

AUTOMATION **2023**

JULY 2023 Volume 4

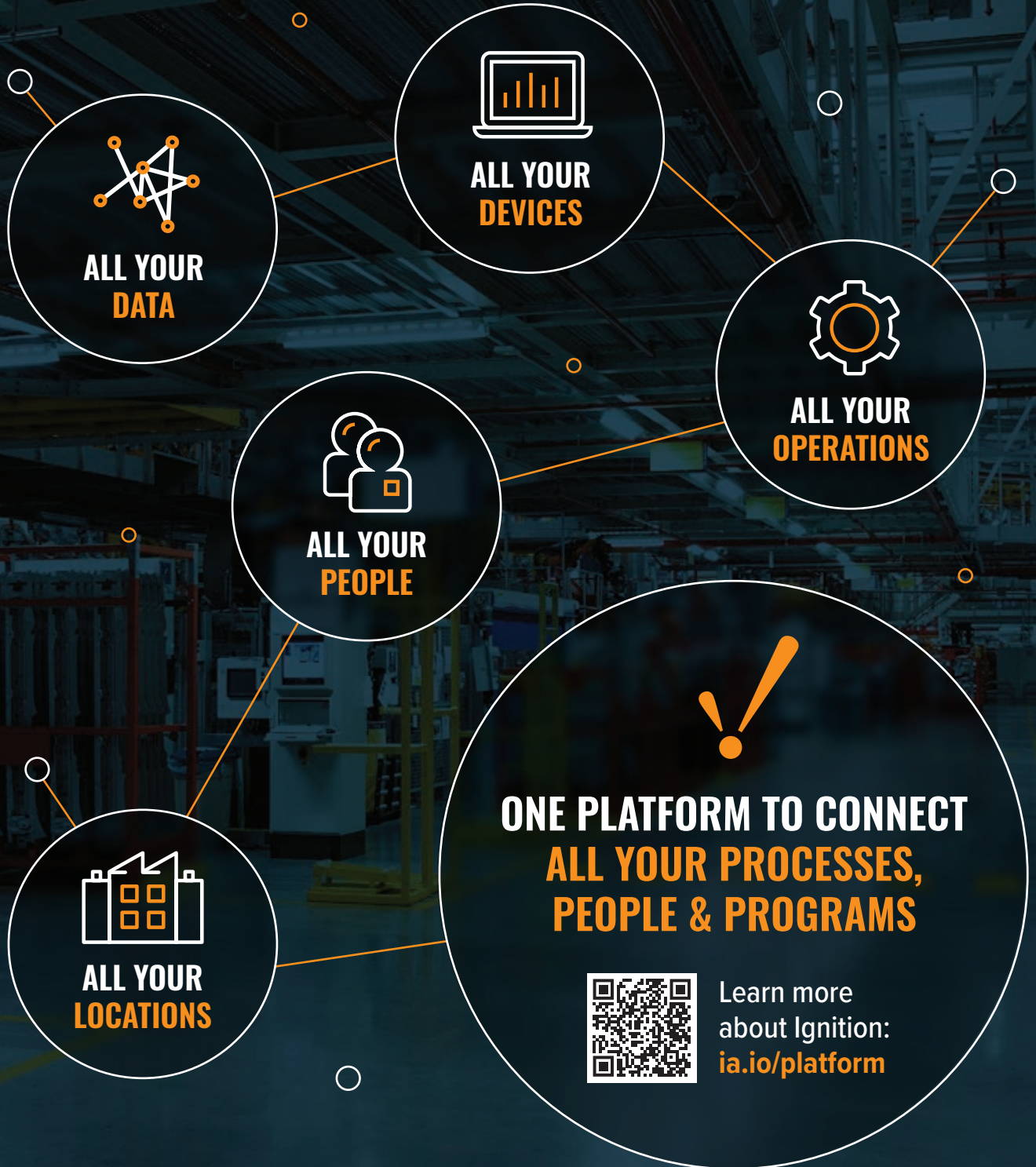
- ▶ Thriving Amid Disruptive Innovation
- ▶ Advanced Manufacturing Automation Strategies Open Up
- ▶ Transformative Technologies Enable Innovation

INSIDER INSIGHTS
from Technology Suppliers

8th Annual Industrial Automation & Control Trends Report

Connect The Dots With Ignition!

The Unlimited Platform for Total System Integration





We offer process application expertise through our products, solutions and services.

SUPPORT + SUCCESS

You optimize your process for maximum safety, reliability and efficiency, with minimum impact on the environment.

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

70
years

The pulse of
measurement
technology

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

Endress+Hauser 

8th Annual Industrial Automation & Control Trends Report

Buffeted by labor shortages, supply chain issues and more, industrial automation professionals face challenges like never before. At the same time, the rise of hyperautomation, robotics, digital architectures, and open industrial standards promise space and support for innovation to thrive.

“The world of manufacturing is an exciting, ever-changing landscape that is continually being driven to new heights of productivity, efficiency, and quality through the application of innovative technology,” says [Bill Lydon](#), a 40-year industry executive, editor, consultant, and commentator. Here in our 8th annual Industrial Automation & Control Trends Report, Bill reveals how advances in more than a dozen technology areas are enabling digital transformations and corporate resilience. Supplementing Bill’s thoughts on the trends driving industry forward is our Insider Insights section. This is a collection of views from technology vendors who are helping to empower manufacturers and shape the future of industrial automation.

Many of the trends cited in this special edition of the AUTOMATION 2023 ebook have long been simmering but now seem poised to break through. Take some time to review them and decide which might propel your company to succeed in new ways. Drop us a line on social media or via email to let us know what resonates. [Bill Lydon](#) and all of us at Automation.com, the news and media subsidiary of the International Society of Automation, would love to hear from you.

Lynn DeRocco

Automation.com Managing Editor

lderocco@automation.com

About AUTOMATION 2023

The AUTOMATION 2023 ebook series covers Industry 4.0, smart manufacturing, IIoT, cybersecurity, connectivity, machine and process control and more for industrial automation, process control and instrumentation professionals. To subscribe to ebooks and newsletters, visit: www.automation.com/newslettersubscription.

AUTOMATION 2023 is published six times per year (January, March, May, July, September, and November) by Automation.com, a subsidiary of International Society of Automation (ISA). To advertise, visit: www.automation.com/en-us/advertise.



groups/68581

automationdotcom

@automation_com



company/internationalsocietyofautomation

InternationalSocietyOfAutomation

@ISA_Interchange

Renee Bassett, Chief Editor
rbassett@automation.com

Chris Nelson, Advertising Sales Rep
chris@automation.com

Richard T. Simpson, Advertising Sales Rep
rsimpson@automation.com


Gina DiFrancesco, Advertising Sales Rep
GDifrancesco@automation.com



Advertisers Index

AUTOMATION 2023 VOLUME 4


1898 & Co.56


aDolus Technology 53


AutomationDirect6


Axiomtek USA..... 41


Beamex38


Beckhoff Automation7


Copia..... 15


Endress+Hauser3


Festo10


HiveMQ..... 26


ICONICS & Mitsubishi Electric.....20


Inductive Automation2

AUTOMATION TRENDS REPORT


IPR Technology..... 44


MAVERICK Technologies &
Rockwell Automation17


Moore Industries.....9


Moxa..... 23


Opto 2247


Prime Technologies, a TMA
Systems Company 35


SEW-EURODRIVE.....14

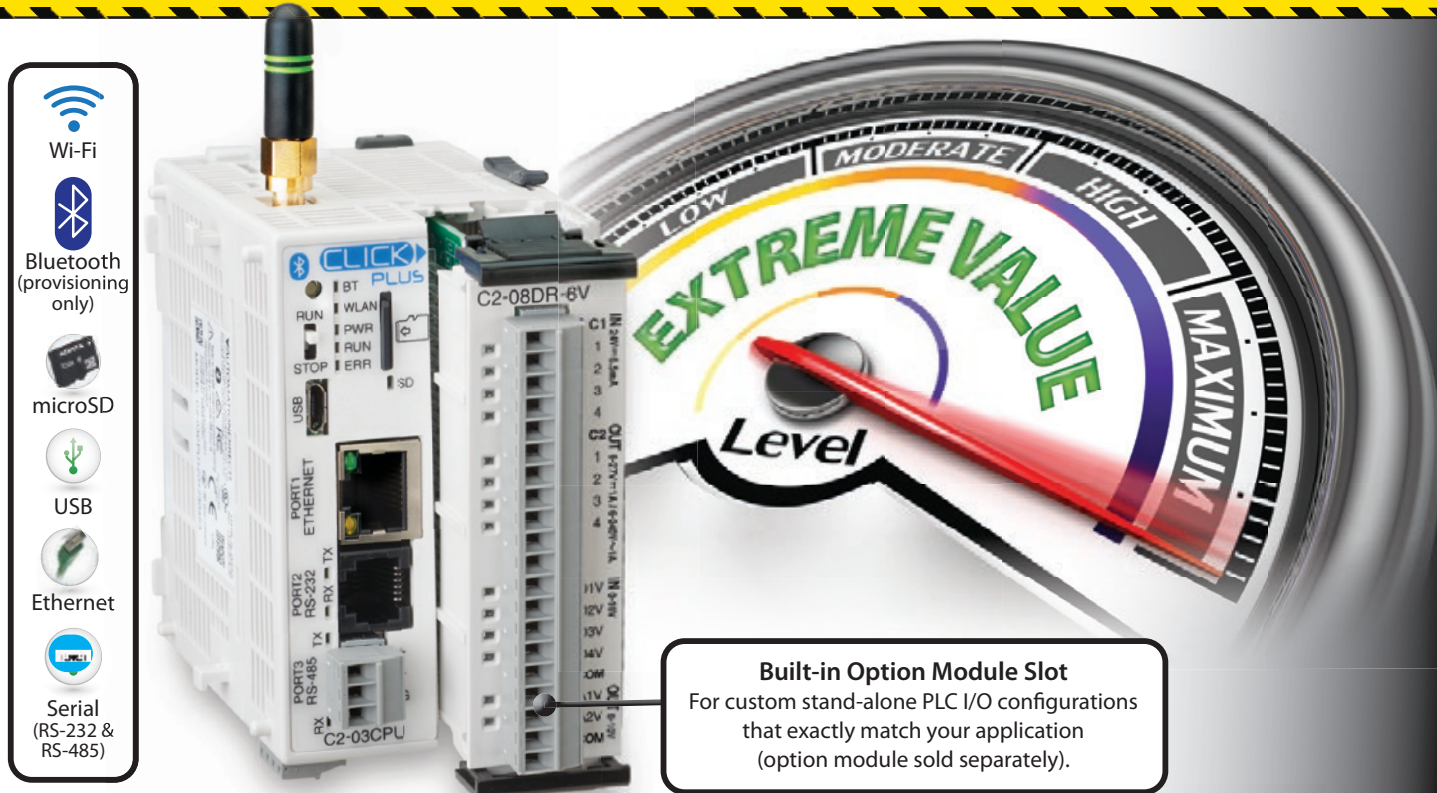

SICK..... 13


Skkynet..... 50


TXOne Networks 29


Yokogawa..... 32

CAUTION VALUE OVERLOAD!



Wi-Fi

Bluetooth (provisioning only)

microSD

USB

Ethernet

Serial (RS-232 & RS-485)

Built-in Option Module Slot
For custom stand-alone PLC I/O configurations that exactly match your application (option module sold separately).

CPU units starting at only **\$97**

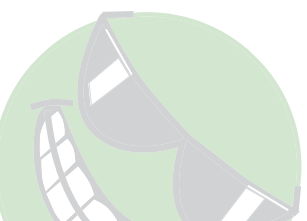
CLICK PLUS PLCs provide the same simple, practical control the CLICK PLC line is known for but with some surprising bells and whistles. Data logging, Wi-Fi connect-ability, MQTT communication, and increased security measures are just a few of the impressive features offered with the CLICK PLUS PLC series.

Using the same **FREE** streamlined PLC programming software as its predecessor, CLICK PLUS PLCs provide straightforward, no-learning-curve programming. Combine that with a starting at price of just \$97.00 and the CLICK PLUS PLC is undoubtedly the unmatched value leader!



Use any CPU with option module(s) as a complete PLC for small systems or expand the I/O with stackable I/O modules for larger applications.

www.CLICKPLCs.com



Order Today, Ships Fast!



AUTOMATIONDIRECT.com
1-800-633-0405

the #1 value in automation

*See our Web site for details and restrictions. © Copyright 2022 AutomationDirect, Cumming, GA USA. All rights reserved.

Inside the cabinet? Outside? You choose with our powerful, ultra-compact IPCs



www.beckhoff.com/c6015

www.beckhoff.com/c7015

Small enclosures. Harsh environments. Evolving requirements. As engineers, we know these factors must be addressed constantly. Every new machine presents unique challenges and opportunities to innovate. So our ultra-compact Industrial PC series gives you freedom to choose the perfect controller for every machine. Maybe it's the C6015 with dimensions of just 82 x 82 x 40 mm and outstanding installation flexibility. Or maybe your machine calls for the IP65/67-rated C7015 for cabinet-free installation. All IPCs in this series deliver powerful control to simultaneously run automation, HMI, edge computing/IoT and other communication – all on one controller. They make ideal gateways to the cloud and support flexible I/O system expansions – inside or outside of the cabinet. The choice is yours.

New Automation Technology

BECKHOFF

Table of Contents

AUTOMATION 2023 VOLUME 4

AUTOMATION TRENDS REPORT

4 INTRODUCTION

5 ADVERTISERS INDEX

FEATURES

59 Thriving Amid Disruptive Innovation

By Bill Lydon, Automation.com

Companies that can leverage disruption and choose innovation over entrenchment position themselves for success.

63 Advanced Manufacturing Automation Strategies Open Up

By Bill Lydon, Automation.com

Pushed by tech-savvy users and other trends, manufacturing management systems are shifting toward open, secure, and interoperable control and automation architectures.

72 Transformative Technologies Enable Innovation

By Bill Lydon, Automation.com

Advances in 14 technology areas are empowering digital manufacturing transformations.

Designing safety loops? The solution may be simpler than you think



Designing safety loops to meet safety standards and budget constraints can be a challenge. The exida approved SIL 3 capable **SLA Multiloop Safety Logic Solver and Alarm** meets this challenge with simple programming and I/O versatility to reduce complexity and cost of your safety instrumented systems.

The simple solution to complex problems



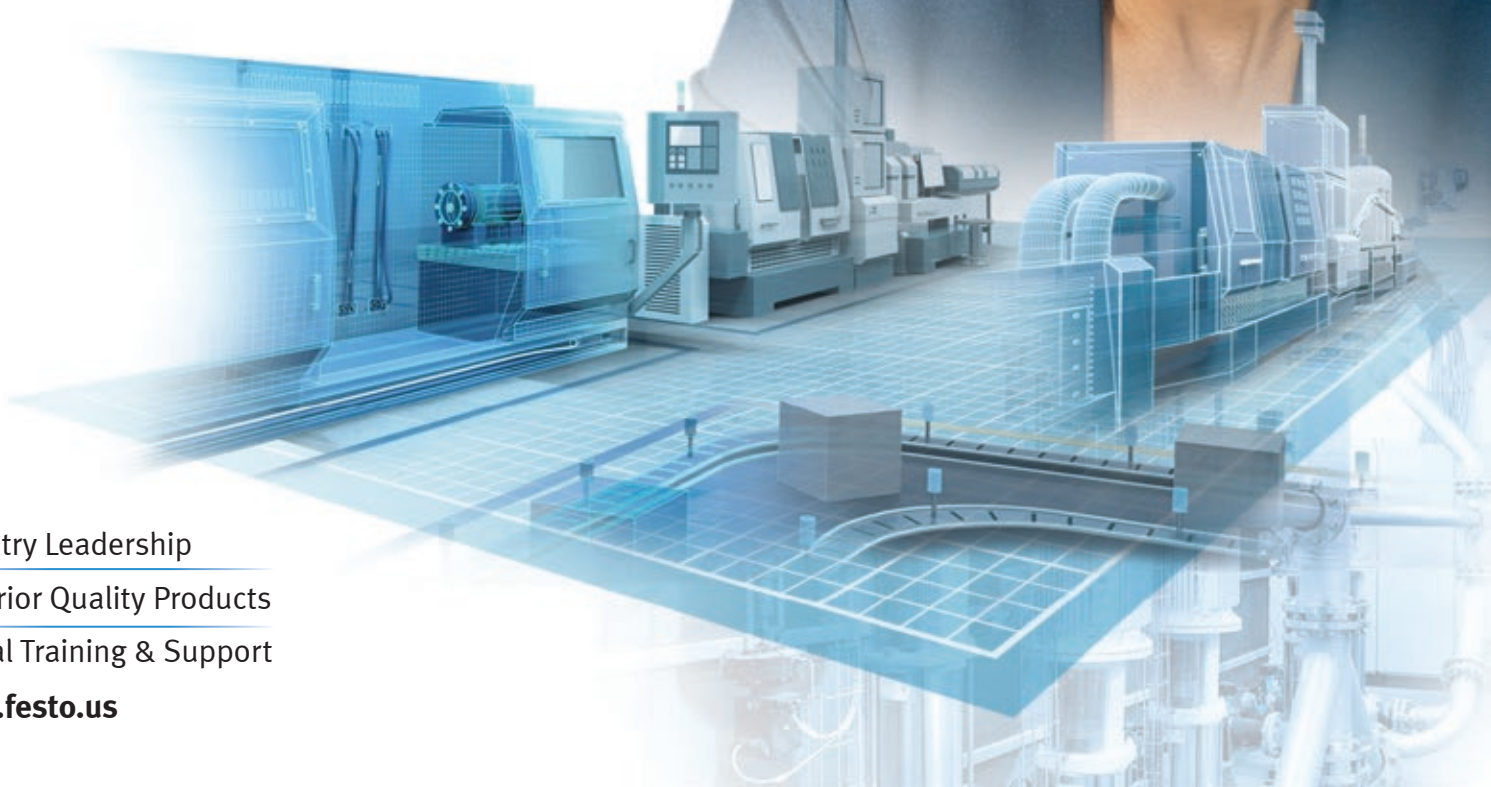
Learn more about the Moore Industries
SLA Safety Logic Solver and Alarm
Call 800-999-2900
or visit www.miinet.com/SLA



FESTO

Innovate today for a new tomorrow

Realize your vision with Festo's approach
to smart automation. Partner with Festo today.



Industry Leadership

Superior Quality Products

Global Training & Support

www.festo.us

Table of Contents

INSIDER INSIGHTS

AUTOMATION 2023 VOLUME 4

AUTOMATION TRENDS REPORT

- 18** The Ticket to the Future of Process Automation
By Carol M. Schafer, MAVERICK Technologies & Rockwell Automation
- 21** No/Low Code SCADA Trend Benefits the End User
By Thomas J. Burke, ICONICS & Mitsubishi Electric
- 24** Choose the Right Switch for Every Application
By Felipe Costa, Moxa
- 27** Developing a Unified
Namespace to Drive Operational
Improvement
By Dominik Obermaier, HiveMQ
- 30** More IT-based Cyber Attacks
Likely to Affect OT Systems
By Mars Cheng, TXOne Networks
- 33** Reinforcement Learning AI—A
Disruptive Technology for
Manufacturing
By Kevin Finnan, Yokogawa
- 36** Navigating Regulatory
Compliance in the Food &
Beverage Industry
By Don Wildauer, Prime Technologies,
a TMA Systems Company



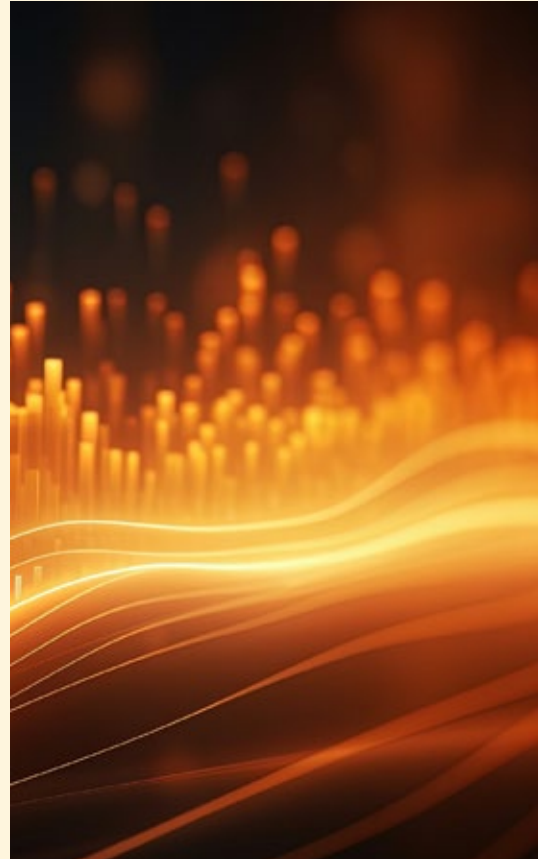
Table of Contents

INSIDER INSIGHTS

AUTOMATION 2023 VOLUME 4

AUTOMATION TRENDS REPORT

- 39** Data Quality: The Key to Successful AI-based Process Control
By Heikki Laurila, Beamex
- 42** Unleash the Power of Data: AI at the Edge
By Ryan Chen, Axiomtek USA
- 45** Safeguarding Assets and Networks, and Ensuring an Effective Cybersecurity Response
By David Jennings, IPR Technology
- 48** Low-Code/No-Code Development Tools
By Terry Orchard, Opto 22
- 51** Cumulative Change: From OPC Classic to OPC UA
By Xavier Mesrobian, Skkynet
- 54** VEX and Its Relation to SBOMs and Software Supply Chain Security
By Eric Byres, aDolus Technology
- 57** Cybersecurity Risks for Plant Safety
By Tim Gale, 1898 & Co.





SICK

Sensor Intelligence.

BRINGING AUGMENTED REALITY TO THE WORLD OF ROBOTICS

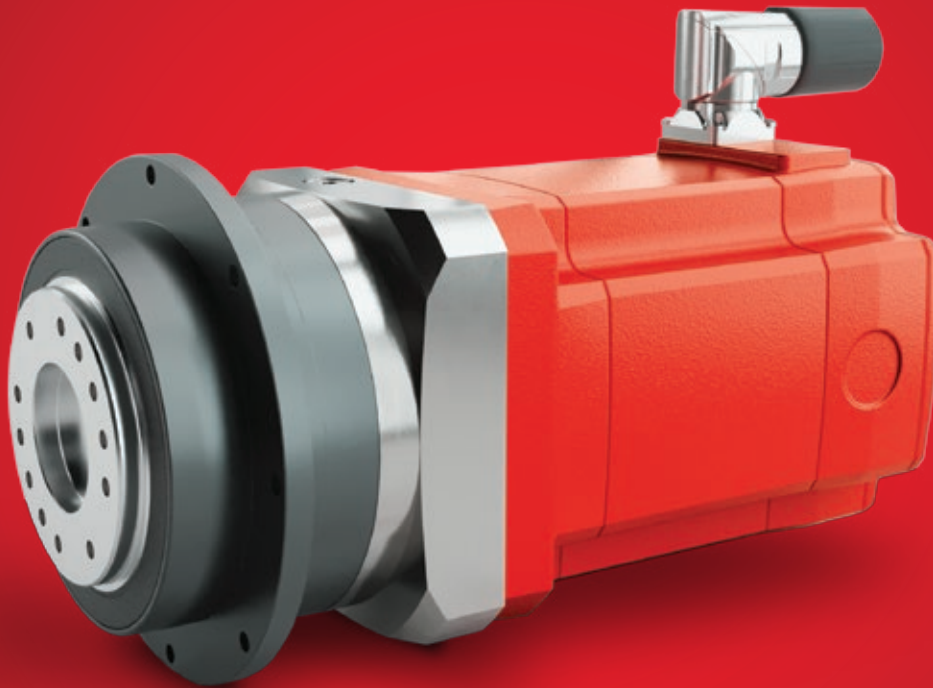
Robotic solutions are in greater demand than ever before in many areas of the value chain in industry – from production and quality assurance to packaging and shipping.

The SICK Augmented Reality Assistant (SARA) app can be integrated into your robotics applications.

It turns almost any commercially available smart phone or tablet into a wireless diagnostic system and uses augmented reality technology for fast and targeted troubleshooting that minimize downtimes.

Contact us today and
learn more: info@sick.com

Precise. Powerful. Modular.



Servo motors and gear units from SEW-EURODRIVE

Servo motors and gear units from SEW-EURODRIVE offer a high degree of dynamics and performance with a compact design, making them excellent for confined spaces. Multiple frame sizes and torque ratings makes them the perfect fit in material handling, hoist and gantry applications, and a wide variety of machine automation applications. Their modular design allows for direct gear unit mounting without adapters or couplings. Pair that with the option of single-cable technology and you've got a flexible, precise servo drive solution.

Servomotor Guide
(PDF)



SEW
EURODRIVE

www.seweurodrive.com



Modern tools to standardize and streamline industrial automation

Vendor-agnostic, single platform to manage PLCs and control devices in development and in production

Git Version Control

- Track all changes to PLC code
- Visualize differences between versions
- Accelerate review processes
- Enable engineers to work simultaneously on the same codebase

Automated Backup & Change Detection

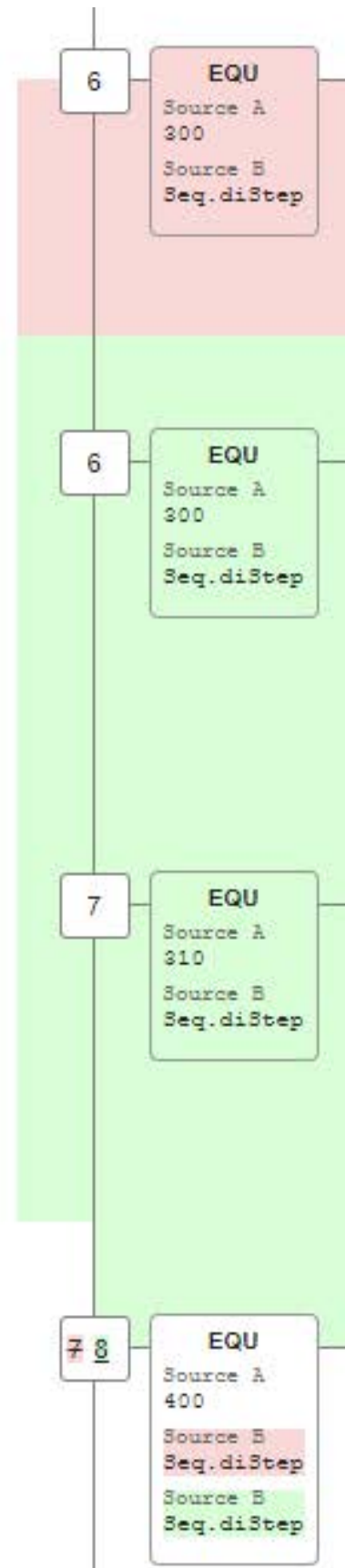
- Automatically back up running control programs, including PLCs, robotics, vision systems, and network switches
- Visualize the data in one central location
- Detect any unauthorized changes
- Visually compare code for quick troubleshooting and recovery

“...our senior engineers are saving up to a day a week because of faster code reviews. Plus, we're reviewing more frequently. We're catching more mistakes before they get deployed or tested.”

John Sullivan
Project Director
DMC Engineering

Copia renders industrial code from Rockwell Automation®, Siemens®, CODESYS®, Beckhoff®, Schneider Electric®, WAGO®, ABB®, and Lenze® in a web browser.

 Learn more and request a custom demo at www.copia.io



Insider Insights

Automation trends from technology suppliers helping to empower manufacturers and shape the future of industry.

NAVIGATING A SUCCESSFUL DCS MIGRATION IS CHALLENGING.

Successful DCS migrations don't happen by accident. They are accomplished through careful planning and thoughtful execution. "The Essential Guide to a Successful DCS Migration" is the culmination of years of experience and key learnings from today's thought leaders.

Take advantage of this free resource.

Get the guide

mavtechglobal.com/guide



MAVERICK™
TECHNOLOGIES
BY ROCKWELL AUTOMATION

The Ticket to the Future of Process Automation

By Carol M. Schafer, Lifecycle Services, Rockwell Automation & MAVERICK Technologies

It takes focused effort and dedicated resources to keep a continuous or batch process operation up and running. First, there's the considerable time and money spent on maintenance, repairs, and system modifications. Many process operations run at 100% capacity, squeezing everything possible out of every production run and pushing legacy systems to their limit. Then there's the severely stressed supply chain; skilled worker scarcity; and the pressure to decarbonize, meet tightening regulations, and make progress on aggressive corporate sustainability goals. It's unsurprising that many manufacturers are hard-pressed to explore modernization.

Digital transformation (DX) might sound enticing, but it's often challenging for plant managers to get a large-scale distributed control system (DCS) project funded and supported. They also know a project of this magnitude isn't without operational risk to daily production, quality, and profitability requirements. Many ask themselves if it's worth it as long as things are running.

However, there are risks to legacy systems, too, including:

- ▶ **Lack of flexibility.** Aging systems can't adapt quickly enough to changing

production needs or easily interface with modern software applications.

- ▶ **Unplanned downtime.** It's expensive to bring a continuous process back online. A single equipment failure could cost tens of thousands of dollars—and the repair doesn't even improve performance. When unplanned downtime involves a safety issue, the cost can be much higher.

Opportunity loss may be the highest expense of all.

- ▶ **Skilled resource scarcity.** Sticking with equipment several generations old can jeopardize future operations because fewer people know how it works.
- ▶ **Cybersecurity vulnerability.** Even the most modern facilities find cyber threats and protecting intellectual property (IP) challenging. On older systems, even installing the latest patches is problematic.
- ▶ **Sustainability and compliance.** Reacting to changing industry regulations and standards (sustainability, decarbonization, etc.) is more difficult using obsolete or older systems.

While all of these are inconvenient and cost money, opportunity loss may be the highest expense of all. Saving money to boost the bottom line is important, but transitioning to a new process automation system can also impact revenue streams. Automation systems must eventually evolve. The specialized knowledge that keeps old systems online can be ported into a new control system, reducing dependence on a few key employees, as well. Unless there is a lifecycle support process in place, plant performance will drop over time.

Conversely, DX offers benefits to:

Productivity. Modern process automation solutions use a state-of-the-art DCS. These scalable systems allow for fluctuation in production levels and product type. Asset utilization is improved, and predictive maintenance programs anticipate failure points. Also, innovations such as integrating process and power platforms improve diagnostics and consolidate networks, technology, and maintenance.

Data. DX extracts huge amounts of data from a control system and converts it to information that's vital to asset utilization, waste reduction, inventory control, and resource management. Paper-based manual processes are replaced by real-time reports displayed on high-performance human-machine interface (HMI) graphics that enhance operator awareness, keep workers safe, provide faster operation visibility, and allow better process parameters and I/O control.

Cybersecurity. With millions of threats against process industry infrastructure annually, hardening critical manufacturing

assets and bringing a facility into compliance with IEC 62443 provides IP and operations protection. Patches and updates can upload automatically and remotely.

Sustainability. Decarbonization, zero net impact, and similar are being mandated. Modern process control systems provide enterprise-wide views into environmental impact and business health with automated reporting and alarms that support regulatory compliance and reduce risk.

Other positive DX outcomes include well-documented operating systems, increased computing power, better connectivity, interoperability between systems, software simulation and digital twins, and benefits specific to an industry, operational needs, and future expansion plans.

Upfront planning, pre-engineering, and working with experts who know how to bring you the best return on investment (ROI) are the keys to a successful modernization project. Begin by gathering internal stakeholders and starting the conversation. Next, talk to an automation solutions supplier who knows your industry. An exciting world of maximized performance, flexibility, and sustainability is key to success now and for years to come.



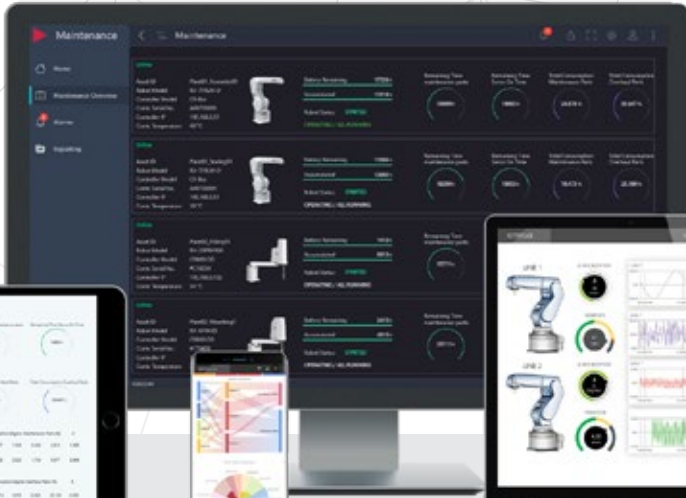
Carol M. Schafer is a global senior marketing manager for [LifecycleQ Services at Rockwell Automation](#). She has 30 years of experience in automation and controls marketing and industrial instrument and systems sales.

What is your manufacturing equipment trying to tell you?

ICONICS automation software combined with Mitsubishi Electric's hardware and predictive maintenance factory automation robot solutions helps manufacturers unlock key insights from their equipment that may otherwise go unnoticed, improving manufacturing operations, efficiency, productivity, and profitability.

Watch Demo

See the Predictive Maintenance Factory Automation Solution in Action



Interested in a Complimentary Digital Transformation Assessment?

Contact Us

No/Low Code SCADA Trend Benefits the End User

By Thomas J. Burke, Mitsubishi Electric

Far too often, companies needing an automation system become locked in with the system integrators (SIs) hired to design, install, and maintain their automation systems. SIs in turn commonly develop solutions, often due to limitations inherent within the tools they use, that are more technical in nature and include code (SI-developed software modules) to perform the required functions. An emerging preference, and one end users should request from their integration partners, is to deploy no/low code, ready-to-use solutions that a company can install and maintain with little to no outside help.

Reasons end users should consider no/low code solutions

No-code solutions are often considered better for end users for several reasons:

1. **Ease of use:** No/low code platforms provide a visual interface and drag-and-drop functionality that allow users to build applications or automate processes without writing code. This simplicity makes it accessible to individuals with limited programming knowledge, empowering them to remain domain experts and use a powerful tool to create their own solutions.

2. **Rapid development:** No/low code tools enable faster development cycles since these eliminate the need for traditional software development processes. Testing is both minimized and simplified as development is based on leveraging the combination of existing, richly developed features, rather than having to create from scratch.

Developing no/low code solutions requires SCADA vendors to give significant thought to the internal architecture of their products, building a modular and robust platform.



3. **Reduced dependence on developers:** With no/low code solutions, end users can take more control over their projects and reduce their reliance on professional developers.
4. **Lower costs:** No/low code platforms can significantly reduce development costs since these eliminate the need to hire expensive developers or outsource development work.
5. **Increased agility:** No/low code tools enable end users to respond quickly to changing business requirements.
6. **Empowerment and innovation:** No/low code solutions democratize application configuration, which enables individuals from various backgrounds to contribute their ideas and create innovative solutions.

No matter which type of vendor you choose, it is crucial to go with one that suits your company's current and future needs, and that delivers the highest-quality product and service. It is also important to consider how no/low code vendors design and produce their products. Developing no/low code solutions requires SCADA vendors to give significant thought to the internal architecture of their products, building a modular and robust platform. The platform must be high-performing, scalable, and reliable, and embrace techniques for high availability and redundancy. This technology requires 20 to 30 years of extensive expertise and experience across a broad range of market

applications to deliver the needed out-of-the-box functionality.

Digital solutions for factory automation

An example of a no/low code SCADA vendor with the required expertise and experience is [ICONICS](#), a group company since 2019 of global automation leader Mitsubishi Electric Corporation. The two companies have joined forces to offer a one-stop end-to-end solution with products that integrate extremely well. ICONICS software complements Mitsubishi Electric's hardware offerings, allowing data to be integrated from all other data sources and automation platforms to deliver a comprehensive view with insight into your operational environment. Together, ICONICS and Mitsubishi Electric provide a complete solution to empower customers to solve their automation challenges.



Thomas J. Burke is the global director of industry standards for [Mitsubishi Electric](#), leading strategic development and adoption of networking standards. He is also the

strategic industry advisor for the CCLink Partner Association (CLPA), responsible for strategic growth of the organization and adoption of the CC-Link IE TSN technology. Thomas is the former OPC Foundation president and executive director, where he pioneered the OPC Unified Architecture (OPC UA) as the foundation of information integration and interoperability.

Enjoy **1 Year**
Additional Warranty
And 5 Year
Standard
Warranty



Special promotion:
Now until Dec 31, 2023

EDS-2000/G2000-EL/ELP Series Industrial Unmanaged Ethernet Switches

Scan the QR code
to [learn more](#)



- 5 or 8 Ethernet port options
- SC/ST fiber models are available for the EDS-2008-EL Series
- Full Gigabit ports for the EDS-G2000-EL/ELP Series
- Supports 12/24/48 VDC input
- Microsecond-level latency
- High EMC resistance
- QoS and BSP* DIP switch configuration

*Quality of Service (QoS) and Broadcast Storm Protection (BSP) can be configured via DIP switches.

Choose the Right Switch for Every Application

By Felipe Costa, Moxa Americas

All industrial networks have specialized requirements, so selecting the right equipment is paramount for optimizing your automation and control systems. In the age of Industry 4.0, digital connectivity is critical for every manufacturer, OEM machine builder, and end user throughout the industrial trades. A networking backbone forms the core of all connectivity, but not all networks should be created equal. There is an increasing need for operational technology (OT) digital systems to connect with each other and with more traditional corporate information technology (IT) infrastructure. This creates additional capabilities as well as challenges.

For this and other reasons, there are a multitude of network switches and devices on the market so that users can select the exact components needed to meet their application requirements. However, with such a wide variety, choosing the right devices can be overwhelming. Selected components must support particular functions for each situation, such as access control and security capabilities, segmenting, routing, VLANs, and more. However, an abundance of unnecessary features can needlessly inflate equipment costs and increase configuration challenges. When industrial digital networking originally rose to prominence in the automation and

control system arena, serial-based media, often using proprietary protocols, were generally localized to the plant floor. These closed networks created difficulties for users by forcing reliance on particular vendors for support and future expansions.

More than ever, today's leading unmanaged switches provide flexibility for end users and machine builders, with compact size, rugged housing, support for multiple power inputs, and fiber optic connections.

For the most critical applications, [managed ethernet switches](#) and routers are preferred because of their intrinsic advanced capabilities, customized safeguards, and access control methodologies, along with Security Level 2 IEC-62443 cybersecurity certification. While these types of devices provide the greatest feature set, they require knowledgeable effort to set up and maintain them. However, that can be minimized by

utilizing [MXview One Series](#) software. When it is necessary to broker multiple remote connections and cloud data pathways, a tailored solution like [Moxa Remote Connect Suite \(MRC\)](#) is recommended.

For many new small- to medium-size localized machine automation applications, or for port expansion on the edge of existing networks, unmanaged ethernet switches might be selected because of their relative configuration simplicity and favorable price/performance ratio. These sorts of network topologies typically rely on other centralized and managed networking elements that are already in place for an uplink. More than ever, today's leading unmanaged switches provide flexibility for end users and machine builders, with compact size, rugged housing, support for multiple power inputs, and fiber optic connections.

Another option that is gaining traction for these types of industrial applications are smart ethernet switches, which provide advantages from both managed and unmanaged switches. Smart switches provide basic security features, performance, diagnostics with statistics and network redundancy, and other capabilities. Although they are not as sophisticated as managed switches, they do offer a middle-of-the-road approach to switch selection.

Years ago, automation and control systems often ran on their own separate networking "islands," but in today's connected world, this is no longer an option. Ethernet switches are now essential devices for OT applications and for integration with IT systems. The need for



tough, high-performance, and cybersecure network switching devices has never been greater.

A wide portfolio of managed and unmanaged switches is available so that users can ensure reliable communication at the level of security and configuration simplicity that best suits their application. Managed options are sometimes required to robustly secure the network, but unmanaged switches are often preferred, particularly when increasing network device and port count on previously secured networks.



Felipe Costa is the cybersecurity director, official ISA/IEC-62443 industrial cybersecurity instructor and cybersecurity expert certified at ISA and product marketing manager—networking & cybersecurity at [Moxa Americas](#). Felipe has presented and published articles all over the world, including at the NASA Artificial intelligence Congress in the United States of America. With over 18 years of experience in the industrial sector while dealing with a wide array of technologies and products, Felipe is dedicated to developing mission-critical solutions that include cybersecurity by design.

The Enterprise MQTT Platform for Industry 4.0

HiveMQ is the enterprise MQTT platform that lays a powerful foundation for Industry 4.0. It solves data connectivity and interoperability challenges by providing a secure, reliable, and scalable data abstraction layer between OT and IT systems. HiveMQ helps manufacturers achieve digital maturity by integrating data from factory machines, systems and applications to enterprise and cloud platforms, enabling advanced data processing and analytics use cases.

Trusted by over 130 customers worldwide



Business Critical Reliability:

Operate mission-critical systems reliably 24/7 with zero message loss and redundant clustering technology.



End-to-End Security:

Ensure applications and data meet the highest security standards with end-to-end encryption and configurable security controls.



Scalability to Support Growth:

Add any number of sites and scale to millions of connected devices seamlessly with a linear design for scalability



Observable Insights:

Troubleshoot and keep all factory systems running as planned with tools and metrics for transparency and observability.



Flexible Integration:

Focus on your core business instead of using developer resources with OT-IT data integration into enterprise applications and infrastructure like Apache Kafka.



Simple-to-Deploy:

Achieve rapid time-to-value with a platform that is flexible enough to deploy on-premise, in any cloud, or via the fully-managed and feature-rich HiveMQ Cloud offering.



Developing a Unified Namespace to Drive Operational Improvement

By Dominik Obermaier, HiveMQ

In modern manufacturing, operational excellence requires seamless exchange of data between siloed systems, often the biggest challenge for businesses shifting to data-driven decision-making. Unified Namespace (UNS) offers a compelling solution that is gaining speed by standardizing data structures. By centralizing data in a single hub, UNS facilitates a unified approach to problem-solving and process optimization, with the potential to revolutionize Industrial IoT.

Traditional manufacturing operations (Figure 1) often involve multiple isolated systems that hinder data sharing and analysis. The client-server architecture has many integration points, couples devices, and leads to growing complexity when use cases scale.

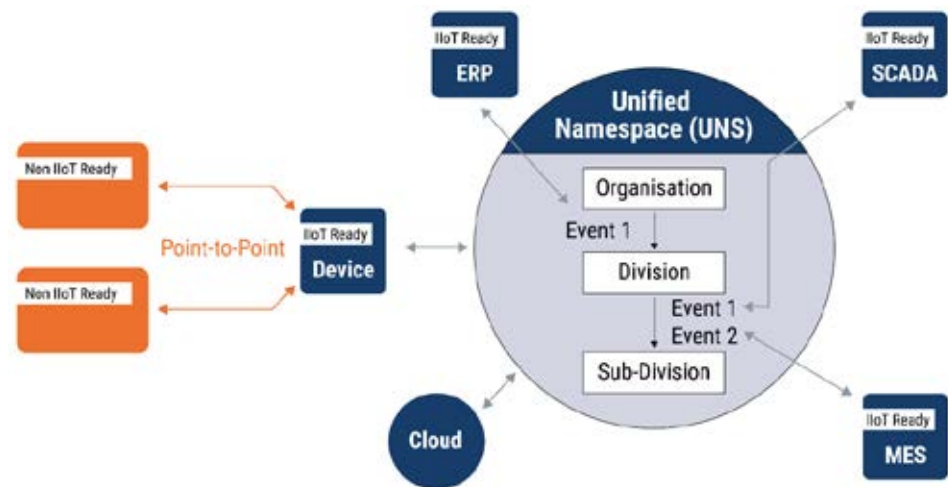
By centralizing data in a single hub, UNS enables accessibility and facilitates collaboration, promoting a unified approach to problem-solving and process optimization.

Besides the associated high costs, traditional industrial data architectures create data gaps, technical debt from point-to-point connections, and lack of scalability. A paradigm that draws from a modern distributed architecture addresses these challenges.



Figure 1. Data movement in a traditional industrial architecture.

Figure 2. Data movement using the Unified Namespace (UNS) concept.



UNS (Figure 2) abandons data silos across technology stack layers and centralizes data, making it readily available to any system at any given time for a single source of truth. Rather than keeping data siloed within the various industrial processes and manufacturing systems, companies can organize it in a common language and data platform for easier data-driven improvements across the business.

Creating a UNS requires an open architecture that uses a standard IIoT protocol such as MQTT and MQTT Sparkplug, which make it easy to swap or add components from different vendors into the UNS data ecosystem. The data transfer mechanism must be lightweight and report by exception, which MQTT satisfies to ensure data is only published upon change. The architecture must also be edge-driven, meaning data is pushed into the UNS by an MQTT broker at the edge of the network as opposed to collecting modeled machine data from various intermediary sources.

The HiveMQ MQTT Platform seamlessly satisfies the requirements and can help any

industrial company implement a UNS with a reliable, scalable and secure MQTT platform. The result is one digital infrastructure hub whereby all components communicate using a standard protocol and point to a central repository of information with a hierarchical enterprise structure.

Organizations that implement a UNS can then avoid disruption as they continue to collect data from legacy equipment while deploying new smart assets. By adopting a common data infrastructure, any person working on the plant floor, any OT software system, or any enterprise IT system gets equal real-time access to contextualized operational data to drive better decision-making and operational improvements.



Dominik Obermaier is CTO and co-founder of [HiveMQ](#), and a frequent speaker on IIoT, MQTT, and messaging. He is a member of the OASIS Technical Committee, part of the standardization committee for MQTT 3.1.1 and MQTT 5, and the co-author of the book *The Technical Foundations of IIoT*.



✓ Protected

✓ Protected

✓ Protected

Industrial Cybersecurity. **Simplified.**



Keep the Operation Running

Copyright © 2023 TXOne Networks. All rights reserved.

txone.com

More IT-based Cyber Attacks Likely to Affect OT Systems

By Mars Cheng, TXOne Networks

As information technology (IT) and operational technology (OT) continue to converge, attackers have more factory OT network entry points, which means more vulnerabilities to safeguard against.

According to the [Trend Micro Security Predictions For 2023](#) report produced in collaboration with TXOne Networks, an upward trend in IT-based cyberattacks inadvertently affecting OT systems connected to IT networks is predicted—in addition, revealing OT systems as underutilized attack vectors through which malicious actors can move between OT and IT environments.

In 2021, Trend Micro revealed that 61 percent of automated manufacturers have experienced cybersecurity incidents, many causing downtime. TXOne Networks analyzes the global trend of automated factories to identify potential threats and to propose an adaptive cybersecurity solution for industrial control systems (ICS).

Potential threats to automated factories

The Industrial Internet of Things (IIoT), industrial robots, augmented reality (AR), and additive manufacturing (AM) are among the targets of cyber threats.

IIoT. The adoption of IIoT technologies were expedited during the pandemic to keep operators safe while maintaining production. However, this introduces the potential to expose vulnerabilities—especially in OT environments—that were once air-gapped. Wireless is also a problem, as endpoint devices use WirelessHART or BLE to upload endpoint information to the cloud via a network gateway.

61% of automated manufacturers have experienced cybersecurity incidents, many causing downtime.

Network defense solutions can learn the trusted behavior of each piece of equipment. When the trusted behaviors of each device are known, attackers can be prevented from carrying out further attacks.

Industrial robots. Robots are becoming more autonomous and mobile, collaborating with each other (and with humans) to perform physical operations in many large-scale manufacturing facilities. Industrial robots consist of a controller, robot, and workpiece. Engineers often upload or

download extension kits. If the content is not inspected, the engineer may unintentionally download infected kits, execute them, and threaten the network.

If equipment is exposed to a public network, attackers can exploit vulnerable network protocols. In some cases, public downloadable off-line programming (OLP) software can modify controller parameters, production logic, or robot status to tamper with factory production outcomes. In 2021, a cyber intruder penetrated a Florida water treatment facility twice in one day and was attempting to poison the supply when detected.

AR. Improperly stored AR devices may allow the theft of factory data and the destruction of cloud data. When suppliers or technicians are required to enter a factory area, AR devices that are not adequately protected by physical security can be—and have been—stolen, along with confidential factory information, which may include anything from production processes to pharmaceutical or food ingredients. AR devices are considered trusted sources. In the wrong hands, they can be used to access enterprise cloud data and expand the impact throughout the factories.

AM. Many manufacturing plants are introducing AM technology to manage supply chain issues, particularly in automated factories related to aerospace, automotive, or medical industries. AM technology is a computer-controlled process of creating a 3-D object by depositing materials one layer at a time. SANS researchers have found that thousands

of insecure AM devices are exposed to the public network and can be controlled without authorization.

When most AM devices used unencrypted files (G-code format) to control printing, attackers have the opportunity to steal confidential product information. Malicious firmware can make the device persistent, causing excessive heating that can cause large-scale disasters in factories.

Looking ahead

TXOne Networks believes that effective cybersecurity solutions that ensure the operation, reliability, and digital safety of ICS and OT environments are best achieved through the OT zero trust methodology, as well as security inspections, “allow” lists, network segmentation, and virtual patching reinforcement.

To learn more about protecting automated factories across the lifecycle of your equipment, download TXOne Networks’ [OT Zero Trust Handbook](#).



Mars Cheng is a threat research manager at [TXOne Networks](#) leading the PSIRT and threat research team. He is responsible for coordinating product security and threat

research given his dynamic background and experiences in both ICS/SCADA and enterprise cybersecurity systems. Mars has directly contributed to more than ten CVE-IDs and three published pieces in Science Citation Index (SCI) applied cryptography journals.



Take Charge

To take charge and be sure your operations and system are in sync at optimal capacity, you need to be atop autonomy. And to get there, Yokogawa delivers resilient solutions for you, a process using our smart manufacturing and IA2IA (Industrial Automation to Industrial Autonomy), deploying OpreX as our true enabler to achieve total optimization throughout the supply chain. Integrating discrete systems in society, we move together with you toward the system of systems in which everything is intricately connected and goals are achieved beyond those of a single system. Yokogawa. Atop autonomy for the planet.

OpreX™

yokogawa.com/ia2ia/

The names of corporations, organizations, products, services and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation or their respective holders.

YOKOGAWA 

Co-innovating tomorrow™

Reinforcement Learning AI—A Disruptive Technology for Manufacturing

By Kevin Finnan, Yokogawa

A growing number of manufacturing organizations are adopting artificial intelligence (AI). In a 2021 McKinsey Global Survey, 56 percent of respondents said their organizations had done so—up from 50 percent the prior year. In the simplest definition, AI is the simulation of human intelligence processes by machines, particularly computer systems. AI has grown into a broad category that comprises several technologies, such as computer vision, machine learning (ML), natural language processing (NLP), and reinforcement learning.

Commanding the hype most recently has been generative AI, which builds upon NLP to analyze and generate language-based data, including text and speech. Released by OpenAI in November of 2022 as a research preview, ChatGPT was trained to generate humanlike text, allowing it to engage in a conversational manner and produce extensive content. (“Chat” denotes chatbot functionality and “GPT” is an abbreviation for Generative Pretrained Transformer, the AI model.)

By encompassing computer vision and other AI technologies, generative AI can create images and video, as well as audio and code. The technology appears poised to revolutionize industrial operations.

According to Verdantix, some use cases that are already leveraging generative AI are asset performance management, predictive maintenance, design optimization, and supply chain management.

While the content generation aspect would not appear appropriate for manufacturing automation or process control, another ChatGPT building block, reinforcement learning, is. Reinforcement learning AI uses neural networks and training through trial and error to make predictions. A reward model focuses the AI on optimal outcomes. According to the company website, OpenAI trained ChatGPT using Reinforcement Learning from Human Feedback (RLHF), which included substantial dialogue with people.

Reinforcement learning AI has, in fact, proven successful for direct control of a plant.

Experts in the manufacturing and process industries have estimated that more than 65% of process control loops are underperforming and up to 30% are operating in manual mode. For companies striving toward autonomous operations

with little or no human presence at plants, underperforming controls and manual operations have emerged as major issues.

In a 2021 global survey of end users conducted by Yokogawa, 42% of the respondents stated that the application of AI to plant process optimization would have a significant impact on industrial autonomous operations in the next three years.

Reinforcement learning AI has, in fact, proven successful for direct control of a plant. In March of 2023, ENEOS Materials Corporation and Yokogawa announced an agreement in which Factorial Kernel Dynamic Policy Programming (FKDPP), a reinforcement learning-based AI algorithm, will be officially adopted for use at an ENEOS Materials chemical plant. The agreement followed a successful field test in which a solution called autonomous control AI demonstrated a high level of performance while controlling a distillation column at the plant for nearly a year. This is the world's first example of the adoption of reinforcement learning AI for direct control of a plant.

While ChatGPT and FKDPP are achieving things that, until recently, were not possible, the ways they operate are very different. ChatGPT generates answers based on vast volumes of human-generated information that exists on the Internet. FKDPP, on the other hand, does not learn from anybody. It derives the optimal control method for complex situations by self-learning on a simulator based on the reward systems provided. It can accomplish this with as few as 30 trials.

The autonomous control AI controls distillation column operations that were beyond the capabilities of such existing technologies as proportional-integral-derivative (PID) loop control and advanced process control (APC). These had necessitated manual operations based on the judgements of experienced plant personnel. Even given ambient temperature variations up to 40°C, the autonomous control AI maintained stable control of the liquid levels and maximized the use of waste heat. Stability and high product quality prevailed throughout the year.

By eliminating the production of off-spec products, the autonomous control AI reduced costs in terms of feedstocks, fuel, and labor. While producing high-quality products that met customer standards, the autonomous control AI reduced steam consumption and CO₂ emissions, each by 40%. The autonomous control AI is able to resolve conflicting requirements, for example, by achieving the proper balance between reducing energy consumption while maintaining product quality. Ultimately, the AI solution enables alignment between management and operations.



Kevin Finnan is a market intelligence and strategy advisor at [Yokogawa](#). He has over 30 years of experience in a variety of vertical markets and has launched more than 40 products in automation and measurement technologies.



The leader with industry-proven calibration and maintenance asset management software

SCALABLE

Ideal for companies ranging in size from single users to enterprise firms

MULTI-LINGUAL

Works across languages to meet the needs of global organizations

CUSTOMIZABLE

Configure to meet the needs of organizational objectives

COMPLIANT & PRE-VALIDATED

Ensure compliance, even for industries with the strictest regulations

INTEGRABLE

Seamlessly integrate with various systems and applications

USER-FRIENDLY

Meet the needs of a range of users within an organization

For more than three decades, we have developed software and provided client services meeting the most demanding calibration and asset management challenges.

Schedule a demo today to learn how Prime Technologies' solutions can transform your operations.

sales@primetechpa.com | primetechpa.com

Navigating Regulatory Compliance in the Food & Beverage Industry

By Don Wildauer, TMA Systems

Regulatory compliance is of utmost importance in the food and beverage industry, as it helps protect consumer health, maintain product integrity, and promote fair competition. This particular sector is subject to numerous regulations and standards to ensure the safety and quality of products. As organizations grapple with stringent guidelines, embracing effective compliance strategies has become paramount to achieving sustainable growth and maintaining public trust.

Ensuring consumer safety

Regulations governing the food and beverage industry aim to safeguard public health, prevent foodborne illnesses, and maintain industry-wide quality standards. Compliance with these regulations is essential for businesses to gain consumer trust, avoid legal repercussions, and safeguard their reputation. Key regulatory bodies like the Food and Drug Administration (FDA), the United States Department of Agriculture (USDA), and the European Food Safety Authority (EFSA) have established stringent guidelines covering various aspects of production, labeling, packaging, and distribution. By adhering to strict quality control measures and maintaining thorough

documentation, companies can ensure the safety and efficacy of their products, earning the trust and loyalty of consumers.

Compliance with regulations related to fair trade, labor practices, and environmental sustainability is not only a legal requirement but also a way for businesses to demonstrate their commitment to social responsibility.

Meeting ethical standards

Regulatory compliance extends beyond product safety to encompass ethical standards. In recent years, there has been a growing emphasis on sustainability, responsible sourcing, and ethical business practices. Consumers are increasingly demanding transparency and accountability from companies and manufacturers. Compliance with regulations related to fair trade, labor practices, and environmental sustainability is not only a legal requirement

but also a way for businesses to demonstrate their commitment to social responsibility. By integrating these principles into their operations, organizations can build a strong brand reputation and gain a competitive edge in the market.

Embracing technology

Automation tools, data analytics, and digital solutions can streamline compliance processes, improve data integrity, and facilitate regulatory reporting. For instance, companies can implement advanced supply chain management systems that enable traceability and provide real-time visibility into the origin and movement of ingredients and products. Additionally, leveraging artificial intelligence (AI) and machine learning (ML) algorithms can help identify potential compliance risks and predict adverse events. Embracing technology-driven solutions not only enhances efficiency but also strengthens compliance measures.

Collaboration and knowledge sharing

With the complexity of regulations, it is vital for organizations in the food and beverage industry to foster collaboration and knowledge sharing. Industry associations, trade groups, and regulatory bodies can facilitate discussions, workshops, and conferences to exchange best practices and address common challenges. Collaboration with technology providers, regulatory consultants, and legal experts can also offer valuable insights and guidance to ensure

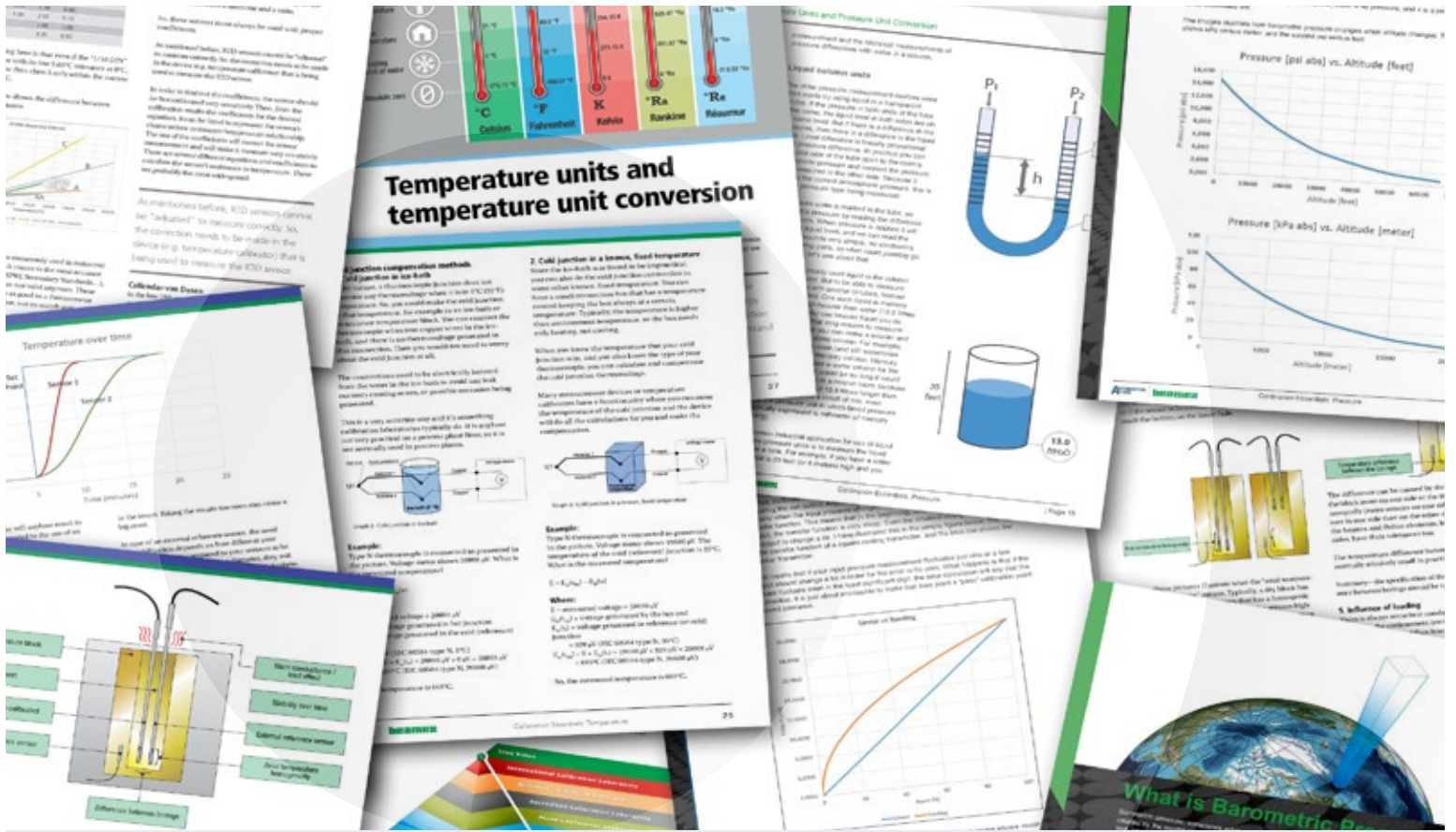
compliance. By building strong networks and sharing experiences, businesses can collectively navigate the complexities of regulatory compliance.

By prioritizing consumer safety, meeting ethical standards, and investing in technology, organizations in the food and beverage industry can not only comply with regulations but also enhance their overall operations and reputation. One piece of technology worthy of investment is Calibration Management Software (CMS). When organizations can adhere to calibration protocols that ensure accurate measurements throughout the manufacturing process, it not only extends the life of the company's assets but also builds consumer confidence. As businesses adapt to the evolving regulatory requirements, they can embrace compliance as a competitive advantage, driving innovation and ensuring the well-being of consumers and the environment.



Don Wildauer is the VP and general manager of [Prime Technologies at TMA Systems](#). Originally from Cherry Hill, New Jersey, Don has resided in the Valley Forge, Pennsylvania,

area for many years. He received a Bachelor of Electrical Engineering and Minor in Mathematics from Villanova University, and holds a Master of Management in Business Administration from Pennsylvania State University. Don brings more than 30 years' experience leading and growing global technology businesses. Prior to joining TMA Systems in 2022, he served as senior vice president at Prime Technologies.



CALIBRATION ESSENTIALS: PRESSURE

Unlock the secrets to calibrating your pressure instrumentation with our comprehensive 40-page guide. **PACKED WITH EXPERT STRATEGIES AND RESOURCES**, you'll gain access to everything you need to ensure accurate and reliable pressure measurements in your process. [Download your copy today.](#)



CALIBRATION ESSENTIALS: TEMPERATURE

In 64-pages this eBook is designed to help you understand the importance of accurate temperature measurement and provide practical tips for successful calibration. **FROM BASIC CONCEPTS TO ADVANCED TECHNIQUES**, our eBook covers everything you need to know about temperature calibration. [Download your copy today.](#)



Experience a better way.
To run your business.
To calibrate.



Data Quality: The Key to Successful AI-based Process Control

By Heikki Laurila, Beamex

Process control is a crucial part of manufacturing and industrial operations, ensuring processes are consistent, efficient, and effective. With the increasing use of automation and digital technologies, artificial intelligence (AI) is becoming a critical tool in process control. However, the quality and accuracy of measurement data are essential when using AI, as inaccurate data can lead to incorrect predictions and decisions.

One of the key benefits of using AI in process control is its ability to analyze large volumes of data in real-time. Manufacturing and industrial settings generate thousands of sensors and other data sources continuously, making it difficult for human operators to monitor and make decisions quickly enough to optimize performance. AI can process this data more quickly and accurately, supporting decision-making based on real-time data.

AI algorithms can also analyze data from multiple sensors to detect correlations and patterns that might not be immediately obvious to the human eye. This can help identify potential issues before they become critical, allowing for corrective action before production is impacted. AI can also be leveraged to enable predictive maintenance



New jobs will emerge as AI creates new opportunities. Given the need to ensure data accuracy, this includes jobs in the field of measurement and calibration.

by using data from sensors and other sources to predict when equipment is likely to fail, reducing maintenance costs, and extending equipment lifespan.

However, one of the biggest challenges in using AI in process control is data quality. AI algorithms rely on high-quality data to make accurate predictions and decisions. Proper calibration of process measurements is critical in AI-based process control. It is essential to calibrate all measurements

regularly to maintain the accuracy of the data they generate.

Ensuring the high quality of measurement data highlights the need for the process industry to use more

address challenges such as data quality, proper calibration, and the need for skilled personnel. By doing so, we can unlock new opportunities for innovation and growth in manufacturing and industry.

Proper calibration of process measurements is critical in AI-based process control. It is essential to calibrate all measurements regularly to maintain the accuracy of the data they generate.

effective calibration processes. Fully paperless calibration processes that allow the calibration data to move digitally throughout the process guarantee high-quality data and data integrity. Calibrating all measurements regularly will be even more critical in the future as the process industry continues to adopt AI.

There are concerns about the potential impact of AI on jobs, as AI becomes more prevalent in manufacturing and industrial settings. However, new jobs and industries will emerge as AI creates new opportunities for innovation and growth. This includes jobs in the field of measurement and calibration, with the need to ensure data accuracy becoming even more essential.

In conclusion, AI-based process control is transforming the way we approach manufacturing and industrial operations. However, to fully realize the benefits of AI-based process control, it is necessary to

The saying “Everything is based on measurements” is even more valid with AI-based process control. The only way to ensure high-quality measurement data in a process plant is by running a high-quality calibration program that ensures all measurement instruments are calibrated regularly, traceably, and with sufficient certainty.

To learn more about automating your calibration processes, visit www.beamex.com.



Heikki Laurila is the product marketing manager at Beamex. He started with Beamex in 1988 and has worked in production, service, the calibration laboratory, as quality manager, product manager, and product marketing manager. Heikki holds a BSc in Information Technology & Electronics. His family consists of himself, his wife and their four children. In his free time, he enjoys playing the guitar.



12th Gen Intel®
Core™ i7/i5/i3



I/O Expansion
Interface



5G, Wi-Fi6/6E
Compatibility



200W Power for
Accelerator Module



Temperature Range
-20°C to +70°C



EN 61000-6-2
Certified



IPC960A Series **NEW!** High-Performance Edge AI Systems



ICO520 **NEW!** Compact DIN-Rail Edge System



High-Performance
& Cost-Effective



5G-ready



Modbus/CAN;
OPC UA; SNMP

Customize **Your** Solution
With Our **USA-Based**
Design Engineering Services
solutions@axiomtek.com

intel
partner Titanium
IoT
Solutions

Unleash the Power of Data: AI at the Edge

By Ryan Chen, Axiomtek USA

As Industry 4.0 continues to evolve, AI is growing to become a staple of many industrial applications. Advancements in edge computing technologies, low-latency wireless networking, and the maturation of neural networks have helped bring AI decision-making capabilities to IIoT applications. According to Markets and Markets, the global AIoT Industry Market size is projected to reach \$24.9 billion by 2028 at a CAGR of 37.7% from 2023 to 2028.

In today's AI-driven landscape, organizations are seeking ways to leverage AI's power at the edge. The implementation of AI in edge computing allows for real-time analytics, drastically reducing latency to near zero for end users while improving data delivery. Enhanced security is another benefit, as locally processed data reduces the amount uploaded to the cloud, further improving the analysis and encryption of sensitive material. Gartner predicts that by 2025, 75% of enterprise-generated data will be processed outside the cloud.

For industrial devices in the field, downtime on a machine can be an exorbitant financial burden. AI models can be trained to analyze sensor data to detect patterns and anomalies, facilitating predictive maintenance. In manufacturing, incorporating the capabilities of edge AI

with machine vision for real-time analysis of images and data empowers production lines to self-identify issues, which reduces the reliance on manual inspections, improving the production quality while making substantial savings in overhead costs.

By implementing AI at the edge, businesses unlock real-time insights, maximize efficiency, and elevate their competitive edge.

As AI technology continues to mature, an optimal computing platform to facilitate AI in your operations is paramount to maintaining a competitive advantage through enhancing efficiency, mitigating risks, and reducing costs.

Ideal edge device features for AI computing

Purpose built

In the realm of demanding industrial applications, edge AI devices adhere to industry certification standards to bring peace of mind to businesses, ensuring their resilience in the face of challenging environmental conditions. Some applications may require a system to withstand exposure to various



settings, so features such as vibration resistance or a wide temperature range are necessary to ensure consistent performance and longevity in diverse operational environments. A robust edge AI system also requires a powerful processor to handle the computational demands effectively.

5G and Wi-Fi 6

The widespread adoption of IoT has fueled the era of big data. 5G and Wi-Fi 6 have opened the door for devices to transfer vast amounts of generated data quickly and seamlessly. The network capabilities of 5G and Wi-Fi 6 reinforce complex edge computing infrastructures and enable the processing and analysis of data near the source, minimizing the need for communication with centralized clouds, thereby reducing latency and enhancing real-time decision-making.

AI technologies

The computation capabilities of edge devices have been enhanced by developments in edge-specific AI hardware accelerators, graphics processing units (GPUs), field programmable gate arrays, and specialized AI accelerating chips. These implementations allow edge devices to effectively handle AI workloads, improving energy efficiency, and enabling faster inference.

Modular hardware

Modularity allows for the customization of edge devices to ensure that they have the necessary hardware and connectivity options for rapid integration into operations. With this approach, the engineering services of hardware manufacturers are able to provide tailored solutions for specific applications leading to a faster time to market. A modular design of edge devices also allows for the ease of maintenance to replace components. As AI technology continues to mature, a modular design encourages futureproofing, as individual components can be upgraded to newer technologies without the need to replace an entire system.

In manufacturing, incorporating the capabilities of edge AI with machine vision for real-time analysis of images and data empowers production lines to self-identify issues.



Ryan Chen is the director of engineering at [Axiomtek USA](#). With a Master's in Electrical Engineering and over 18 years of hardware design associated with ODM project management

experience, he specializes in the development of IIoT architecture and customized solutions for industrial automation applications.

The
LANDSCAPE

of OUR

DIGITAL WORLD

is

EVOLVING

So are the THREATS it faces!



Protecting the assets and data of your organization is critical.

At **IPR TECHNOLOGY** we give your business the tools and weapons **YOU** need to defend against digital threats. Our comprehensive approach empowers you to:

- **IDENTIFY** vulnerabilities within your infrastructure,
- **PROTECT** your networks, systems, and applications with robust security, and
- **RESPOND** to threats and attacks immediately.

Maintaining your customer's trust and protecting your professional reputation is as important to us as it is to you.

Don't wait until it's too late.

Secure your digital future today!

**Contact
IPR Technology, Inc.
812.577.4122**

Or
Visit

<https://ipr.technology>

to schedule a consultation with one of our experts.

IPR Technology, Inc. is a leading provider of cybersecurity consulting services. While we strive to provide the best protection possible, no system is completely immune to all threats. We recommend implementing a layered security approach and staying vigilant to ensure the highest level of cybersecurity.

Safeguarding Assets and Networks, and Ensuring an Effective Cybersecurity Response

By David Jennings, IPR Technology

In today's interconnected and digitized industrial landscape, cybersecurity is a critical concern. Industrial cybersecurity aims to protect valuable assets, secure networks, and establish robust response mechanisms against cyber threats. That includes best practices associated with industrial equipment management, highlighting its broader significance beyond preventing hackers' infiltrations. The core aspects of industrial cybersecurity are asset identification, network protection, and cybersecurity response. These allow organizations to develop a comprehensive cybersecurity strategy that addresses potential vulnerabilities and risks, and establishes effective incident response protocols.

Asset identification and network protection

A comprehensive understanding of an organization's assets is key to creating security protocols. Critical asset identification, categorization, prioritization, tracking, and management processes are all vitally important. Conducting regular vulnerability assessments helps identify weaknesses and potential entry points for cyber threats. Risk assessment and threat modeling techniques,

penetration testing, and vulnerability scanning play important roles in identifying vulnerabilities and evaluating their potential impact. Comprehensive asset identification allows organizations to explore various risk mitigation strategies, including patch management, configuration management, access control, and user management practices. They can proactively reduce the attack surface and strengthen their overall security posture by adopting these strategies.

A comprehensive understanding of an organization's assets is key to creating security protocols.

A multi-layered, defense-in-depth approach is essential to protect industrial networks. This includes developing perimeter security measures, segmenting networks, and deploying intrusion detection and prevention systems (IDPS) to safeguard against external and internal threats. Securing communication channels protects sensitive industrial data from unauthorized access and interception. Encryption techniques, secure remote access



mechanisms, and virtual private networks (VPNs) help establish secure communication channels within industrial networks.

Industrial control systems (ICS) are at the core of critical infrastructure. Security considerations for programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and human-machine interfaces (HMIs), along with continuous monitoring for anomalies within ICS networks, are all priorities.

Ongoing cybersecurity education and awareness programs are necessary to foster a security-conscious culture and mitigate human-related risks.

Preparing for cyber incidents can minimize their impact. A good response plan features incident identification and classification, response teams, and comprehensive response plans that outline roles, responsibilities, and escalation procedures. It also requires timely detection and accurate analysis, security information and event management (SIEM) systems, threat intelligence, and log management and analysis. Once an incident is detected and analyzed, a swift response is essential to contain and eradicate threats and restore systems. Then a post-incident analysis should be conducted to identify lessons learned and improve future response.

Industrial cybersecurity best practices

Employees play a vital role in maintaining the security of industrial systems. Ongoing cybersecurity education and awareness programs are necessary to foster a security-conscious culture and mitigate human-related risks. Regular security audits and assessments are essential for evaluating cybersecurity controls and identifying areas for improvement. Security frameworks such as NIST Cybersecurity Framework or ISA 62443 should be implemented. Effective cybersecurity requires continuous monitoring of industrial networks and proactive threat hunting. The emphasis here is on real-time monitoring, anomaly detection, and threat intelligence to identify and promptly respond to emerging threats. Securing the industrial supply chain is vital to prevent the introduction of compromised components or software. Organizations should consider cyber insurance as a risk mitigation strategy for transferring potential financial losses. Additionally, a good understanding of legal compliance and regulatory obligations regarding cybersecurity is crucial.



David Jennings is a highly successful, results-driven professional engineer with [IPR Technology](#). He works closely with clients to improve and innovate their industrial

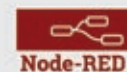
controls systems while focusing on cybersecurity and digital safety. David has over 20 years of professional experience in industrial control systems. His areas of focus are SCADA controls and visualization, ICS networking, cybersecurity, and data collection and reporting.

groov EPIC™

Your Digital Transformation-ready Edge Platform



- Industrial design
- Enterprise-grade security
- Programming choices
- Web & mobile visualization
- Cloud connectivity
- Secure remote access



Learn more today at www.opto22.com



Made and supported in the U.S.A.
Call us toll-free at 800-321-6786 or visit www.opto22.com
All registered names and trademarks copyright their respective owners.

OPTO 22
Your Edge in Automation.™

Low-Code/No-Code Development Tools

By Terry Orchard, Opto 22

One of the keys to success with the Industrial Internet of Things (IIoT) is accessibility. Not just the accessibility of device data and control, but also the software they interact with. Having approachable low-code and no-code IIoT tools is extremely valuable when it comes to connecting devices, software, and services together in an effective way. Node-RED is versatile open-source software that does not require a high level of programming expertise to use, and as such, getting started with it is very easy. At its core, Node-RED is powered by a JavaScript runtime engine called Node.js; however, no knowledge of JavaScript is needed to use it. Essentially, if you can draw out a flowchart of where your data comes from, how it needs to be processed, and where you want it to end up, you're already half-way to making it happen.

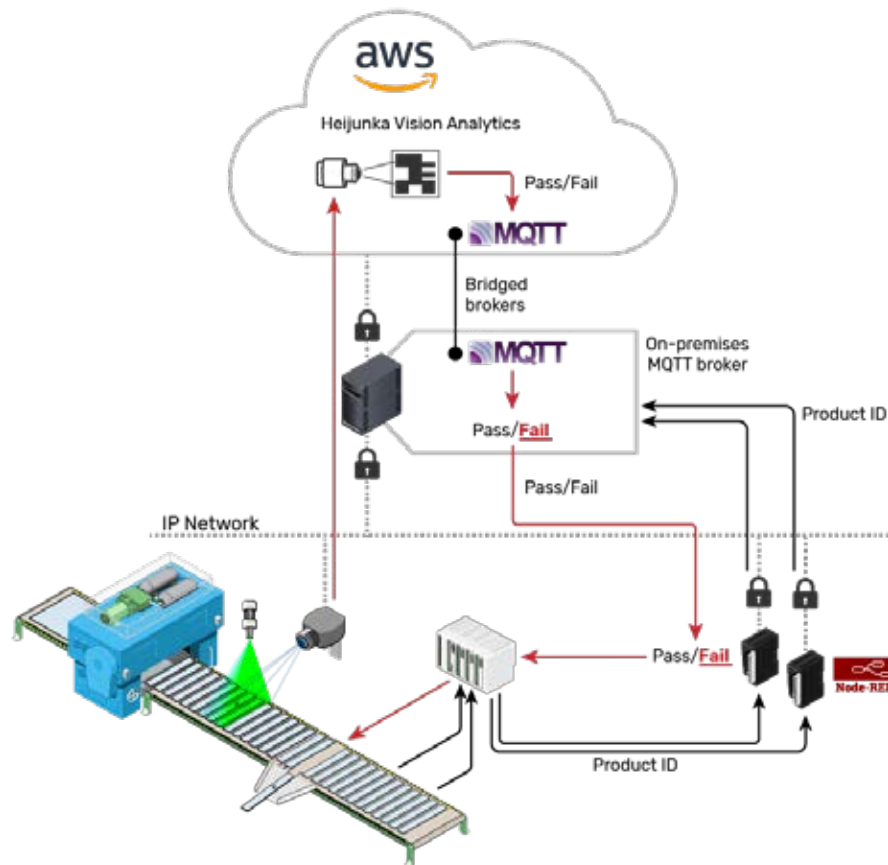
Three key aspects that make Node-RED such a great development tool are that it is accessible, extensible, and flexible. It's possible to use it from any modern web browser without any code whatsoever—no extra software is needed. The flow of data is created not by writing it out but by placing individual tasks on a workspace as separate node, and wiring them together to move, modify, and send data wherever it needs to go. Having a visual interface makes it simple for anyone to take the input from a sensor, add a timestamp to the reading, and upload it to a database

without writing any code. The user only has to organize a few nodes in the right order.

Node-RED really shines in IIoT applications because it's not limited to a specific sensor, service, or UI. In fact, it is extensible to many hardware and software endpoints. The functionality of Node-RED can be expanded by installing external node packages to interface with anything from a Modbus device to a web service—and anything in between. Systems that were previously completely disconnected can be brought together as long as there is a node out there that can send and receive the data. Having the flexibility to talk to a huge variety of hardware and software allows the creation of projects that would otherwise be impossible.

If you can draw out a flowchart of where your data comes from, you're already half-way to making it happen.

To bring it all together, every node handles data with a standard format: JavaScript objects. These structured objects are easy to understand without writing any code to produce or consume them, and



A hybrid architecture using two *groov* RIO modules on each production line to allow cloud-hosted analytics to securely control action in the physical process at the edge of the network.

they can easily be sent, received, and saved in text format. Because all nodes have this common language, there's no friction when it comes to tying something like a controller or sensor together with a separate database, web service, or a different device entirely. Having all this in one place means previously detached systems can effortlessly connect with each other.

It is also important to consider reliability and security. While a Node-RED server can be installed on a cloud server, PC, or even a Raspberry Pi, a power-safe, industrially hardened device is more appropriate. The *groov* family of devices from Opto 22, both EPIC and RIO, are built for industrial environments and are already set up with encryption and authentication. Secure by

design, they also provide easy account and project management. These combined factors make *groov* an ideal hardware platform for Node-RED. Being able to interconnect systems as well as process and combine their data without being an expert programmer can change the way companies approach any automation application.



Terry Orchard is a technical marketing specialist at [Opto 22](#). Having a background in programming and mathematics, Terry knows the value of making a complex

topic more approachable and applies that through instructional videos, tutorials, and developer guides.

The solution
to integrate
OT to IT now
at Microsoft
Azure



Cogent
DataHub®

Cogent DataHub® allows you to seamlessly integrate your live processes using standard protocols like OPC, MQTT and Modbus, and connect to SCADA systems, data lakes and historians securely and in real-time.

Solve your IoT connectivity issues. Secure your OT to IT data communications. Reduce your cybersecurity risk profile. Share your data with any application, partner or customer. All in one solution now available at Microsoft Azure Marketplace.

[Learn more >](#)

SKKYNET™

SECURE INDUSTRIAL IoT REDEFINED

Cogent DataHub® is a registered trademark of Real Innovations International LLC, used under license

Cumulative Change: from OPC Classic to OPC UA

By Xavier Mesrobian, Skkynet

Clearly, the future for OPC is OPC UA. But change in the industrial world is cumulative, with each improvement using the past as a stepping stone to the future. The move from OPC Classic to OPC UA need not be abrupt—it can be gradual, smooth, and steady. Today engineers and system integrators can get the best of both worlds by integrating OPC Classic and OPC UA, and using each to its full advantage. The question is: what is the best way to make a gradual change, to gain the most benefit with the least effort and disruption?

Any migration from OPC Classic to UA, no matter the size of the system, will go better with a plan. Here are some suggestions:

- ▶ **Conduct a survey** and create a list of all existing devices, equipment, and software that use or are connected via OPC DA, OPC A&E, and OPC HDA, both servers and clients.
- ▶ **Address networking issues.** Identify all networked connections that rely on DCOM, and prioritize them for immediate attention.
- ▶ **Identify replacement pairs.** If there are any connections in the system where

the OPC Classic server and client can be replaced together by OPC UA, prioritize upgrades for them as resources allow.

- ▶ **Create a gateway strategy.** For connections where one side must stay OPC Classic and the other requires OPC UA, find and install gateway hardware or software to make the conversion.

Today engineers and system integrators can get the best of both worlds by integrating OPC Classic and OPC UA, and using each to its full advantage.

Networking issues

The biggest challenge for OPC Classic users recently is the Microsoft DCOM Security Patch (KB5004442) that forces all OPC Classic communication over DCOM to run with maximum security. Systems running with the patch can no longer avoid DCOM security configuration issues by simply shutting down security.

Fortunately, the patch does not affect local COM connections. It is still possible to use OPC Classic securely if the server and client connections are not connecting across a network. And secure networking is also possible in one of two ways without using DCOM: by using an OPC gateway or by tunnel/mirroring.

Gateway for OPC Classic to UA

OPC Gateways convert between OPC Classic and OPC UA. A software gateway can be installed on the computer running the OPC Classic server or client, and convert the data stream to or from OPC UA. If you have an OPC UA client or server that you need to connect to OPC Classic, this option is straightforward. The gateway makes a local connection to the OPC Classic server or client, avoiding DCOM. It then communicates across the network using OPC UA. When choosing OPC gateway software, look for an application that maintains the original data hierarchy from OPC DA. That way the final data structure will remain intact from the data source to its destination.

Tunnel/Mirroring for OPC Classic Networking

When both sides of a network connection must remain OPC Classic, you can use OPC tunnel/mirroring, where software components convert OPC Classic to TCP for networking. One component connects to the OPC server locally, and then opens a TCP port and waits for an incoming tunnel/

mirror connection. A similar software component at the client end makes the network connection via TCP and receives the data. It then converts the data feed back to OPC Classic, making it available to the OPC Classic client. A good tunnel application will support bidirectional communication and mirror the data, maintaining a consistent image of the data set in real time on both sides.

The tunnel/mirror approach has an additional benefit—it can connect across *isolated* networks. The recent NIS 2 Directive and an ISA-95 standard for industrial cybersecurity specify isolating OT (Operations Technology) data from IT networks using DMZs. Some tunnel/mirror solutions allow you to add a third tunnel/mirror component to a DMZ, mirroring between the data source, the DMZ, and the data user.

In the long run, OPC UA is likely to replace OPC Classic. But for some time to come engineers and system integrators will be using both protocols. Change in the industrial space is cumulative, after all. Those who understand both protocols, and can integrate and use each to its full advantage, will get the best of both worlds.



Xavier Mesrobian is the vice president of sales and marketing at [SkkyNet](#). He is a seasoned technical sales and marketing executive with a strong foundation on net new business opportunities.

Software Supply Chain Visibility

Need to avoid production downtime from **ransomware**? Need to **respond fast** when incidents do occur?

The **aDolus FACT™ platform** continuously monitors files and automates software validation and vulnerability management to protect your operating environment and prevent downtime.



Ensure software is legitimate and safe – and won't introduce risk



Generate SBOMs when your suppliers can't (or won't) provide them



Avoid financial or reputational damage caused by production downtime



Satisfy regulatory requirements for software supply chain security



Search for vulnerabilities and risky components across your entire facility



Enhance existing workflows and MoC processes to include supply chain cybersecurity



BOOK A DEMO

VEX and Its Relation to SBOMs and Software Supply Chain Security

By Eric Byres, aDolus

Software supply chain attacks are a constant and urgent concern for cybersecurity professionals. Adversaries actively exploit this attack vector, targeting the software of victims' trusted suppliers and open source repositories. This threat has prompted a regulatory response and market demand for Software Bill of Materials (SBOMs) to provide transparency into the third-party components in software. But as SBOMs proliferate, the number of vulnerabilities exposed has skyrocketed.

Vulnerability Exploitability eXchange (VEX) prioritizes this mountain of vulnerabilities. NTIA describes a VEX document as a "companion artifact" to an SBOM. VEX documents allow product manufacturers to identify vulnerabilities in third-party components within their products and communicate their exploitability to customers. This is important, because not all vulnerabilities require action. A vulnerability might exist in a subcomponent but be inaccessible to attackers, or the vulnerable function is not included in the product. For example, the HeartBleed vulnerability in OpenSSL required the heartbeat function to be included during compilation for it to be exploitable. For many ICS products, this

function was never used; therefore, the products were not susceptible to attack.

VEX documents allow product manufacturers to identify vulnerabilities in third-party components within their products and communicate their exploitability to customers.

VEX documents enable and automate efficient communication between vendors and their customers with respect to exploitable (and non-exploitable) vulnerabilities. Consider this sequence of events:

1. An asset owner has a product used in a critical system and must provide a security report on it to regulators. The owner contacts the control system supplier and requests an SBOM so they can check the components and component vendors to assess any vulnerabilities within.
2. Unfortunately, the owner discovers that there are more than 200 vulnerable components in the product. Worse,

some are listed as critical in the National Vulnerability Database (NVD). Alarmed, the asset owner contacts the supplier again.

3. The support rep at the supplier is busy assisting many other customers with the same question and replies to each explaining that although the critical vulnerabilities exist in theory, they are not exploitable in their product.
4. The following month, a new critical vulnerability in one of the product's components is announced and the cycle repeats. Much time is wasted for the supplier and all the customers.

With VEX documents, the scenario unfolds more elegantly. The asset owner obtains the SBOMs and vulnerability assessment, as well as VEX documents, from the supplier. Coordinating these documents with their asset management system, they can determine which of the 200 vulnerabilities are actually exploitable and, therefore, a risk. Typically, only a small fraction of them will be a concern, with estimates ranging from 2.7% to 15%.

VEX reduces the problem to something that asset owners can manage: it's actionable rather than paralyzing. Furthermore, VEX documents can contain remediations for vulnerabilities so asset owners can take steps to mitigate risk without contacting their suppliers.

Product managers who need to communicate the exploitability of vulnerabilities in their products, security



As SBOMs proliferate, the number of vulnerabilities exposed is skyrocketing.

engineers who are responsible for patching software in critical operations, and systems integrators working with multiple vendors on behalf of their customers can save both time and money using VEX as part of their vulnerability management strategy.

Typically, only a small fraction of vulnerabilities will be a concern, with estimates ranging from 2.7% to 15%.



Eric Byres is CTO of [aDolus Technology](#) and an internationally recognized expert in OT security. He has chaired standards efforts, won numerous awards, and created

the Tofino Firewall, the world's most widely deployed OT security appliance.

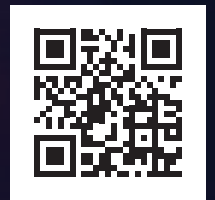
1898 CO[®]

PART OF BURNS  MCDONNELL



— ● ●
24/7/365

**CRITICAL INFRASTRUCTURE
THREAT PROTECTION & RESPONSE:
STAY AHEAD OF OT-IT CYBER THREATS**



LEARN MORE

Cybersecurity Risks for Plant Safety

By Tim Gale, 1898 & Co.

Traditional cybersecurity simply focuses on protecting data and information systems. However, industrial cybersecurity needs to go a step further. It must address the need for the protection of critical process control and safety systems.

A successful attack on OT and IT systems could disrupt the normal function of critical processes, leading to equipment failure, environmental damage, and endangerment to human lives. To mitigate these risks, the availability and integrity of systems that perform safety controls, alarms, and interlocks (SCAI) must have safety at the foundation of their design and operating environment.

Safety system security

The main goal of cybersecurity is to protect the availability of safety systems as a critical layer of protection against catastrophic events. The most secure approach is to preserve the independence of basic process control and safety systems. Separate controllers, networks, and engineering stations result in a more difficult environment for cybersecurity threats to compromise.

Typically, these combined network systems and engineering stations in basic process control and safety systems are designed to increase convenience and capital

savings. By maintaining separate systems, the risk of cybersecurity vulnerability is limited. There are no additional barriers when it comes to the ability to perform routine maintenance and/or provide appropriate proof test capabilities on separate systems.

A successful attack on OT and IT systems could disrupt the normal function of critical processes, leading to equipment failure, environmental damage, and endangerment to human lives.

Broader cybersecurity program

A broader ongoing cybersecurity program is required to help mitigate cybersecurity attacks and recognize the risk of technological change in the OT environment. The following are some practices to consider:

- ▶ **Develop an incident response plan.** A good response plan includes lines of communication and protocols for a



cybersecurity attack. For this reason, tabletop exercises should be performed regularly.

- ▶ **Analyze risks.** It is worth the investment in time to explore the possibility of cybersecurity risks. Only when a company knows the potential threats can it begin to reduce them to an acceptable level.
- ▶ **Design for protection.** Industrial control systems should be designed with protection in mind. The main goal is to limit the ability to navigate across the network. Endpoints should also be hardened against known vulnerabilities.
- ▶ **Incorporate software.** Robust anti-malware software is critical. It can help to protect industrial control systems against dangerous malware that can cause major disruptions in processes and huge costs to businesses.
- ▶ **Check for safety gaps.** An industrial cybersecurity management system needs to be comprehensive in order to deliver an effective level of security. Companies must regularly examine their overall incident response plans and make updates as necessary.

A better approach to design

To design most critical safety functions, engineers should follow the guidance of the Cyber Informed Engineering (CIE) and Consequence-Driven Cyber-Informed Engineering (CCE) frameworks from [Idaho National Laboratory](#). Both systems involve an attentive process to engineer risk out of critical systems.



Tim Gale is an industrial cybersecurity and process safety manager for [1898 & Co.](#), part of Burns & McDonnell, and has more than 30 years of experience in the oil & gas, specialty chemical, pulp & paper, food & beverage, pharmaceutical, and mining industries. Tim is a trusted cybersecurity adviser to numerous multinational clients and has performed vulnerability and risk assessments across North America, Europe, and Asia. As a process control engineer with experience in design, commissioning, and startup of process control and process safety systems, he has a unique foundation for assessing and evaluating process hazards, control system architectures, and cybersecurity risks.

Thriving Amid Disruptive Innovation

Companies that can leverage disruption and choose innovation over entrenchment position themselves for success.

By Bill Lydon

The world of manufacturing is an exciting, ever-changing landscape that is continually being driven to new heights of productivity, efficiency, and quality through the application of innovative technology. Manufacturing professionals who keep up with both the trends influencing their industries and the latest available automation techniques, technologies, and solutions can be drivers of change and important contributors to the overall success of their companies. One of the biggest trends now is disruption—pushes for change that can spur innovation.

Disruptive innovations create new value, so users can achieve better results and, in many cases, support more functionality. Such innovations may be new technologies like artificial intelligence or

mobile robots, new applications of existing technology like sensors becoming “smart” and connected, or new methods or procedures that replace traditional solutions. Historic industrial examples include hydraulics replacing mechanical methods like cable and pulley systems, digital systems replacing pneumatic PID controllers, and mechatronics replacing gearboxes and mechanical camming with programmable coordinated motion.

●●●●● **Disruptive innovations** create new value so users can achieve better results and, in many cases, support more functionality.

Disruption can also challenge organizational structures, including roles and responsibilities, in ways that are not initially obvious. The push for sustainability—creating a business that has minimal negative or potential positive impact on the environment, community, society, or economy—has resulted in new roles like chief sustainability officer or head of ESG. That means energy and resource optimization have become higher priorities on the operations side, since those goals can be achieved efficiently with the application of automation and controls technology to optimize manufacturing processes and effectively monitor, alarm, and report.

Disruptive innovation can be subtle, as when the creative use of current off-the-shelf technology combines with creative thinking to create fresh solutions. It can also feel threatening to those who have found success with traditional methods. Many times, established suppliers will see disruptive innovations as unattractive for a range of reasons and try to ignore them.

One example in the industrial automation industry is the initial resistance of traditional suppliers to replacing proprietary human-machine interface (HMI) hardware and software with PCs and Microsoft Windows-based software. Fast-forward to today and providers of desktop- or tablet PC-based HMIs now must respond to the advent of the “smart helmet”—a combination of safety helmet and smart goggles that gives the wearer access to virtual instructions, safety information, and mapping software displayed on its integrated “safety screen.”

Why you should care

Companies that do not take advantage of the appropriate disruptive innovations are likely to become uncompetitive at some point and may even be leapfrogged by nimbler startups. Conversely, companies that leverage disruptive innovations position themselves to become leaders in their industry.

Amazon, Uber, iTunes, and Airbnb are well-known examples of the latter. While not directly related to manufacturing and automation, they do illustrate the creative application of technology to dramatically change commerce. Historically, you can find numerous examples of industrial companies using innovative thinking and technology to become leaders.

Ford dominated the early automotive industry. More than 100 years ago, Henry Ford and his team at the Highland Park assembly plant launched the world's first moving assembly line. It simplified the production of the Model T's 3,000 parts by breaking production into 84 distinct steps performed by groups of workers as a rope pulled the vehicle chassis down the line.

Andrew Carnegie built his steel-making business leveraging technology with new processes, such as the Bessemer process. He installed new material-handling systems, including overhead cranes and hoists to speed up the steel-making process and boost productivity. Carnegie was relentless in his efforts to drive down costs. He would tear out and replace equipment at his mills if better technology was developed to reduce costs and make his mills more efficient.

Federal Express Corporation, founded in 1971, leveraged barcode and computer technology to achieve dramatic growth. One of FedEx's great contributions was the tracking system launched in the 1970s, which has become standard in shipping. It was initially an internal process for quality control. When the system went online, it included early prototypes of handheld computers that scanned package barcodes with wands.

●●●●● **The best ideas**
don't arise in an intellectual vacuum. If you want to go beyond problem solving, it is essential to be fed ideas from multiple sources.

Moving forward creatively

We have been conditioned to believe that the only way to get big results is to make a big change. This can sometimes be true, but these opportunities are typically expensive and rare. Many times, the little-change ideas can be just as powerful as the big ones. Smaller changes have the advantage of being additive, instead of being an overhaul. Thus, they may be able to yield big results while being less costly, less risky, and less disruptive.

You might think creativity starts with a random idea, but the truth is that the best ideas don't arise in an intellectual vacuum. If you want to brainstorm innovations that go beyond problem solving to achieve productivity and performance enhancements as well, it is essential to be fed ideas from multiple sources, and to pay attention to trends.

On the following pages are the trends I see shaping industrial automation. Gleaned from multiple sources and conversations, I discuss how the foundations of manufacturing management are shifting toward advanced manufacturing strategies, as well as the transformative technologies that are enabling innovation across industry segments and around the globe. As always, I invite you to share your thoughts, criticisms, and perspectives as well, and I look forward to talking with you through [LinkedIn](#) or via [email](#).

The cumulative leverage of applying a variety of new methods and products to facilitate positive change can be powerful. Make the most of disruptive innovations today to create new value and help your company succeed.

ABOUT THE AUTHOR



Bill Lydon is contributing editor of Automation.com and ISA's *InTech* magazine. He has more than 25 years of experience designing and applying automation and controls technology, including computer-based machine tool controls, software for chiller and boiler plant optimization, and a new generation building automation system. Lydon was also product manager for a multimillion-dollar controls and automation product line, and later cofounder and president of an industrial control software company.

Advanced Manufacturing Automation Strategies **Open Up**



Pushed by tech-savvy users and other trends, manufacturing management systems are shifting toward open, secure, and interoperable control and automation architectures.

Worldwide manufacturing has had a wakeup call with pandemic and disruptions of supply chains. Outsourcing operations to achieve lower costs has created pain and is a pressure point with negative impacts on sales and increasing profitability risk. Demographic changes are creating unprecedented workforce challenges. Technology is advancing rapidly, and all of us are more tech-savvy thanks to advances in consumer electronics. Operational technology (OT) professionals too have gained new skills from working with their IT counterparts, gaining new insights into the ways technology can be speedily and successfully applied in industry. These and other trends have accelerated investment in advanced manufacturing automation strategies and allowed the building blocks for Open Integrated Industrial Automation to fall into place.

By Bill Lydon

All these manufacturing business management trends, which have long been simmering, now seem poised to affect industrial companies

and automation professionals worldwide. Here is a look at some of the forces pushing industry in new directions, and some of the responses rising to become trends of their own.

Push from global labor shortages

Companies are increasingly faced with a lack of workers, largely due to demographic trends. According to the latest UN reports, two-thirds of the global population live in countries with below-replacement fertility rates, while average lifespans continue to grow. This means that many populations are rapidly aging and overall numbers will soon begin to shrink (if they haven't already). At the start of this century, 32 countries had a median age above 35 years; by the end of this decade, that number will more than double, and in 25 of those countries, half the population will be more than 45 years old. Falling fertility rates in China, Canada, Italy, and elsewhere mean fewer new entrants into the workforce every year. Even manufacturers that outsourced production to other countries in search of low-cost labor are finding that those costs may not be lower, and skilled labor may not be available.



Push from tech-savvy users

Users today have become significantly more sophisticated, technologically. Consumer electronics advances ranging from smart phones to wireless doorbell cameras to self-driving cars make average people more tech savvy and provide engineers with cost-effective automation they can experiment with at home. Manufacturing business management leadership is increasingly learning of and embracing technology investments that can improve profits, efficiency, competitiveness, supply chain resiliency, or direct labor cost.

Information technology (IT) moves forward at its own pace, and industrial professionals who experience greater cooperation with IT people are learning to leverage new technology. While the established industrial automation industry has experienced relatively

few changes over the years compared to other industries, in fact many of the major industrial automation innovations of the recent past were accomplished using commercial off the shelf (COTS) technology created by the computer industry. Those innovations include the adoption of Microsoft Windows, industrial Ethernet networks, and application virtualization.

Even more telling is the contrast between the level of usability, flexibility, and multivendor interoperability in the business enterprise and IT groups, as opposed to traditional industrial automation supplier offerings. Open systems create ecosystems that leverage more human and investment capital to create solutions than any single company. An example is optimizing industrial production using open historians and analytics tools such as TensorFlow, which can create manufacturing and process optimizers superior to existing offerings.

Push from technology advances

Germany's Industry 4.0 initiative ignited worldwide cooperative efforts in other countries, including China, Japan, Mexico, India, Italy, Portugal, and Indonesia. As countries and industry have recognized the need to modernize with Industry 4.0 technologies, this initiative is defining a model for all industrial manufacturing organizations to use. Sustained competitiveness and flexibility in the face of dynamic technological growth can only be accomplished by using automation at the center to enable a successful transition.

Manufacturers throughout the world are modernizing with an eye toward completely integrated manufacturing businesses. The holistic vision is real-time linking of supply chain, design, manufacturing, outbound logistics, and lifecycle service. This integration can only be accomplished by leveraging the latest technologies. These include low-code/no code development tools; the OPC/OPC-UA unifying ecosystem; and artificial intelligence, machine learning, and expert systems.



Over the years, industrial automation architectures have also been marked by more computing power being pushed toward final field devices. The limiting factor at each step has been the cost, ruggedness, and reliability of technologies. This has changed with significant commercial, consumer, and Internet of Things (IoT) technology, as well as communications advances at low cost that are pervasive in daily life. The smartphone is an obvious, ubiquitous example of a rugged, powerful computer with integrated communications and display.

Push from digital transformation

Digital transformation initiatives are creating an integrated real-time system from sensor to enterprise and cloud. Manufacturing and production companies are increasingly digitalizing to overcome the inefficiencies of siloed systems that create overlaps in processes and gaps in knowledge that stifle collaboration and efficiency.



Along with the growing integration is a push to flatten complex, hierarchical architectures. The most commonly used industrial automation architecture model to define manufacturing operations management is the five-level Purdue Reference Model (PRM), which later formed the basis for the ISA-95 standard. It has served the industry well for years, being easily deployed with the existing available technology. The model is typically expressed as Level 5 - Business Systems, 4 - Plant Level (ERP, MRP, and MES), Level 3 - Operation Unit, Level 2 - Machine/Process Automation, Level 1 - Controller, and Level 0 - Sensor/Actuator.

Traditional automation systems generally reflect this architecture with software running on general purpose computers at levels 2, 3, 4, and 5. Levels 2, 3, and 4 typically have database and communications interfaces that buffer and synchronize information between each level, in addition to associated HMI and user interfaces. The constraints of computing costs and networking bandwidth dictated this configuration based on past technology. The multilevel computing model is complicated and creates a great deal of cost, ongoing

configuration control, and lifecycle investment. Fortunately, this model is changing to enable a more efficient and streamlined automation system architecture.

Rise of digital manufacturing architectures

Although manufacturing has traditionally been kept apart from the rest of an organization's business systems, digital transformation is empowering companies to realize a holistic enterprise. This is achieved with a real-time digital manufacturing architecture (DMA).

Industrial automation is changing from the hierarchical Purdue models to more responsive architectures, achieving the goals of integrated real-time manufacturing. Within these more responsive and direct models, field devices communicate information directly with applications, including historians, advanced cloud analytics, and real-time maintenance monitoring. This simplifies the applications of these functions and eliminates complexity, performance drag, Level 2 and Level 3 software costs, and ongoing software maintenance.

The shift to a DMA is a fundamental building block for transformation that has implications from the enterprise level to the farthest end of manufacturing and production—sensing and control devices. The distributed system using a DMA includes embedded processors in sensors, actuators, barcode readers, cameras, and other field devices that can be controlled locally but, equally important, can also be accessed at any time remotely for complex calculations and adjustments.

DMA requirements are also driving industrial cybersecurity integration with mainstream IT, cloud, and IoT protection technologies and methods to create more secure manufacturing environments. Major technological advances include incorporation of firmware/hardware in controller intelligent sensors, actuators, and other field edge devices.

The most effective architecture requires orchestrating and optimizing all elements of the process for flexibility



in the face of external changes, including supply chains, customer demands, costs, availability, energy, and sustainability requirements. The emerging DMA technology leverages advances in distributed computing and open systems to accomplish this and achieve synchronized, real-time, optimized production. Customer orders, supply chain factors, and factory operations are fed into the digital twin, an ideal operating model of the plant and its processes. Real-time linkages throughout the system create a closed loop with constant feedback, whereby analytics, artificial intelligence, and machine learning adjust and optimize operations.

Rise of hyperautomation and robotics

Hyperautomation is described as an advanced automation strategy to drive profound digital transformation to gain a competitive advantage. It involves the orchestrated use of multiple technologies, tools, and platforms, including artificial intelligence (AI), machine learning, event-driven software architecture, robotic process automation (RPA), robotics, business process management (BPM), and low-code/no-code technologies. In the context of industrial manufacturing, hyperautomation is the digitalization and integration of the entire business from plant process to business enterprise, including ERP, supply chain, logistics, and customer fulfillment.

The use of robotics, and particularly collaborative robots, has become a high return on investment opportunity for manufacturers, and more robots are being installed than ever before. In February 2023, the International Federation of Robotics (IFR) reported that the global stock of operational robots hit a new record of about 3.5 million units. China's massive investment in industrial robots has put the country in the top ranks of robot density, surpassing the United States for the first time.

Overall, the number of operational industrial robots relative to the number of industrial workers hit 322 units per 10,000 employees in the manufacturing industry, according to IFR. Worldwide, annual manufacturing robot installations more than doubled between 2015 and 2021; in 2021 the world's top five most automated countries were

South Korea, Singapore, Japan, Germany, and China. Asia remains the world's largest market for industrial robots, with 74% of all newly deployed robots in 2021 installed there.

Rise of open industrial standards

As industrial digitalization becomes a top manufacturing company strategic objective worldwide, users are investing time and effort into innovative open industrial standards and data model initiatives. The pieces are falling into place to transition from vendor-driven industrial automation architectures (optimized for a single vendor's products and a curated partner ecosystem) to open industrial standards.

Why? Because the user is always responsible for efficient and continuous production and for manufacturing plants to run most efficiently, they must leverage systems from various vendors. But I have asked automation system vendors over the years what responsibility they take for consequential damages from downtime due to their systems failures and none are willing to be liable for their own, let alone anyone else's.

Users say the burden of proprietary systems is that each requires unique vendor education, unique vendor-oriented knowledge, special tools, and unique repair parts to get them running again. So, because users are responsible for system availability, they invest in training their own people at vendor classes and stocking the proprietary repair parts needed to improve system availability. They focus on a single major automation vendor architecture, which gives them "one throat to choke," but also forces them to buy from a limited controlled source. Contrast this with enterprise computing systems built on open standards with a much larger base of widely available training, multiple competing suppliers, and common components, interfaces, and software.

Open industrial standards and data models, common in the enterprise software and IT communities for many years, have greatly



benefited users there. Organizations striving to provide roadmaps, models, and standards for manufacturing digitalization want to achieve a similar standards-based, open, secure, and interoperable control and automation architecture. These manufacturers no longer believe the mythical benefits of a single major automation vendor architecture.

Demise of single vendor architectures

Vendors promote the single major automation vendor myth with the premise that manufacturers must use a single supplier's unique integrated system architecture. This false premise asserts that only they and their approved partners can provide the best solutions in all categories to meet their customer requirements. These suppliers have gated partner ecosystems, and they expose their unique interfaces only to partners allowed into the programs, limiting the use of other innovative solutions.

Ironically, these major vendor partner programs illustrate a major problem, since superior products that their partners offer are not allowed in. Further, when the major automation vendor introduces new offerings, they exclude partner products that are competitive with them. This ignores the fact that manufacturing businesses *must* efficiently integrate and leverage solutions from a wide range of suppliers to be competitive. The open systems that have significantly improved consumer and enterprise computing over many years show why this is so.

●●●●● **The computer industry** has proven, many times over, that no single vendor can provide as strong and reliable a solution as an ecosystem of suppliers, powered by open architectures.

The single-vendor premise was accurate in the early days of industrial automation and control when proprietary IT systems were purchased from a single vendor such as IBM, Univac, Burroughs, NCR, Control Data Corporation (CDC), Digital Equipment Corporation, or Wang. This approach gave way to open systems in the 1980s led by PCs, portable applications, open networking, and the open server revolution.

The change ushered in dramatic efficiency, new applications, and improved business performance and productivity that has eluded industrial automation. The computer industry has proven, many times over, that no single vendor can provide as strong and reliable a solution as an ecosystem of suppliers, powered by open architectures.

The situation was well stated by Don Bartusiak when he was Exxon's chief engineer for process control, and he repeats it even now as president at Collaborative Systems Integration focusing on open systems: "Just think about how much value you're getting from all the third-party apps that you can load on your smartphone. We can't do anything like that in our [manufacturing] world."

Bartusiak described how the closed ecosystems and proprietary architectures of today's industrial automation systems are forcing users to make significant compromises on projects. This is because closed ecosystems limit the ability of consumers to choose the best solution.


Many have argued, myself included, that the industrial automation industry has dramatically lagged in the adoption of technology and that these closed ecosystems have been a major cause of stifled integration and innovation. Many vendors have partner programs and interfaces that are promoted as "open," but these are highly gated, bureaucratically controlled, and ultimately closed ecosystems. This situation continues to stifle innovation. For example, major industrial automation companies introducing Internet of Things (IoT) and cloud architectures will propose to have their own gated ecosystems for third-party applications. Each closed architecture continues to muddle the industry.

ABOUT THE AUTHOR



Bill Lydon is contributing editor of Automation.com and ISA's *InTech* magazine. He has more than 25 years of experience designing and applying automation and controls technology, including computer-based machine tool controls, software for chiller and boiler plant optimization, and a new generation building automation system. Lydon was also product manager for a multimillion-dollar controls and automation product line, and later cofounder and president of an industrial control software company.

By Bill Lydon



Transformative Technologies Enable Innovation

Advances in 14 technology areas are empowering digital manufacturing transformations.

You might think creativity starts with a random idea, but the truth is that the best ideas and most useful trends don't arise in an intellectual vacuum. If you want to brainstorm innovations that go beyond problem solving to achieve productivity and performance enhancements as well, it is essential to be fed ideas from multiple sources, and to pay attention to trends.

The subtle part of disruptive innovation is that, many times, it is the creative use of current off-the-shelf technology combined with creative thinking that builds new solutions.

TRANSFORMATIVE TECHNOLOGIES

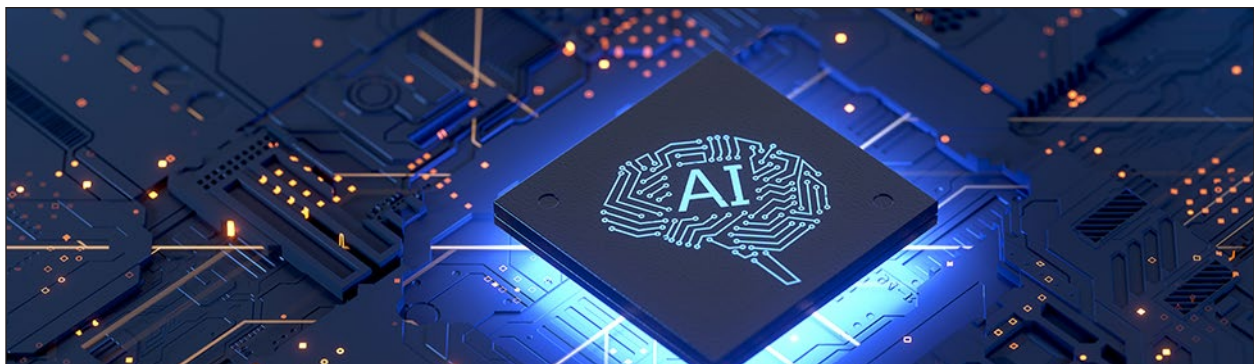
- Artificial Intelligence, Machine Learning, & Expert Systems
- Automated Material Flow
- Cloud and Edge Computing
- Digital Twins
- Ethernet IP Industrial Edge Field Devices
- IIoT and Intelligent Sensors
- Low-Code & No-Code Development
- Mobile & Remote Worker/Connected Worker Technology
- Predictive Maintenance Applications
- Remote Expert Services
- Robots and Cobots
- Semantic Technology/Data Analytics
- Spatial Computing/Intelligent Vision
- Wireless Private 5G Networks

Artificial Intelligence, Machine Learning, & Expert Systems

Artificial intelligence (AI), machine learning (ML), and expert systems provide the means for manufacturers to cut operating expenses, improve operations with increased staff efficiencies, quality, and productivity, improve operations, and reduce maintenance and repair costs. There are an increasing number of no-code, self-serve software tools that simplify application of these technologies by industrial subject matter experts rather than data scientists. Industrial automation and control systems have a wealth of data that can be utilized more effectively with these technologies.

In addition, AI processor chips enable high-performance applications to run within controllers and edge computers for demanding applications. Server and cloud AI/ML/expert system solutions are suitable for a wide range of industrial applications. While network communication speed and latency factors pose limitations for many real-time industrial and process applications, AI chips embedded in industrial edge devices and sensors can overcome the limits.

Makers of AI chips, including Nvidia, Intel Myriad-X, Google Edge TPU, and Hailo, have proven the technology in areas such as video analytics with image recognition and related applications. AI chips can be applied to edge computers using aggressively priced plugin board modules that conform to the popular M.2 and mPCIe connector standards. These standards are found in many computers, including embedded industrial PCs, and allow the addition of high-performance



AI processing without degrading other applications in the computer. This is analogous to early PC coprocessor add-ons used to achieve high-performance floating-point mathematical calculations and video display coprocessors used to display high-resolution, high-performance graphics.

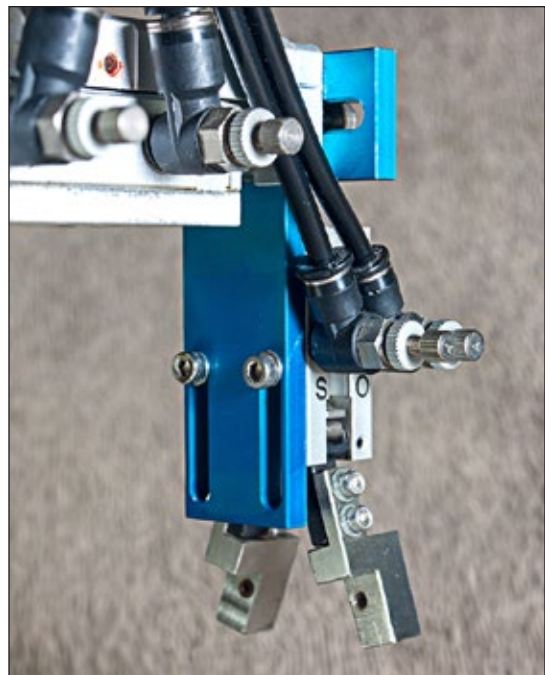
Automated Material Flow

Driverless vehicles, personal robots, and other innovations may be in the future for today's average consumer, but for industry, the technologies available now increase productivity and efficiency, automating industrial material flow. These technologies transform operations by supporting lean production methods and eliminating numerous non-value-added human touches, each requiring multiple manual double-checks and associated activities, such as adding handwritten tags to pallets of material.

Material flow status is also synchronized in real time with physical production activities and coordinated with warehouse management system and quality-control software. Work centers are streamlined with minimal material buffer quantities required due to synchronized and just-in-time delivery of materials and assemblies. Automated material flow facilitates the manual workstation “Lean 5S” method of organization in which the location of everything in the workspace is defined and clearly marked with material delivered based on production plans.

Robotics, mechatronics, vision, and other technologies are being combined to create automated material handling systems that provide just-in-time material flow to machines and people. Some standard components are conveyor systems, linear magnetic transport systems, robots, warehouse management systems (WMS), autonomous mobile robots (AMRs), and automated guided vehicles (AGVs).

Advances in AVG technology include laser navigation that is accurate to a quarter of an inch,



contactless charging, and enabling the facility to avoid the requirement for in-floor wires. This works in concert with IT, engineering, and operations groups systems managing material flow for production from shop floor to the enterprise systems.



Cloud and Edge Computing

Cloud computing delivers secure and powerful applications often at a lower cost than supporting on-premises computing centers. Suppliers such as Amazon Web Services (AWS), Google Cloud for manufacturing, and Microsoft Azure provide cloud architectures and services that are important industrial digitalization building blocks. Their cloud software architectures and tools are built on open standards, are highly refined and easy to use, and support the development of a wide range of industrial applications, including historians, artificial intelligence, expert systems, machine learning, and digital twins. Evidence of commitment by web services providers like AWS, Microsoft, IBM, and Capgemini is their participation in the OPC Foundation by technology companies.

Industrial edge computing devices are used to sense, control, and run local programs, as well as communicate with industrial controllers and applications some distance away or in the cloud. Edge devices are part of the distributed computing architecture performing tasks and, in many cases, productively interacting with enterprise and cloud computing applications. There are now a wide range of edge computers at various power and price points, from multicore processors to Raspberry Pi devices.

The major value of edge computing is executing applications close to physical production, achieving fast response times with very low latency and capturing real-time data. This is required for real-time closed loop manufacturing business operations to be profitable and competitive. The incorporation of higher-level functions directly into this new breed of powerful field devices and industrial controllers, coupled with real-time transaction processing business systems, is diminishing the need for industrial middleware software.

Business systems have evolved more rapidly than industrial systems to meet the requirements of business functions, including supply chain, customer service, logistics, and internet commerce. Middle level software and computers have served their purpose of buffering, synchronizing, translating, and refining sensor and controller information, but they have also created brittle systems with a great number of middle level computers, duplicate databases, complex configuration control, and software that is expensive and difficult to maintain.

Edge computing is computing that takes place at or near the physical location of either the user or the source of the data. Distributed functions at the edge include optimization, expert systems, and artificial intelligence with new classes of devices. These devices include:

- ▶ **Edge Gateways Supporting Legacy Systems.** Industrial edge gateways are typically rugged industrial computers running middleware software that connects to PLCs, drives, and other edge devices to contextualize information and map it to data enterprise software and databases. Edge gateways are ideal for providing edge computing functions that leverage installed legacy controls and automation-extending capital equipment investments.
- ▶ **Edge Industrial Computing Platforms.** Rugged edge computing platforms provide gateway functions plus many other functions, including distributed control, optimization, webservers, OPC UA server and clients, artificial intelligence (AI), REST APIs, image recognition, and cloud communications (AWS, Azure, etc.). Many incorporate multiuser environments, such as Docker and

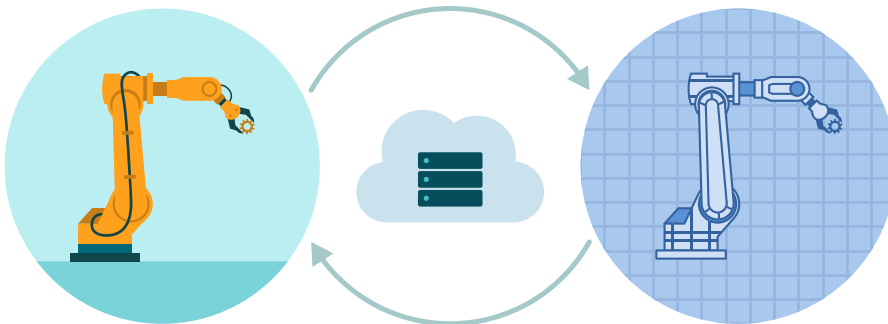
Kubernetes, enabling the addition of user applications written in standard programming languages, including Python and JavaScript.

- ▶ **Intelligent/Smart Field Edge Devices.** Intelligent/smart field edge devices are a new class of smart field devices, including sensors and actuators, that are intelligent and communicate directly to controllers, enterprise, and cloud applications. These devices incorporate distributed control functions that include optimization, web servers, OPC UA server and clients, REST APIs, and cloud communications (AWS, Azure, etc.). User based initiatives are defining the new architecture based on these concepts including the NAMUR Open Architecture (NOA) and Open Process Automation Forum (OPAF) standards.

Digital Twins

The digital twin has become one of the most powerful concepts of Industry 4.0. It should be familiar to automation and control people, since it is a higher level of closed-loop control that ideally incorporates all the factors of a manufacturing business that affect efficiency and profitability of production, including incoming material quality, order flow, economic factors, customer orders, production plans, work in process (WIP) flows, and machine efficiencies.

Digital twins are a virtual representation of a real-world process that is constantly updated with its real-time twin to achieve complete manufacturing closed-loop control that is optimized and responsive to changes. The implementation of model-based, real-time, closed-loop monitoring, control, and optimization of the entire manufacturing and production process, this concept is helping organizations



achieve real-time integrated manufacturing. The digital twin virtual model of ideal manufacturing operations and processes constantly benchmarks actual production metrics in real time, providing a wealth of information that organizations use to identify and predict problems before they disrupt efficient production. This is a prominent example of a practical macro-level, closed-loop control that is now feasible with the advanced hardware, software, sensors, and systems technology currently available.

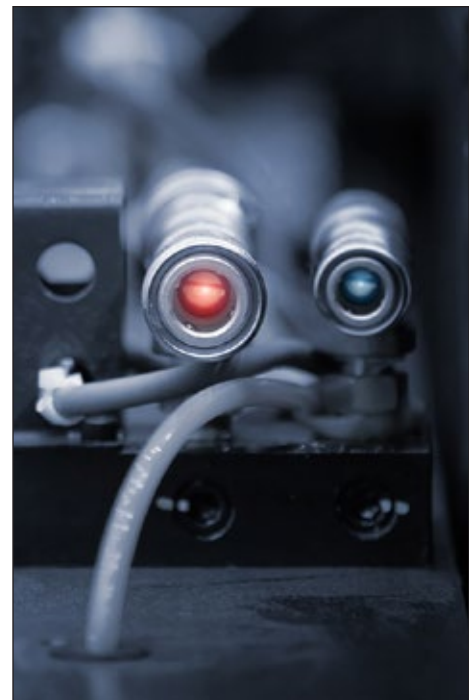
A critical part of the creation of a digital twin is the need to have a complete information set, including the capture of real-time information with a wide range of sensors based on these requirements. To facilitate this information collection, some common strategies include:

Leveraging Existing Connected Sensors

This is typically the popular first step, since it does not require physical installation of new sensors. What it does require is application engineering and a software project to link information to the IT network. It may also call for new software to be added to SCADA, PLC, HMI, and DCS systems in order to accomplish communication with enterprise and other systems.

Adding New Sensors to Existing PLCs & Controllers

If there are unused sensor interfaces on the controller or available slots to add new interface cards that can accommodate more sensors, then adding new sensors to existing controllers can be an option. This also requires application engineering to add these sensors to the program in the controller, and possibly the addition of new software to HMI and DCS systems that facilitate communication with enterprise and other systems. With this strategy, there is a risk that making changes in these controllers and systems will create performance and operating issues, so a significant amount of systems and application engineering to ensure reliable operation may be needed.



Installing Edge Devices

In addition to practical concepts, like the digital twin, the Industrial Internet of Things (IIoT) has led to companies bringing a wide range of edge devices to market. These edge devices are designed to capture information and communicate directly to enterprise systems and cloud applications, particularly Amazon Web Services and Microsoft Azure. Many new sensors are not required to be part of the control and automation strategies in the plant, but they are required to monitor operating parameters for a complete digital twin and close the information loop. Edge devices typically connect directly to the IT network. The advantage to this is that they are non-intrusive, having no or very minimal impact on existing control software architecture. This can be an efficient way to communicate directly with production, maintenance, and business systems.

Install Smart Sensors

There are new classes of smart sensors emerging that can communicate directly with production, maintenance, and business systems. Wireless sensors can be an efficient way to acquire data with standard technology, including WirelessHART and ISA100, primarily used in process applications. For discrete points, the IO-Link wireless version is an option. There are also a number of sensors that communicate over standard wireless ethernet Wi-Fi with various software interfaces.

OPC UA Normalizing & Integrating Data

OPC UA is emerging as a fundamental technology for implementing the digital twin. Digital Factory OPC UA technology provides an efficient and secure infrastructure for the communications of contextual information, from sensor to business enterprise computing, for all automation systems in manufacturing and process control. OPC UA is leveraging the accepted international computing standards and putting automation systems on a level playing field with the general computing industry. OPC UA uses common computing industry standard web services, which are the preferred method for system communications and interaction for all networked devices. The World

Wide Web Consortium (W3C) defines a web service as “a software system designed to support interoperable machine-to-machine interaction over a network.” This is precisely the task of automation systems. OPC UA is being built into a number of sensors and other devices in order to simplify the communication process.

A Path to Holistic Integration

With the implementation of the digital twin, manufacturers may be able to achieve greater profits and competitiveness through real-time closed-loop manufacturing optimization. This is an example of holistic integration of all the factors of production, and though the digital twin is virtual, it represents one of the most tangible examples of the Industrial Industry of Things that is bringing value to today’s manufacturers.



Ethernet IP Industrial Edge Field Devices

Internet Protocol communication transports are transforming industrial systems with open IP-based transport protocols, including SPE, Ethernet APL, and 5G wireless. The industrial edge is entering mainstream computing and IoT with the integration of Single Pair

Ethernet standard 10BASE-T1, making IP communications embedded in end field devices, including sensors and actuators, cost effective.

Ethernet-based networks supporting industrial controls and automation leverage the advantages of ethernet infrastructure products produced in high volume, such as lower costs of hardware, software, and support. SPE finally is the way to unlock more information directly from sensors, actuators, drives, motor starters, and other devices.

Single Pair Ethernet (SPE)

Single Pair Ethernet (SPE) Ethernet network IEEE 802.3cg technology provides communications over two wires using the Internet Protocol

(IP). SPE delivers standard unmodified Ethernet built on the IP to enable intelligent field devices, including sensors, motor controls, and actuators, to achieve industrial digitalization and accomplish the vision of Industry 4.0. SPE leverages standard IP message routing to deliver data anywhere in an ethernet architecture. SPE has significant engineering, maintenance, and installed cost advantages over standard ethernet with over 75% smaller cable diameter, reduced weight, cost, and 30% more bend radius than CAT 5. It also provides a potential to reuse existing installed twisted pair field wiring to carry SPE communications, simplifying plant and machine retrofits.

The standard also provides a Power over Data Line (PoDL) option with up to 50 watts of power for edge devices. There is an option for SPE Multidrop 802.3cg with auto negotiation at 10<bits/s, PoDL, 16 device drops, and 50-meter length. Multidrop for sensor networking has tremendous installed cost advantages over point-to-point networking.

Hazardous Areas Advanced Physical Layer (APL)

SPE is also the basis for the Advanced Physical Layer (APL) to bring Ethernet to field-level instruments in hazardous areas. Ethernet at the field level will make digitalization for process industries a reality with its universality and speed. Current and voltage will be limited to have intrinsically safe circuits suitable for Zone 0, Zone 20, or DIV 1 installations. The main goal is to adopt proven technologies and options in the field of process automation.

Since Ethernet-APL is logically ethernet, any industrial network protocol device that electrically conforms to 10BASE-T1L Ethernet physical layer standard (IEEE 802.3cg-2019) can take advantage of this physical layer. EtherNET/IP, Profinet, and other protocols can run simultaneously on an Ethernet-APL network, as they do today on standard ethernet with the same bandwidth and latency issues. This provides for transition from these legacy protocols to new open intelligent protocols.





OPC Ecosystem Unifying Industrial Manufacturing

The OPC Foundation has become the unifying focal point for information technology, operations technology, industrial/process controls, manufacturing automation, Internet of Things (IoT), and cloud organizations participating in more than 65 joint working groups. These groups are focused on defining and implementing standard contextual and semantic data models from sensors/actuators and other industrial field devices to enterprise and cloud systems. The goal is to have secure, reliable communications between multiple vendors with platform- and domain-agnostic interoperability, from sensors to enterprise to cloud applications. OPC Foundation standards, semantic data models, and this type of ecosystem simplify application engineering and enterprise software development while improving system quality.

There are more than 850 OPC Foundation members and thousands of OPC-compliant products. In addition to a wide range of industrial members, the active participation of IT technical leaders is notable, including Microsoft, AWS, Google, IBM, and SAP. OPC Foundation standards are becoming widely adopted by IT, OT, and cloud suppliers, creating a valuable and efficient distributed industrial manufacturing architecture. OPC UA Companion Specifications offer complete use case models and templates that achieve a unified, vendor-independent data interchange that decreases application engineering labor and improves quality.

The OPC Foundation's globally available UA Cloud Library was co-developed with the Clean Energy and Smart Manufacturing Innovation Institute (CESMII) and has grown to encompass:

- ▶ More than 250 active users
- ▶ More than 65 information models, including AutoID, DEXPI, MDIS, and MTConnect
- ▶ VDMA Use Case Companion Specifications

The UA Cloud Library makes OPC UA information models available in the cloud on a global scale, giving users an efficient way to find and use OPC models. This simplifies application engineering for users by allowing access to all known OPC UA information models via an open, global, single-source of truth. It also facilitates global OPC UA information model coordination and harmonization efforts by making it easy to search and cross-reference the latest OPC UA companion specifications in real-time. The application of OPC UA companion spec becomes as simple as adding a printer to a computer.

MQTT Support

Supporting bandwidth-restricted communications methods, the OPC UA PubSub extension enables communication between OPC UA applications using a publish-subscribe message pattern instead of request-response. UA PubSub is a generic mechanism designed to work over any message-based middleware, including MQTT, for bandwidth-constrained networks. It provides a complete solution with support for binary and JSON encodings with end-to-end security, as well as other protocols. Standard configuration information model and file format integrated with OPC UA information models provide continuity, simplifying configuration and application engineering.



MQTT Sparkplug Alternative

Another possibility that allows users to create unique data model definitions specific to their company is the Sparkplug open-source specification hosted at the Eclipse Foundation. It provides MQTT clients the framework to integrate data from their applications, sensors, devices, and gateways within the MQTT infrastructure. The aim of the Sparkplug Specification is to define an MQTT Topic Namespace, payload, and session state management that can be applied generically for the requirements of real-time SCADA/control HMI solutions.

OPC Foundation Field Level Communications

The OPC Foundation Field Level Communications (FLC) is modernizing the most basic industrial communications with mainstream computing Symantec/contextual communications, modernizing the most basic industrial communications to the industrial edge, including sensors, actuators, and field devices.

OPC UA FX is the first IP field device approach incorporating industry global standard semantic contextual data connectivity and is a serious contender to become the unifying industrial protocol to support open architecture multivendor industrial digitalization. OPC FLC is the first multivendor open standard semantic contextual data connectivity communication solution between sensors, actuators, controllers, enterprise, and cloud that meets all the requirements of industrial factory automation and process automation. OPC

UA FX continues to make rapid progress to modernize the most basic industrial communications with mainstream computing data concepts to the industrial edge. It can be used to transport data over any IP network and inherently supports a wide range of transports. Ethernet advanced physical layer (APL) two-wire Ethernet for process automation and hazardous locations is based on IEEE and IEC standards with preparations for APL testing in the OPCF Certification Lab. The OPC foundation is working closely to align with the TSN Profile for Industrial Automation (TSN-IA-Profile), which will be standardized by the IEC/IEEE 60802 standardization group. This will help ensure that a

single, converged TSN network approach is maintained so that OPC UA can share one common multi-vendor TSN network infrastructure with other applications.

IIoT and Intelligent Sensors

There is a growing trend to embed intelligence in sensors, which is a foundational part of Industry 4.0 concepts. Sensors communicate with controls and automation systems, and simultaneously and directly with business systems. This is also part of the NAMUR New Open Architecture (NOA), a collaboration with VDI/VDE and several prominent industry leaders, including ABB, BASF, Bayer Technology Services, Bilfinger Maintenance, Endress+Hauser, Evonik, Festo, Krohne, Lanxess, Siemens, and Fraunhofer ICT.

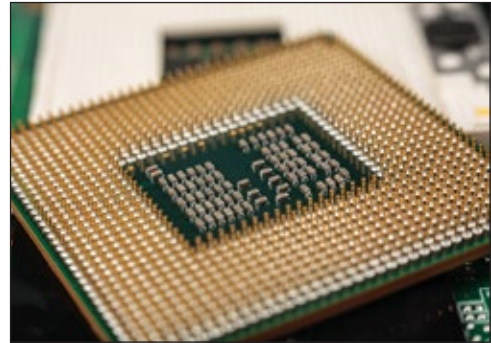
IIoT is becoming a reality with sensors and actuators embedded in physical objects, from roadways to pacemakers, and linked through wired and wireless networks, leveraging the Internet Protocol (IP). Industrial controllers are starting to follow this trend by providing data refinement, local historians, analytics, and advanced control at the source end devices. Modern controllers are communicating with all levels of systems using the “IP plumbing” that is pervasive in manufacturing plants, including capabilities to send email and FTP files, and serving up WEB pages. Open communications is being supported using XML, SOAP, SNMP, and OPC UA.

Over the past 10 years, there have been tremendous technological innovations and refinements that are starting to be deployed in level 0 and level 1 devices. These devices incorporate powerful new CPU chips to simplify automation architectures. The rapid increase in the power, memory, and communications integrated on CPU chips with associated lower costs is driven by the high-volume production of smart phone and tablet computers.

The new breeds of industrial controllers and embedded industrial end devices are incorporating this power and adding features that include embedded web servers, email clients, and web services. These capabilities



enable level 0 and level 1 devices to communicate directly with level 4 and level 5 systems. It is common now to see dual-core CPUs in controllers, and a number of companies have announced quad-core-based controllers. These more powerful industrial controllers are becoming automation computing engines that are starting to collapse the typical 5-level model and make automation systems more flexible and responsive.



The incorporation of higher-level functions directly into this new breed of powerful industrial controllers is starting to eliminate the need for middle level software. Middle level software and computers have served their purpose of buffering, synchronizing, translating, and refining sensor and controller information. But they have also created a great number of middle level computers, databases, and software that is expensive and difficult to maintain. The interim solution is the migration to more powerful computers and the virtualization of existing middle level software. This migration and virtualization improve performance and centralize software maintenance and configuration control. Over time, the functions of this middle level software are being taken over by the new, more powerful controllers. The new, high level of communications and computing at end devices is opening the possibilities for holistic and adaptive automation to increase efficiency. This is a logical evolution in step with the Internet of Things trend and will lead to more responsive and efficient production.

Low-Code & No-Code Empowers Citizen Developers

A software revolution ignited by no-code/low-code platforms is empowering industrial people to be citizen developers. They are creating applications in AI, expert systems, predictive maintenance, optimized machine operations, and flexible manufacturing using drag-and-drop interfaces instead of manual coding and employing quality-tested models. Now, automated solutions can be developed faster adjusted more efficiently as needed. This higher level of adaptability is critical in manufacturing with its constantly changing conditions. This is analogous to how spreadsheets democratized the use of computers for

a wide range of applications, enabling subject matter experts to directly apply their knowledge.

Since 1969, industrial automation and control professionals have been empowered with no-code ladder logic programming that evolved into the IEC 61131-3 International Electrotechnical Commission (IEC) standard, first published in 1993. The standard continues to be enhanced and extended in IEC committees and by the not-for-profit PLCopen trade organization, which is comprised of a broad range of volunteer industry experts continually defining and adding new functions to meet new industry needs. Noteworthy enhancements are industrial safety, motion control, robotics, OPC UA, and other functions described on the PLCopen website.

Mobile & Remote Worker/Connected Worker Technology

Mobile devices give employees information and capabilities that have traditionally been fixed in the control room so they can work more efficiently and effectively. Smart phones, tablets, and smart glasses incorporate front-facing, high-definition camera, audio, and visual input. This capability has been available for some time, but the cost has become significantly lower, driven by commercial and consumer products.



New technology is enabling remote monitoring capabilities to improve operational effectiveness. This presents users with opportunities and challenges to be evaluated for practical applications. The goal is to improve manufacturing or processing uptime and efficiency. Subject matter experts are becoming increasingly hard to find, and companies need to find ways to use them more efficiently. The latest remote monitoring tools allow experts to analyze problems and abnormal situations, as well as determine ways to improve and optimize operations, without traveling to the site.

Worker productivity and responsiveness are being improved with technologies that directly connect workers to manufacturing systems, making them an informed, integral part of production in real time. Mobile computing and communications technology cost reductions and increased performance continue to increase the capabilities and value of workers in production, and the connection of workers is being accelerated using the expanding range of commercial off-the-shelf technologies, including voice and video headsets, smart glasses, and virtual reality devices. Productivity enhancers include:

- ▶ Manuals and equipment identification and lookup from anywhere
- ▶ Real-time superimposed data
- ▶ Audiovisual linking to subject matter experts
- ▶ Direct access to production

Predictive Maintenance Applications

Going beyond scheduled maintenance analytics, expert systems and artificial intelligence are analyzing machines, processes, and new sensors to perform predictive maintenance with more precision. This enables the detection of failure patterns in machinery and parts early on so manufacturers can take preventative action and avoid costly malfunctions. Advancements in technology for low-cost vibration sensing in particular has been dramatic. Predictive maintenance coupled with connected workers creates a highly efficient approach that also integrates plant workers' experience into the system and analysis.

Remote Expert Services

Connectivity and edge processors empower suppliers to offer remote expert monitoring services. Experts and analytic software continuously monitor controllers and control systems for abnormal situations and advise site personnel of current problems or predictions of future problems. Control suppliers that offer these services have experts and software that can quickly detect issues with the controllers, components, and software that they provide. Since most plants have equipment from multiple suppliers, the value of this service may be limited if the provider does not monitor all equipment and applications. In some general equipment and process control applications, contract experts can detect and advise on plant production issues. Subject matter experts in specific manufacturing and process areas can be used on demand for special problems and issues. A big advantage of the services approach is that a third party has a remote, 24/7 operations center to constantly monitor a company's systems.

Some providers collect performance analytics information to learn how machinery is performing and provide alerts when data falls outside of predefined parameters. This requires developing rules with input from plant staff because they understand the plant operations. Alternatively, manufacturing companies can run an inference engine with rules based on the dynamics of the operation. Once most of these problems and issues are identified, someone needs to be onsite with the right tools, information, and spare parts to get things working. Determining the best methods to achieve improved uptime and efficiency is the overall challenge.

Robots and Cobots

The cost and ease of use in robotics has changed dramatically, particularly with collaborative robots. More possibilities are being created with the growing trend of modular industrial robot components, which can be used to assemble optimal robot structures for different applications. In addition, easy to use software tools are allowing people and plants to define robot actions without programming.



Collaborative Robots

Collaborative robots can improve manufacturing in worker safety for companies of any size. These lightweight, inexpensive robots have safety features specifically designed to foster cooperation in a production environment. Collaborative robots can sense humans and obstacles, and automatically stop whatever they're doing if it would cause harm or destruction. Protective fences and cages are not required, lowering implementation cost. These robots are attractive investments, with a typical cost of less than \$40,000 US. Additionally, the robots can be deployed without hiring specialized engineers to program the simplified software. Moving the arms and end effectors to the desired positions is straight forward. This is a physical form of the popular computer programming concept "what you see is what you get (WYSIWYG)." It is intuitive and has been proven in many implementations to broaden the application of technology.

Integrated Vision

Coupling robots with vision systems and image recognition software expands their use for more free-form applications. Robots can grab dissimilar parts in assembly settings, pack boxes in shipping facilities, organize bins, load machine tools, inspect parts, and perform many other helpful tasks.

End Effectors

End effectors include devices for picking up a wide range of parts of various types. It is the last link, or end, of the device at the end of a robotic arm designed to interact with the environment. In addition, end effectors with built-in tools are being used in industrial applications for grinding, sanding, welding, riveting, screwing bolts to specific torque, spray painting, machine part tending, and material handling.

The number of innovative robotics end effector devices has increased significantly. It is worth noting that there is an acceleration of robot use in other applications, such as restaurants, construction, and healthcare. This in turn creating a broader array of end effectors.

Semantic Technology/Data Analytics

The ultimate goal of semantic technology is to help people and machines understand data. It is a significant advantage over traditional unstructured information. Semantic technology combines elements of semantic analysis, natural language processing, data mining, knowledge graphs, and related fields. It encodes meanings separately from data and content files, and separately from application code, enabling machines and people to understand, share, and reason with them at execution time. With semantic technologies, adding, changing, and implementing new relationships or interconnecting programs in a different way can be just as simple as changing the external model that these programs share.



With traditional information technology, meanings and relationships must be predefined and “hardwired” into data formats and the application program code at design time. This means that when something changes, previously unexchanged information needs to be exchanged, or two programs need to interoperate in a new way, requiring humans to get involved. Offline, the parties must define and communicate the knowledge needed to make the change and then recode the data structures and program logic to accommodate it. These changes must then be applied to the database and the application. Then, and only then, can they implement the changes. This is a common issue that requires PLC representation of data to be mapped to application data representations.

These technologies formally represent the meaning involved in information. For example, ontology can describe concepts, relationships between things, and categories of things. These embedded semantics with the data offer significant advantages, such as reasoning over data and dealing with heterogeneous data sources.

Semantic technologies provide an abstraction layer above existing IT technologies that enables bridging and interconnection of data, content, and processes. Second, from the portal perspective, semantic technologies can be thought of as a new level of depth that provides far more intelligent, capable, relevant, and responsive interaction than with information technologies alone. Semantic technologies would often leverage natural language processing and machine learning in order to extract topics, concepts, and associations between concepts in text.

The IEEE has held an International Conference on Semantic Computing since 2007, and a conference on Knowledge Graphs and Semantic Computing has been held since 2015. The 18th IEEE International Conference on Semantic Computing (ICSC2024) addresses the derivation, description, integration, and use of semantics for all types of resources, including data, document, tool, device, process, and people. The scope of ICSC covers such topics as analytics, semantics description languages and integration, interfaces, and applications.



Spatial Computing/Intelligent Vision

Spatial computing is a technology that enables computers to blend in with the physical world in a natural way. It brings people into the digitalization loop so they can dramatically increase manufacturing operations and create experiences and applications that were previously impossible. Spatial computing devices display the real world and, simultaneously, real-time operating parameters in a way that appears three-dimensional. The number of smart glasses and helmets being used has grown dramatically and they are gaining popularity in industrial applications. One reason is that they allow integrated audio for hands-free operation and communication with other workers and remote experts. Some also feature multiple 360-degree cameras, Wi-Fi, Bluetooth, and GPS that can be used for personnel tracking in hazardous areas.

This equipment can be used to bring up assembly instructions, procedures, and operating manuals with step-by-step instructions in the worker's field of vision. In assembly areas, employees can be guided with pick-by-vision instructions that show customer order information. Assembly of individual items can be confirmed with voice-controlled barcode scans using the camera built into the glasses. Repair guides, graphical plant diagrams, troubleshooting tips, remote experts, and early safety warnings can also be displayed. Plant personnel who need to look at and hear equipment and processes to diagnose issues remotely can be shown information that allows them to prepare the proper tools and parts before going out in the field.

Rather than a supervisor physically having to come to help a production line worker, augmented reality allows the supervisor to see exactly what the worker is seeing and provide help remotely. This allows organizations to multiply their experienced personnel and efficiently provide valuable mentoring to new people. QR codes can also be added to equipment that automatically bring up information using smart devices. Another viable technology is wired or wireless industrial video cameras, with or without audio, that can keep track of machines and process vital signs remotely. Combined with image recognition software, videos can provide real-time, closed-loop quality monitoring and control.

A great example is factory workers using a smart phone, tablet, or smart glasses. They can simultaneously view a physical machine, real-time variables, and technical manuals. Spatial computing is related to both augmented reality (AR) and virtual reality (VR). AR means overlaying digital content onto the real world, typically using a phone or smart glasses. Mixed reality (MR) employs a blend of AR and VR, enhancing the user's understanding of operations, for example, showing a representation of the inside of a machine and the real-time operating data. Devices that employ spatial computing might also have speech recognition features to support voice commands, enabling hands-free operation. In addition, people can collaborate with remote experts that will see the same information and can advise workers.

While using robotic systems helps with general efficiency and productivity at an assembly plant, there are additional benefits that accompany the incorporation of a vision system with that robot. A robotic vision system consists of one or more cameras connected to a computer. The computer contains a processing software program that helps the robot interpret what it sees, for example, identifying parts in assembly processes without requiring specific placement and performing real-time quality analysis.

Wireless 5G Private Networks

Wireless 5G private networks are emerging in manufacturing as a method to support mobile workers and monitor and control equipment. Industrial digitalization requires getting reliable, timely,

and actionable information for real-time control and in the hands of stakeholders, including process operators, maintenance technicians, environmental health and safety people, and supply chain people. This information is in many areas, including production plants and outdoor areas out of the reach of Wi-Fi and public cellular signals.

The reach of wireless 5G private networks eliminates the need for operators walking around with sheaves of paper to record procedures, information, and inspection results and then having to transfer all of that into a computer system, which is time-consuming and prone to errors. Private cellular is furthering digitalization goals to take advantage of such things as analytics, machine learning, and digital guided procedures with pervasive communications throughout operations.

The broad use of wireless 5G technology benefits from the economies of scale that is created by refined technology. It is superior to industrial Wi-Fi, with higher speeds, easy deployment, and lower initial and lifecycle cost. Certainly, radio, satellite, and cellular connections are good choices for remote equipment in applications like water/wastewater, oil & gas, and pumping stations. In a factory or process plant, it may be appealing to add a communication device to a machine to remotely troubleshoot and diagnose issues. However, though this piecemeal approach may be warranted in special cases, it may be more advantageous to take a systems-level approach. A well-managed, cyber-secure connection to the automation system network allows secure access to the entire system and simplifies administration. Older controllers without Ethernet connections can be interfaced to the plant system network using Ethernet gateways, which are available from a number of suppliers.

ABOUT THE AUTHOR



Bill Lydon is contributing editor of Automation.com and ISA's *InTech* magazine. He has more than 25 years of experience designing and applying automation and controls technology, including computer-based machine tool controls, software for chiller and boiler plant optimization, and a new generation building automation system. Lydon was also product manager for a multimillion-dollar controls and automation product line, and later cofounder and president of an industrial control software company.