January/February 2020

InTech

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

1945 ISA 2020

Predictive maintenance analytics

Data science for HAZOP studies

IIoT edge computing

Track and trace systems

Industrial cybersecurity product spotlight

Cyber-related process hazard analysis

How Shell conducts cyber PHA assessments based on ISA-TR84.00.09

www.isa.org/intech

Don't Take Safety Lightly...

get reliable signal towers, audible devices and industrial lighting for all of your machines, systems and processes.

PATLITE®

HSST Series - 50mm Manual Control Signal Tower Stations

- Low-cost kit to control signal tower manually
- Three-tier light with red, amber, and green modules
- Includes three-button switch box and power adapter
- Tower meets IP54 standards
- Conforms to RoHS2 CE directive
- Direct-mounted
- Various accessories available

LKEH Series - 100mm Combination Large Light Tower and Horn

- Ultra-bright continuous or flashing LEDs
- Alarm volume up to 105 dB
- 32 alarm tones
- 1 to 4 LED tiers (modules)
- Meets IP53 standards
- Optional field configuration SD card (sold separately)

www.automationdirect.com/stacklights

Industrial LED Lighting

Models available include:

- Indoor / Outdoor models
- Up to 2100lx illuminance
- Many sizes for a variety of applications
- AC / DC versions
- Various construction types to meet environmental and installation needs
- IP69K models available

STARTING AT $76.00 (CWF3S-24-CD)

www.automationdirect.com/industrial-lighting

Audible Signal Horns and Buzzers

Models available include:

- Indoor / Outdoor models
- Up to 110dB Horns and up to 90dB Buzzers
- Selectable alarm tones
- AC / DC versions

STARTING AT $32.00 (BM-212H)

www.automationdirect.com/audible-alarms

Also Available

Patlite pre-assembled stack light units and accessories featuring:

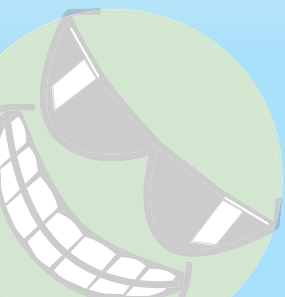
- 25mm, 30mm, 40mm and 70mm units
- IP69K models available (WC9 models)
- All high-intensity LED units with prism-cut lenses designed for enhanced visibility
- Superior impact and heat resistance

STARTING AT $65.00 (LR4-202WJNW-RG)

FREE Technical Support — Located in USA

FREE shipping - orders over $49 — 2-day Shipping

30-day Money-Back Guarantee — 30 day



VOTED Best in SERVICE 15 YEARS

Order Today, Ships Today!

AUTOMATIONDIRECT.com

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

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

January/February 2020 | Vol. 67, Issue 1

www.isa.org

InTech

COVER STORY

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. Vol. 67, Issue 1.**

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

Subscriptions: For 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

Ever Wish Your Temperature Transmitters Could Talk?

RTD and Thermocouple sensor failure can be costly for any process or operation. Wouldn't it be great if your temperature transmitter gave you early warning of impending sensor failure? Moore Industries smart HART dual input temperature transmitters do just that with built-in features like Sensor Drift Detection and Sensor Corrosion Detection that alert you when your sensors are on the path to failure.

Bring predictive failure analysis right to the field with Moore Industries latest smart HART temperature transmitters.

Learn more about the Moore Industries Smart HART Dual Input Temperature Transmitters.
Call **800-999-2900**
or check **www.miinet.com/HART-Temperature**

How has ISA changed your professional life?

By Renee Bassett, *InTech* Chief Editor

The International Society of Automation is a septuagenarian.

This year marks the 75th anniversary of ISA—formerly the Instrument Society of America. For 75 years, this nonprofit organization has set the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems in industry and critical infrastructure.

Even if you've never been a member, ISA has likely been a part of your professional life. So, this is the year to tell your story and listen to the stories of others. Maybe you are one of the 400,000 people around the world who have bought an ISA book, attended an ISA conference, or enhanced your professional standing with an ISA accreditation, certification, or training course. What do you remember about the people you met, or the lessons learned?

Maybe you stood on the shoulders of those who came before by creating systems or solving problems using ISA-95, ISA-88, or other standards as your foundation and guide. How did that affect your career? Maybe the ISA Automation Conference and Exhibition was the first professional event you ever attended? Whether it was in Abu Dhabi or Atlanta, who brought you there, and what did you discover?

Maybe you were around when Mike Marlowe worked to get the ISA-99 standard adopted by the U.S. government as the foundational standard in the cybersecurity of critical infrastructure. Or maybe you're a current member of the newly formed ISA Global Cybersecurity Alliance. What are you hoping to contribute to our industry?

Maybe you're John Berra, president of Emerson Process Management and recipient of an ISA Lifetime Achievement Award, or you have a story about one of the three industrial communications protocols he developed: HART, Foundation Fieldbus, and OPC. What do you think industrial automation will look like in the next 25, 50, or 75 years? More importantly, what skills will automation professionals need?

Throughout the six issues of *InTech* magazine in 2020, but especially in our September/October 75th Anniversary Commemorative Issue, we will celebrate and reminisce and look toward the future. We will ask volunteer leaders to share their insights, and ask the people working to transform industrial automation within or adjacent to ISA to help identify the trends shaping automation. We'll review the technological milestones, starting in 1945 when the then-fledgling Instrument Society of America was founded, shine a spotlight on the technologies of the most-recent 25 years, as the third industrial revolution has given way to Industry 4.0, and speculate on the needs for the next 25.

We want to hear from people working to transform industrial automation within or adjacent to ISA over the past 75 years.

And we'll celebrate 75 years of industrial automation evolution and professional development. Member leaders will celebrate together at the ISA Annual Leadership Conference in San Juan, Puerto Rico, USA this October. In the meantime, consider renewing your membership (visit https://ISA.org/membership) and adding your voice to the celebration of ISA's 75 years of setting the standard for automation. Email your stories to 75in2020@isa.org. ■

ISA celebrates 75 years of support for automation people and technology

The International Society of Automation (www.isa.org) celebrates 75 years of industrial automation evolution and professional development in 2020. The anniversary is an occasion to not just look to the past but to provide a view into the future.

ISA was founded in 1945 as the Instrument Society of America, and much has changed over 75 years, including the association's name. Now the International Society of Automation, ISA still "sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure," says ISA executive director Mary Ramsey.

ISA develops widely used global standards, certifies industry professionals, provides education and training, publishes books and technical articles, hosts conferences and exhibits, and provides networking and career development programs for 40,000 members and 400,000 customers around the world.

Throughout the year, both online and in print through its *InTech* brand publications, ISA will review the technological milestones of the automation evolution, said *InTech* chief editor Renee Bassett. "We will shine a spotlight especially on the technologies of the most recent 25 years, as the third industrial revolution has given way to Industry 4.0," she said.

Automation.com's Bill Lydon will share his insights on technological developments that have enabled manufacturing and process applications to increase quality, productivity, and profits over the years. An example is the ISA-95 (ANSI/ISA-95) Enterprise-Control System Integration standard.

"The latest development of [ISA-95], B2MML [business to manufacturing markup language], creates compatibility with enterprise computing, cloud computing, Internet of Things, and Industry 4.0," says Lydon. "B2MML adds value to ISA-95 by providing consistent terminology and object models and bridging information technology and operational technology systems. B2MML expresses ISA-95 (IEC/ISO 62264) data models in a standard set of XML schemas written using the World Wide Web Consortium's XML Schema language (XSD). It is an open-source XML implementation of the ISA-95 and IEC 62264 standards. There is a joint initiative to bring B2MML into the OPC UA framework, which provides a secure and reliable architecture for manufacturing industries."

The Sep/Oct issue of *InTech* will include the 75th anniversary commemorative supplement. In it, ISA members, customers, and supporters will celebrate, reminisce, and attempt to predict the future, said Bassett. "We will call on the people who have been working to improve and transform industrial automation within or adjacent to ISA over the years. We want to know how the standards and trainings have influenced them and their companies, and what new skills are becoming important as automation evolves." The anniversary celebration will culminate for ISA members at the association's Annual Leadership Conference in October. ■

For digital transformation, learn from peers, says ARC council

Companies in all industries are engaged in transformational initiatives, but true digital wisdom still eludes many. "I'm struck by the mound of evidence of how hard it has been to achieve success," says Mike Guilfoyle, vice president of consulting and research firm ARC Advisory Group. "Despite monumental efforts and resources, data is still hard to access, organize, and use. Companies continue to organize around tech stacks, getting lost in fruitless technology comparisons. Leaders struggle to connect strategy and execution."

Workforce and organizational culture barriers to digital transformation remain in part because "the digital wisdom necessary to transform simply isn't being accumulated," says Guilfoyle. "In my opinion, that reality should neither surprise nor, frankly, scare anyone off." But it should cause you to look to your peers for support.

"I've seen a recent spike in how often I'm asked by executives for benchmarks or competitive comparisons," says Guilfoyle. "Often, these questions tend to focus on use cases, data, or technology around things like asset performance, process efficiency, and cost within a specific industry or process."

ARC's Digital Transformation Council, formed in January 2018, is a peer group that cuts across vertical industries and operational processes. This member-driven community serves industry, energy, and public-sector professionals, and today more than 200 global professionals across nine industries participate.

By expanding their peer network beyond those they know well, members of the Digital Transformation Council are "naturally forced to bring a more open perspective," says Guilfoyle. "This can help them quickly learn 'why' others do things, more than simply 'how' they are done. Instead of simply seeking to imitate, they learn how to problem solve better when it comes to digital transformation. Armed with that wisdom, they are much more willing and able to tackle entrenched issues around data, organizational culture, and the like."

The Digital Transformation Council holds its third Annual Meeting on 3 February 2020 at the Renaissance Orlando Hotel at SeaWorld in Orlando in conjunction with the 24th Annual ARC Industry Forum. For more information, email dtc@arcweb.com. ■

ISA Global Cybersecurity Alliance starts 2020 with expanded membership

The ISA Global Cybersecurity Alliance (ISAGCA) is starting the new year with new projects and new members. ISAGCA is organized into four focus areas: awareness & outreach, compliance & prevention, education & training, and advocacy & adoption. These focus areas are collectively working on the following projects in 2020:

- A condensed guide to implementing the ISA/IEC 62443 series of standards.
- A consolidated matrix that cross references all cybersecurity-related standards to ISA/IEC 62443 principles.
- A road map for expanded cooperation with worldwide governments that are currently referencing the standards in their regulatory requirements or recommended practices.
- A multidimensional reference guide that will map system life-cycle phases and stakeholder roles to specific automation cybersecurity knowledge, skills, and abilities needed to manage each phase.
- Industry vertical overlays to the ISA/IEC 62443 standards for building automation, medical devices, and other sectors.
- A database of expert speakers for speaking opportunities at industry events.

"Unifying and intensifying the work of experts around the world, regardless of affiliation, is a key part of ISAGCA's mission," said ISA executive director Mary Ramsey. "We believe that automation providers, cybersecurity vendors, asset owners, government agencies, research groups, and others involved in cybersecurity efforts are stronger together."

ISA GLOBAL CYBERSECURITY ALLIANCE

"Unifying and intensifying the work of experts around the world, regardless of affiliation, is a key part of ISAGCA's mission."

The ISA Global Cybersecurity Alliance has more than tripled the number of its founding members with the addition of 22 new companies and organizations (see box). At the end of July, ISAGCA announced Schneider Electric, Rockwell Automation, Honeywell, Johnson Controls, Claroty, and Nozomi Networks as its initial founding members.

End users, asset owners, government agencies, and other cybersecurity-focused organizations are also encouraged to join ISAGCA. Notable members include Chevron, ExxonMobil, Honeywell, Schneider Electric, Yokogawa, exida, Control System Security Center, YPF, Japan Information Technology Promotion Agency, Royal Dutch Shell plc, TÜV Rheinland, DNV GL, and TÜV SÜD. Current members of LOGIIC include BP, Chevron, ExxonMobil, Shell, Total, ConocoPhillips, and other large oil and gas companies. To learn more, visit www.isa.org/isagca. ■

Attendees to discuss Industrial IoT and smart manufacturing

Industrial Internet of Things (IIoT) has emerged as a major technology with a big impact on industrial automation systems—and on the automation professionals involved with the design and maintenance of such systems. Make plans to be in Texas in April for the 2020 ISA IIoT & Smart Manufacturing Conference and learn how automation is the foundation of IIoT and why it is useful to understand the difference between edge, fog, platform, and hybrid architectures. Held 15–16 April at the Moody Gardens Hotel in Galveston, Texas, with a day of focused training on 14 April, this conference's topics encompass advances in connectivity, automation, and security within the context of hybrid manufacturing operations across multiple vertical industries.

For more information and to register, visit https://isaautomation.isa.org/2020-iiot-smart-manufacturing-conference. ■

Add your Voice to the Celebration

75 years of setting the standard for automation

The Sep/Oct 2020 issue of *InTech* will include the 75th Anniversary Commemorative Supplement.

In addition to technology timelines, Automation Innovator Profiles, and predictions for the future, the supplement provides ways for supporters to buy ads, share stories of ISA history, or position their companies as part of the Industrial Automation Innovators Showcase.

Show your support for the organization that supports your people, products, and customers. Email stories, congratulations, and questions to 75in2020@isa.org.

ISAGCA additions as of the end of 2019

- aeSolutions
- Bayshore Networks
- Beijing Winicssec Technologies Co. Ltd.
- Digital Immunity
- Dragos
- exida
- ISA Security Compliance Institute
- ISA99 Committee
- Idaho National Laboratory
- LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity)
- Mission Secure, Inc.
- Mocana Corporation
- Munio Security
- PAS Global
- Radiflow
- Senhasegura (supporting member)
- Tenable
- TiSafe
- Tripwire
- WisePlant
- Wallix Group
- Xage Security

Security at the edge with microsegmentation

by Courtney Schneider

ABOUT THE AUTHOR

Courtney Schneider is cyber-policy research manager for Waterfall Security Solutions, (https://waterfall-security.com), a global industrial cybersecurity company, protecting critical industrial networks since 2007. This article first appeared as a blog post of the Industrial Internet Consortium.

Industrial and Industrial Internet of Things (IIoT) networks almost always represent engineering risks, as well as conventional "business" risks. IIoT is the ultimate mind meld of information technology (IT) and operational technology (OT) networks. The IIoT connects edge devices in OT networks directly to the Internet to enhance operational efficiencies. What confuses security designs for IIoT deployments is differing *kinds* of risk.

OT practitioners and engineers plot risk on a spectrum from unacceptable physical consequences to safe, correct, continuous, and efficient physical operations. Conventional security practitioners, however, focus on protecting information, cyberresilience, incident response, data recovery, and business continuity. Conventional cyberassets are part of a sea of networks, some needing more protection than others, managed for *business* risk.

What then of IIoT security, which basically melds these two concepts of physical and business risk together: the ubiquity of IT networks layered on physical control and industrial networks? How do we implement a security program to simultaneously satisfy these very different needs from IT, OT, and engineering teams?

Physical and business risk

IIoT security planning starts with a cyberrisk assessment. Not all IIoT deployments pose nefarious threats to the physical world. When deploying hardware that is only physically able to monitor but not control anything, we generally face only conventional business risks. Conventional enterprise security principles apply, and direct connectivity to enterprise and even cellular and Internet networks is appropriate.

For example, consider a system of thousands of solar-powered rainwater measurement devices distributed throughout a watershed as part of a water treatment flow prediction system. If the switches are compromised, or for that matter physically kicked under a rock by passing tourists, there are no grave consequences to the water system. The system is massively redundant, and device inputs are constantly correlated with external inputs, such as official meteorological reports of rainfall in an area.

But suppose the rainfall-monitoring devices can also control switches that are connected to, say, an irrigation system to activate or deactivate irrigation in an area based on the rainfall it receives. Now there are potential physical consequences of compromise. Worst-case physical consequences might include flooding, washouts, and physical damage to irrigation canals.

If monitor-only IIoT edge devices are connected to conventional control networks, we have a different problem. For example, what if the monitor-only rainfall sensors that are deployed inside the boundaries of a large water-treatment facility were connected

Unidirectional gateways provide protection to edge devices when endpoint protections in those devices are not sufficient.

to the facility's OT network? These connections exist because that water-treatment OT network is the easiest one for the IIoT sensors to access. In such an example, compromised monitor-only sensors give attackers an opportunity to pivot their attacks into the facility's control-critical network.

Microsegmentation

When unacceptable physical consequences of compromise are possible for IIoT deployments, we need strong protections for the edge devices. In these scenarios, a good place to start is microsegment control-critical sets of equipment or networks using unidirectional gateway technology.

Unidirectional gateways are described in section 9.2.6 of the Industrial Internet Consortium Industrial Internet Security Framework (https://www.iiconsortium.org/IISF.htm). These gateways are the strongest of the network segmentation options described in the framework. Unidirectional gateways provide additional protections to edge devices when endpoint protections in those devices are not sufficient. They enable safe flows of monitoring information to enterprise and cloud systems for big data analysis and other benefits, while physically preventing any information flow back into the edge devices.

Where to deploy the gateways is the question—in complex OT networks, unidirectional gateways may be deployed close to the edge devices, close to the connection to enterprise or Internet networks, or anywhere in between. What has emerged as a best practice is perhaps obvious in hindsight—enterprise security teams need to sit down with engineering teams and work out a strategy. Both teams need to agree on where to deploy at least one layer of unidirectional protections. ■

Blockchain, AR changing food and beverage operations

By Darcy Simonis

Many factors affect the way food and beverage manufacturers handle their processes. Whether it is the need for more efficient processing, the growing population, or evolving consumer preferences and attitudes, food and beverage manufacturers must constantly look for ways to stay ahead. New technologies that are part of Industry 4.0 can help, allowing automation professionals to have a positive impact throughout the supply chain. Three innovations that are changing the way food and beverage makers operate are augmented reality (AR), three-dimensional (3D) printing, and blockchain technology.

Food through AR

For many consumers, AR is a normal part of everyday life. Since the boom of Snapchat filters and lenses, AR has become extremely popular and is now more commercially accessible than ever. With the AR market in Europe alone estimated to hit $12 billion by 2024, industries are finding many ways to integrate this cutting-edge technology into daily practice—and the food and beverage industry is no different.

Staff working in a food and beverage facility can be trained through virtual instructions and scenarios in which it is possible to virtually visualize working and operating in the facility. This method could enable a more productive workforce to be trained at a quicker rate compared to traditional and manual training.

AR can also enhance the consumer experience. Some manufacturers have designed products with labels displaying nutritional or recipe information with AR. However, some suppliers are taking this one step further. An online New York bakery, for instance, uses AR to display a 3D view of its products for customers to view before they place an order. Using AR in ways like this could increase sales, as it means the customers can see the food or finished product before they commit to a purchase.

3D printing food

Another technology that is being increasingly used in the food and beverage industry is 3D printing. Currently, 3D printing technology is being applied to industries such as automotive, aerospace, and packaging, and it is predicted that the global revenue for the 3D printing market will reach $21 billion this year. But it is also making its way into the food and beverage sector.

One German company is using 3D printing technology to create printed jelly meals for elderly care-home residents who have difficulty chewing or swallowing solid foods. As the potential uses of 3D printing are developed, the benefits of this technology are becoming more understood. Food that is 3D printed can produce precise results and save time and effort.

While 3D printing has the potential to provide innovative food to the growing population much faster than traditional methods of manufacturing, it also provides options for the industry to be more environmentally sustainable. 3D printing only uses the required amount of raw materials to make a finished product, and the hydrocolloid cartridges that are used in 3D printers form a gel when mixed with water and leave minimal waste.

Blockchain technology

Consumer attitudes to food have also changed. Whether it is ensuring that produce is grown sustainably or that plastic waste is kept to a minimum, consumers now want to know every detail about the product they are buying—and blockchain technology can provide just that.

Through blockchain, consumers can verify the history, origin, and quality of a product. Blockchain is benefitting the industry as it builds trust between the supplier, manufacturer, and consumer, which in turn can increase brand loyalty. It can also reduce food waste by identifying problems along the way, such as contamination or storage issues. If problems are detected at an early stage of the production process, they can be resolved before the product hits the shelves. This could help reduce food waste and eliminate the need for product recalls.

Although blockchain technology is a new approach, most food manufacturers should already have software installed that monitors, records, and traces product ingredient details. Software like the 800xA distributed control system or the ABB Ability manufacturing operations management system can trace and record an ingredient and log the data in a database for manufacturers to refer to. The Absolut Company, for example, uses System 800xAat its Nöbbelöv distillery in the south of Sweden to help operators see and correct key process deviations in the sensitive fermentation process. ■

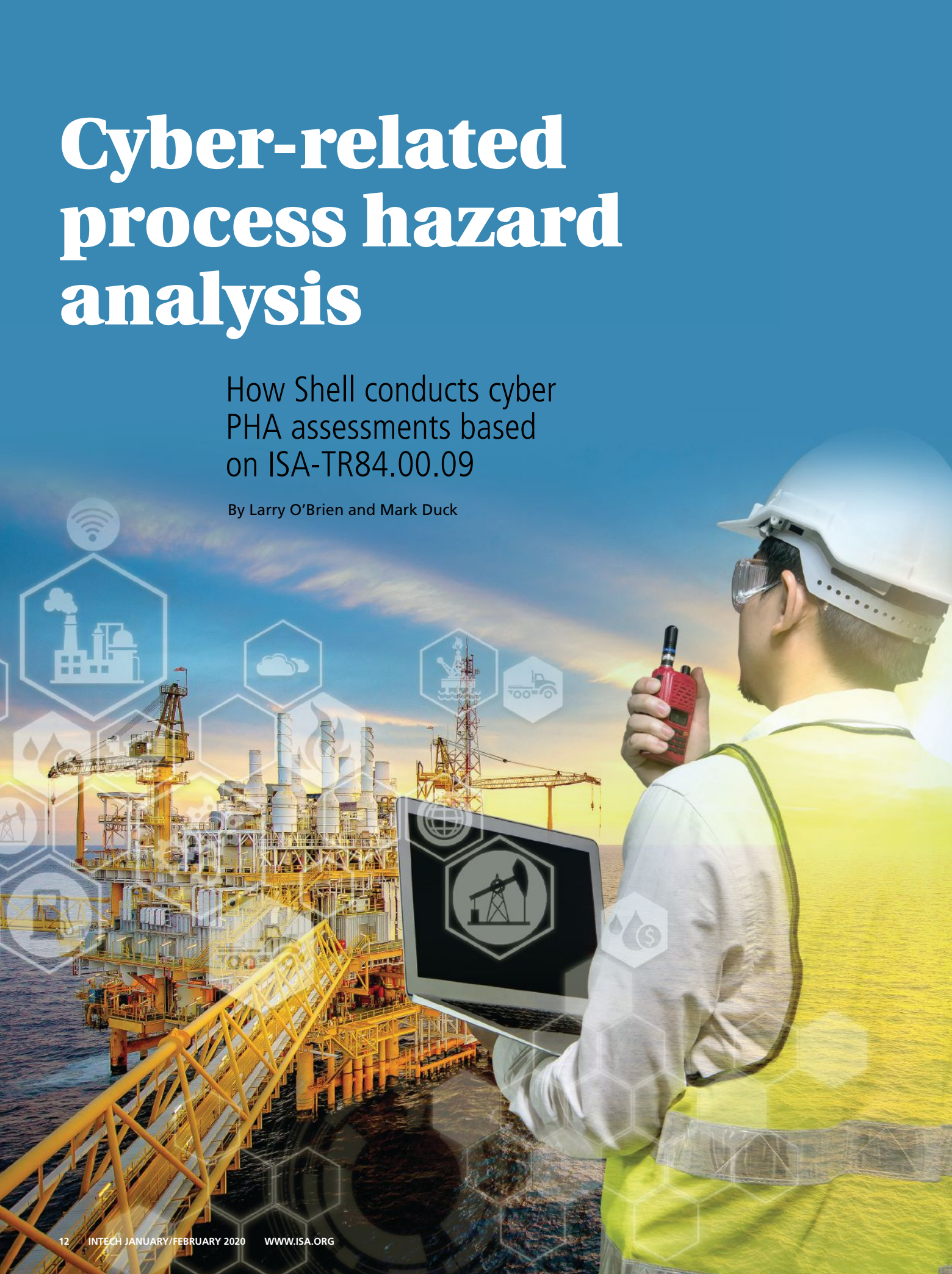
ABOUT THE AUTHOR

Darcy Simonis is industry network leader for ABB's Food and Beverage division. Find out more at https://new.abb.com/food-beverage.

Cyber-related process hazard analysis

How Shell conducts cyber PHA assessments based on ISA-TR84.00.09

By Larry O'Brien and Mark Duck



The introduction of process safety system–specific malware into the manufacturing world in 2017 intensified the discussion around the convergence of safety and cybersecurity. If a cyberattack could compromise safety in the physical world, we must view cybersecurity in the context of safety. Similarly, approaches taken in the safety world to evaluate risk and to design safer systems must consider cybersecurity-related threats to the integrity of safety systems.

Key end user companies from the oil and gas, marine transportation, and offshore exploration and production industries discussed these and related issues in a session at the 2019 ARC Industry Forum in Orlando. In that session, Mark Duck, who is with the Shell Projects & Technology organization, talked about an approach Shell is exploring to integrate cybersecurity risk assessment into traditional process hazard analysis (PHA) methods.

For example, hazard and operability (HAZOP) studies could be used to determine the impact of cybersecurity threats and vulnerabilities on the safety of plant operations. Similarly, methods like HAZOP should be adapted to consider the cybersecurity risk to the integrity of the selected safety barriers for each specific hazard risk scenario.

These approaches are not limited to the oil and gas industry. They could be applied to an even wider range of industries, including those that are not the primary users of process safety systems.

The industry needs: (1) a clear way to think about how cybersecurity risk, if realized, could degrade the integrity of safety barriers, and (2) a standard methodology to assess this risk. In the first case, using a bow-tie model and the concept of escalation factors can help frame where cybersecurity threats and vulnerabilities can affect safety barriers. In the second case, the industry has already taken steps to address how cybersecurity risk assessment can be integrated into the functional safety life cycle.

FAST FORWARD

- A bow-tie model and the concept of escalation factors help explain how cybersecurity vulnerabilities can affect safety barriers in the oil and gas industry.
- To integrate cybersecurity risk assessment into the functional safety life cycle, ISA and IEC cybersecurity standards have embraced the concept of cybersecurity process hazard analysis (PHA).
- Shell learned several lessons when undergoing its own cyber PHA (based on ISA-TR84.00.09) assessments.

Cyberrisk viewed as a safety concern

The International Electrotechnical Commission (IEC) 61511 Functional Safety standard now requires a safety instrumented system (SIS) security risk assessment. ISA has published a technical report (ISA-TR84.00.09-2017) that documents a SIS cybersecurity risk assessment procedure, called cybersecurity PHA or cyber PHA. The link to PHA is a step in the cybersecurity risk assessment process to: (1) review the output of the PHA to identify worst-case health, safety, security, and environment (HSSE) consequences for the asset, and (2) identify any hazard scenarios where the initiating event and all control barriers are "hackable."

Consequences						Increasing likelihood				
Severity rating	HSSE				Non-HSSE	A	B	C	D	E
	People	Assets	Environmental	Reputation	Consequencial business loss	Rare	Unlikely	Possible	Likely	Almost certain
0	Zero injury	No damage	No effect	No effect	No loss					
1	Slight injury	Slight damage	Slight effect	Slight effect	Slight loss					
2	Minor injury	Minor damage	Minor effect	Minor effect	Minor loss					
3	Major injury	Moderate damage	Moderate effect	Moderate effect	Moderate loss					
4	Single fatality	Major damage	Major effect	Major effect	Major loss					
5	Multiple fatalities	Massive damage	Massive effect	Massive effect	Massive loss					

Figure 1. Example risk assessment matrix.
Source: Shell

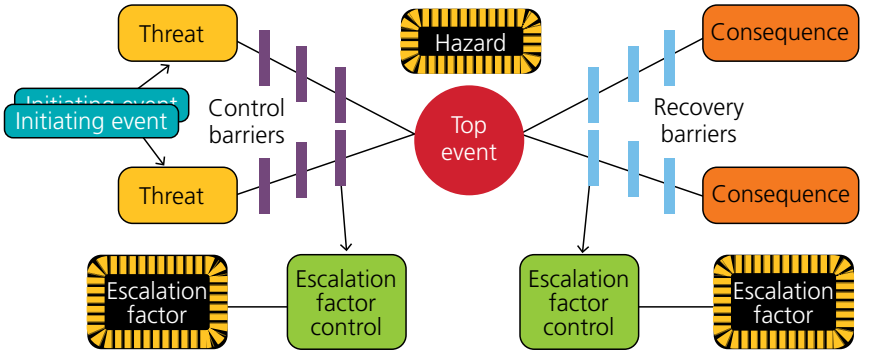


Figure 2. Example bow-tie model. Source: Shell

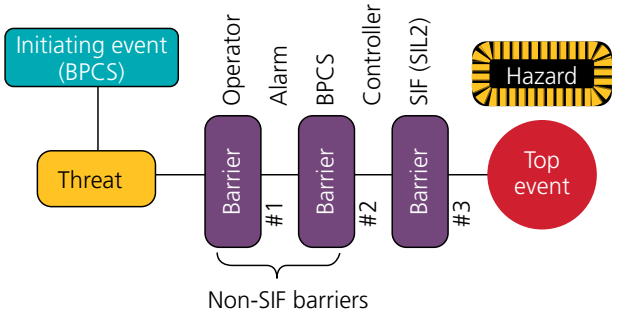


Figure 3. Partial bow-tie showing threat and barriers including SIF with SIL and top event.

NAMUR has also published a worksheet (NA 163) titled "Security Risk Assessment of SIS." A cyber PHA methodology can be used to assess the risk associated with identified cybersecurity-related escalation factors and recommend mitigations to reduce the risk to an acceptable level. Linking concepts and tools used in the process hazard analysis world with cybersecurity risk assessment can help bring these two, traditionally separate, risk management processes together with a goal of improving the robustness of our safety systems against cybersecurity attacks.

Most cybersecurity risk scenarios only deliver a consequential business-loss consequence along with a potential impact on company reputation. PHAs, on the other hand, typically do not consider consequential business loss. But a cybersecurity risk assessment must include this consequence category, as shown in the example risk assessment matrix (figure 1).

This consequence category can be calibrated in terms of duration of production loss. The worst-case severity is calibrated by determining the maximum number of hours, days, weeks, etc., it would take to bring production back online in case of, for example, a ransomware attack that affects all servers and workstations in the industrial automation and control system (IACS).

The cost is the value of lost and deferred production plus the materials and labor required to respond to the incident. The list of systems required to bring production back online will likely be a subset of all systems in the IACS. From a cybersecurity risk scenario point of view, this list would be the critical systems, including all safety systems.

Shell's process safety pedigree

Shell is well known for its emphasis on safety. The company takes a comprehensive and multifaceted approach to managing process safety risk including managing the HSSE risk associated with the asset process (a particular aspect of the chemical manufacturing process for example), integrity of safety barriers, risk to production loss, and other factors.

Shell uses many methods to evaluate risk in process safety that are consistent with those outlined in the IEC/ISA 61511 process safety standards. These include the use of risk assessment matrices that consider likelihood; consequence of risks to people, assets, community, and environment; and severity of the consequence. The company also uses bow-tie models (figure 2) to visualize the various elements of risk scenarios, such as hazards, top events, and barriers, including escalation factors and escalation factor controls.

A "hazard" is an agent with potential to cause harm. A "top event" is an uncontrolled release of a hazard, such as hydrocarbons, toxic substances, energy, or objects at height. An "escalation factor" is any situation, condition, or circumstance that may lead to the partial or full failure of a barrier (e.g., independent protection layer).

An example of this is making unauthorized trip setting changes to a safety instrumented function. This escalation factor could be controlled by improving the logical and/or physical access controls for the safety instrumented system. Identification of escalation factors is part of the process of managing the integrity of independent protection layers. These tools, among others, can be used to start the journey of integrating the process safety and cybersecurity risk assessment processes.

The challenge

Today's challenge is to create an interface between process safety risk assessment methods and cybersecurity risk assessment methods. Historically, the HSSE risk assessment process has not considered sabotage (cybersecurity attacks are a form of sabotage). Given the level of sophistication seen in recent cybersecurity attacks on industrial control systems, the potential for simultaneous cybersecurity attacks on one or more independent layers of protection must be considered during the HSSE risk assessment process.

Safety instrumented systems and other control and recovery barriers have cybersecurity vulnerabilities that must be mitigated. These vulnerabilities represent "escalation factors" in the bow-tie model that must be mitigated with appropriate "escalation factor controls."

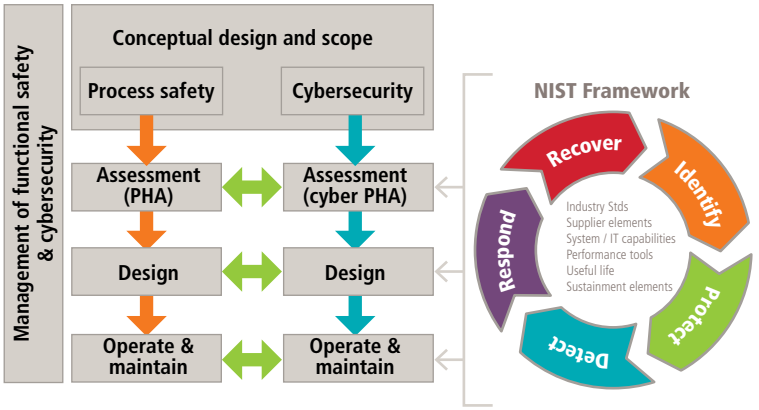


Figure 4. Cybersecurity integrated with process safety.

One possible interface between the cybersecurity risk assessment and the HSSE risk assessment process is to focus on cybersecurity escalation factors associated with barriers that have cybersecurity vulnerabilities. One advantage to this approach is that it is already part of the existing HSSE risk assessment process.

Historically, HSSE risk assessments have not considered sabotage, but safety instrumented systems and other control systems have cybersecurity vulnerabilities—a type of sabotage risk that must be mitigated.

It is common for one or more of the selected control or recovery barriers to be vulnerable to cybersecurity threats. Some examples are safety instrumented systems, PLC-controlled fire water pumps, and fire and gas systems—essentially any barrier based upon microprocessors running firmware/software and, potentially, connected to a network.

A cybersecurity escalation factor for these types of controls is the combination of cybersecurity threats and vulnerabilities associated with the equipment used to implement the control. In this context, cybersecurity escalation factors are just one type of escalation factor among many other types of escalation factors that can degrade the integrity of a safety barrier.

During a PHA, there is the possibility that the initiating event and all the control barriers selected for a hazard scenario have cybersecurity escalation factors. Where this is a high-consequence scenario (e.g., potential fatality), an effort should be made to add at least one control barrier that does not have cybersecurity escalation factors, such as a pressure relief valve or non-programmable safety instrumented function (SIF). If this is not possible, the cybersecurity risk assessment team should consider that a cybersecurity attack on these specific control barriers has a higher likelihood of leading to the top event, and they should identify a robust set of cybersecurity countermeasures to manage this risk.

Maintenance and cybersecurity

Industrial assets typically have a maintenance program to maintain the various components of the asset and must often prioritize work based upon some criteria. A common way to do this is to organize the assets in terms of system criticality. If a backlog of maintenance activities exists, then ensure the components with the highest criticality are taken care of first.

A common issue with cybersecurity controls in an industrial control system (ICS) environment is the related maintenance required to sustain them over time. Often, the maintenance associated with cybersecurity controls is a lower priority than instruments, valves, etc., because of the lower perceived value. One way to resolve this issue is to assign the cybersecurity controls used to manage cybersecurity escalation factors a criticality rating based on the barrier being protected, and then factor this into the overall maintenance strategy.

The need for doing cybersecurity risk assessments for process safety is called out in IEC 61511 Part 1 (2016). This requires that "a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS." The requirement further specifies additional details supporting the risk assessment.

Although this is a needed step, there are potentially many other safety systems, in addition to SISs, that are subject to cybersecurity vulnerabilities. The following are examples of other programmable safety systems subject to cybersecurity vulnerabilities:

- fire water pumps
- tanker loading systems
- ballast management systems (example: offshore semi-submersibles)
- mooring systems (example: offshore semi-submersibles)
- helicopter refuels
- hazardous area ventilation
- deluge systems
- sprinkler systems
- navigation aids
- collision avoidance systems
- communication systems

The trend to integrate these programmable safety systems with basic process control systems will likely continue and must be considered in the context of the IEC 61511 safety life cycle, which includes ensuring cybersecurity risks are adequately addressed. Considering these challenges, companies must make sure that cybersecurity risks to the availability of all barriers are understood, mitigated, and even "designed out," where possible, during the PHA process.

Emergence of cyber PHA

This raises the question of how we develop a cybersecurity risk assessment that meets the requirements of the world of process safety. The concept of cybersecurity process hazard analysis

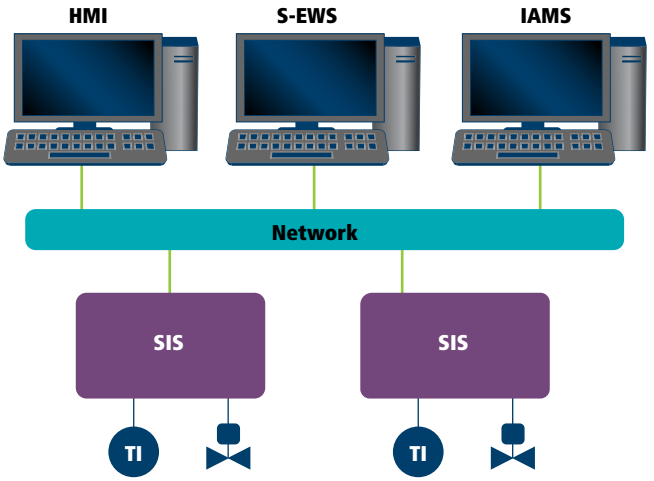


Figure 5. Safety instrumented systems interface to HMI, engineering workstations, and instrument asset management systems.

(PHA) has emerged in the industry over the past several years and is finding increasing acceptance among end users. ISA and IEC cybersecurity standards have embraced this method. A methodology (and supporting information) for integrating process safety and cybersecurity risk assessment is documented in the following:

- ISA/IEC d62443-3-2 (draft) – *Security Risk Assessment and System Design*
- ISA-TR84.00.09-2017 – *Cybersecurity Related to the Functional Safety Lifecycle*
- NAMUR Worksheet NA 163 – *Security Risk Assessment of SIS*

Several service providers have emerged over the past few years that have developed their own methodologies for doing cyber PHA that are consistent with the recommendations outlined in the standards. These companies range from smaller software and engineering service providers to large, integrated process automation suppliers.

Shell's lessons learned

Shell concluded its ARC Industry Forum presentation by sharing several lessons learned from undergoing its own cyber PHA (based on ISA-TR84.00.09) assessments. Although some are not strictly cybersecurity related, they nevertheless emerged in a cybersecurity risk assessment. Awareness of these issues would benefit the ICS cybersecurity community.

For example, not all safety instrumented systems have a hardware key switch to manage the various modes of operation, such as "run, program, remote" modes. In cases where a hardware-based key switch is not provided, consider using a "software" lock to enforce separation of duties for the SIS. For example, the supervisor in the plant should unlock the SIS to allow the engineer to make configuration changes. Another example is making sure that critical SIS parameters such as "trip limit" cannot be changed online. A download, using separation of duties, should be required to change trip limits and other critical parameters.

End users should also pay attention to how the safety system engineering workstation user roles and associated privileges are set up. Companies should ensure that the "principle of least privilege" is enforced. In other words, minimize the number of people with privileged accounts and set up roles to support separation of duties.

Companies should also rigorously manage bypasses, and operators should have a real-time view of all active bypasses. A best practice is to use separation of duties to enable bypasses along with an administrative process that creates a record of the bypass. Rigorous management (or elimination) of remote access to safety system engineering workstations and instrument asset management systems (IAMS) should also be employed. Periodic audits of who has remote access should be implemented. Remote access by privileged users should be normally disabled, done under "permit to work," and monitored locally.

Unauthorized changes to SIS instrument settings, such as sensor type, scale, or range, can render a SIF inoperable. This can potentially be done from the IAMS or through handheld devices used to interface with intelligent instrumentation. End users should ensure some form of "instrument lock" is in place, such as a hardware jumper or software lock. This will let them use separation of duty to make changes to instruments. Some end users have employed data diodes for this purpose as well.

The trend to integrate programmable safety systems with basic process control systems will likely continue and must be considered in the context of the IEC 61511 safety life cycle.

Run periodic audit reports to detect unauthorized downloads to SIS or changes to instruments. Changes should match corresponding administrative controls such as "permit to work (PtW)" or "management of change (MOC)" records. If user accounts for the safety engineering workstation (S-EWS), human-machine interface (HMI), and IAMS are integrated with Microsoft Active Directory, risk assess the implementation to make sure these credentials are properly protected.

Good password policy should also be followed. Ensure that privileged account passwords are not leaked or shared. Use administrative policies that state this. If passwords are "stored," do so in a secure manner. Do not pass around files with passwords.

Overall, companies should identify and address cybersecurity risks to safety barriers during design. Using concepts such as cybersecurity escalation factors and ensuring high-consequence hazard scenarios are mitigated using barriers without cybersecurity vulnerabilities can help achieve this goal. A cyber PHA should be included as part of any new project and as part of the contract when designing an automation system. Companies should perform a cyber PHA for existing assets when a change occurs that affects the safety system or when the cybersecurity threat landscape has changed.

There is still much to learn about the intersection of cybersecurity and safety. This requires collaboration between both communities for the continued protection of assets, people, and communities in today's challenging cybersecurity environment. ■

ABOUT THE AUTHORS

Larry O'Brien, vice president, research, ARC Advisory Group, is part of the cybersecurity and smart cities and infrastructure teams at ARC, with a 20-year background in process control, process safety, and field devices/field networks. O'Brien is part of the cybersecurity and smart cities and infrastructure teams at ARC and has supported many end-user clients in the oil and gas and refining industries.

Mark Duck, principal technical expert, ICS Security, Shell Global Solutions, is a Certified Information Systems Security Professional and Global Industrial Cyber Security Professional with more than 30 years of experience in the aerospace, manufacturing, and oil and gas industries. He has 11 years of experience with Shell working on capital projects related to industrial cybersecurity controls for automation systems. He has also been a key contributor to the development of Shell's global industrial cybersecurity standards.

View the online version at www.isa.org/intech/20200201.

Analytics for predictive, preventative maintenance

After years of stagnation come sweeping changes in technologies, users, expectations

By Michael Risse

A new year and decade provide an occasion for predictions regarding the state of analytics in the process industries. After three decades of data generated by digitizing control systems, stored in historians, and imported from ad hoc analytics in spreadsheets, the static and past tense model for analytics is getting long in the tooth. The need for new and improved offerings to actually achieve insights will only become more acute because industry data volumes are accelerating. In fact, industry analyst IDC recently predicted that the average process manufacturing plant will generate and store much more data in 2025 as compared to today (figure 1).

The big data era is far from over; indeed, we are only at the end of the beginning for process industry data volumes, velocity, and variety. This means there will be an even bigger disconnect between the opportunity and reality of advanced analytics in the process industries.

To address the increasing data volumes and close the gap from sensors and data to insights and actions, three key improvements will emerge over the next decade of analytics as the past three decades of the historian/spreadsheet era is left behind. These improvements will be enabled by continuing advances in software and computing technology, the driving force of innovation for the past 30 years. Computing is ever more pervasive, inexpensive, and accessible. The question is, if it was free, what would an organization do with it?

From past to predictive maintenance

The first improvement is a sweeping transition from historical to predictive analytics. Most of the common analytics terms used today reflect a bias toward the past tense. Reports: what happened? Overall equipment effectiveness: what was the equipment effectiveness? Root cause analysis: what caused this? This is historical and backward looking. Certainly, there are exceptions to this view—dashboards and other forms of real-time monitoring for asset performance management (APM) as an example—but most spreadsheet analytics clearly are not a forward-looking exercise.

Further, the use of APM solutions is typically limited by their cost and complexity to expensive, mission-critical assets such as turbines that can justify the resources and keep up with the "drift" in every plant due to changing prices, conditions, formulas, and raw materials. And even dashboards are typically based on a predefined and not dynamic context, and as such report on current data with past tense context.

Thus, the future state of analytics is less about the new concept of prediction, and instead more about democratizing this capability. More assets will be involved, ones that certainly could not have been justified in the past due to the expense of sensors, data collection, storage, and traditional APM solutions. Rather than best practices based on a fleet of assets, preventative maintenance will be based on a sample size of one. Broadly deployed, predictive analytics will enable early alerts to avoid incidents, along with other warnings of developing problems, with notice given well in advance. Figure 2 depicts how advanced analytics can be used for predictive analytics.

FAST FORWARD

- There will be a sweeping transition from historical to predictive analytics.
- There will be an expanded role for subject-matter experts, typically process engineers, in cutting-edge analytics efforts.
- Engineers will quickly create insights to improve outcomes, empowering them to do the right thing.

To realize the benefits of prediction for more and

Data generated and stored (terabytes per day)

Industry	2019	2020	2021	2022	2023	2024	2025
Power	1.15	1.34	1.61	1.98	2.48	3.19	4.52
Water	0.32	0.34	0.37	0.40	0.44	0.49	0.57
Gas	0.53	0.56	0.61	0.67	0.73	0.82	0.95
Semi-con	1.73	2.18	2.89	3.97	5.58	8.11	13.54
Elec assembly	1.26	1.47	1.77	2.18	2.73	3.50	4.97
Med dev	2.01	2.28	2.64	3.14	3.77	4.63	6.18
Petrochem	1.26	1.47	1.77	2.18	2.73	3.50	4.97
Oil and gas	1.00	1.14	1.32	1.57	1.89	2.31	3.09
Pharma	1.27	1.35	1.46	1.60	1.76	1.96	2.29
Auto OEM	1.90	2.15	2.50	2.96	3.57	4.37	5.84
Auto suppliers	1.20	1.31	1.47	1.68	1.94	2.27	2.83
Heavy industry	0.76	0.84	0.94	1.07	1.23	1.44	1.80
Aerospace	0.89	1.01	1.18	1.39	1.68	2.06	2.75
Light industrial	0.32	0.34	0.37	0.40	0.44	0.49	0.57
Food and beverage	0.85	0.90	0.98	1.07	1.18	1.31	1.53
CPG	0.74	0.79	0.85	0.93	1.03	1.14	1.34
Chem	1.26	1.47	1.77	2.18	2.73	3.50	4.97
Paper and textiles	1.12	1.26	1.47	1.74	2.10	2.57	3.43
Metals	0.98	1.08	1.21	1.38	1.58	1.85	2.32

Source: IDC

Figure 1. This table shows how the amount of data generated in the process and other industries will increase dramatically over the next five years.

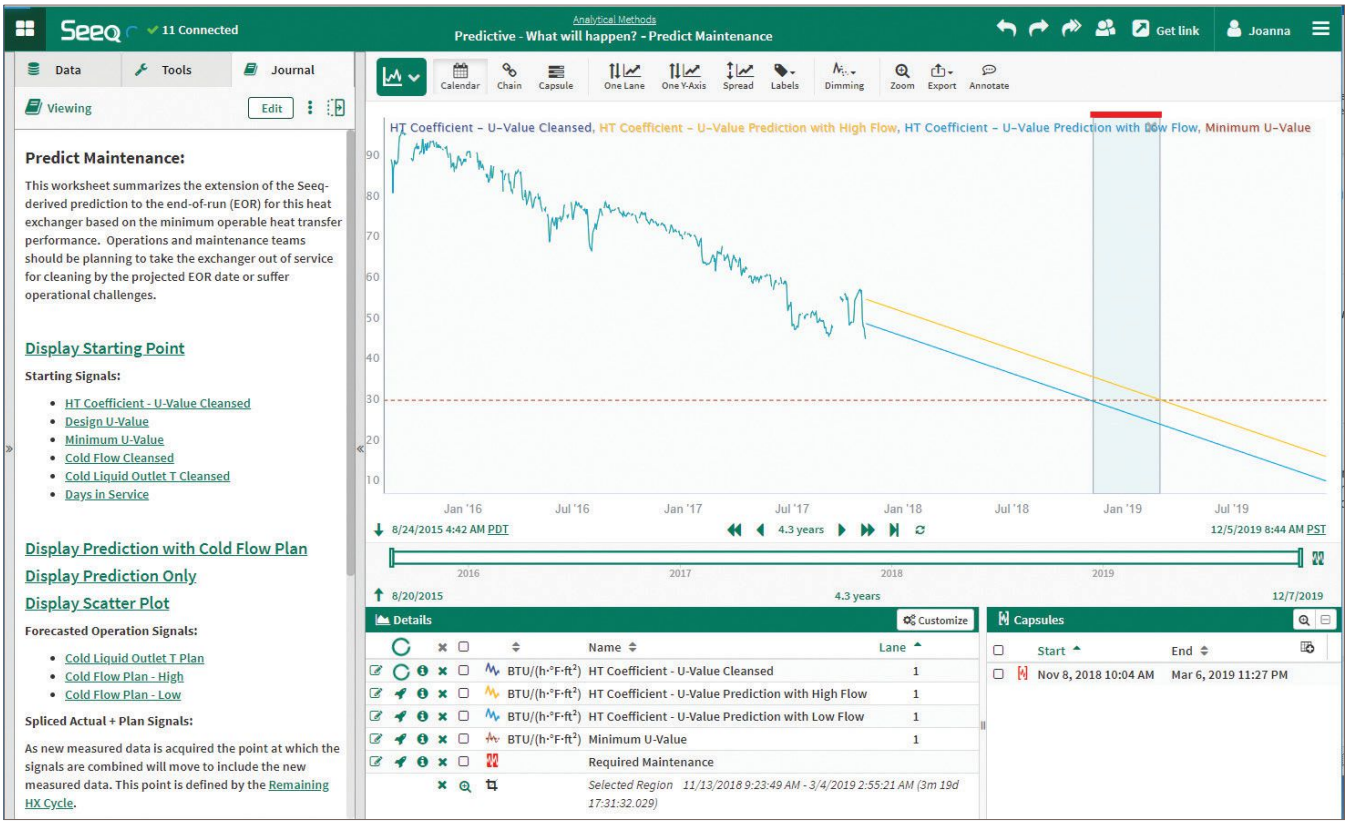


Figure 2. This screenshot shows how advanced analytics was used to predict required maintenance for a heat exchanger.

more assets, engineers will move to the forefront of advanced analytics efforts.

Engineers in the lead

The second improvement is an expanded role for subject-matter experts (SMEs), typically process engineers, in cutting-edge analytics efforts. These SMEs have the required education, expertise, and history with the plant and processes: they know what to look for and what it means. "Self-service" or "ad hoc" are the terms used for these types of solutions, which ensure local access to insights by putting the power in the hands of SMEs.

The future state is therefore not replacement of SMEs, which is the message associated with machine learning and initiatives based on information technology (IT), but to instead improve the available tools so they can implement predictive and prescriptive analytics. Although there has been much excitement about data scientists and their role in improving production outcomes, such as the *Harvard Business Review*'s "Sexiest Job of the Century" article back in 2012, more recent articles and anecdotes from end users tell a different story. The fact is, while data scientists know their algorithms, they do not know plant processes and context, or first principles models and how changes affect operations.

There has also been a more recent spate of articles on the need for data translators or data liaisons to work between data science and engineering teams. But all of this can be avoided if advanced analytics vendors simply close the gap and bring data science innovation to SMEs by creating self-service features. Yes, machine learning is a critical component for analytics next, as described in the advanced analytics section below. But although these and other algorithms are important, they are not sufficient. Application-specific expertise is critical and required.

Furthermore, a new generation of analytics cannot end with SMEs. Self-service is what they have been doing for 30 years with spreadsheets. Therefore, new solutions must empower teams and networks of employees to share production and operations insights within the organization. This may just sound like fancy language for dashboards and reports, but there is a critical difference, which is maintaining a connection between the created analysis and the underlying data and providing all users with click through access to this data. Engineers, teams, managers, and organizations can use these new capabilities to distribute benefits throughout a plant and a company.

Insights in time

With more assets connected and contributing to predictive plant maintenance, and tools in the hands of the engineer to participate in innovative plant analytics, the third improvement for the next generation of analytics is to do the right thing. In the context of process manufacturing, the most data intensive and scientific of industries, that may sound ridiculous, but it is a critical difference for future state analytics. Predictive analytics will provide a view into the future, with SMEs and others developing insights in time to impact outcomes.

For example, with spreadsheet-based and other forms of traditional analytics, it often takes longer to do the analysis than the batch takes to complete. This means batches are discarded rather than fixed during the cycle time, so the right thing—finding and fixing the problem during the cycle—does not have a chance to happen. Another example is where there is a question of the right course of action for an asset versus a unit or overall plant objective, where it may be better to postpone a maintenance action to achieve a more important goal, such as continuing production.

A SME should be able to see and identify the trade-offs and make the right decision to optimize overall outcomes. This is transformative analytics: a break from the past tense approach of the long times to insight associated with spreadsheets. In speaking with SMEs, this provides them with ability to do the right thing by quickly examining a given data set with context, data, and priorities as a framework for priorities.

The end goal of future analytics: enable the right decision in time to improve the outcome.

Thus, the end goal of future analytics: enable the right decision in time to improve the outcome. This is why the previous points—a complete view of plant health and requirements and an empowered engineer—are so important. Only with the full context of priorities, costs, and requirements can the right decision be made on a consistent basis. Rather than a "prescriptive" approach that assumes all states, requirements, and outcomes may be defined and known in advance, SMEs and other plant employees can analyze and make decisions in the moment because fast analytics are possible. An example of these concepts is in the sidebar.

Attaining these objectives will be possible, as mentioned earlier, by the continuing innovation in software that has defined every aspect of our personal and professional lives over the past 30 years. Undermining the change are paradigm shifts in where and how analytics will be executed.

Cloud and on-premise edge computing

Analytics workloads are particularly suited for the cloud because most use cases require the scalability, agility, quicker deployment, and lower costs associated with the cloud to analyze more assets and processes. Therefore, companies of all types, including process manufacturers, are moving their IT infrastructure and data to public and hybrid clouds to access on-demand computing resources. And for those companies not willing to move their

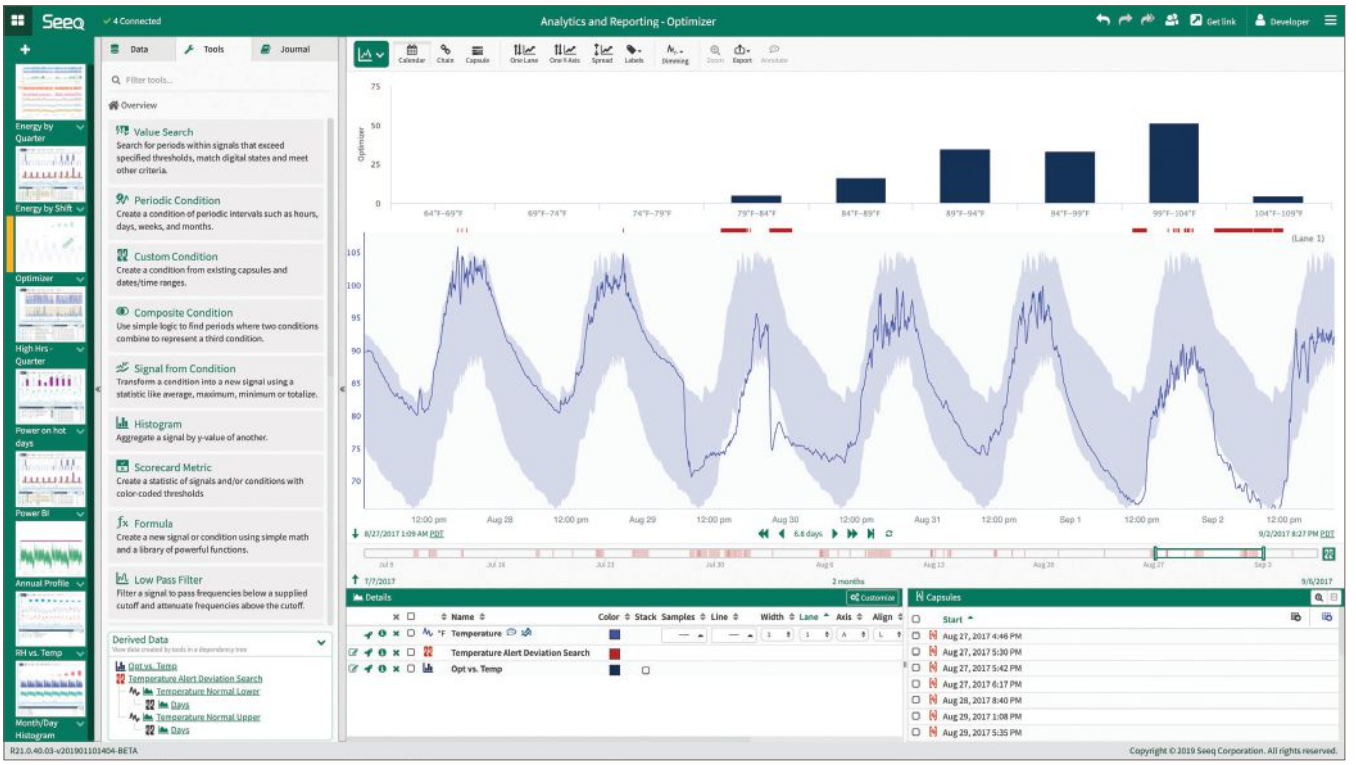


Figure 3. Advanced analytics software empowers engineers and other experts to interact directly with data of interest, and to easily share results across an organization.

data to the cloud, the cloud is coming to them in on-premise hardware solutions with cloud platforms, such as AWS Outpost or Microsoft Stack. Process manufacturers will therefore likely use a mix of public and private cloud offerings, as well as on-premise components, for analytics.

The trend is in its infancy, though some industries are ahead in embracing the cloud, for analytics as well as other use cases. Consequently, the big public cloud platforms are paying more attention to the largest sources of data, with manufacturing leading all sectors of the economy in terms of data volumes.

For example, Microsoft, Amazon, and Google have specifically focused on the oil and gas sector as a starting point for their efforts. This is clearly a sign of market interest, and it is also a sign of the maturity of the cloud offerings: Amazon brought out AWS in 2002, and then introduced S3 (storage) and EC2 (virtual machines) in 2006. Cloud computing competition then increased with Microsoft's and Google's cloud platform introductions in 2008.

What this means is that the current model for big data storage in process manufacturing—on premise, historian-based, and proprietary—is undergoing a transition, enabling new alternatives for how and where analytics are run. The new model might be a data lake for data aggregation, on-premise or in the cloud, or a comprehensive Industrial Internet of Things solution, such as a next-generation data storage platform. At a minimum, current process historian vendors need to introduce road maps with safe passage for data from on-premise offerings to the cloud.

Advanced analytics

Spreadsheets lead the way in analytics today, but this general-purpose tool is not suited to the task of implementing predictive and prescriptive analytics. Replacing spreadsheets comes with a new entry to the dictionary: "advanced analytics." Just as adding "smart" to a noun denotes a thing with sensors for telemetry and remote monitoring services (e.g., smart refrigerator, smart parking lot), adding "advanced" to "analytics" brings analytics into a modern framework to address today's challenges.

What has happened is that vendors have recognized there is too much data from too many sensors, and potentially of too many types, for one person to simply solve problems manually with a spreadsheet. Therefore, through the introduction of machine learning or other analytics techniques, engineers' efforts are accelerated when seeking correlations, clustering, or any needle within the haystack of process data. With these features built on multidimensional models and enabled by assembling data from different sources, engineers gain an order of magnitude in analytics capabilities, akin to moving from pen and paper to the spreadsheet (figure 3).

Engineer's tool

Advanced analytics innovations are not a black box replacement for the expertise of the engineers, but a complement and accelerator to their expertise, with transparency to the underlying algorithms to support a first principles approach to investigations. It is a natural next step in the history of statistical and control processes, rather than a data science approach to investigations.

Predicting sewer spills

Municipalities use wastewater treatment pump or lift stations to keep waste flowing through the system by increasing sewage pressure. Municipalities monitor flow rates to determine if there is too much wastewater at a station, and to see if pumps are cycling too frequently.

When the process goes awry, raw sewage can spill out of manholes or other apertures. A field team can of course be dispatched to clean up the result, but the utility is not always the first to know about the spill. In fact, the first notification of a wastewater spill often comes from a member of the public, hours and sometimes days after the spill.

This model was used to detect a blockage and potential sewage spill 13 hours before the event, giving personnel time to take corrective action.

This can intensify public health and environmental effects and the cost of clean-up efforts, including associated fines. Following a sewage spill at an environmentally significant site, one municipality sought a way to reduce the likelihood and impact of future spills.

The utility now uses Seeq for an online sewer blockage detection system. The team developed a blockage model based on data from a recent spill, and this model detects blockages much faster than previous methods. With advanced analytics, the model identifies blockages by detecting the absence of "normal fill and pump behavior" in near real time. The absence of pump runs or extended fill time during peak times signifies an abnormality and possible blockage.

The blockage model gives the utility the opportunity to head off spillages, safeguarding the environment while improving public perception. It is also an example of many of the concepts described in this article, including the democratization of assets (predictive analytics on a lowly pump, not a massive turbine), engineer-led solution definition, and access to insights in time to affect outcomes. The figure shows monitoring of the wastewater lift station pump operation to detect blockages in the system, and it shows how repair crews are given sufficient time to correct the problem before an overflow occurs. ■

At the same time, advanced analytics recognizes the path to quicker insights must leverage innovations in adjacent areas to address the scope of data available for investigation.

Wrapping complex functionality in easy-to-use interfaces is a common experience in our lives as consumers, for example, the ability to search in Google. These same approaches are now being adopted by analytics offerings for engineers in process manufacturing.

Looking forward

We are nearing the end of an era defined by on-premise data collection and spreadsheet-based analytics as the next generation of predictive, engineer-led, and timely analytics replaces the status quo. Using advanced analytics, insights will be shared to enable the required collaboration among experts within a single process plant and across an entire organization. These developments will work in concert to advance analytics from backward to forward looking, enabling process plants and facilities to spot developing problems and close control loops. ■

ABOUT THE AUTHOR

Michael Risse (michael.risse@seeq.com) is the CMO and vice president at Seeq Corporation, a company building advanced analytics applications for engineers and analysts to accelerate insights into industrial process data. He was formerly a consultant with big data platform and application companies, and prior to that worked with Microsoft for 20 years. Risse is a graduate of the University of Wisconsin at Madison, and he lives in Seattle.

View the online version at www.isa.org/intech/20200202.

RESOURCES

"Analytics next: Beyond spreadsheets"
www.isa.org/intech/20190802

"Empowering an effective PAT methodology"
www.isa.org/intech/20190402

"What's next for big data in process manufacturing"
www.isa.org/intech/20180601

Better performance begins at the edge

IIoT advanced computing happens on the factory floor

By Rich Carpenter

Discrete manufacturers and original equipment manufacturers (OEMs) are experts when it comes to operating their equipment. They run and develop these systems daily, always learning and improving. Once stable operation is established, these companies must proceed to incorporate technologies and methods, such as data analytics, to improve performance. Cloud-based analytics are an option, but many users have discovered it is expensive or against established information technology (IT) policy to move data for all analytics to the cloud.

Engineers and designers of manufacturing and OEM systems develop expertise integrating the right automation platforms to obtain the necessary functionality, even though this task may not be their core strength. They are aware of the need for good operating metrics and are looking for smart ways to add them to an already functional system.

A lot can be learned by observing a system in operation and obtaining user feedback. However, quantitative values, such as throughput rates, failure counts, change-over frequency, and other data, are usually needed to support

FAST FORWARD

- Data analytics provide valuable feedback to optimize maintenance, increase uptime, and improve real-time control.
- Industrial data sources include sensors, controllers, and smart devices at the operating edge, so it makes sense to collect, preprocess, and analyze data locally.
- Only transport data as appropriate to the cloud. Edge data can be analyzed locally to make better control decisions and then cleansed, transformed, and packaged for transmission to the cloud.

Figure 4. Edge devices and controllers can combine control platform data with other externally sourced data, analyzed in context with each other, to provide an informative HMI experience.

more in-depth analysis. Automating the data gathering process is the most effective way to obtain enough source information for analyzing how a system is running and where it can be improved.

The need for improved operations, coupled with emerging types of powerful edge components, is driving more data processing, and sometimes analytics, to be performed at the edge. Where appropriate, the results may also be sent to the cloud for comparison across multiple plants or for OEMs who have equipment distributed across a diverse customer base. This article addresses the value of analytics for industrial manufacturing applications and compares edge processing solutions.

What are analytics?

Analytics projects require the historization of vast amounts of raw data, but this alone does not create business value. Instead, such value is only realized through better comprehension of how a system is currently running and how it could operate better. Analytics are any evaluation of raw data to improve it into useful information, which in turn can give users insights to help them increase throughput, improve quality, and optimize maintenance.

Acting based on analytics results may be a procedural activity initiated by engineers or operators. In some cases, it is now possible to directly and programmatically use analytical results to inform control platforms about improved operating parameters.

Programs for applying analytical methods can operate in many locations. They may run on edge-located controllers, on site-located systems, or in the cloud. Some analytics projects may operate in two or all three of these locations.

Edge data sources

Part of the reason analytics are becoming more relevant is due to the increasing richness of available data. For manufacturing and machine control applications, the data needed to support analytics can come from any sort of edge-located basic sensor, smart sensor, smart instrument, digital device, or more complex local system. Collectively, increasingly intelligent edge-located sensors and devices are generally known as Industrial Internet of Things (IIoT) devices.

A simple photo eye can indicate how many times a machine cycles or a part is produced. Instruments monitor pressures, flows, and power consumption. Smarter subsystems may calculate uptime, energy use, and quality pa-

Figure 1. Smart edge devices like this Emerson PACMotion VFD can provide extensive data about operation, energy consumption, and diagnostics—if the right edge components are in place to obtain it.

rameters. Smart manifolds offer early indication of air leakage, which leads to excess energy consumption and higher operating costs. There are many other examples of smart edge devices like variable speed drives (VFDs), analyzers, power meters, and intelligent valve controllers (figure 1).

All of these may provide multiple data streams using conventional wiring and networked signals or newer wireless connections. The data typically includes one or more near-real-time process variables, and other less-real-time extended configuration and diagnostic information.

In addition, data sources can include less traditional digital sources like the Internet and company intranets, which have information relevant to production processes, such as raw material prices, energy prices, weather conditions, and demand for finished products. Gathering the data effectively calls for installing the right technologies in the right locations to obtaining it from many types of sources on varying time scales.

Importance of edge processing and analytics

In recent years, there has been an emphasis on cloud computing, which is a good method for aggregating many sources of data. However, for many plant-level data analytics needs, the cloud-only method is not usually the best solution. There are examples of predictive maintenance performed on high-value equipment using data sampling techniques at the edge to provide early warning signs of failing equipment.

The edge of any industrial system is the natural place to begin an analytics initiative because that is where the source data is created. Many data points may be involved, and each point can potentially have a high sample rate. Common sense informs us it might be burdensome and perhaps costly to transmit all this data to the cloud. Edge-located preprocessing of the raw data refines it into more concise values.

Traditional analytics were based on data obtained mainly from equipment control systems, because those digital systems were already connected to the sensors for command and control. Furthermore, the computing resources needed for storing data and analyzing it were only available at the server or perhaps desktop computer level.

Today, many end users are embarking on IIoT initiatives and taking advantage of IIoT devices to obtain rich new data streams, economically bypassing traditional control systems. A new generation of edge-capable components are best suited to interface with the growing number of IIoT data sources and can offer many benefits for processing and analyzing this data closer to the edge.

Edge analytics advantages

Due in part to the growing capability of industrialized hardware and associated software, it is more practical than ever to perform advanced computing at the factory floor with a range of edge-capable component options (figure 2). Some advantages of edge analytics are:

- improved data privacy
- better data fidelity and responsiveness
- resilience against data transmission interruptions
- reduced data communications
- a better opportunity to "close the loop" for control

Many companies are rightfully concerned with data privacy. Data obtained at the edge and analyzed at the edge is easier to secure, generally because it is kept local. Even if the data must be transported to analytics applications located elsewhere onsite, or in the cloud, the latest edge controllers and devices use modern and secure IT-based protocols for communicating.

Data generated using traditional operational technology–based devices, most commonly programmable logic controllers (PLCs), may lack security measures or may have added-on security instead of built-in security. Con-

Figure 2. The availability of increasingly powerful edge processing industrialized hardware and software means computing can easily be performed on the plant floor.

Figure 3. Advanced edge controllers, such as Emerson's Outcome Optimizing Controller, provide robust automation on a real-time operating system, with the added advisory and analytical capabilities of Linux-based processing.

ventional systems can be preserved and interfaced by edge computing devices. They can secure them, perform analytics, and provide upstream connectivity.

Another important reason to move analytics to the edge is because the data source is closer to the processing, providing near-real-time fidelity and responsiveness with minimal communications. Certain analytics require this performance.

Cloud-based analytics, on the other hand, must use data that is potentially time delayed by transmission, suffering from longer sample rates, and subject to transmission interruptions. Edge-based analytics avoid most of these issues.

Even when data must be transferred to higher-level systems, edge analytical results may be a much smaller data set than the entire amount of source data points. Moving data, especially at high resolution, and cloud storage for large amounts of data, can be cost prohibitive.

Edge analytics have also enabled a much better solution for "closed-loop" operations by directly applying results to an operating process without requiring operator intervention. Analytics performed closer to the edge, sometimes onboard the same component as the real-time controller, are more readily integrated back into the automation control platforms, without the many interposing communication layers involved with cloud-based solutions.

Ways to integrate edge analytics

As noted previously, PLCs conventionally have supplied much of the industrial edge data used for analysis. This is changing as IIoT devices are more widely incorporated, and because edge components are gaining better processing and networking capabilities.

The three leading edge components are controllers, devices, and gateways—each with varying capabilities for gathering, transmitting, and processing data for industrial systems. Edge controllers can perform extensive data preprocessing and run analytics applications, in addition to executing real-time control (figure 3). Edge devices may perform local analytics but are not involved in controlling equipment. Gateways perform little or no data preprocessing prior to transmission.

While each of these components plays a role, edge controllers are the most capable of the three. This new class of IIoT controller includes all the capabilities of edge devices and edge gateways, combined with the high-speed deterministic control features found in a typical PLC, including support of IEC 61131 languages.

The architecture of modern edge controllers includes support for open-source capabilities, allowing companies to rapidly incorporate IT-friendly languages, protocols, and concepts like Python, OPC UA, web servers, and databases. Edge controllers are analytic-friendly and can host third-party applications to help end users reach their analytics goals.

Edge controllers have the capability to run nondeterministic analytics or connect to a cloud infrastructure for additional information, and the unique ability to directly bring this information into the deterministic control scan in order to apply more informed decisions and optimize plant processes. This ability for connected equipment, like connected people, to make more intelligent decisions is driving a major transformation in the industrial space.

Users can install edge controllers in new greenfield applications, initially

using them as PLCs but eventually expanding their role to include analytics. Or, edge controllers can be retrofit into brownfield systems to add analytical and IIoT capabilities.

Edge alternatives

Although edge controllers are the most complete option, other edge components like devices and gateways can be used as cost-effective alternatives or in conjunction with edge controllers in some applications. Edge devices typically support local applications with analytics on the device and can communicate data like an edge gateway. They are a good fit for use in conjunction with an existing control system that will remain in service, when it is desirable to add analytics capability.

An edge device might be used when the analytics require high-fidelity data, which can require too much network bandwidth to transfer to the cloud or where the cost of cloud systems and storage is too high to be practical. Because they are installed local to the source data, they are also a good approach when gaps in data collection due to network connectivity issues would otherwise significantly affect the quality of the analytics.

Edge gateways typically include protocol drivers to connect to plant controllers as well as cloud connectors to connect to leading cloud infrastructures such as Microsoft Azure and the Amazon IoT cloud. The purpose of the edge gateway is simply to collect data from industrial devices, package it, and send it to industrial clouds, whether public or private.

How companies are using edge analytics

Manufacturers and OEMs are learning how to implement edge analytics, and it is not an all-or-nothing proposition. They can start in just one targeted area, apply edge analytics concepts as supplementary to already-operating controls, or choose new platforms and use the available capabilities progressively as needed.

Edge gateways are typically used to get visibility to a geographically distributed set of assets. The edge gateway connects to the asset, packages the data, and transports the data to a cloud or hosted infrastructure. This consolidated data is often accessed in order to check the health of the equipment, avoiding the significant expense of travelling to each site.

Edge devices typically augment an on-premise machine or plant by collecting data from the device, aggregating it with other information available, and then analyzing this data to optimize control decisions. For example, the edge device may combine production data from a machine control system with data collected through supplementary sensors added outside of the control platform—such as for vibration, pressure, and temperature—and use this information in context to detect overall process problems and support a human-machine interface (HMI) (figure 4). This processing, for example, could observe an increase in air pressure required to manage machine motion, which could indicate leaks in the system.

An edge controller is more like a modern car, where the driver still performs direct control but is advised by an onboard navigation system as to the best route. A real-time operating system (RTOS) portion of the edge controller manages the deterministic control system, while a second general-purpose operating system (OS) side may be connected to IoT devices and broader information available from supervisory computing and even the Internet. The RTOS and the OS may constantly exchange information to optimize production processes. For example, the controller side may be managing reservoirs of water as they move through a purification process. The general-purpose side may be checking the forecasted energy prices and communicating to the control side the optimal time to run equipment for energy savings.

Start with analytics at the edge

End users are aware that analytics initiatives are an important avenue to better understanding, and therefore improvement, of their industrial systems. They also know there may be large quantities of untapped data in IoT sensors, smart field devices, and even existing OT systems. However, the idea of creating an overarching cloud-based system to take advantage of the data can be daunting.

The availability of powerful edge components enables another practical approach. Installing modern edge controllers and edge devices is a comparatively easy way to begin taking advantage of analytics. These edge components can perform the analytical role themselves or support future cloud-based systems.

There are many reasons to keep analytics close to the field, especially to obtain the best data fidelity and communications robustness. More compelling for some applications is the ability of edge controllers to close the loop by directly using analytical results to inform the real-time control system of optimal operational settings. ■

ABOUT THE AUTHOR

Rich Carpenter (Richard.Carpenter@emerson.com) is the general manager for product management for Emerson's Machine Automation Solutions business unit and has responsibility for its portfolio of control system, operator interface, industrial PC, and Industrial IOT software and hardware products for industrial automation.

View the online version at www.isa.org/intech/20200203.

RESOURCES

"AI equipment health monitoring and prediction technology"
www.isa.org/intech/20181205

"Digitalization delivers value and competitive advantage"
www.isa.org/intech/20190603

"Digital transformation creates new opportunities for system integrators"
www.isa.org/intech/201904channel

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 CT 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
DIGITALIMMUNITY STAY PRODUCTIVE, STAY SECURE
WisePlant Smart, Safe & Secure
MSI Mission Secure, Inc.

Traceability improves food and beverage production

By Steve Winski

Systems combine to better monitor and control product and packaging

As food safety becomes more and more a concern, the ability to track products within a facility is of vital importance to manufacturers and consumers. In 2018, the Food and Drug Administration (FDA) reported 137 product recalls due solely to misbranding and undeclared allergens. These are all classified as Class 1 recalls where, under FDA regulations, there is a significant risk to health.

Not only do these recalls have significant consequences to public health, they also put companies at risk. A Deloitte study on recall execution effectiveness estimates that a food recall can cost a company up to 10 million dollars. In addition, a company's stock price can decline up to 22 percent within two weeks after a recall is announced.

As consumers demand more accurate and clear information on purchased products, it is up to manufacturers to improve packaging, labels, bar codes, date codes, and even nutritional and allergen information. One answer to this is a continued focus on traceability, which is a challenge many food and beverage companies face. When you know where your product is and what is happening around it at all times, you are able to better control the environment surrounding it and avoid potential waste, rework, and even product recalls.

And though traceability is a primary end goal for many food and beverage companies, accomplishing it is not always easy. Many companies have track and trace systems in place that monitor and control packages and products, but they are often incomplete. The solution to this is finding a more comprehensive software and sensor solution to provide a complete package and product monitoring and control system to track and trace products throughout the facility.

FAST FORWARD

- Traceability in the food and beverage industry enables manufacturers to eliminate human error, improving efficiencies and increasing productivity.
- Complete coding management and packaging verification solutions are insurance against coding and packaging errors.
- With a modular sensor and software solution, manufacturers can ensure their products will leave the factory in the right packaging with the correct label and coding information.

What causes labeling and packaging errors

With the increasing complexity of packaging types, it has become more challenging for food and beverage manufacturers to reduce, if not eliminate, errors in coding and packaging products. This is particularly important in situations where mistakes can cause a risk to consumer health.

Errors in the packaging process happen for a number of reasons, but many of these errors are human error. For example, the wrong date code being entered into the printer can cause waste and rework.

One of the more common mistakes is because of the frequency of artwork changes and promotional offers. It is increasingly difficult for manufacturers to eliminate errors on packaging lines because of the sheer number of products being produced in different packages, especially when temporary promotional packaging is implemented. When the incorrect packaging is selected, the entire batch needs to be scrapped, producing significant waste.

Other errors can occur from the printer or coder. A coder may fail to print, or a printer may print a poor-quality code that is illegible and needs to be redone. Although eliminating these errors may seem impossible, it is really easier than you might think. When you catch these errors early, you can avoid significant production losses in time and money.

"One simple mistake on packaging lines can result in huge commercial damage to your business: both in financial loss and damage to brand and customer confidence," said Mike Hughes, managing director of AutoCoding Systems. "Even if you are lucky enough to identify an error before it enters the distribution chain, it's likely that you will still incur significant rework or scrap costs to rectify the problem. And there's an added risk of shorting customer deliveries on shelf-life critical products."

Taking steps to remove human error

Sensor solutions play a large role in the production of food and beverage products. In basic track and trace systems, sensors are needed to identify one- and two-dimensional codes, read and write to radio frequency identification

Vision sensors can verify the correct code was used and that it actually printed.

(RFID) tags, and provide high-resolution images for downstream processes.

The most common solution used in these systems is bar-code readers—used primarily to identify markings and codes on packages. But a track and trace system goes beyond just bar-code readers. It also encompasses vision solutions, Ethernet, software databases, and more. Greater functionality is possible when using a comprehensive software database that connects with sensor technology.

Complete coding management and packaging verification solutions are insurance against potential coding and packaging errors. You will gain increased speed, reliability of line setup, and reduction in job changeover time.

Modular sensor and software products can eliminate the risk of coding and packaging errors that can lead to emergency food recalls. When implemented on packaging lines, companies can effectively manage the deployment of coding and data and the checking of packaging before products leave the factory.

Essentially, software verifies that all coding data and packaging is correct. Vision sensors then verify that the correct code was used and that it actually printed, helping to validate codes and prevent recalls for food safety before products leave the facility. This leads to increased traceability and accountability for food and beverage manufacturers.

By catching mistakes at the source, significant changeover delays or rework to recode or correct the packaging are avoided entirely. With these types of solutions, you gain better control over your packaging line and the integrity of your products.

Job setup and changeover time is also dramatically reduced. When manually setting up a packaging line, it can take up to 15 minutes, with quality paperwork adding another five minutes. This 20-minute time frame can be reduced down to one minute or less with a comprehensive solution such as this.

"By automating the setup of your coders and other packaging line devices, potentially to the point where you can receive instructions directly from your ERP [enterprise resource planning] or MES [manufacturing execution system], you save on downtime and reduce the number of repetitive, low-value tasks your staff would otherwise carry out on a day-to-day basis," Hughes said. "It's also important to have the option to build on your chosen solution's core functionality to add features like OEE [overall equipment effectiveness] reporting, paperless quality control, inspection reporting, and more."

Control the packaging line

To keep up with a changing business environment, new technology, and demanding consumers, food and beverage manufacturers are acknowledging that automation must play a significant role in their factories to improve efficiency and reduce costs. As such, the need for equipment connectivity on the factory floor has never been more prominent. For equipment and applications to work together with minimal human intervention, they need to be able to communicate, share data, and report back on performance and quality.

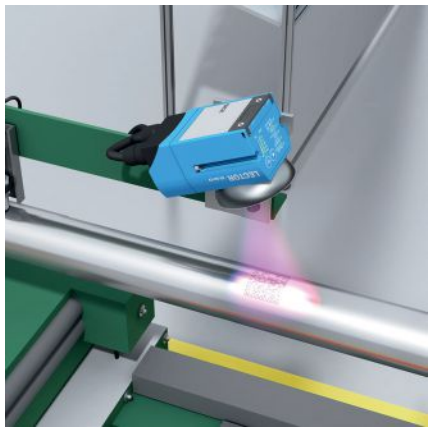
A modular sensor and software package is very effective at helping to meet a retailer's code of practice related to coding and packaging verification. However, there are additional capabilities that can be rolled into packaging lines for process improvement reasons, not just for compliance reasons.

Information relating to a product (i.e., date coding rules, packaging artwork, bar codes, coding profiles) can be entered into a secure database, thereby allowing validation before use. The stored data is used to set up and control the relevant devices on the packaging line. This removes the need for operators to program the devices and, in turn, removes the risk of human error.

However, one challenge with some of these systems is they may require the use of a single manufacturer's "networking systems." What is needed is a solution that works well with all equipment typically found in a packaging line. This means you will not have to make costly changes to your packaging line just to get it implemented but can use a single system to control multiple devices from different vendors. The devices may perform different functions—coding, inspection, labeling, and verification—but they all exist on the same line. So, for your convenience, you want to be able to control them easily.

With a system like this, you can set up and control all types of packaging line equipment, including multiple brands of printers, labelers, checkweighers, metal detectors, and x-ray equipment. This increases your traceability throughout the facility, as everything can remain connected, regardless of the supplier.

In addition, an automatic solution should manage the entire packaging workflow process. From making artwork changes in the system database to equipment setup to retrieving product information from the database, you want better access to all data on your



Packaging verification solutions with an image-based code reader can even detect codes on shiny surfaces.

packaging line so you can make better decisions to remain competitive.

A complete solution like this gives the consumer goods industry a way to greatly reduce date-coding errors and downtime related to product changeovers. You will have dynamic control of your packaging line, ensuring that it stops if a device malfunction is detected or if there are too many misreads or no-reads detected from a sensor.

Add modules for functionality

Any automated system should be scalable with the potential to add additional functionality as required. A modular sensor and software solution can provide additional features that address very specific challenges manufacturers face.

Extensive reporting is available from inspection devices like checkweighers or metal detectors to provide access to more data on your packaging line. You can also receive line performance reporting to capture real-time manufacturing data with accurate reports. These reports display your packaging lines, devices, and product performance. This helps improve your overall equipment effectiveness to drive gains in throughput and efficiency to increase profitability.

Additionally, a pallet labeling system is available for auditable and controlled labeling of pallets from different lines with information like batch code, order ID, line ID, stock keeping unit (SKU), and SSCC18 (serial shipping container code) information.

Better reporting allows for more effective coding automation and the automatic generation of batch codes and best by dates. This all drives line availability and improves the overall packaging process.

Finally, you can make your quality control process paperless. Digitizing quality checks allows you to incorporate in-line and off-line quality control processes into a workflow control. Data is then recorded in the audit trail to utilize electronic reporting.

"A purely manual, paper-based system is becoming challenging for many manufacturers to maintain. The general trend is that these compliance-driven requirements are becoming more detailed and prescriptive," Hughes said. "The audit regime, particularly if your business manufactures on multiple sites for multiple retailers, can become exhausting. One group technical director recently told us that on average, one of his sites is being audited somewhere, for something, every couple of days."

With a paperless system, product traceability is at an all-time high. Information becomes available to anyone in the system, instead of just those who have access to the paper.

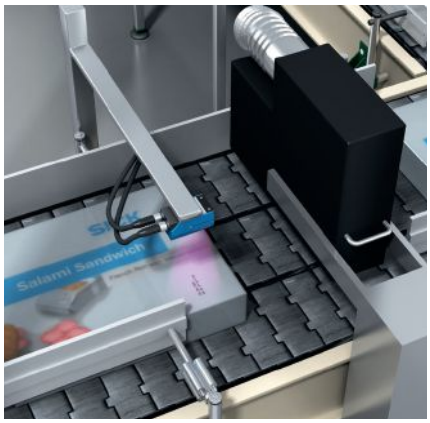
Packaging line problems

A modular sensor and software system that can verify packaging and coding issues has value in many different industries. In one instance, a major global manufacturer of pet food required a solution that would address a number of issues it was experiencing.

USER EXAMPLE

Print correct date codes

The manufacturer's main pain points were printing the wrong date code on products, not printing date codes on products, and selecting incorrect primary and secondary packaging for the products. As a result, it looked to a modular solution for software and sensors to solve all of these problems.



Capabilities can be rolled into packaging lines for process improvement reasons, not just for compliance reasons.

A multitouch human-machine-interface was implemented, using a hand scanner and RFID reader for user login. This gave operators a robust and reliable interaction point with the system. In addition, the software faithfully eliminated coding and packaging errors.

On the company's primary packaging lines, secure deployment of the expiration date and other data was sent to the coders. The printer is automatically set up with the correct coding information. The line also stops entirely if the printer goes into a fault state.

The sensors on the system detect whether or not a code is present. If one "No Read" is detected, it will reject the product, but not stop the line. If more than three "No Reads" are detected, the

Accurate detection of codes on packaging of all shapes and sizes is essential.

entire line will stop until the problem is fixed. This means the company can get ahead of the problem before it results in significant waste and potential recalls.

For packaging errors, a verification process was put in place. Expiration dates and other data is sent to the carton printers. Sensors verify correct packaging using inline checking of bar codes. They also verify that the correct code is placed on the box.

USER EXAMPLE

Identify similar packaging

In another example, a major prepared meals company needed to differentiate between products with similar packaging. The company manufactured a number of different soups and sauces, all of which used very similar packaging. As a result, incorrect pots were often used with products. In addition, numerous product changeovers led to increased downtime while waiting to manually set up the equipment.

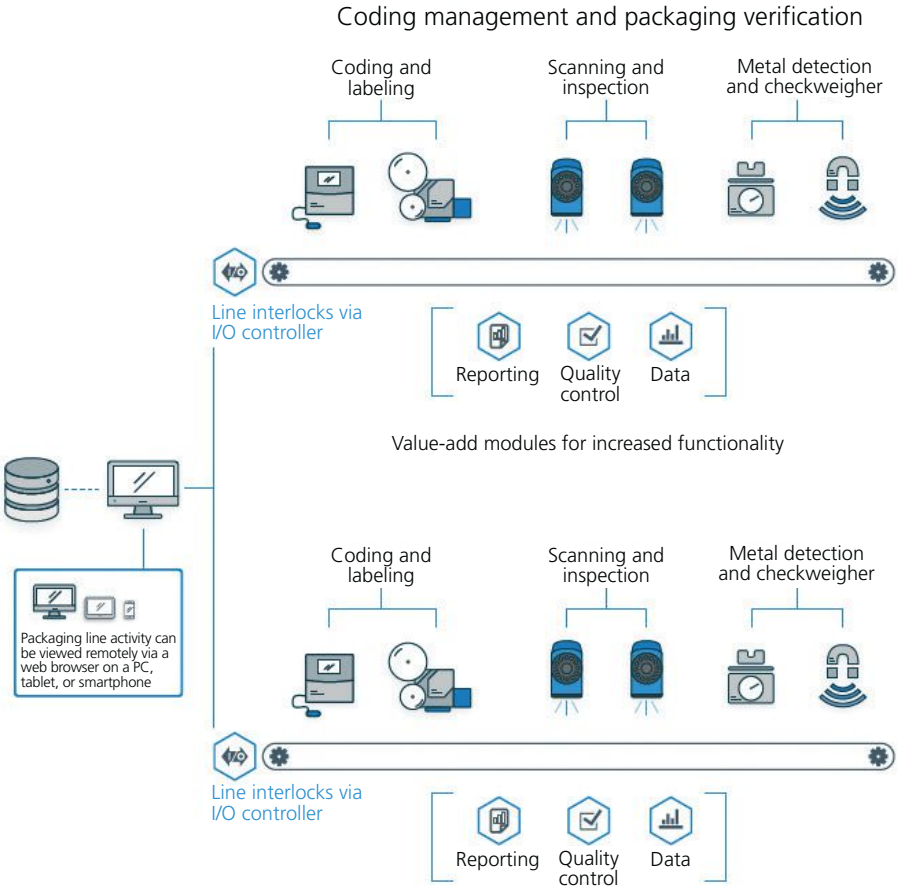
All this was solved with a modular approach. Various bar-code scanners now scan every spinning soup pot to confirm the correct one is being used. Expiration dates and other data are sent to the printers and then verified by sensors. Packaging errors were greatly reduced, if not entirely eliminated, and the system was better able to accommodate the various product changeovers, leading to increased uptime.

USER EXAMPLE

Prevent incorrect labels

Another company utilizes a modular system to ensure the correct labels are used for each product. The company uses similar packaging for all products, but each product type needs a different side label, top label, and bottom label attached. Because the packaging and each individual product look very similar to one another, the manufacturer was running the wrong labels on packaging.

When this happened, the entire line had to stop and then workers needed to backtrack and find where the incorrect labeling started. It took a significant amount of time to retrace the problem to where it started. The manufacturer was fortunately able to save the product, but workers had to remove the incorrect labels and run them down the line again to replace them. To avoid high labor costs for quality control, the company decided on a vision sensor and software package that more reliably detects mistakes and avoids rework.



How a coding management and packaging verification solution works.

Future-proof traceability

Packaging and coding mistakes account for a high proportion of food product recalls, having a devastating impact on food manufacturers' brand and business costs. Taking appropriate measures to prevent such a recall has to be a priority for food and drink suppliers.

With a modular sensor and software solution, manufacturers can ensure their products will leave the factory in the right packaging with the correct label and coding information. This comprehensive package and product monitoring and control setup can eliminate these errors.

Additionally, by automating the setup of printers and other packaging line devices, with the potential to link directly to an MES or ERP system, there is a significant reduction in job setup and changeover time. By reducing downtime, the packaging line can run for longer periods with improved efficiency and increased productivity. ■

ABOUT THE AUTHOR

Steve Winski (Steve.Winski@sick.com) is the national sales manager for consumer goods at SICK, Inc., based in Minneapolis. He holds a BS in computer and electrical engineering from Purdue University and has more than 35 years of experience in controls, automation, and manufacturing software.

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

IIoT & SMART MANUFACTURING CONFERENCE

Training: 14 April 2020
Conference: 15–16 April 2020
Moody Gardens Hotel
Galveston, TX, USA

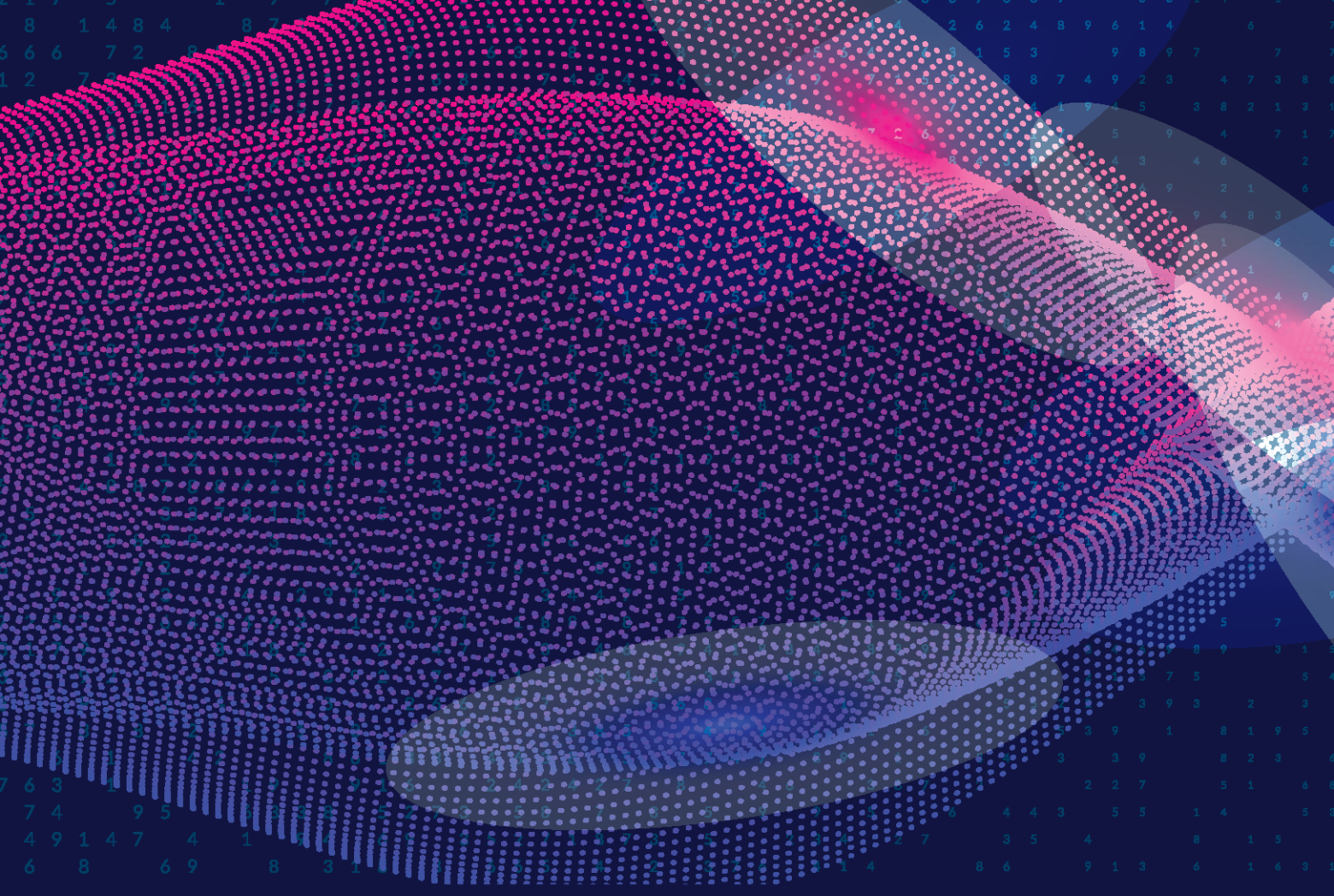
ISA is proud to introduce a new conference focused on the vast world of Industry 4.0. Dive into the technologies transforming almost every vertical industry. Attend thought-provoking keynotes and technical sessions and enjoy unique networking opportunities with industry experts from areas including connectivity, cybersecurity, and much more.

www.isa.org/iiot

Conference topics include:

- Navigating the IIoT Landscape
- System Design & Architecture
- Cybersecurity & Safety
- Implementation & Management
- Smart Manufacturing
- Digital Transformation
- AI/Edge Computing
- Industrial Communications/Network Technologies

International Society of Automation
Setting the Standard for Automation™



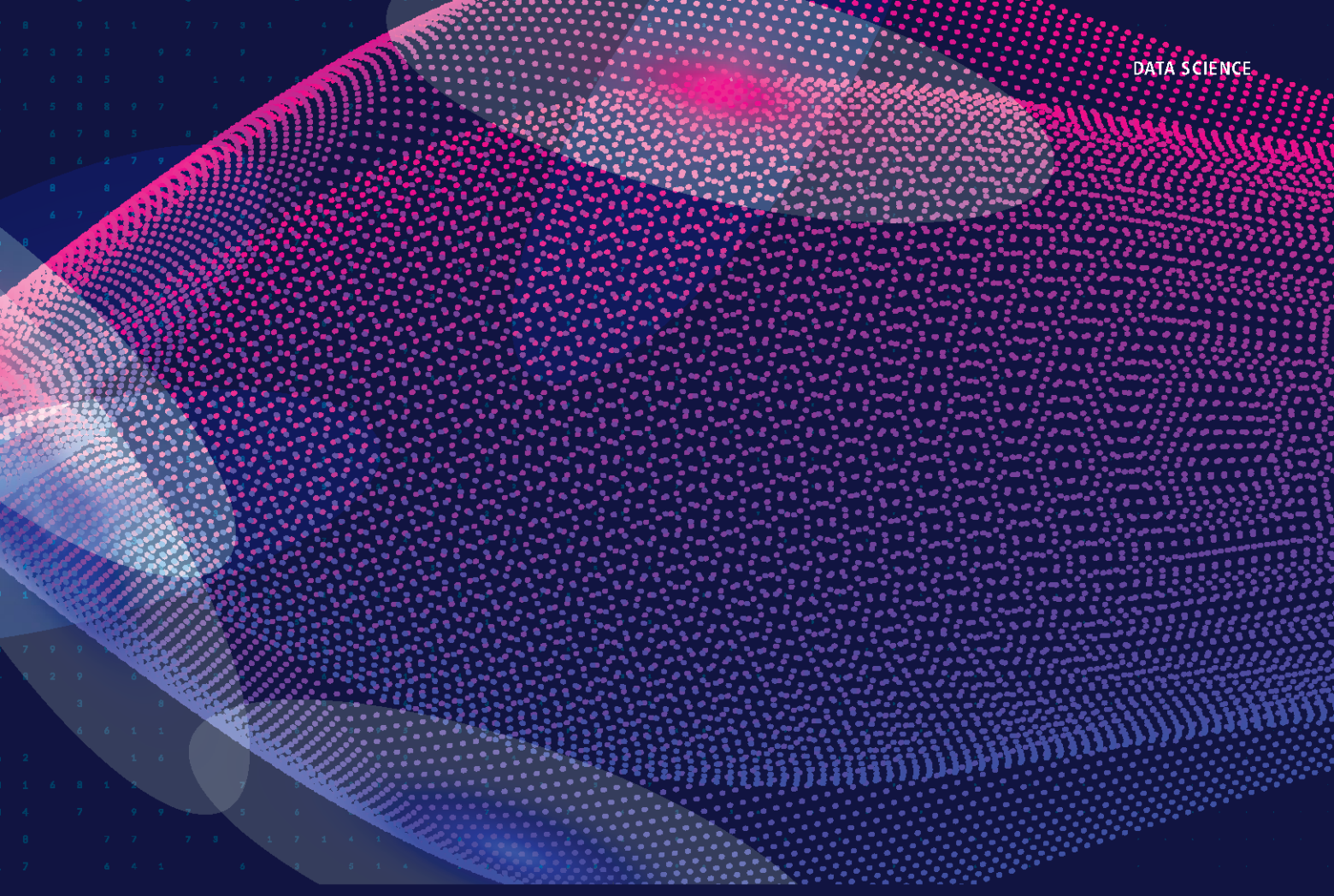
Applying data science

By Edward M. Marszal

Internet technology can unite PHA, HAZOP studies, LOPA, and hazard registers

Process hazards analysis (PHA) studies, especially hazards and operability (HAZOP) studies and layer of protection analysis (LOPA) reports are ubiquitous in the process industries, but the information generated during these studies is not being used to its fullest extent. Management desires to have multiple scenarios rolled up into easier-to-use hazard registers, and to be able to visualize them with graphical approaches like bow-tie diagrams. Unfortunately, the data that is currently contained in most HAZOP and LOPA studies is not structured to allow easy hazard register generation and bow-tie visualization. The use of the "cause local – consequence global" approach to HAZOP has made the facilitator's life easier at the expense of others who need PHA data but cannot find what they need because the resulting documentation is not logical.

This article discusses the use of standardized data structures that are already revolutionizing PHA documentation. Extending these standardized data structures will allow the development of tools that can display a single set of data as a HAZOP worksheet, LOPA worksheet, or bow-tie diagram. Furthermore, the hazard analysis can be modified using any of these visualization techniques and have the results



to hazard analysis

carried back across all diagram and worksheet types. Adoption of a unified hazard assessment data structure will benefit all users of PHA data and facilitate use of PHA data by other critical stakeholders, automatically.

Process hazards analysis

Chemical process facilities spend considerable resources on process hazards analysis studies. Initially, many organizations performed PHA in a minimal-cost, minimal-compliance fashion, in order to "check the box" for regulatory compliance. Many bad habits were formed in this early phase of PHA adoption that are still with us today, but which can hopefully be rectified with a combination of better software and better motivated PHA facilitators. Since the early adoption phase of PHA, many sophisticated organizations not only committed to the PHA process, but also expanded the use of PHA information, leveraging the information for engineering and management tasks that were performed by other process stakeholders. One of the first extensions of PHA information was LOPA.

Beyond LOPA, managers of process plants were interested in summarizing the information from PHA into lists of significant hazards. These managers would regularly refer to these hazard lists and ensure that all of the safeguards affecting the risk of these scenarios were

FAST FORWARD

- Relational databases are becoming obsolete for PHA, as Internet technology like cloud computing brings new and better ways to store and work with data.
- As industry migrates to an Internet technology paradigm, best practices from the IT world, including unified data structures, XML, and JSON, become more important.
- The unified hazard assessment data structure provides a platform where a single data set can be used for multiple purposes.

Applying data science to hazard analysis

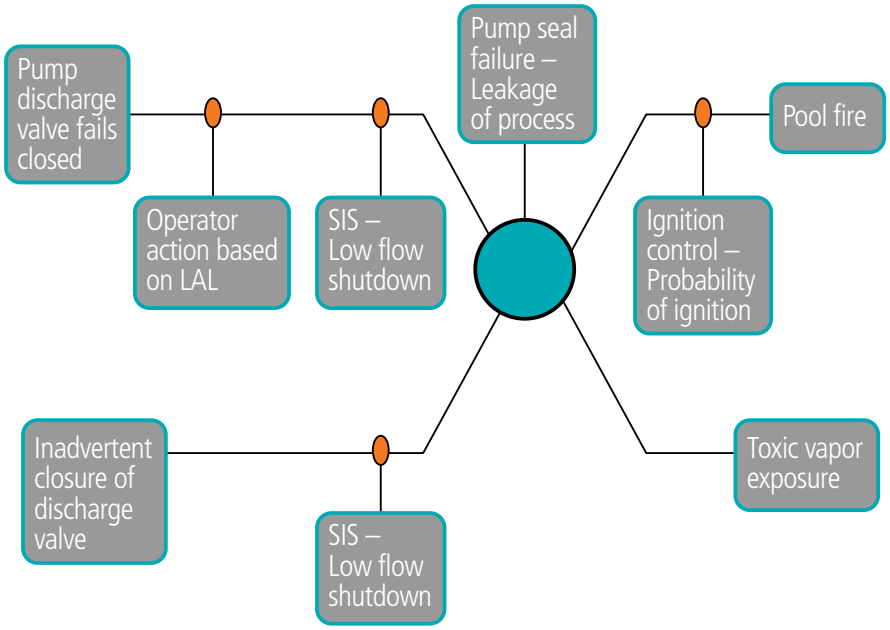


Figure 1. Typical bow-tie diagram.

properly designed, implemented, and maintained. These lists of significant hazards and information relating to them are typically referred to as hazard registers. While hazard registers became a powerful tool for managing risk, understanding the hazards and communicating them throughout the organization and even to external stakeholders was difficult due to the highly technical nature of the information and the dense use of acronyms and jargon.

Bow-tie diagrams

To aid in the understanding of hazard scenarios, the visualization technique of bow-tie diagrams was developed. When a hazard scenario is visualized as a bow-tie diagram, it is a graphical representation of the development of the scenario. The bow-tie diagram reads from left to right (figure 1). On the left a series of causes of the hazardous event are listed. A line is drawn from each cause to the "knot" in the bow tie.

The knot in the bow tie represents the realization of the hazardous event. In the process industries the "knot" is typically a loss of containment of process chemicals. Along each line from the cause to the bow-tie knot are "barriers." Barriers are events, systems, or situations that prevent the cause from resulting in the loss of containment scenario—which in bow-tie analysis jargon is typically referred to as the hazard or hazardous event. Barriers between the cause and the loss of containment are referred to as "preventive" barriers as their successful operation prevents the loss of containment from occurring.

On the right side of the bow-tie knot is the description of what occurs after the loss of containment. This consists of a series of consequences that can occur as a result of the loss of containment event, with lines drawn from the "knot" to the consequences. As with the causes, all of the consequences may have barriers that will either prevent or mitigate (i.e., reduce the magnitude of) the consequence if they operate effectively.

The key benefit of the presentation of a risk scenario as a bow-tie diagram is that the visualization accelerates and facilitates understanding of the scenario. The combination of the visual cues and textual information is a much richer representation of the hazard scenario information.

The preceding discussion clearly shows that there are myriad valuable uses for the information developed during PHA. It would seem that you should be able to simply press a button, and switch from viewing the data as a PHA to viewing it as a LOPA, then a hazard register, and finally as a bow-tie diagram. Further, it seems like you should be able to make edits to the bow-tie diagram and have them cascade back to the LOPA study, and then you should also be able to view the quantitative aspects of the LOPA while you are viewing the bow-tie diagram.

Unfortunately, this is not currently the case. At the current moment, each of these different uses of PHA data use different software applications, each of which use different data structures to represent data. Even worse, the data structures in the different applications for different study types are completely and irreconcilably different from each other such that data cannot be shared between applications.

To address this situation and maximize the utility of the data that the process industries are investing in, a few changes need to be made in how PHA is performed and documented. First, a change in the mindset about how PHA facilitators document studies will be required. Facilitators must be willing to document studies based on where the hazard manifests itself as opposed to the location of the cause of the hazardous event. But most importantly, industry needs to move to a common, consistent, standardized data structure for PHA: the unified hazard assessment.

Basics of structuring data

Before delving specifically into the problem of defining a consistent structure for PHA data, we should begin by discussing how data is structured in general. Although this section will rely on terminology that was developed for relational databases, it is applicable to other methods of data storage and retrieval that are vastly superior to the use of traditional relational databases for hazard analysis studies.

The primary concepts of relational databases for storing data are tables, records, fields, relationships, and identifiers (IDs). A table is a structured list of data that all describe a given item;

for instance, a PHA study will generally have a table that describes all of the study nodes. The best way to think about a data table is by visualizing a spreadsheet. A table contains many rows and columns of information where each column of information is a specific piece of information, such as a node number or a node description.

A database generally contains many different tables that describe the different aspects of a system. For example, a PHA database might contain a table for nodes, deviations, and causes. The reason that different tables are required is because, often, there are multiple instances of one type of item that all relate to a single instance of another. With PHA, for instance, a single node will have many different deviations associated with it, and a single deviation can have many causes. To address this phenomenon, we set up multiple tables of information, and organize the linking between the tables using relationships.

In database science there are three types of relationships: one-to-many, many-to-one, and many-to-many. A one-to-many relationship means that for a single item in the primary table, there can be many items in the secondary table that are associated. In other words, the primary table, the "parent" in the relationship, can have many "children" in the secondary table. In a typical PHA, a single node has many deviations, and each deviation has many causes. A relational database manages these relationships first by understanding how they are defined, and then by tracking the IDs of the records.

Cause indexing

When you look at a PHA report, a single deviation contains multiple rows that contain causes of the deviation. Although it looks like a single table to the viewer, in reality the software is combining the two different tables into one visualization. The deviation table, in fact, does not actually contain any information about causes at all! Instead, each cause contains the identifier (ID) of the deviation that it is associated with.

This activity is referred to as cause indexing. What the PHA software does in order to display that view that most of us are familiar with is to first display the deviation from the deviation table and subsequently search the causes table to find all of the causes that are associated with a given deviation. It does this by comparing a "Deviation ID" field in each cause record with the ID of the deviation that is currently being displayed.

A many-to-one relationship is the opposite of one-to-many and works very similarly. A many-to-many relationship between tables is the most complex situation. Here, a single record in the primary table can have multiple associated records in the secondary table, but, individual items in the secondary table can also have relationships with multiple records in the primary table. The best example of this in PHA is recommendations. Each PHA cause (scenario) can have multiple recommendations associated with it, but each of those recommendations can also be associated with multiple causes.

PHA software first displays the deviation from the deviation table and subsequently searches the causes table to find all the causes that are associated with a given deviation.

In this complex case, an entirely separate table needs to be created simply to store the relationships between the primary and secondary table. As alluded to earlier, each table contains multiple records. Each record is like a row on a spreadsheet and contains all of the different attributes of a specific entry on the table. Each record then is composed of multiple different fields. Each field is a specific data entry of a given data type.

For instance, if a PHA study contains a table of safeguards, that table might contain individual fields for tag (text string), description (text string), probability of failure on demand (floating point number), effectiveness determination (Boolean), and ID (GUID). All of these structures combined together result in the overall database structure.

Relational database challenges

The discussion in the preceding section used terminology that is consistent with relational database technology, which is commonly used to store PHA data. However, use of relational databases is becoming obsolete in applications like PHA studies, as Internet technology and cloud computing offer better ways to store and work with data. All of industry, and all of society, is migrating to a paradigm where information is stored in the cloud, and all knowledge work will be performed by interacting with the cloud, generally through a web browser. Even when desktop applications are developed today, they are generally a thin wrapper that essentially holds a web page.

Relational databases accessed through the cloud work great when the user would like to interact with a single record of a single table in a database. But, when a user desires to work with and view multiple different records of multiple different tables, the result is a dreadful and slow user experience, as the web page tries to kludge up a concatenation of all the requested information in a single form. This form then updates every time the user shifts focus from one element to another—especially if anything was edited, because that is what is required to maintain contact with the database server.

The primary problem is the transactional nature of a relational database. When a user requests a piece of information, the database must know specifically what table, record, and field to get. It then grabs that piece of information, transfers the data between server and client, and the client processes the information by presenting it on the screen.

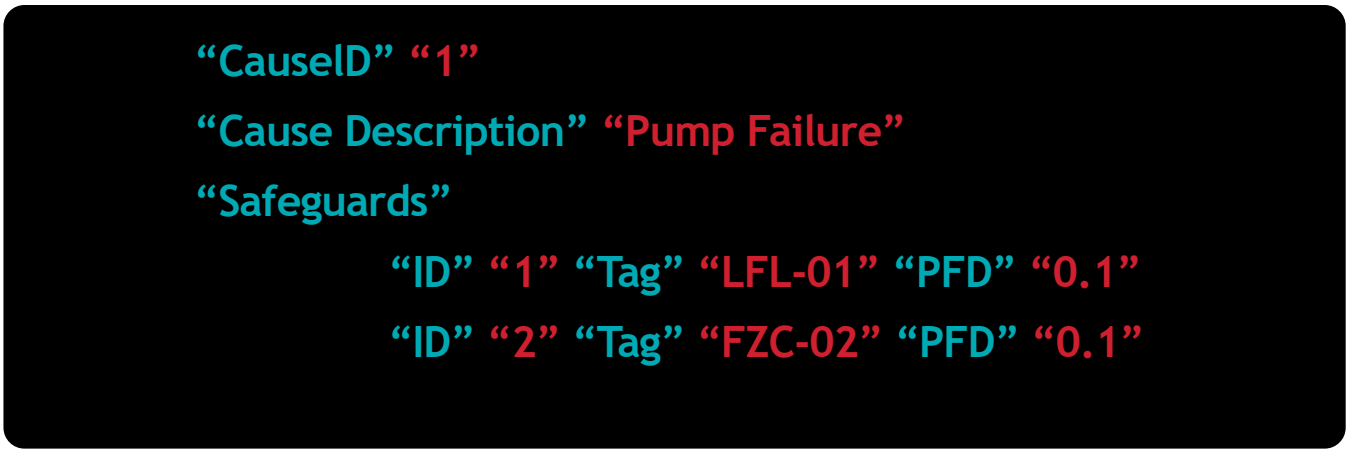


Figure 2. PHA data in JavaScript Object Notation (JSON).

As described in the previous section, in order to present a PHA worksheet on a computer screen, data needs to be obtained from multiple fields, in multiple records, of multiple tables. Furthermore, drawing the information on the screen is complicated by the fact that the application needs to change the view as a function of how many records in secondary tables are associated with a given record in a primary table. This requires thousands (or even tens of thousands) of individual database transactions to occur between the client and server to obtain the information for a single screen view.

The problem is usually further exacerbated by third-party "controls" used during the programming process. Many software vendors do not have the talent to directly access the database, and instead rely on third-party controls that they configure to access the desired data. Unfortunately, these controls—such as text boxes and grids—have bloated and slow code, because they are designed to be flexible, not fast.

A new paradigm

The elite companies in Silicon Valley have developed better ways to handle this problem and are using them frequently and widely in their software and web sites. Unfortunately, most PHA software has not caught up with the times. The state-of-the art approach is to eschew traditional relational database technology in favor of the flexible data object models that were born in cloud computing. Specifically, the data transaction speed problem was solved using Extensible Markup Language (XML) and subsequently its even lighter cousin JavaScript Object Notation (JSON).

In the new paradigm, when a web page wants to get data from a database server, it does not request a single field at a time, it requests that a large collection of data is "serialized" into a JSON object, and that single object is conveyed from server to client in a single transaction. As a result, a best-in-class, cloud-based PHA application only communicates with the server twice per worksheet—once to load the data from the server, and then once again to return the edited data back to the server. In the interim, the web page keeps the entire data object in memory on the client. When users interact with the data, they are interacting with the data on the client—at lightning speed—not the data on the server.

New data structures like XML and JSON have all the advantages of a relational database. They can easily store multiple tables, each with multiple records and multiple fields. They can also manage relationships between tables, in all formats, the same way that relational databases do. Figure 2 presents an example of some PHA data being stored as a JSON object.

While some applications are built with a relational database server that serves up the data to build a web page and then stores the results after the page is edited, more and more, the relational database is not used at all. The JSON objects are simply stored on the server as the end result.

Unified hazard assessment

A single data structure cannot be both cause indexed, as is the most common approach for HAZOP, and also consequence indexed, as is the most common approach for LOPA. Furthermore, neither of these data structures is suitable for hazard registers or bow-tie diagrams. But the latter two are indexed by a "hazard" or a "hazard scenario"— the approach that also underlies a unified hazard assessment data structure.

The unified hazard assessment data structure provides a platform that allows a single data set to be used for multiple purposes. HAZOP studies can generally be performed using the same

The state-of-the art approach is to eschew traditional relational database technology in favor of the flexible data object models that were born in cloud computing.

workflow as always, but you need to take some additional care where things are documented. Also, at least one additional data field will need to be completed, or at least separated out of the cause or consequence description, where it usually resides. With regard to data structure, the HAZOP worksheet needs to show, for each deviation, one or more hazard scenarios. Each hazard scenario can show multiple causes and multiple consequences. Other than that, the PHA worksheet will look essentially the same.

Once the HAZOP has been documented using the unified hazard assessment approach, development of the LOPA is dramatically simplified. The data structure for each hazard scenario record should include a Boolean variable that indicates whether or not the hazard scenario requires a LOPA. In this way, when the user starts by viewing the HAZOP study, he or she should be able to click on a single tab or button and have the software automatically redraw the user interface for LOPA.

The data transaction speed problem was solved using Extensible Markup Language (XML) and its even lighter cousin JavaScript Object Notation (JSON).

There is an even more powerful aspect to bow-tie diagrams using the unified PHA format. Currently, most bow-tie diagrams are simply a visual representation of a hazard scenario, but with an underpinning of a unified hazard assessment data structure, the bow-tie diagram can include all the quantitative aspects, such as the frequency of the initiating event, the safeguard probability of failure on demand, and the overall scenario frequency and risk ranking. This will enable performing a HAZOP or LOPA using the graphical format of the bow-tie diagram (figure 3).

The last information presentation format that needs to be addressed is the hazard register. This is the easiest of all the problems to solve after the development of the unified hazard assessment data structure. Basically, the data that is developed in a HAZOP worksheet is sufficient to meet this need, as long as it is hazard-scenario indexed. In fact, one might want to limit the data presented to even less than what is shown in a HAZOP worksheet.

Unified hazard assessment is a method to restructure and optimize PHA data so that it can be used for more than just process safety management compliance. A standardized unified hazard assessment data structure and complaint methods for documenting PHA data allow a single data set and a single software tool to be able to seamlessly present data as PHA (HAZOP), LOPA, hazard register, and bow-tie diagrams. ■

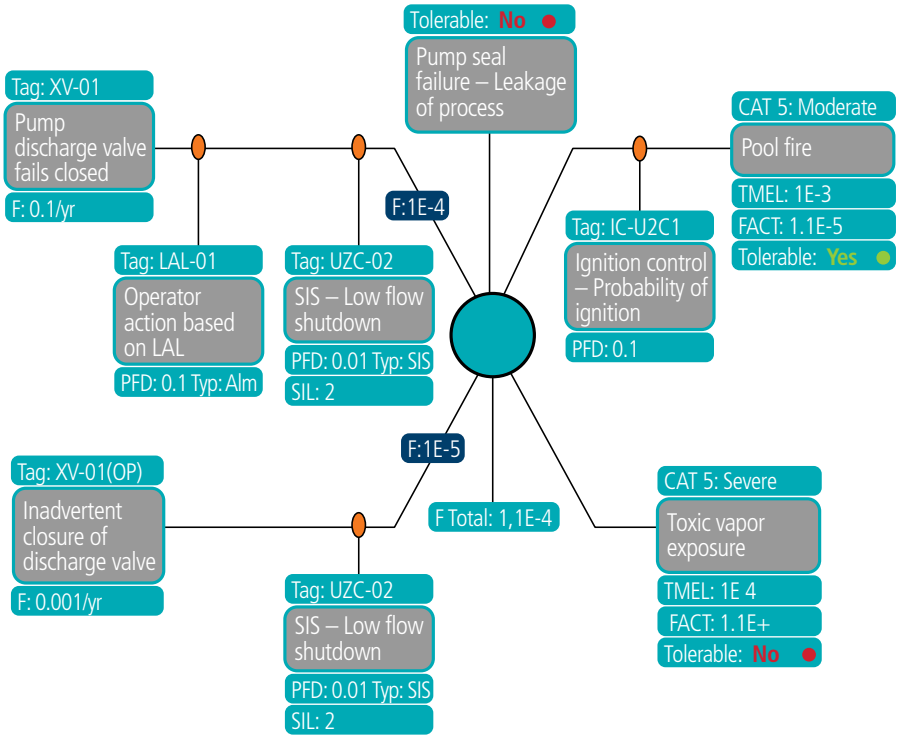


Figure 3. Bowtie diagram including quantitative LOPA data.

This article was adapted from a paper originally published for the Texas A&M Engineering Experiment Station's Mary Kay O'Connor Process Safety Center 22nd annual international symposium, held 22 – 24 October 2019. Read this article online for a link to the full paper.

ABOUT THE AUTHOR

Edward M. Marszal (edward.marszal@kenexis.com) is president and chief executive officer of Kenexis, an independent consulting engineering firm that provides technical safety services for process industries and other industries that manage risks related to chemicals or stored energy. The company is helping change the way that safety and security are incorporated into industrial business practices by providing best-in-class software tools, associated training, and comprehensive technical support.

View the online version at www.isa.org/intech/20200205.

Volunteers in action

Local learning:

Gruhn to speak on safety, HMIs, more

ISA past president Paul Gruhn, PE, CFSE, will be presenting at local meetings around the country during the first quarter of 2020. As a global functional safety consultant with aeSolutions, a process control and process safety consulting, engineering, and integration services company based in Greenville, S.C., Gruhn has gained extensive experience consulting with sites around the world.

Gruhn presented at the ISA Toledo, Ohio, section meeting on 14 January; the ISA Manchester, Conn., meeting on 29 January; the ISSS Northeast Chapter (Plantsville, Conn.) meeting on 30 January; and the ISA Brazos (Freeport, Texas) meeting on 6 February. He will speak at the ISA Wilmington (Newark, Del.) meeting on 25 February. Contact the meeting manager to attend.

If your group would like Gruhn to speak in your area, just ask. Gruhn says he has a long list of possible speaking topics he is happy to share. Below are the topics of his first six talks of 2020.

The Next Bhopal

Preventing disasters—and the incidents of lesser consequence leading up to them—requires probing beneath their seemingly superficial, distracting, and highly visible exteriors. Doing so shows how similar all industrial disasters are. The patterns that led to the Bhopal disaster are in many of the processes that we operate today. This presentation summarizes fundamentals of a portion of the Bhopal plant's process design, changes that were made contrary to the original specifications, problems encountered, and the numerous design and operational changes that were made (with the best of intentions) that simply led to further problems. It also covers how these issues came together to cause the worst industrial disaster in history. We need this awareness to prevent major industrial disasters and the more frequent "minor" process safety events that precede them today. This was the topic at the ISA Toledo, Ohio, section (14 January) and ISA Brazos (Freeport, Texas) 6 February talks.

Human-machine interface (HMI) design

Poor HMI designs have been identified as factors contributing to abnormal situations, accidents, fatalities, and billions of dollars of lost production. HMIs often impede rather than assist operators. Although decades of research have identified better implementation methods, change is difficult, and people continue to follow poor design practices. Just as a computer is not a typewriter, new HMI designs should not mimic those of old. The problem is that many designers simply do not know any better. This presentation will review why certain HMI designs are poor (with many examples) and show how they can be improved. This was the topic at the ISA Manchester, Conn., (29 January) talk.

Process industry accidents

Using a collection of videos, photographs, and stories, this presentation covers lessons learned from a variety of process accidents. Topics include: Do not hire low bid (you get what you pay for); everyone needs training (yet they often do not get it or accept it); even trained people make mistakes (and sometimes they do really stupid things); we are not as immune or indestructible as we may think; reuse of software is not always successful; near misses are often not followed up; the past is often ignored (and history definitely repeats itself). This was the topic at the ISSS Northeast Chapter, Plantsville, Conn., (30 January) talk.

Process safety management

Subtitled "Jenga, Drift, and Preventing Process Industry Accidents," this talk covers many well-publicized process industry accidents over the past several decades. Much has been written about them, and many lessons learned have been proposed. However, evidence indicates that the number of industry accidents has not decreased. More recent realizations of the complexity of modern processes, and the organizations responsible for designing, building, running, and maintaining them, has brought a broader understanding of accident causation, and what can be done to prevent further incidents. This will be the topic at the ISA Wilmington, Newark, Del., (25 February) talk. ■

Scenes from the 2019 Leadership Conference

ISA volunteer leaders gained new skills and new friends at the annual leadership conference held in San Diego in October 2019. The 2020 conference in San Juan, Puerto Rico, 23–26 October, will mark ISA's 75th birthday.

Be there!
ISA Strategic Leader Meeting
6–8 March 2020
Austin, Texas
www.isa.org/slm

Anniversary snapshot:

Milestones of industrial transformation

1945
- Instrument Society of America (ISA) founded

1950s
- Mechanical systems give way to electronics

1960s
- 4–20 mA standard settles signal controversy
- Adaptive control introduced

1970s
- Microprocessors invade measurement and control
- Births of the DCS, PLC, and process modeling
- ISA accredited by ANSI

1980s
- Rise of the personal computer, Microsoft Windows, HMIs, and Fieldbus standards
- Birth of historian software

1990s
- Fieldbus Wars, IS88 Batch and IS95 Enterprise Control System standards developed
- Rise of the Internet

2000s
- OPC UA developed
- Germany introduces Industrie 4.0
- Wireless 802.15 standard enables WirelessHART and ISA100a
- Birth of the Internet of Things
- Rise of process optimization

2010s
- ISA becomes the International Society of Automation
- Rise of Industrial Internet of Things, edge and cloud computing, machine learning and artificial intelligence, autonomous vehicles and drones, industrial virtual reality
- Birth of 5G communications

2020s and beyond
. . . to be continued

Certification

ISA Certified Automation Professional (CAP) program

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

CAP question

The branch of automation that deals with the design and implementation of a centralized control system for heating, air conditioning, and ventilation is:

A. atmospheric environmental automation engineering (AEAE)
B. building automation engineering (BAS)
C. air flow engineering (AFE)
D. heating, ventilation, and air conditioning (HVAC) engineering

CAP answer

The answer is *B,* "building automation engineering (BAS)." BAS has become a very important branch of automation in many industries, especially those that require sterile access areas or the need for pressurized gradients from room to room to control particulates.

HVAC (mechanical) engineers design the equipment and ductwork, but BAS engineers design and implement the control systems that help regulate fresh air intakes, room pressure, temperature and humidity, and recirculation. BAS engineers also aid with placement of smoke detectors and dampers and interfaces to the fire alarm and protection systems.

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

ISA Certified Control Systems Technician (CCST) program

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

CCST question

If a flow sensor is connected to the DCS system and the flow is displayed in volumetric units, what calculation would need to be performed in the control system to display the flow rate as a mass flow rate?

A. mass flow rate = volumetric flow rate × pipe cross-sectional area
B. mass flow rate = volumetric flow rate × sensor input in mA
C. mass flow rate = volumetric flow rate × fluid density
D. mass flow rate = volumetric flow rate / pipe cross-sectional area

CCST answer

The answer is *C,* mass flow rate = volumetric flow rate × fluid density.

To calculate mass flow rate, perform this calculation:

volumetric flow rate × fluid density

For example, using gallons for volume and LB for mass:

= gallons/min × LB/gallon
= LB/min

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

Congratulations new certification holders!

Below is a list of individuals who have recently passed either our Certified Automation Professional (CAP) or one of the three levels of our Certified Control System Technician (CCST) exam. For more information about the ISA CAP and CCST certification programs, please visit www.isa.org/training-and-certifications/isa-certification.

Certified Control System Technicians

Level 1

Neal Andrews
Andeavor, U.S.

Michael Bouse
U.S.

David Brant
University of Florida, U.S.

Todd Braun
U.S.

Daryl Buschmann
U.S.

Nicholas Carlson
U.S.

Andrew Hildenbrandt
U.S.

Keith Kuehn
U.S.

Daniel Malinowski
U.S.

Antonio Mar
U.S.

Kevin Martin
U.S.

Clifford Standridge
Facility Services University of Florida, U.S.

Daniel Whitacre
SABIC, U.S.

Thomas Whitehead
Boston Scientific, U.S.

Nicholas Fiddler
U.S.

Michael Gaskin
U.S.

Martin Plym
U.S.

Peder Winkel
University of Florida, U.S.

Jeffrey Hyder
U.S.

James McShane
Inland Empire Utilities Agency, U.S.

Federico Sordo Mendo
U.S.

Yassir Sheikhaldeen
U.S.

Daniel Ellis
IIS Inc., U.S.

Richard Roggenkamp
U.S.

David Trumbull
U.S.

Certified Automation Professionals

Thomas Quattlebaum
U.S.

Edward Johansen
Ascend Performance Materials
U.S.

Bryan Salmon
Chevron, U.S.

Jerry Pablico
U.S.

Muhammad Asad Ghaffar
Intech Process Automation, Pakistan

Dheeraj Kumar
Saudi Arabia

Charting a new era of ISA/IEC cybersecurity standards

The widely used ISA/IEC 62443 series of standards, developed primarily by the ISA99 committee, *Industrial Automation and Control Systems Security,* with simultaneous review and adoption by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

At a year-end meeting in Mannheim, Germany, the committee took stock of where it is and where it wants to go as a new decade unfolds. There is much the committee can build on as it closed out the final years of the past decade with several notable successes. This included a decision by the United Nations (UN) Economic Commission for Europe to integrate the widely used standards into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe. It also included completion of several key standards in the series, including:

- ISA/IEC 62443-4-1, *Product Security Development Life-Cycle Requirements,* which specifies process requirements for the secure development of products used in an IACS and defines a secure development life cycle for developing and maintaining secure products. The life cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management, and product end-of-life.
- ISA/IEC 62443-4-2, *Technical Security Requirements for IACS Components,* which provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications.

Looking ahead in 2020, an important standard expected to be completed in the coming months is ISA/IEC 62443-3-2, *Security Risk Assessment for System Design,* which is based on the understanding that IACS security is a matter of risk management. That is, each IACS presents a different risk to an organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. Further, each organization that owns and operates an IACS has its own tolerance for risk. For these reasons, ISA/IEC 62443-3-2 will define a set of engineering measures to guide organizations through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels.

An important standard expected to be completed soon is ISA/IEC 62443-3-2, *Security Risk Assessment for System Design*, which is based on the understanding that IACS security is a matter of risk management.

The new year will also likely see the publication of a revision of ISA/IEC 62443-2-1, with the revised title *Security Program Requirements for IACS Asset Owners.* This standard specifies asset owner security program requirements for an IACS. An asset owner, in the context of the standard, also includes the operator of an IACS.

The revision of ISA/IEC 62443-2-1 reflects a new stage in ISA99's growth and progression in which much of the important content has been defined, but there is a continual need to review and update material while identifying and correcting gaps and inconsistencies that may exist in the various standards that make up the series.

This stage will be evident in a new revision of ISA/IEC 62443-1-1, *Models and Concepts,* for which a first update draft has been prepared for review by the committee. This foundational standard established the context for all of the other standards in the series.

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

2020 meetings

Details are still being worked out, but ISA99 and its partner IEC committee, TC65 WG10, are planning to meet just outside of Houston in Galveston, Texas, in conjunction with the ISA Cybersecurity Standards Implementation Conference, during the week of 11 May, and then tentatively in September near Schiphol Airport in Amsterdam.

For information on viewing or obtaining any of the ISA/IEC 62443 standards, visit www.isa.org/findstandards. For information on ISA99, its meeting plans, or other related matters, contact Eliana Brazda, ISA Standards, ebrazda@isa.org. ■

Industrial router with firewall

The Lock 150 is an industrial router with firewall sharing access that secures remote connections and protects all devices behind it, in order to build, manage, and scale remote IoT control operations. With modular technology, networks and IoT infrastructures can be scaled from one object to thousands for a secure internal and external IoT ecosystem.

The Lock 150 can be installed in fewer than five minutes without the need for software installations, network configurations, or special IT skills. It has the capacity for up to 10 concurrent VPN connections. Integrated Wi-Fi is an alternate connectivity method and doubles as a wireless device access point. The router is compatible with all existing company products and includes end-to-end encryption between the company's devices.

Tosibox, www.tosibox.com/product/lock-150

Industrial asset monitoring, risk assessment

A new joint solution expands industrial asset monitoring, change management, and risk assessment capabilities for industrial enterprises. Asset Guardian change-management technology manages PLC, DCS, and HMI/SCADA software assets and provides a single point of reference for current asset information, including operational status, location, and controller logic versions. It has been combined with the iSID industrial threat detection system for real-time visibility of networked industrial assets, ports, and protocols on an OT network. By passively analyzing all data traffic, iSID can detect and counteract abnormal network activity in real-time, such as abnormal network access or asset changes and changes in the sequence of SCADA processes.

In this integrated solution, iSID's asset inventory now incorporates the asset information stored in the Asset Guardian database, including detailed asset information that is not available from traffic monitoring. This detailed information, such as logic version, ownership, and geolocation, produces a more granular risk score calculated by iSID for each asset. Changes to assets, such as new firmware or PLC logic, are detected on the network in real-time by iSID and sent to Asset Guardian for verification, authorization, and validation against the "golden image" of the binary stored in its database.

Radiflow, https://radiflow.com

Industrial network cyber defense

A new hardware/software joint offering helps utilities, oil and gas facilities, and other industrial manufacturing sites to identify and defend against cyberattacks. The solution is a joint venture between Ixia, a Keysight Technologies business, and Nozomi Networks. The Ixia Vision network packet broker (NPB) collects data from all locations connected to an operational network and delivers it to Nozomi Networks Guardian for real-time processing and analysis.

Aggregating traffic removes duplicate packets and unwanted traffic to improve performance and visibility into critical systems and processes to secure connected operational environments. The joint solution can also be integrated with security information and event management, as well as other systems, to establish an automated threat response. In addition, the NPBs integrate with tools such as firewalls to improve policy enforcement and mitigate unwanted traffic.

Nozomi Networks, www.nozominetworks.com

Modbus-filtering firewall

A developer of Modbus firewalls for industrial control networks has released PortBloque E, adding Ethernet firewall functionality and Modbus TCP/UDP deep packet inspection to filter and block harmful and unwanted Modbus traffic. These capabilities make the PortBloque E suitable for automation, utility, and energy operators who want to protect serial Modbus devices from Internet attacks. The browser-based interface gives operators customization flexibility. Operators can control Modbus traffic by slave IDs, function codes, and block commands that repeat too soon. Additionally, operators can define a permissible range of slave registers and values to prevent malicious memory access. The offering also provides bidirectional conversion between Modbus RTU/ASCII and Modbus TCP/UDP.

Sequi, https://sequi.com/portbloque-e

Thank You to Our 2019 and 2020 Sponsors

ISA Corporate Sponsors

MAVERICK™ TECHNOLOGIES
A Rockwell Automation Company

WisePlant®
Smart, Safe & Secure

Honeywell

Life Is On | Schneider Electric

inductive AUTOMATION

AUTOMATIONDIRECT.com

ISA Promotional Sponsor

beamex
A BETTER WAY TO CALIBRATE

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

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

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

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.

Electrical engineer

Central Arizona Project: The engineer will help guide the Central Arizona Project (CAP), a 336-mile system that brings Colorado River water to central and southern Arizona, in identifying and designing solutions to technical engineering problems. Responsibilities include providing complete and professional design services and technical leadership for planning and constructing new features of the CAP and modifying, operating, and maintaining existing features through engineering expertise and coordination of related disciplines. This includes the preparation of plans and specifications, internal work packages, and materials and cost estimates. The position requires five years of applicable electrical engineering experience with a BS in a related computer or engineering field . . . see more at Jobs.isa.org.

Manager, plant quality

Lennox International: The plant quality manager in Grenada, Miss., will lead a team that creates and manages processes, training, standards, and goals to increase factory capability and quality. He or she will collaborate with cross-functional teams to introduce and implement new technology, quality tools, and manufacturing processes. A bachelor's degree and eight or more years of related experience or an equivalent combination of education and experience is required. Additional qualifications include experience with quality testing and quality systems management, Six Sigma Green or Black Belt certification, and experience in multishift operation . . . see more at Jobs.isa.org.

Instrumentation/calibration technician

NanoString Technologies: The technician is responsible for installations, preventive maintenance, calibration testing, troubleshooting, and general repairs on a variety of components, analytical equipment, and instrumentation intended for laboratory and manufacturing use. This individual will also maintain the environmental monitoring system and temperature mapping of lab cold storage units. The ideal candidate has excellent organizational skills and will assist management in communication. This Tuesday-through-Saturday position will be trained for the first three months in the Seattle office and then transfer to the Bothell, Wash., office. The position requires three or more years of equipment management–related experience and a BS in a relevant science or engineering field . . . see more at Jobs.isa.org.

Lead UI engineer – Sensors

Medidata Solutions: In this New York City position, the engineer will provide technology leadership to a diverse, remote engineering team, perform research to define user personas, communicate and collaborate with stakeholders to test and refine user personas and design concepts, and manage the UX design workflow in the context of a larger project development project. The successful candidate will be able to establish, articulate, and drive a user-focused vision, communicate effectively across technical and nontechnical teams, organize and present complex data in a simple and compelling way, evaluate the usability of competing interface designs, and analyze and document user needs. The position typically requires a minimum of 12 years of related experience with a bachelor's degree, eights years and a master's degree, or five years and a PhD . . . see more at Jobs.isa.org.

Lead cybersecurity attack and penetration tester

Pfizer: This position in Groton, Conn., is for the technical lead for attack and penetration testing and red team assessments within Pfizer Digital Global Information Security. Responsibilities include performing and coordinating manual attack and penetration testing using the latest technologies, leading and performing assessments, researching new security threats, managing and maintaining security testing frameworks, and mentoring newer team members. A bachelor's degree in a technical field, five or more years of experience managing security and operational services, and three or more years in pharmaceutical or another regulated industry is required. ITILv3 certification and security certifications (CISSP, GIAC, CEH) are preferred . . . see more at Jobs.isa.org.

Senior software engineer

HSBC: This engineer in Pune, India, will develop a technical platform to support the adoption of quality engineering initiatives across global IT, work collaboratively with various stakeholders in the evaluation and implementation of emerging group standard tooling, and provide consulting support to IT teams across the group on quality engineering practices. The position requires hands-on experience in designing and developing platforms and process automation, especially for large-scale and complex banking applications and architectures . . . see more at Jobs.isa.org.

Completely automate and eliminate operators?

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 travels globally to attend automation events and regularly provides news reports, observations, and insights here and on Automation.com.

Completely automate and eliminate operators? I believe the answer is obviously "no," because well-trained operators provide an advantage by ensuring efficient and safe operations of complex process plants. The majority of those in operations management agree good operating people are valuable.

Automating and clearly documenting functions that are well defined and deterministic enable operators to focus on the most important tasks, problems, exceptions, and unexpected issues. Automation professionals can take advantage of ISA 106 to achieve these goals.

The ISA 106 models define how to capture information about physical assets, from the enterprise level down to an individual device, and the requirements that define a procedure. They establish the functional requirement for the automated procedure and tie these requirements directly to objects in the physical model. The implementation module defines a set of ordered tasks, which may have their own subtasks to perform step-by-step actions in a defined order. There are three elements contained within each task: (1) command: something to trigger the individual action; (2) perform: do the action(s); and (3) verify: confirm successful completion of the task.

Each task's command-perform-verify sequence can include a mix of automated and human operations as appropriate for the specific assignment. For example, a human may need to verify if an automated task has been performed correctly, or vice versa. After each command has been performed and verified, notification is sent to the next task in sequence.

Larger activities, such as plant startup or shutdown, are important, but the same tools can be used for more routine procedures, such as isolating and starting up a redundant pump system, performing online maintenance of a piece of equipment, or even something as "simple" as performing an in-line valve performance test; all of which normally require communication with someone physically at the asset to verify, or in some cases manually intervene in, the process.

Procedural automation can be used to capture and share corporate knowledge, including best practices, and to minimize errors with a resulting decrease in incidents, improved safety, and higher throughput. This is particularly important with an aging workforce and the difficulty in finding experienced operators.

Procedures represent the knowledge necessary to operate a system and are critical components of continuous operations. Historically, procedures have been executed by humans reading from a manual, checklist document, or a static display. The ISA 106 technical report describes the concepts by which procedures are integrated into the basic process control system (BPCS).

The intended audience for the document is technical and operations managers and engineering personnel who are responsible for the operation or automation of continuous process operations, members of engineering departments of owner/operators, engineering personnel of engineering and procurement companies, automation vendors and system integrators, and other process engineering practitioners.

Safety

Safety statistics show the majority of incidents not related to outright mechanical failures happen during abnormal situations, primarily unit startups and shutdowns. For example, the Kern Oil Refinery fire in January 2005 occurred during a crude unit startup, and the BP Texas City disaster in March 2005 took place during the restarting of a hydrocarbon isomerization unit. Unfortunately, there are many more examples.

The recipe for disaster is when an infrequent operation is required, but the key individuals are not available, leaving inexperienced operators to follow inadequate or incorrect instructions. Something can get out of control, leading to an abnormal condition with the undesirable outcomes of equipment damage, environmental release, injuries and fatalities. Procedural automation benefits are:

- improved safety
- improved startups and shutdowns to improve efficiency and throughput
- efficient transitions to increase production and quality
- improved disturbance recovery
- capture and retention of "tribal" knowledge
- improved communications with common definitions and terminology

By applying ISA 106, a single process plant, a complete facility, or even an entire company can achieve significant improvements in operational efficiency and safety.

For more information, visit www.isa.org/isa106. For information about the ISA106 committee, contact Charley Robinson, ISA standards, crobinson@isa.org. ■

2020 Analysis Division Symposium

26–30 April

Training: 26 & 30 • Conference: 27-29

This annual event is recognized as the outstanding forum for discussions of new and innovative analytical techniques, developments, and applications.

Topic areas include:

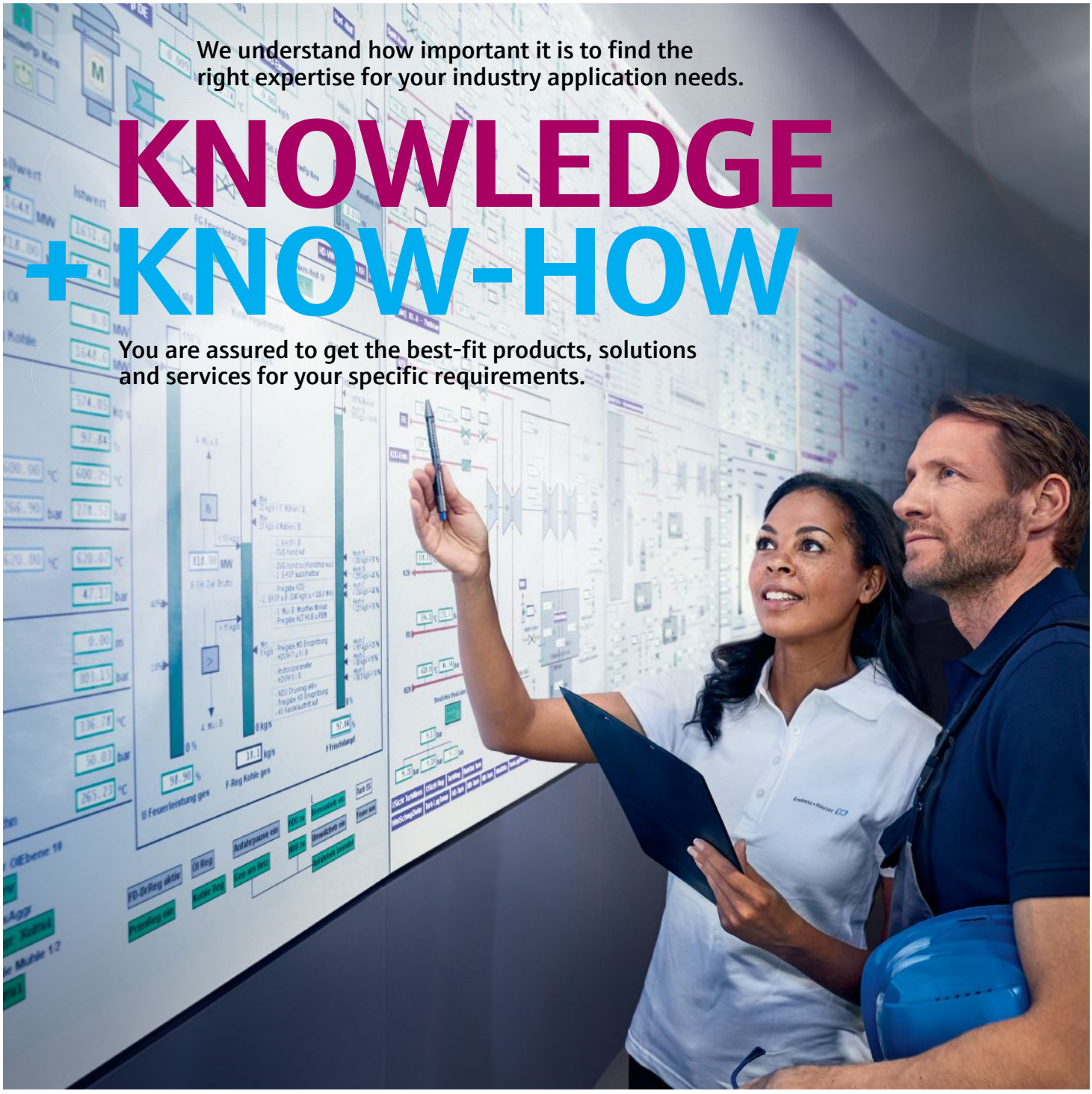
- Chemical Analyzers
- Gas Detectors
- Systems Integration
- Sampling Systems
- Physical Properties

Venue:

Long Beach Convention & Entertainment Center
Long Beach, CA, USA

International Society of Automation
Setting the Standard for Automation™

www.isa.org/ad

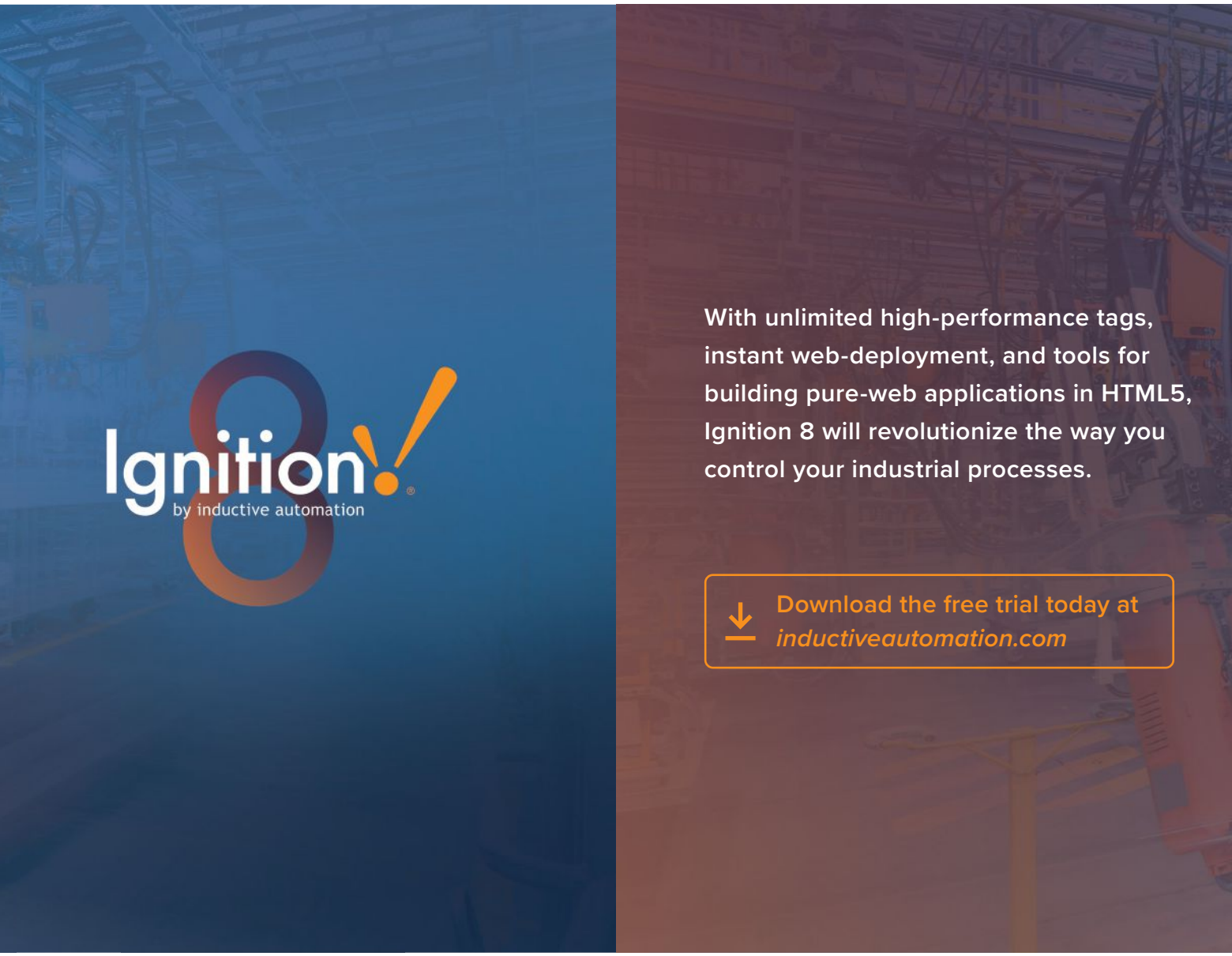


Customers around the world trust us when it comes to process automation. Our shared goal is plant safety, availability and efficiency. We are with you every day, everywhere.

People for Process Automation

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

Endress+Hauser


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

January/February 2020

InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

1945 ISA 2020

- Predictive maintenance analytics
- Data science for HAZOP studies
- IIoT edge computing
- Track and trace systems
- Industrial cybersecurity product spotlight

www.isa.org/intech

DCSNEXT®

Don't replicate. Innovate.

THE OPTIMAL DCS MIGRATION PROCESS.

50+ MIGRATIONS PER YEAR ACROSS VIRTUALLY ALL INDUSTRIES AND PLATFORMS.

Because every enterprise is unique, each DCS solution identifies your specific requirements in a comprehensive four-step approach.

Define Your Process and System Boundaries
Investigate and Collect Data
Analyze Data
Plan the Solution

Our platform independence allows us to select the right system without bias. The right system, implemented through the best process, by the most talented team of experts, ensures that your operations become safer, more efficient, more reliable, easier to maintain and easier to use.

MAVERICK™ TECHNOLOGIES

A Rockwell Automation Company

Learn more about our DCSNext solution

mavtechglobal.com/dcsnext