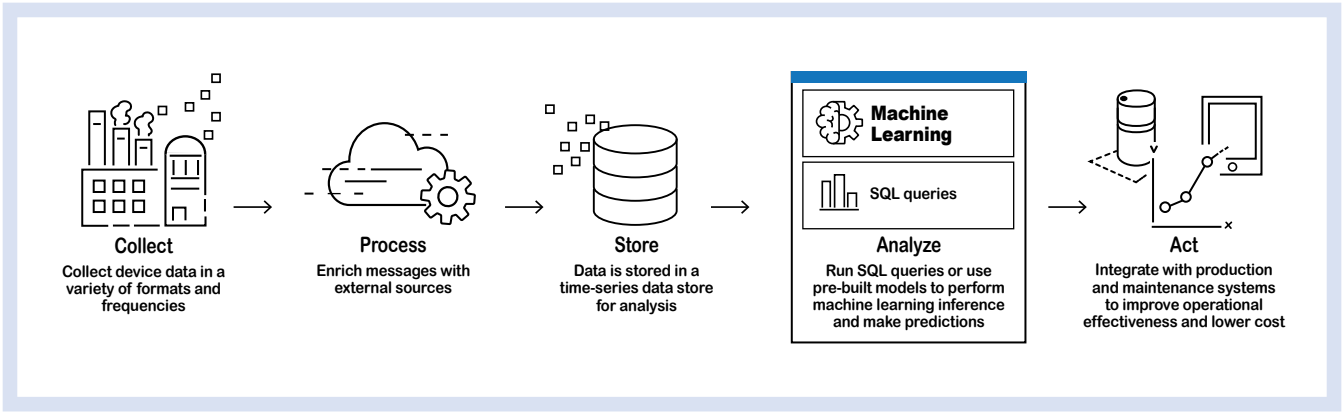
5. **Partner ecosystems for digital twins emerge.** Originally a concept pushed by the PLM and computer-aided design communities to describe 3D virtual models of products, digital twins have been extended to include connections to the physical world and opportunities for virtually commissioning machines. As companies outside complex discrete manufacturing embrace this extended definition of digital twin, it is becoming clear that individual vendors cannot deliver the full solution. So partnerships are emerging. Siemens announced a partnership and investment in Bentley Systems in 2018 and gave a compelling demo of a process industry digital twin in the Siemens booth. The year 2018 also saw the announcement of the PTC-Rockwell partnership and investment, which was featured prominently in the PTC booth. And partnerships continued in 2019, with ABB and Dassault Systems announcing one as well. Finally, the Schneider Electric and Aveva partnership was on full display, with a number of the Aveva product offerings and solutions well integrated into the Schneider Electric booth.

A two-horse race: Azure v. AWS

The 10 or more vendors vying to become the cloud leader for industrial operations 10 years ago have been winnowed down. Either executives chartered with the endeavor moved on (GE, Google) or the strategy has moved to partnerships and enabling multicloud environments (IBM, SAP). Some are still trying—but with little success inside the factory (Oracle). But both Microsoft Azure and Amazon AWS now have a degree of accumulated advantage that makes it very unlikely any other vendor can catch back up.

It was already apparent last year that Azure and AWS had become the two market leaders when it comes to infrastructure as a service (IaaS) cloud and platform as a service (PaaS) IoT providers for the IIoT. Microsoft has a deep history in the industrial space and has done an admirable job of converting its multidecade long SQL and OS partnerships with OT vendors into being the preferred choice for recently launched IIoT platforms from these same companies. However, last year AWS was increasingly seen as a viable alternative, beyond its traditional success with independent software vendors offering a SaaS to industrial companies. Alibaba continues to be a significant player when deploying cloud on the ground in China.

As a core information technology (IT) provider, Microsoft has had a leadership position in industrial operations for decades, starting with the operating system that automation vendors switched to in the 1990s. And then it was the database that was switched to for both homegrown systems and many manufacturing execution system (MES) vendors. Not to mention, at many industrial compa-



AWS Smart Factory diagram

nies, "MES" stands for "Microsoft Excel spreadsheet."

In 2016 General Electric and Microsoft Corporation developed a partnership to unite each of the companies' cloud technologies. The two organizations hoped to increase their IIoT strength by combining GE's Predix Platform and Microsoft Azure. Running GE Predix technology on an Azure platform was a natural step, and GE hoped that by partnering with Microsoft its customers would find value in artificial intelligence, data visualization, and natural language technology. More recently, Microsoft did an admirable job of extending its many existing partners to Azure, including Rockwell Automation and Schneider Electric.

In December 2019, 60,000 attendees descended upon Las Vegas for AWS re:Invent. Just like Amazon Web Services generally, the re:Invent conference is fast-growing and overwhelms with its sheer breadth of content. AWS CEO Andy Jassy clearly took pleasure in the success of AWS: after just 13 years, the division has grown to $36B in revenue, and is still growing at 35 percent compound annual growth rate. At the event, there were several key announcements:

- Enabling machine learning (ML) at scale with SageMaker. This essentially launches an integrated development environment for ML to speed developing, debugging, deploying, training, and maintaining new algorithms.
- Outposts, the cloud-native managed service run at the edge to enable hybrid architectures, has moved from preview to general availability.
- The continuation of AWS's strategic move to enter smart factory.

AWS demonstrates a clear leadership role among Silicon Valley disruptors such as Uber, Netflix, and Airbnb. But in our industry, AWS is coming from behind and playing the role of disruptor. AWS has, however, had tremendous success partnering with SaaS providers in the industrial space. For example, both Infor and Siemens have chosen AWS as their cloud providers.

As LNS continues to advise many clients, the path forward for AWS is still emerging. There is both significant momentum to capitalize on now and significant headwinds to overcome in the future. Industrials including Georgia-Pacific and Volkswagen for its Industry 4.0 initiative are starting to make enterprise commitments to AWS. The AWS ecosystem is starting to grow. Siemens—the world's largest automation vendor that also has PLM, MOM/MES, and an IIoT platform in its $4B software portfolio—has chosen AWS as its preferred partner. AWS also continues to make significant investments in industry-specific hiring and providing coinvestment for customers and partners.

Reasons to not choose AWS remain. Consumer-facing food and beverage and consumer packaged goods companies are (often) hesitant to store any business or operational data with AWS that could affect their trading relationship with Amazon. AWS of course refutes any claims that they use customer data to benefit other areas of Amazon, and any access to this data would be in direct violation of their privacy policy, but the lack of trust is real.

Data science and machine learning skills at industrial companies will continue to lag Silicon Valley companies for the foreseeable future. The vision for democratizing ML for all is one that will resonate with the industrial space. With the release of SageMaker Studio, Experiments and Debugger, AWS is making ML easier. Also, managed services like Amazon Forecast, which uses machine learning for highly accurate forecasting, is making ML more accessible. But there is still a skill gap for a process or manufacturing engineer to directly jump in and begin building.

Lastly, the AWS Outposts Hybrid offering is a step in the right direction, but it does not yet address all offline use cases needed for some remote operations.

How to choose a cloud provider

Industrial companies need to know how to choose a cloud provider for industrial operations. Other than specific geographic and regulatory requirements (China and Alibaba Cloud), there are very few compelling reasons to look beyond AWS and Azure for cloud capabilities in industrial operations. This mainly leaves architectural and risk considerations to address.

- Should I go with a single-cloud versus multicloud strategy? Answering this question requires balancing vendor lock-in concerns with loss of some cloud-native capabilities, scale, and the added cost of managing a multicloud environment.

Hewlett Packard: Back in the manufacturing game

LNS Research views HPE as making lots of strategic moves to win the manufacturing IT world and to accelerate the convergence of OT and IT. We believe industrial companies should actively consider it as part of the mix for industrial transformation.

According to Tom Comstock, analyst with LNS Research, there is good news for industrials with IT/OT convergence plans: Hewlett Packard Enterprise is all-in on SaaS applications. Comstock attended the HPE Discover 2019 event in Las Vegas because HPE is focused on edge and hybrid cloud computing and on intelligent data. The event, and especially president and CEO Antonio Neri's keynote, were filled with major announcements. The biggest overall message: HPE's commitment to "as a service."

The company announced that it will offer all its products and services in a consumption model by 2022. Announcements continued to flow, with major ones around a new line of mission-critical storage systems, HPE Primera, that the vendor positioned as needing only six cables, five clicks, and 30 minutes to bring online. In addition, HPE rolled out a series of enhancements to HPE GreenLake (its offering that provides public-like cloud services—consumption-based pricing, fully managed by HPE—for systems and software on premise). In particular, HPE is now offering HPE GreenLake for the midmarket.

Comstock said, "I'm old enough to remember when HP and Digital Equipment (acquired by HP) were major players in manufacturing, delivering products, solutions, and services to manufacturers worldwide. HP offered solutions to the OT world leveraging manufacturing ISVs' solutions wrapped with HP services and technology." The company has, of course, gone through a significant transition, including the formation and spinoff of HPE in 2015, and later HPE's spinoff of the bulk of its service business in 2017. HPE Discover 2019 was "back to the future" with a focus on manufacturing and OT as highlighted by its "accelerating productivity" demonstration, which had center stage in the transformation showcase.

HPE clearly signaled its intent to deliver solutions for manufacturing again. The company announced integrations and turnkey edge-to-cloud solutions with partners ABB, Microsoft, and PTC, for real-time intelligence and control in industrial environments. HPE Fast Start Conditioning Monitoring is the first of these manufacturing-specific solutions to be made available and envisions HPE helping industrials define use cases to connect and monitor manufacturing equipment. It includes HPE Pointnext services to wrap around its edge systems, the company's HPE Edgeline OT Link platform, and ISVs' product offerings.

In this case, HPE Fast Start Conditioning Monitoring uses PTC's ThingWorx IIoT platform. It provides connectivity to a wide range of data sources and workflows for real-time insight into operational equipment. Users can add artificial intelligence with HPE AI in later stages of implementation; the demo in the showcase was exactly such a scenario.

Other manufacturing-focused announcements included solutions for edge appliances for the Microsoft Azure stack leveraging ABB, Microsoft, and Rittal as ISVs, and wireless connectivity solutions for OT using ABB Ability smart sensor technology.

It is quite clear that HPE wants to be a major provider of systems, infrastructure, solutions, and "business outcomes and experiences" for the OT world. In addition, HPE GreenLake has significant potential where manufacturers continue to be reluctant to trust operations to anything that depends on Internet connectivity (i.e., the cloud), but often do not have the IT resources required to handle the complexity of IT systems. HPE GreenLake offers an attractive alternative: fully managed systems, priced "as a service," installed on-premise, with full connectivity to the cloud of choice. ■

- How do I implement a multicloud strategy? Should we split by areas of the value chain (connected cars versus connected factories), regions, or business units, for example?
- What is the balance of IaaS versus PaaS versus SaaS? Should I build directly on top of AWS and directly consume AI and IoT services? Should I build on top of an IIoT platform like MindSphere and consume more purpose-built applications? Should I just buy relevant SaaS offerings like Seeq, which is an advanced industrial analytics vendor that was prominently showcased at re:Invent?
- Some reasons to lean toward AWS as opposed to Azure are: cost as a top decision criterion; being unconcerned with "co-opetition" issues with Amazon; having a dedicated digital or data science team that wants to quickly build new applications or advanced analytics algorithms; or the organization's SaaS or PaaS providers are moving toward AWS as a preferred provider. AWS is already the clear leader for partnering independent software vendors (ISVs) providing SaaS or PaaS.

AWS is making significant investments both internally and externally with codevelopment dollars, quickly making them a meaningful partner in the industrial operations space. For most traditional automation vendors and ISVs, this will likely mean a two-cloud strategy tied to either AWS or Azure is optimal. It also means if customers want a third provider, the burden goes to them, and it would likely be IBM with Red Hat. ■

ABOUT THE AUTHOR

Matthew Littlefield is founder of LNS Research and an expert on industrial transformation. Contact him at www.linkedin.com/in/matthew-littlefield or https://twitter.com/m_littlefield.

View the online version at www.isa.org/intech/20200405.

The quest for the most magical algorithm

By Michael Risse

The challenges of machine learning and cognitive computing in the context of process manufacturing may be a poor forum for humor and irreverence. Then again, perhaps not: It often requires a sense of humor to express the challenges.

The tale begins with a request for proposal (RFP). This RFP says vendors will be given a cleansed and structured dataset from which they are expected, via their algorithms, to find insights. It is a beauty contest for data science, and whoever finds the most valuable insight wins.

So, what's wrong with this picture?

Well, everything. It's Monty Python's King Arthur searching for the Holy Grail: insights, by way of the Holy Hand Grenade of Antioch, from algorithms and algorithms alone.

The starting point of this misadventure is the data. Data never starts out cleansed and organized. Someone has to do the work to make it so, and, in doing so, the data is substantially modified. By disconnecting data from the source, relevant updated or new data is removed. By defining the dataset for analysis, the opportunity to include related data sources that come up in the process of analysis, perhaps asset history or pricing data, is lost. By cleansing the data—a majority of the effort in many data science projects—data important to the analysis may be deleted because one person's noise is another person's critical data point.

A disconnected perspective

In summary, to create a dataset separate from its context is to create a disconnected perspective representing a static view of a constantly changing process. A smarter approach is ensuring the freedom to explore all data from all sources.

Unfortunately, after the data is defined and modified to the point where it no longer reflects reality, the next stage of the realism gap is time. Obviously yesterday is not today. Something, even if we do not know what, could have changed between the point of data capture and today, because many things can change in operating environments.

Formulas, raw materials, regulations, ambient temperature, recipes, and best practices all change. Assets get maintenance, sometimes to their detriment; personnel change each shift; sensors drift; and market prices adjust—which all undermine the sustainability of analytics efforts.

The constant change in the plant assets, markets, and products is why so many algorithm-based optimization exercises end upside down: Instead of algorithms feeding insights to employees, employees spend their time feeding data to the model to keep up with changes.

Then there are the participants in these efforts: data scientists. With all due respect for the education and expertise of data scientists, who are lucky enough to be working at what is the sexiest job of the 21st century according to the *Harvard Business Review,* most data scientists do not know process engineering. They do not have engineering degrees or front-line plant experience, or know first principles. They are highly educated and trained in computer sciences, but not in the reality of plants and processes.

Electricity and pressure

One example among the many strange remarks heard from data scientists performing analytics is "electricity consumption increases when pressure increases." This is true, except when what was being described was simply a pump turning on—not a breakthrough finding. Without the expertise and experience of employees who know the systems and processes, the application of algorithms to plant issues is wasted effort.

As a result of these challenges to the data, the state of change, and the expertise deployed on these efforts, what often results are findings incomplete relative to the complexity and number of data sources in the plant. And the "findings" will include many insights easily dismissed by anyone with plant experience, including irrelevant or already known insights. They may be obvious correlations, or simply backward to reality, but to anyone with process engineering expertise this will be obvious.

Fortunately, there is a better way. Rather than bringing data to data scientists, what is needed for a successful data science adventure is to unite the three required components for advanced analytics success.

First is the data—specifically, providing access to all of it or as much of it as possible. Second is empowering process engineers and their expertise. And the third is consulting with data scientists as required to take advantage of their fluency with algorithms to solve specific problems. This means that while data will still flow to the data scientists, algorithms will be accessible to the process engineers, chiefly in the form of software applications.

This approach to advanced analytics is as agile as the plant environment, with efforts constantly updated with data, leading to actual improvements in production outcomes. There is no magic to this, or to the algorithms; rather there is a recognition of the multiple challenges faced with data science projects. ■

ABOUT THE AUTHOR

Michael Risse, vice president and chief marketing officer, is a cofounder of Seeq Corporation and the company's resident champion for emerging applications for industrial process analytics. He spent almost 20 years at the Microsoft Corporation, where his last role was vice president of the worldwide small and midmarket segment.

Physical security of a data center

By C. Shailaja

In addition to many layers of software cybersecurity, protect data centers with layers of physical security systems

Data centers are centralized locations housing computing and networking equipment, which is also known as information technology (IT) equipment and network infrastructure. Network infrastructure comprises gateways, routers, switches, servers, firewalls, storage systems, and application delivery controllers for managing and storing data and applications. Data centers store large amounts of data for processing, analyzing, and distributing—and thereby connect organizations to service providers. Many organizations rent space and networking equipment in an off-site data center instead of owning one. A data center that caters to multiple organizations is known as a multi-tenant data center or a colocation data center, and is operated by a third party.

Industrial facilities with on-premise data centers need to secure the hardware and software within them. There are two types of security: physical security and software security.

Physical security is the protection of people, property, and assets, such as hardware, software, network, and data, from natural disasters, burglary, theft, terrorism, and other events that could cause damage or loss to an enterprise or institution. Software security involves techniques to prevent unauthorized access to the data stored on the servers. Because new malicious software (malware) is being developed year after year to break the various firewalls protecting the data, security techniques need to be upgraded periodically.

Physical security controls

Physical security of a data center comprises various kinds of built-in safety and security features to protect the premises and thereby the equipment that stores critical data for multi-tenant applications. For the safety and security of the premises, factors ranging from location selection to authenticated access of the personnel into the data center should

be considered, monitored, and audited vigorously. To prevent any physical attacks, the following need to be considered:

- proximity to high-risk areas, such as switch yards and chemical facilities
- availability of network carrier, power, water, and transport systems
- likelihood of natural disasters, such as earthquakes and hurricanes
- an access control system with an anti-tailgating/anti-pass-back facility to permit only one person to enter at a time
- single entry point into the facility.

Organizations should monitor the safety and security of the data center rack room with authenticated access through the following systems:

- closed-circuit television (CCTV) camera surveillance with video retention as per the organization policy
- vigilance by means of 24×7 on-site security guards and manned operations of the network system with a technical team
- periodic hardware maintenance
- checking and monitoring the access control rights regularly and augmenting if necessary
- controlling and monitoring temperature and humidity through proper control of air conditioning and indirect cooling
- uninterruptible power supply (UPS)
- provision of both a fire alarm system and an aspirating smoke detection system (e.g., VESDA) in a data center. A VESDA, or aspiration, system detects and alerts personnel before a fire breaks out and should be considered for sensitive areas.
- water leakage detector panel to monitor for any water leakage in the server room
- rodent repellent system in the data center. It works as an electronic pest control to prevent rats from destroying servers and wires.
- fire protection systems with double interlock. On actuation of both the detector and sprinkler, water is released into the pipe. To protect the data and information technology (IT) equipment, fire suppression shall be with a zoned dry-pipe sprinkler.
- cable network through a raised floor, which avoids overhead cabling, reduces the heat load in the room, and is aesthetically appealing.

Data center infrastructure

Raised floor systems are required to route cables and chilled-air piping and ducting beneath data center racks. The floor load for a data center is shown in figure 1, which is an engineering plan for a typical data center. The plan encompasses the five critical systems that are part of a data center:

The electrical system includes the electrical panels, such as power distribution units (PDUs), UPS, backup diesel generation panels, and lighting panels, that are housed in the electrical room.

The heating, ventilation and air conditioning (HVAC) systems may include roof-top units and air handling units to distribute conditioned air. Split units or variable refrigerant flow might also be used for temperature control. Cooling the raised floor area and between racks is achieved by a computer room air conditioner that sucks in the hot air above the racks and supplies cold air through the grills in the raised floor.

The fire detection and suppression system includes fire alarm detection and fire protection systems, as well as dry protection systems (such as FM 200) for sensitive areas, such as the server areas. Security systems include CCTV, video, and other access control systems, such as biometrics and perimeter monitoring systems. Plant communication systems and other notification systems are used for making emergency announcements, such as for evacuation.

Data center tiers

Data center tiers are an indication of the type of data center infrastructure to be considered for a given application. It is a standardized methodology used to define uptime of a data center. A data center tier, or level, in other words, is used for differentiating key data center requirements, the focus being redundant components, cooling, load distribution paths, and other specifications. It is a measure of data center performance, investment, and return on investment.

Each of these tiers can be defined precisely (figure 2). Tier 1 is the simplest architecture, while Tier 4 is a robust architecture with redundancy at all levels and hence is less prone to failures. Each higher tier is built over the previous tiers with all their features.

Tier 1 is a type of data center that has a single path

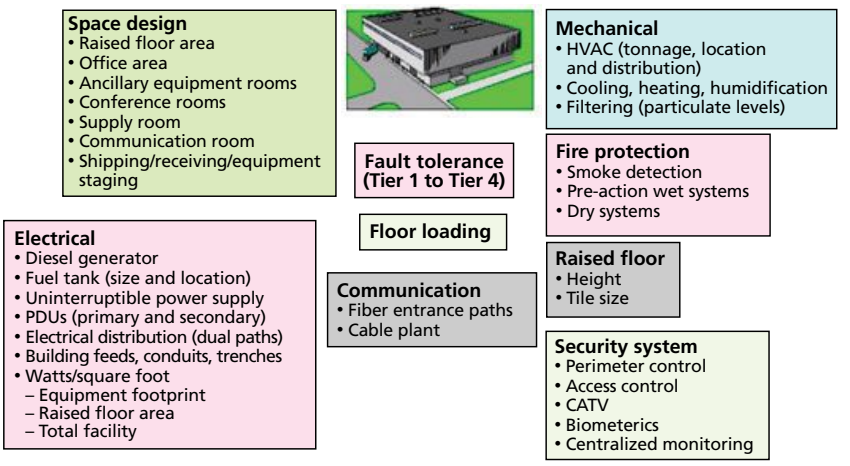


Figure 1. Engineering plan and space design of data center.

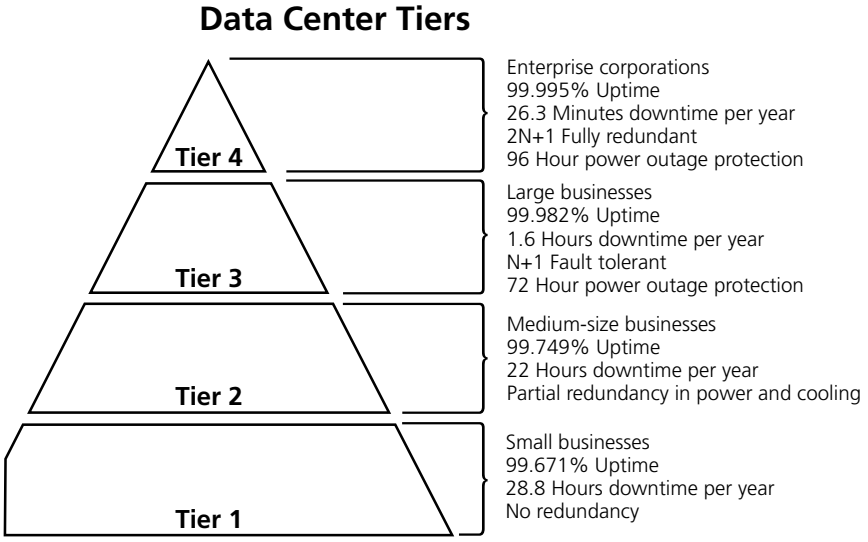


Figure 2. Data center tiers.

for utility sources, such as power and cooling requirements. It also has one source of servers, network links, and other components. Tier 2 is a type of data center that has a single path for utility sources, such as power and cooling, as well as redundant capacity components, such as servers and network links, to support IT load. It is more robust than Tier 1 in terms of the hardware, and gives users a customizable balance between cost management and performance.

Tier 3 is a type of data center that has a redundant path for utility sources, such as power and cooling systems, and an N+1 availability (the amount required plus backup). Redundant capacity components, such as servers and network links, support the IT load so no disruption to service is envisaged during repair. However, unplanned maintenance can still cause problems. A Tier 4 data center is completely fault tolerant and has redundant hot standby for every component and utility source. Unplanned maintenance does not cause disruption in service.

Security in data center

Security of a data center begins with its location. The following factors need to be considered: geological activity like earthquakes, high-risk industries in the area, risk of flooding, and risk of force majeure. Some of these risks could be mitigated by barriers or redundancies in the physical design. However, if something has a harmful effect on the data center, it is advisable to avoid it totally.

The most optimal and strategic way to secure a data center is to manage it in terms of layers (figure 3). Layers provide a structured pattern of physical protection, thus making it easy to analyze a failure. The outer layers are purely physical, whereas the inner layers also help to deter any deliberate or accidental data breaches.

The security measures can be categorized into four layers: perimeter security, facility controls, computer room controls, and cabinet controls. Layering prevents unauthorized entry from outside into the data center. The inner layers also help mitigate insider threats.

First layer of protection: perimeter security. The first layer of data center security is to discourage, detect, and delay any unauthorized entry of personnel at the perimeter. This can be achieved through a high-resolution video surveillance system, motion-activated security lighting, fiber-optic cable, etc. Video content analytics (VCA) can detect individuals and objects and check for any illegal activity. Track movements of people and avoid false alarms.

Second layer of protection: facility controls. In case of any breach in the perimeter monitoring, the second layer of defense restricts access. It is an access control system using card swipes or biometrics. High-resolution video surveillance and analytics can identify the person entering and also prevent tailgating. More complex VCA can read license plates, conduct facial recognition, and detect smoke and fire threats.

Third layer of protection: computer room controls. The third layer of physical security further restricts access through diverse verification methods including: monitoring all restricted areas, deploying entry restrictions such as turnstile, providing VCA, providing biometric access control devices to verify finger and thumb prints, irises, or vascular pattern, and using radio frequency identification. Use of multiple systems helps restrict access by requiring multiple verifications.

Fourth layer of protection: cabinet controls. The first three layers ensure entry of only authorized personnel. However, further security to restrict access includes cabinet locking mechanisms. This layer addresses the fear of an "insider threat," such as a malicious employee. After implementing the first three layers well, cabinets housing the racks inside the computer room also need to be protected to avoid any costly data breach.

There are multiple significant considerations for the critical fourth layer, like providing server cabinets with electronic locking systems. To ensure secured access, the same smart card can be used to access the cabinets. In addition, biometrics may be provided. The above systems can be linked with the networked video cameras to capture the image of the person and his or her activities, and log the data automatically for further analysis and audit. PTZ cameras can be preset to positions based on cabinet door openings.

An integrated IP network of the four layers of security can create an effective, efficient, and comprehensive system for any application. Further integration with the Internet allows for centralized searching, storing, recording, sending, sharing, and retrieving capabilities.

Best practices

A data center audit involves an asset inventory and creates a library of accurate, up-to-date information about all of the equipment in the data center—from servers and cabinets to storage devices. The following are some of the best practices for building up security at a data center facility.

Conduct regular audits. Internal audits check the implemented systems and processes. An external audit is used to check the commitment of internal audits. Audits should check for any vulnerabilities in the data center facilities that are provided to

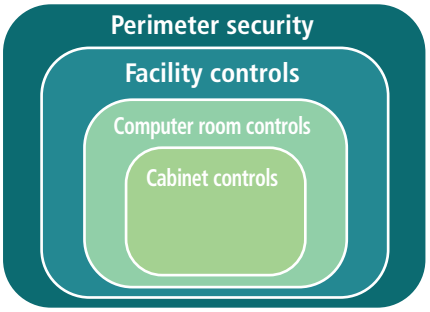


Figure 3. The four layers of data center physical security.

ensure security. Check to see if access control systems, CCTV cameras, and electronic locks are functioning and are being maintained. Check if any job role changes in the employees call for an update in the procedures and systems.

Strengthen access control systems. As an outcome of the audit checks, any facility requiring extra protection should receive additional security. For example, multiple verification methods for personnel entry into a certain area may be recommended, such as an access card and fingerprint or retinal recognition. Make an audit of the entire facility to check if the access control system needs to be tightened.

Enhance video surveillance. Video cameras should include both indoor and outdoor areas of the facility. Similar to the access control systems, coupling these with 24-hour surveillance by security staff can significantly enhance the safety of the facility.

Enforce security measures. This requires employee training on the security measures to be followed and the consequences if procedures are violated.

Establish redundant utilities. Create redundancy in utilities like electricity and water and distribute the same to avoid common-mode failures and to achieve high availability of the systems.

Physical security comprises a four-layer protection that provides a defense-in-depth approach in case control is bypassed. Controls include administrative decisions such as site location, facility design, and employee control/assigning the access level. Physical controls include perimeter monitoring, motion detection, and intrusion alarms. Technical controls include smart cards used for access control, CCTV systems, and intrusion detection systems.

Most organizations focus on software security and firewalls. However, a breach in physical security could cause the theft of data and devices that will make software security useless. It is important to conduct a risk assessment study in compliance with ISO 27001 and implement appropriate security controls to ensure a secure data center. ■

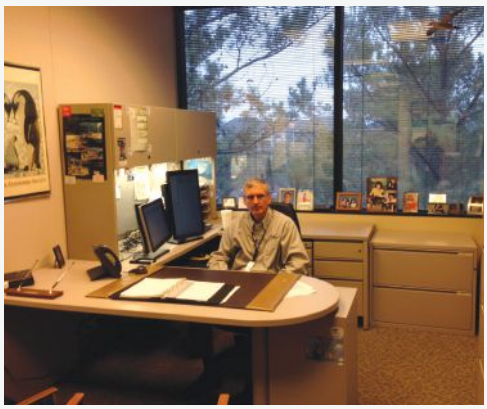
ABOUT THE AUTHOR

C. Shailaja is technology principal and discipline head (instrumentation and controls) for TATA Consulting Engineers Ltd in Chennai, India.

Anniversary Snapshot

Thirty-nine years of professional development

I retired at the end of January 2019 following 42-plus years in the power industry and more than 39 continuous years as a member of ISA and its Power Industry Division (POWID). At that time, I also retired from ISA and other professional society activities to make room for other volunteer leaders. I was blessed to work with a great group of people over the years, and that is what I miss the most. With ISA now celebrating 75 years, it is a good time to share what ISA has meant to me and my career.



Dave at work, circa 2015

I was a student member of a different professional society during college, but it wasn't a good fit for my chosen career in instrumentation and control (I&C). A few years into my career, a coworker suggested that I join the Instrument Society of America (ISA). The monthly *InTech* magazine and the newsletters from the two ISA divisions that I also joined were my first contacts with ISA. Those publications helped me to see that I was a part of a much larger group of professionals who had the same technical interests as myself. In the pre-Internet world, the publications catalog that I periodically received by mail gave me the opportunity to purchase books that also related to my career.

A year or two after joining ISA, a change in employment brought me to Birmingham, Ala., where there was an active local ISA section. It provided regular face-to-face contact with people with the same interests who did not work for the same company; that is where my professional network really began to develop. I also had the opportunity to volunteer for leadership roles, which preceded leadership roles with my employer.

My first volunteer role with ISA was as registration co-chair for the 1985 ISA Southeastern Conference and Exhibit. After that I participated in some of the local education night activities of our local section and eventually found myself as the education chair for the section. In this role I worked with one of our state universities in continuing the production of an annual Fundamentals of Industrial I&C Short Course, which still is given in May each year.

My first two employers did not support me traveling to conferences or doing much in the way of outside training, so ISA was very helpful to furthering my career by providing local technical and leadership educational opportunities. When I moved to Southern Company, my third employer, I learned that if you write technical papers and offer to present them at conferences, it furthers your technical growth and makes your company more likely to let you go to those conferences.

As I progressed at Southern, I was able to represent the company by joining the POWID Executive Committee and the ISA77 standards committee. My most notable roles in POWID were as general chair of the 2003 POWID Symposium in Williamsburg, Va., and then a fairly long assignment as the ISA POWID newsletter editor.

Throughout my career, ISA allowed me to increase my technical knowledge and my leadership skills, expanded my technical and social network, and helped me to grow in other ways and become more widely known in my industry. I highly recommend that all early and mid-career automation professionals get and stay involved in ISA. I wish you all success and happiness in your careers and life in general. ■

Dale Evely, PE and ISA Life Fellow
Southern Company (retired)
ISA POWID Executive Committee (retired)

See more anniversary content at: ISA.org/75in2020

Scenes from the Strategic Leader Meeting

ISA's upcoming 75th Anniversary was on the minds of volunteer leaders who gathered in Austin, Texas, for training and fellowship 6–9 March. "A major theme for the 75th anniversary will be the ever-changing face of the automation profession," said Eric Cosman, ISA Life Fellow and ISA President-Elect and Secretary. The idea of change also dominated the meeting agenda, driven by forces ranging from changing markets and business models to the emergence of disruptive technology. ■

See more ISA photos at: www.flickr.com/photos/isaautomation

ISA5: Documentation is more than symbols

By Ian Verhappen

Many practitioners associate the ISA5 standards development committee strictly with ISA's most widely used standard, ISA-5.1 *Instrumentation Symbols and Identification*. However, the ISA5 committee, "Documentation of Measurement and Control Instruments and Systems," has a broader scope—namely to develop standards, recommended practices, and technical reports for documenting and illustrating measurement and control instruments and systems suitable for all industries. It is also looking for volunteers who want to make a difference.

Change in technology is one of the drivers in updating international standards. Technology has also changed the way standards committees work, with almost all development now done using web conferencing tools. The only requirements to being able to assist are some of your time and a willingness to share knowledge.

The table below presents the working group structure of ISA5. As you can see, several publications, and hence the work of the working groups, have been subsumed by other documents or working groups. However, the work of ISA5 is not all about retirements and consolidation. ISA-5.7 working group chair David Hobart plans to focus on producing a recommended practice for the development and use of piping and instrument diagrams, which often exist under different monikers, such as mechanical flow diagrams, engineering flow diagrams, process and instrument diagrams, and process and control diagrams. Hobart welcomes assistance from others sharing his passion for this document, which will be the template for all subsequent instrument and control work in a project.

Working group	Title	Leadership/ disposition
ISA-5.1	Instrumentation Symbols and Identification	Tom McAvinew
ISA-5.2	Binary Control Logic Diagrams for Process Operations	Merged into ISA 5.1:2009
ISA-5.3	Graphic Symbols for Distributed Control/ Shared Display Instrumentation, Logic, and Computer Systems	Merged into ISA 5.1:2009
ISA-5.4	Instrument Loop Diagrams	Open
ISA-5.5	Graphic Symbols for Process Displays	Merge into next edition of ISA 5.1 as informative content
ISA-5.6	Software Documentation for Control Systems	Open
ISA-5.7	Process and Instrumentation Diagrams	David Hobart
ISA-5.8	Measurement and Control Terminology Review	Merged into ISA5.1
ISA-5.9	Controller Algorithms and Performance	Yamei Chen, Michel Ruel

The ISA-5.9 working group was formed in 2019 in response to a need for improved documentation of the algorithms used in industrial control systems (e.g., PID controllers) and the measures of performance for these algorithms. This working group is also planning documents to aid in the selection and application of the algorithms to benefit manufacturing.

ISA-5.4, *Instrument Loop Diagrams,* was published in 1991 to provide a uniform method of diagramming the physical interconnections of the instruments of pneumatic, fluidic, electric, electronic, and other types of instruments interconnected to form a loop. With the increased adoption of Ethernet, wireless, and potentially virtual/self-configuring systems, this standard is ripe for updating.

Similarly, ISA-5.6, *Documentation for Control Software Applications* (2007), established a system of graphical symbols, charts, matrices, and diagrams to specify and facilitate implementation of software-based control systems for batch and continuous control using programmable controllers, computers, and distributed control systems. The International Electrotechnical Commission (IEC) and other organizations are working on related documents, so this group can help maintain ISA's leadership role in international standards development. To do so, this working group needs leadership and volunteers.

Saving the big one for last: last published in 2009, with a large working group already, ISA-5.1 is due for an update. Chair Tom McAvinew has indicated that he will soon be circulating to ISA5 an addendum to the current standard to suggest slight modifications to refresh the document. Since the committee will have to review and vote on the addendum, it will also kickstart work on a full revision expected to be able to be published within two years. That revision cycle will be a further opportunity to incorporate ISA-5.5 and include new symbols for new sensing technologies, networking, and associated functions.

If you are interested in participating in any of the ISA5 working groups, contact Charley Robinson, ISA Standards, crobinson@isa.org. ■

ABOUT THE AUTHOR

Ian Verhappen is a senior project manager with CIMA. Formerly the vice president of ISA's Standards & Practices Department, he received ISA's Standards Excellence Award in 2018.

Condition monitoring: Old term, incredibly relevant

By Kevin D. Clark, CMRP

It has been around for decades and will continue to be the way we generate the data needed to maintain our assets. But "condition monitoring" as a term does not seem to be cool or sexy anymore. Or perhaps its significance is getting lost as companies seek to do more with less and shift to new systems and processes.

As predictive maintenance grows in practice and paper-based workflows increasingly give way to Industrial Internet of Things (IIoT) platforms and other Industry 4.0 technologies, people want to downplay "condition monitoring" or give it a makeover. Many maintenance pros today would rather call it "asset health" or gloss over it as an incidental step to predictive maintenance. To some, it sounds so…yesterday.

Why do I care about the term? Perhaps because it is such a critical step, representing the basic, fundamental tenet of any maintenance strategy. You start with condition monitoring, first, and then determine asset health—which calls for a deeper analysis of the data you capture.

Condition monitoring provides the baseline data through which maintenance teams can move toward predictive maintenance and forecasting and, ultimately, figure out what asset health looks like. We require this information whether we implement advanced technology or keep inspecting assets with paper, pen, and spreadsheets.

Increasingly, companies are enhancing their systems with IIoT plus machine learning and artificial intelligence. Predictive maintenance is where most organizations want to be. However, without reliable asset condition data, these systems are doomed to expensive failures. To help companies successfully navigate the shift to predictive maintenance, I recommend adhering to these basic steps:

1. **Be clear on what condition monitoring is and what it entails** (even if you do not like the term). Technology is not what drives condition monitoring. It can be done without a single bit of technology, as it was done in time-consuming fashion in the past (or present). Condition monitoring is tracking the condition of an asset through various means, understanding the condition data you compile, and then potentially acting on it—on a conditional basis, not on a scheduled basis. View it as the layer below asset health. Too many people today just want to determine when an asset will fail. Condition monitoring entails tracking the condition of an asset throughout its life, then assessing the data for what it is telling you.

2. **Know what data you need to capture.** Many organizations want to jump right into predictive maintenance from preventive or reactive strategies. They will fail without knowing what type of data to collect from their assets. What kind of assets are you tracking? Vibration monitoring and analysis, for example, makes a lot of sense for rotating machinery. But electrical performance, temperature monitoring, oil analysis, or thermal imaging might as well. To understand when that motor might fail, you might need to monitor current, temperature, and vibration to get the full scope of what you must know.

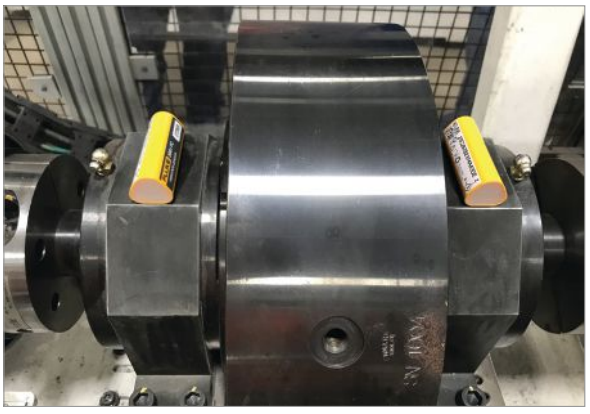
3. **Learn what technology best supports your data collection.** Surprisingly, this may be easier than step 2 if you have thought through what data you need to capture. Fluke Reliability and its competitors have designed sensors and connecting software to go with the computerized maintenance management system or enterprise asset management software you may have in place. These support a wide range of data capture. Also, do you have Wi-Fi? This may affect what types of sensors you can support.

Vendors offer systems to diagnose and analyze data and provide actionable insights. But you cannot go straight to step 3 without doing step 2. Why? Because doing it wrong can set you back. You will go wrong if you are: collecting the wrong data, or insufficient data; not understanding the magnitude of the data (e.g., dwelling on whether or when an asset will fail, rather than its actual condition and health); or spending too little on systems for mission-critical assets or too much on those for non-critical assets.

Now then, maybe your goal—or your executive management's goal or your client's goal—is not predictive maintenance. That is okay for now. My advice is still to put condition monitoring back into your vocabulary and recognize its long-term criticality. It is the linchpin to any successful maintenance strategy. ■

ABOUT THE AUTHOR

Kevin D. Clark, CMRP, is vice president of Fluke Reliability. He joined Fluke in December 2016 and has more than 30 years of experience in operations leadership.



Vibration and power monitoring sensors attached to manufacturing plant machinery, shown in yellow, provide continuous streams of condition data.

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.

The Sep/Oct 2020 issue of *InTech* will include the 75th Anniversary Commemorative Supplement. Show your support for the organization that supports your people, products, and customers. Contact your sales rep for details.

Contact *InTech* today:

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

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

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

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

Reprints

Foster Reprints will work with you to create a customized reprint package, including hard copy reprints, eprints, and mobile-friendly products.

Contact Jill Kaletha at 219-878-6068 or jillk@fosterprinting.com.

datafile

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

USB HART MODEM

The **HM-USB-ISO** USB HART modem meets industry standards for USB and HART connectivity. The small size, 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

ISA

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.

Engineering manager

Tesco Controls: This engineer will be an integral part of the leadership team at a technology and engineering company in Sacramento, Calif., directing a group of 50 engineers, technicians, and support staff to efficiently design and develop control systems for large, complex water projects in North America. The successful candidate will report to the vice president of technical services and interact closely with the sales, project management, and manufacturing teams and other technical managers. Requirements include a strong executive presence, interpersonal skills, and an ability to influence across disciplines. Other requirements are a customer-first mindset; a balance of critical thinking, detailed planning, and the execution of multiple initiatives concurrently; and the technical expertise and project experience to represent clients on complex issues . . . see more at Jobs.isa.org.

Technology and systems integrator

City of Moline, Ill.: Under the supervision of the utilities general manager, the integrator performs specialized, highly skilled technical duties in the operation and maintenance of the digital supervisory control, maintenance, and asset management and communication and reporting systems of the Public Works Department. He or she is responsible for troubleshooting treatment plant and pumping station controls, as well as developing analytical tools and supervisory reports as requested. Duties include running diagnostic programs, troubleshooting computer equipment, communicating with technology vendors, assisting in the development and implementation of alternative workflows, and instructing staff in the use of equipment. An associate's degree in information technology and two years of related experience, preferably in database administration of GIS, is required . . . see more at Jobs.isa.org.

Lead engineer – Driveline and hybrids

Volvo: The driveline and hybrids group in Hagerstown, Md., is responsible for the application and maintenance of the powertrain components from the flywheel to the driven wheels. The engineer provides technical expertise to the organization in the areas of product design, product application, reliability and durability, and problem solving of transmission and axle components. Responsibilities also include creating and maintaining product documentation for the Mack Proprietary Double Reduction axle, as well as providing technical direction to bargaining unit mechanics and test technicians, developing schedules, establishing priorities, and communicating with other departments. A MS in mechanical engineering, seven-to-10 years of experience in the areas of transmission gearbox, axle, and driveshaft systems, and design or validation/development experience of spiral bevel/helical gear is preferred . . . see more at Jobs.isa.org.

Senior cybersecurity engineer

Cummins: This cybersecurity engineer in Columbus, Ind., will conduct software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. The engineer will conduct comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems; conduct vulnerability scans and analyze the findings; identify systemic issues based on the analysis of vulnerability findings, configuration assessments, and derived metrics; troubleshoot hardware/software interfaces and interoperability between integrated systems, and design hardware, operating systems, and software applications to adequately address cybersecurity requirements. The position requires three-to-five years of corporate IT and cybersecurity work experience, knowledge of infrastructure, application, and security best practices, an understanding of industry trends in network architecture, applications, and services . . . see more at Jobs.isa.org.

Senior electrical project engineer

Zeon Chemicals: This supplier of innovative polymers, including synthetic elastomers and specialty chemicals, in Louisville, Ky., seeks a resident electrical and automation expert for the Kentucky plant. The engineer will provide project management to execute multiple simultaneous capital projects from conception to startup, using available resources and best practices to improve the performance and efficiency of the plant. The engineer will coordinate the input of manufacturing and engineering and maintenance to size, specify, select, estimate, design, install, and program process control equipment, electrical power distribution equipment, and other projects according to business needs. The position requires a four-year BS in electrical engineering, proven leadership skills, the ability to develop and manage multiple projects simultaneously, good programming skills, and a good sense for sequential logic . . . see more at Jobs.isa.org.

Old dogs, new dogs, and knowledge integration

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.

Automation and business systems integration is growing at an accelerated pace, leveraging new digital technologies to improve efficiency and competitive position. Most recently this was described in presentations by manufacturers at the annual ARC conference in Orlando, Fla. The many new technologies, including predictive maintenance, analytics, artificial intelligence, smart sensors, and edge devices, are providing the tools to achieve higher quality, productivity, and profits.

An important ingredient to be successful is leveraging experienced people in the company to appropriately apply these technologies using sound automation systems knowledge and know-how. Creating a cultural environment that embraces the integration of multigenerational employees, including the "young guns" and the experienced professionals, combines their unique knowledge and know-how, and leads to superior results.

Not taking advantage of internal knowledge and know-how can be a big mistake. For example, applying technologies, such as artificial intelligence, can have value, but it needs to be done using industrial and process automation professionals' knowledge of operations. The importance of using a team approach was brought into focus in a discussion I had with automation engineers at a major pharmaceutical company where "management" brought in an outside consulting firm of data scientists. They collected process information, analyzed it, and subsequently made automation and control changes that were disastrous and cost a great deal of money. The lesson is, technology is a tool that cannot be used in a vacuum without knowledge and know-how of production processes.

Young automation people just out of college or technical schools have learned the "latest and greatest," but they lack the know-how and activity knowledge gained with years of experience. Know-how and activity knowledge are the practical understanding of how to get something done, as opposed to "know-what" (facts) or "know-why" (science). Know-how is not obvious, explicit knowledge, and it is often difficult to transfer to another person by writing it down or verbalizing it. It is best experienced in the field with an accomplished mentor as a guide.

A few years ago, I interviewed the cofounder of a software company that had a large number of talented new technical people but just could not seem to create effective solutions. He described how this was solved when they paired up "the new dogs with the old dogs," achieving great results. He described the value of this approach, "the new dogs teach the old dogs new tricks, and the old dogs can teach the new dogs old tricks and lessons learned from failed projects; together they created innovative solutions."

The most effective digitalization may require collaboration of a number of traditionally siloed groups including the automation and control group, information technology (IT), quality, manufacturing operations, and others. Effective companies are doing this with each part of the organization respecting the unique knowledge and talents of all to collaborate and achieve superior results. This requires people to have an open mind collaborating with each other.

A worthy goal for an organization is to build a culture of openness and collaboration where people respect each other's talents and are focused on common goals that make manufacturing and production more profitable and competitive. ■

ISA GLOBAL CYBERSECURITY ALLIANCE

THE TIME IS NOW

Industrial Cybersecurity is a Global Imperative

It's time to join forces. We are stronger together.

The ISA Global Cybersecurity Alliance is an open, collaborative body. We welcome members of all kinds:

- end-user companies
- asset owners
- automation and control systems vendors
- cybersecurity technology vendors
- IT infrastructure vendors
- services providers
- system integrators
- industry organizations
- government agencies
- insurance companies
- other stakeholders

Founding Members:

Honeywell
Johnson Controls
Rockwell Automation
Life Is On Schneider Electric
NOZOMI NETWORKS
PAS
CLAROTY Clarity for OT Networks
WALLIX CYBERSECURITY SIMPLIFIED
xage SECURITY
MOCANA
BAYSHORE
radiflow Secure your Assets
senhasegura by MT4
INL Idaho National Laboratory
威努特 WINICSSEC
exida
munio SECURITY
tenable
DRAGOS
TiSafe
ae Solutions
tripwire
DIGITAL IMMUNITY STAY PRODUCTIVE, STAY SECURE
WisePlant Smart, Safe & Secure
MSI Mission Secure, Inc.
1898 & CO.
ACET SOLUTIONS
CYBEROWL
Nova Systems

ALLIED
ELECTRONICS & AUTOMATION

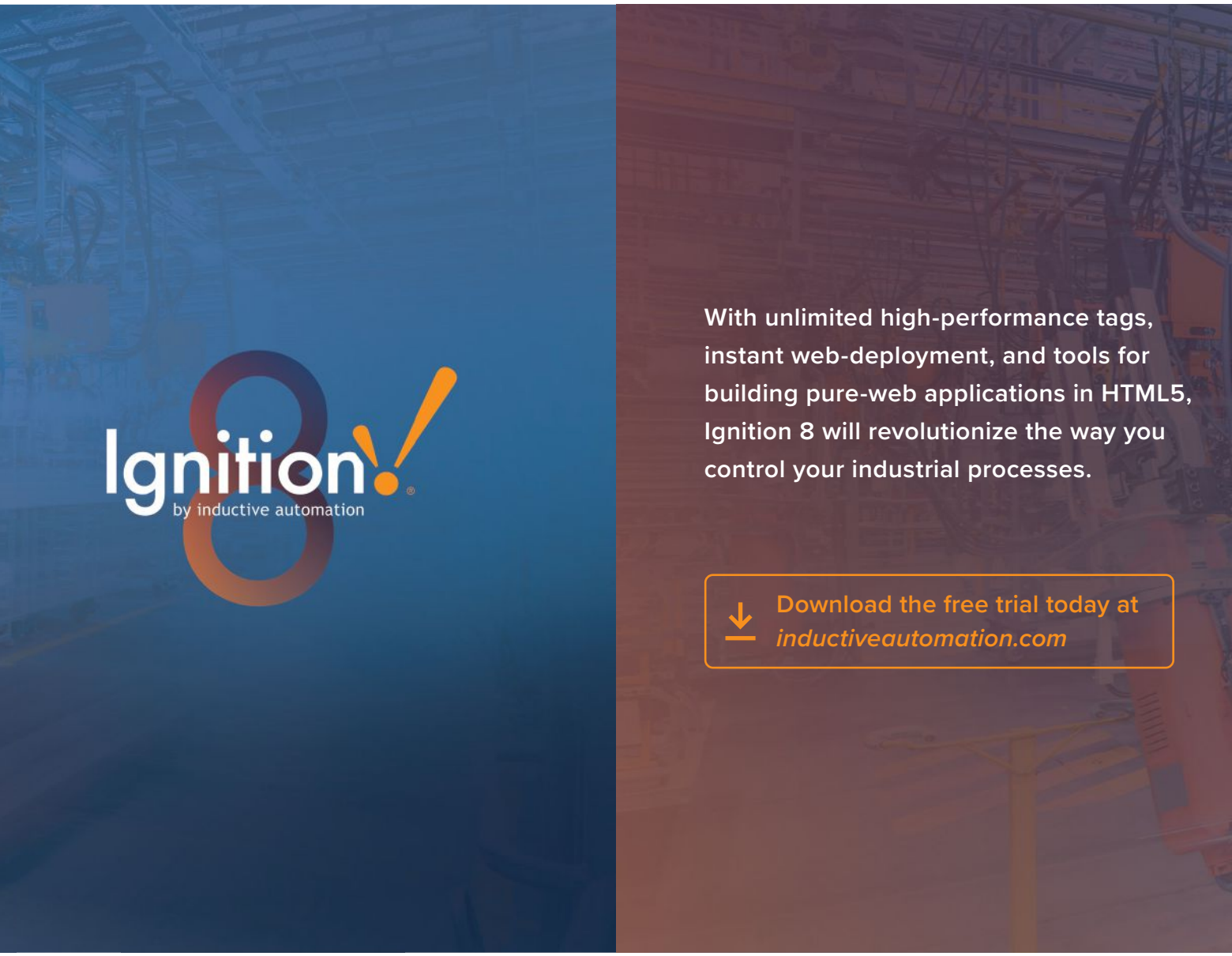
Over 32,000 360° images online now

Front-to-back and side-to-side – get to know your products before clicking "add to cart." Allied's interactive, 360° images give you an extreme close-up of product features and functions for confidence that what you buy is exactly what will arrive at your doorstep.

It's all in the details.

1.800.433.5700

Explore 360° at alliedelec.com/spin360


Ignition!
by inductive automation
8
With unlimited high-performance tags, instant web-deployment, and tools for building pure-web applications in HTML5, Ignition 8 will revolutionize the way you control your industrial processes.
Download the free trial today at
inductiveautomation.com

The #1 Value in Automation

AUTOMATIONDIRECT.com

www.AutomationDirect.com 1-800-633-0405

GET MORE THAN YOU PAY FOR . . .

Over 25,000 quality industrial control products at great everyday prices are available on our webstore 24/7/365, and each one comes with the customer service you deserve.

AutomationDirect: much more than just

AutomationDirect is a non-traditional industrial controls ideas from the consumer world to serve your automatio quality products fast for much less than traditional supp

You need quality products at

Product	AutomationDire Price/Part Number
Proximity sensor, 18 mm, 3-wire PNP DC shielded, with quick disconnect	$15.00 PBK-AP-1H
AC Drive, 5 hp, 460V	$432.00 GS2-45P0
NEMA 12 Enclosure, steel, wallmount (20" x 16" x 8")	$290.00 N12201608

*All prices are U.S. published prices, subject to change without notice. A
Hoffman prices are taken from www.alliedelec.com 4/30/2019. Allen-Bradley prices
Prices may vary by dealer. Many other part numbers ar

For over two decades, we've been offering controls by running our direct business eff on to you. No complex pricing structures o low everyday prices on everything from fu

Programming software for products can be so we help you out by offering **FREE softw** our most popular products, including all o PLC families and C-more Micro HMI. No lice upgrade fees to deal with**!**

www.AutomationDirect.com/price

Our campus is located about 45 minutes north of Atlanta, GA, USA. **We're all here** - our sales and technical support teams, purchasing, accounting, and of course our huge warehouses and speedy logistics team.

You want complete product information to make the right purchase decision.

Whether you're deciding on purchasing our products or learning our products after you buy, why jump through hoops or even pay for the information you need? That doesn't make sense.

We have exhaustive documentation, including overviews, technical specifications, manuals and CAD drawings online, and it's all free to access with no limitations.

We have **over 1,000 videos online** to get you up to speed quickly. When shopping online, if a product you're looking at has video, it will be available right there for you to view.

We even provide FREE online PLC training to anyone interested in learning about industrial controls.

www.AutomationDirect.com/plc-training

You don't want to wait for yo

We have same-day shipping, and it's FR if your order is over $49.*

AutomationDirect has always maintained a hug us to ship over 97% of orders complete the sam 6pm EST; certain items may have earlier order d for details by part).

**Order over $49, and get free 2-day (transit) shipping wi (Certain restrictions apply; Canadian orders may take lo*

You insist on getting better service and you want it FREE.

Our technical support has been voted best in service for 15 years in a row. And it won't cost you a cent!

Many independent industry magazine reader surveys have placed us at the top of their lists for service. In Control Design magazine alone, we were voted tops in service for multiple product categories fifteen years in a row.

www.AutomationDirect.com/support

a ".com"

company using the best
on needs. We deliver
pliers. See below . . .

t great prices.

ct	VS.	Competitor Price/Part Number
		$89.04 A-B 872C-D5NP18-D4
		$1,627.50 A-B 22B-D010N104
		$477.51 Hoffman A-201608LP

utomationDirect prices as of 11/4/2019.
are taken from www.wernerelectric.com 4/29/2019.
e available from vendors.

a better value on industrial
ficiently and passing the savings
r penalty for small orders, just
ses to motors.

e costly,
vare for
ur latest
ense or

ur order.

REE

ge inventory, allowing
he day (if ordered by
leadlines, see Webstore

thin the U.S. and Puerto Rico.
nger based on destination)

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

For almost 25 years, our primary focus has been customer service. That takes many forms: quality products, great prices, fast delivery, and helpful assistance. But regardless of our product selection and other tangibles like pricing, the intangible value of customer service is something that cannot be faked, automated or glossed over.

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

It's common sense.

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

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

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

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

"Should we offer more selection by consistently introducing more new quality products almost continually?
Yes, this is good for our customers."

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

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

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

You want to be confident in our products and our commitment to you.

We stand behind our products and guarantee your satisfaction.

We want you to be pleased with every order. That's why we offer a 30-day money-back guarantee on almost every stock product we sell, including our software. (See Terms and Conditions online for exclusions.)

Check us out at: www.automationdirect.com

AUTOMATIONDIRECT.com

The best values in the world . . .

We've shopped around to bring you the most practical industrial control products that are in-stock, ready to ship and at the right prices!

Reuben in Huntingdon Valley, PA:
"Been shopping here for years and I don't plan on stopping! Great products at a great price. Can't beat the customer service!"

Trent in Coolidge, AZ:
"Always accurate with estimated delivery time, support responsive and helpful, product selection grows every time I visit the site."

Jeff in Sherman, NY:
"Love the products! Productivity PLC lines are awesome, Dura Pulse VFDs are awesome. Great prices on everything."

Murph in Chicago, IL:
"Love this product, I specify materials for breweries and distilleries and all of the panels I design are exclusively AD. Love the fact that we can get replacements sent to anywhere in the US in 2 days. Tech support has been consistently excellent."

Terri in Clinton Township, MI:
"Website is easy to navigate. I can always find what I need. Product has always been in stock and received in a timely manner."

William in Seymour, TN:
"Products are good. Shipping is top notch. However, tech support keeps me coming back. They are patient and look for solutions not just answer questions. Good job!"

Allen in Nashville, TN:
"I have had nothing but excellent service from Automation Direct. The purchases that I have made have worked perfect and arrived quicker than I expected. A+A+A+"

Gregory in Cincinnati, OH:
"I was able to design and built a control system in weeks. Your website and technical information that was available allowed me to do this. In addition, the shipping was flawless. Great job."

A quality product line, with FREE
#1 rated technical support and quick shipping!

Call 1-800-633-0405 or visit us at:
www.AutomationDirect.com