



Automation com MONTHLY

A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

InTech IS NOW
Automation.com Monthly!
Read more on p. 54

IIoT & Digital Transformation

The Role of Cloud Computing in Industry 4.0

Edge Computing Fundamentals

Secure Data Access for Industrial AI

Customize Batteries for Maximum Performance

Enhancing Power Grid Resiliency

Seven ISA Fellows Named for 2025



A MESSAGE FROM ISA

The International Society of Automation (ISA) is a non-profit professional association whose vision is to create a better world through automation by driving the advancement of individual careers and the overall profession. ISA owns Automation.com, a leading online publisher of automation-related content.

This digital magazine, *Automation.com Monthly*, is one way ISA fulfills its mission of empowering the global automation community through standards and knowledge sharing. The magazine is published nine times per year. ISA members receive the magazine as part of their annual [membership](#) and get access to archived magazine issues, including *InTech* and *AUTOMATION 202X*. Qualified non-members can [subscribe](#) to the magazine and other publications.

[ISA](#) helps its members and the global automation community advance technical competence by delivering standards-based technical resources to engineers, technicians, and management engaged in industrial automation. ISA develops widely used global standards; certifies professionals; provides education and training; hosts conferences and exhibits; publishes technical articles and other resources; and provides networking and career development programs.

ISA created the ISA Global Cybersecurity Alliance (isagca.org) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. Through a wholly-owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (isasecure.org) and the ISA Wireless Compliance Institute (isa100wci.org).

EDITORIAL & PRODUCTION

CHIEF EDITOR

Renee Bassett rbassett@isa.org

SENIOR CONTENT EDITOR

Melissa Landon mlandon@isa.org

SENIOR CONTRIBUTING EDITOR

Jack Smith jsmith@isa.org

ISA STANDARDS SENIOR DIRECTOR

Charley Robinson crobinson@isa.org

ADVERTISING PRODUCT MANAGER

Cathi Merritt cmerritt@isa.org

DIGITAL MEDIA PROJECT MANAGER

Matt Davis mdavis@isa.org

ART DIRECTOR

Bonnie Walker

DIGITAL DESIGNER

Colleen Casper

ISA EXECUTIVE BOARD

ISA EXECUTIVE DIRECTOR

Claire Fallon

ISA PRESIDENT

Scott Reynolds

ISA PRESIDENT-ELECT & SECRETARY

Ashley Weckwerth

ISA PAST PRESIDENT

Prabhu Soundarajan

ISA TREASURER

Ardis Bartle

MANAGING DIRECTORS

PUBLICATIONS & SPONSORSHIPS

Rick Zabel

STRATEGIC ENGAGEMENT

Liz Neiman

GOVERNANCE & MEMBERSHIP

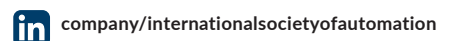
Andrea Holovach

EXTERNAL AFFAIRS

Ed Manns

EDUCATION SERVICES

Dalton Wilson



Mimo: A Large-Language Model Educated on ISA Content

Ask Mimo your questions about industrial automation at

<https://www.isa.org/mimo>

INDUSTRY 4.0

- 7 **The Role of Cloud Computing in Industry 4.0 and Beyond**
Scalability, cost savings, real-time data insights and more are benefits of cloud computing. **By Ravi Soni**

DIGITAL TRANSFORMATION

- 19 **Edge Computing Fundamentals**
Edge computing supports Industry 4.0, smart manufacturing and digital transformation. **By Ryan Treece and Sujata Tilak**

INDUSTRIAL AI

- 27 **Secure Data Access for Industrial AI**
Accessing production data through a DMZ can be done with well-designed tunnel/mirror software. **By Xavier Mesrobian**

REMOTE OPERATIONS

- 30 **Custom Tailor Batteries for Maximum Performance**
Maximize the power supply of remote wireless devices to suit specific remote applications. **By Sol Jacobs**

ENERGY INFRASTRUCTURE

- 36 **Enhancing Power Grid Resiliency**
New technology improves grid reliability and safety through early fault detection. **By James Haw**

RECOGNITION

- 42 **Seven ISA Fellows Named for 2025**
These automation professionals were recognized by their peers for their professional accomplishments and society service. **By Renee Bassett**

THE LATEST

- 46 **Association News**
- ISA/IEC 62443 Standards
 - OT Cybersecurity Summit Keynotes, Tracks
 - ISA 2025 Society Leadership
 - Top 20 Blog Posts of 2025
 - ISA Past President: Proud of a Great Year

THE LATEST

- 52 **More from Automation.com**

TALK TO ME

- 54 **ISA's Magazine Continues to Digitally Transform**
By Renee Bassett

Unlimited SCADA

Unlimited: That's the number of data, tags, connections, clients, and more you get with one Ignition license at no extra charge.

Your finance department will love you.



Data



Tags



Device
Connections



Clients



Scalability



Designers

Ignition!

One Platform, Unlimited Possibilities

Visit [inductiveautomation.com/scada-software](https://www.inductiveautomation.com/scada-software) to learn more.

Version 11
is committed
to security



Cogent
DataHub™



The latest release of DataHub software from Skkyenet provides a new security model for real-time access to process data. Now with LDAP and TOTP support and a new data diode mode, the software makes secure, outbound connections through firewalls, isolating OT networks, fully supporting DMZ architectures, and making secure cloud connections.

[Learn more >](#)

SKKYNET™
SECURE INDUSTRIAL IOT REDEFINED



A MESSAGE ABOUT OUR SPONSORS

ISA's mission and *Automation.com Monthly* digital magazine are supported by advertisers and sponsors. They contribute technical articles, case histories and other technical resources designed to educate, inform and inspire automation professionals and advance their careers. Articles from advertisers are identified with a "Sponsored" tag.

To obtain further information from any of the advertisers in this issue, contact them directly using the information found in their ad or author bio.

For news and product information from suppliers, visit Automation.com. The online directory of [Featured Suppliers](#) lists automation product vendors, machine manufacturers and systems integrators. You can also [subscribe](#) to topical newsletters and alerts that will deliver news, new product and technical resources via email.

A Note to Potential Advertisers

With decades of experience crafting high-quality periodicals, the International Society of Automation (ISA) and its media brand Automation.com have helped thousands of automation and control professionals do their jobs and enhance their careers. We can help you inform these professionals about your solutions through our publications, events and sponsorship opportunities.

Advertisers Index



International Society of Automation
Setting the Standard for Automation™

Page17, 45



inductive automation

Page4



Page18



Page5



Page25

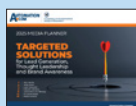


Page26

ADVERTISING & SPONSORSHIP

Rick Zabel, **PUBLISHER** - rzabel@isa.org
Ed Manns, **SALES MANAGER** - emanns@isa.org
Chris Nelson, **ACCOUNT EXECUTIVE** - chris@isa.org
Gina DiFrancesco, **ACCOUNT EXECUTIVE** - gina@isa.org

Send press releases to Press@automation.com
Send ad materials to Materials@automation.com



2025 Media Planner

To order reprints of *InTech* print or digital articles, contact reprints@mossbergco.com or 800-428-3340.

The Role of Cloud Computing in Industry 4.0

By Ravi Soni



Benefits include scalability, cost savings, real-time data insights and more.

Cloud computing is transforming the fast-moving manufacturing world. For those leading the charge in industrial manufacturing, understanding cloud computing's role is not just beneficial—it's essential. Due to its scalability, flexibility and cost effectiveness, cloud computing helps manufacturers reach their business goals of efficiency and innovation.

In simple terms, cloud computing means using the Internet to access and use information technology (IT) services such as storage, servers, databases and software. Instead of having these resources inhouse, which requires significant investment and

maintenance, cloud computing lets users use them as needed through service providers with usually pay-as-you-go pricing. This approach saves money, allows for simple adjustments to operations and reduces the burden of managing complex IT infrastructures.

Cloud computing affects industrial manufacturers by enabling real-time data collection and analysis directly from various data sources on the shop floor, which turns vast amounts of data into actionable insights. This capability allows many insights to inform, describe and predict an event and even prescribe an action to prevent an event such as

machine downtime or a quality defect. Cloud computing also makes it easier for manufacturing professionals to collaborate remotely by sharing expertise and solving problems without geographical limits. Additionally, it supports flexible operations, which allows manufacturers to adapt quickly to market demands or operational changes.

According to the [Hackett Group's research report](#) on the business impact of cloud adoption in the industrial manufacturing sector, cloud computing has enhanced operational efficiency, which is evidenced by a 16% increase in overall equipment effectiveness (OEE) and a 39% reduction in unplanned IT downtime. Supplier management has seen a 33% increase in sourcing savings and a 20% reduction in staffing needs per million dollars of spending. Sales efficiency and customer satisfaction improved notably, with a 42% increase in revenue per salesperson and a 34% boost in customer satisfaction. In addition,

there's a 22% improvement in new product time to market and a 21% reduction in lead times, which demonstrates increased business agility and innovation. These results highlight the critical role that cloud computing is playing in transforming the manufacturing industry.

This article offers a guide on how cloud computing is transforming the manufacturing industry by enhancing operational efficiency, driving innovation and enabling Industry 4.0 initiatives. It also emphasizes the benefits of cloud computing such as scalability, cost savings and real-time data insights (Figure 1). It explores deployment and access models (IaaS, PaaS, SaaS), provides case studies from leading companies and highlights challenges like data security and compliance. It also provides actionable steps for successful cloud adoption, such as the leadership alignment, migration planning and skill development that empowers manufacturers to navigate their digital transformation journeys effectively.

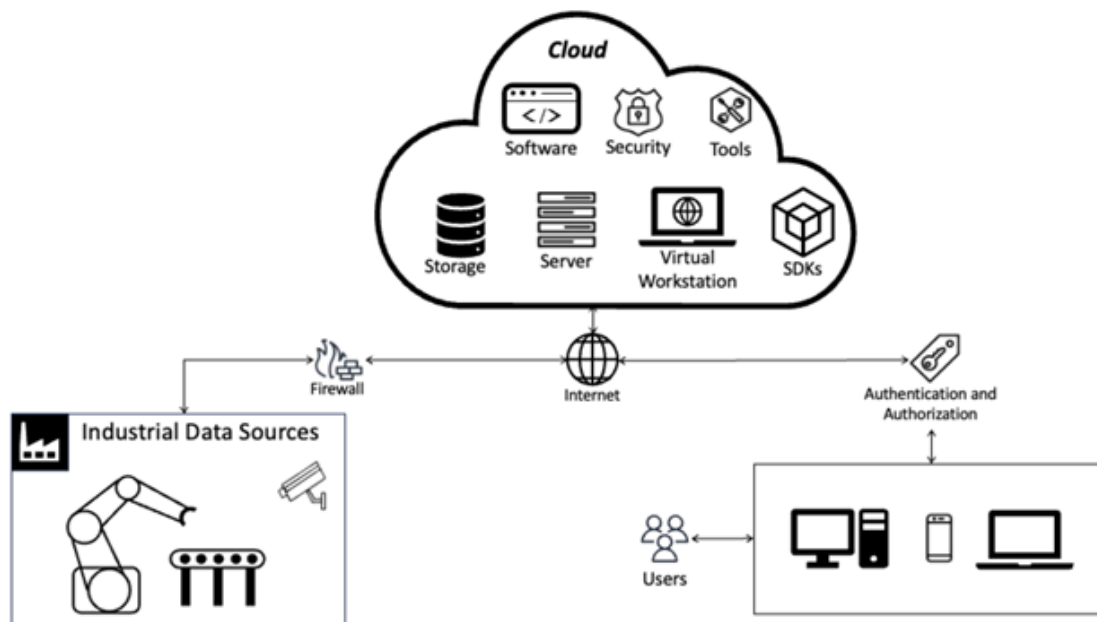


Figure 1: Cloud computing model.

Main cloud benefits for manufacturers

In manufacturing, financial strategy is as crucial as the efficiency of the manufacturing operation. Cloud computing reshapes this strategy through shifting capital expenses to operational expenses, leveraging economies of scale, ensuring responsive capacity management, improving speed and operational agility, freeing up resources to spend on innovation, easily expanding globally and accessing new technologies.

Capital expenses to operational expenses.

Traditionally, manufacturers have had to invest heavily in physical infrastructure before knowing the full scope of its utility. Cloud computing transformed this model. Users pay for computing power as they use it, much like electricity or water utilities. This shift to a pay-as-you-go model means users only pay for the computing resources they use, which offers a flexible financial approach that aligns with production demands.

Leverage economies of scale. The scale of providers amplifies the cost savings of cloud computing. Their vast network and customer base mean the benefits of large-scale operations are passed down to users, which reduces the cost of services compared to hosting their own data center.

Responsive capacity management.

Guessing the right amount of IT infrastructure can lead to wastage or bottlenecks. Cloud computing eliminates this issue. Users can scale resources up or down in response to their manufacturing operations, which

ensures they have the capacity they need without overcommitting resources.

Improve speed and operational agility.

Time is of the essence in manufacturing. Cloud computing dramatically reduces the time it takes to make IT resources available from weeks to minutes. This accelerates innovation and the ability to respond to market changes.

Free up resources to spend on innovation. Running a data center is a significant overhead cost involving maintenance and staff. Cloud computing allows users to offload these tasks and expenses, which frees up capital and resources to invest in areas directly contributing to product innovation and customer satisfaction.

Global expansion with ease.

Manufacturers looking to expand their reach can use the cloud to deploy applications globally efficiently. This capability means users can leverage the same IT applications and serve global teams and customers with reduced latency, which improves the employee and customer experience without a proportional cost increase.

Access to new technologies. Cloud computing enables manufacturers to tap into new technologies such as big data analytics, artificial intelligence (AI) and the Internet of Things (IoT). These technologies can be accessed and integrated into their operations without the need for heavy upfront investment or expert resources, which allows them to gather, analyze and act on data to optimize efficiency and innovation.

Cloud computing deployment models

The cloud deployment model refers to the location of physical infrastructure and who maintains, manages and controls it. Users can choose the deployment model for each application or a business unit based on business needs and goals. It is not uncommon for an organization to use all deployment models simultaneously. Typical cloud deployment models are cloud deployment, public versus private cloud, hybrid deployment and on-premises deployment.

Cloud deployment. In the cloud deployment model, applications are fully hosted in the cloud, which benefits from its agility and scalability. The cloud provider solely maintains the infrastructure. This deployment model is ideal for manufacturers looking to innovate without constraints in physical infrastructure. This model works well where Internet connectivity is not an issue or applications are not latency sensitive.

Public versus private cloud. In a private cloud, cloud computing resources are isolated and dedicated to a single organization. The infrastructure could be maintained by the same organization or a third-party cloud provider. In the public cloud, those resources may be shared with other organizations and infrastructure is maintained by a third-party cloud provider.

Hybrid deployment. The hybrid model connects on-premises infrastructure with cloud resources. This model offers a balance of control and flexibility. It suits

applications that will gradually transition to the cloud while maintaining some components onsite.

On-premises deployment. This model uses virtualization for resource management, which appeals to those who require dedicated resources within their control. Some applications sensitive to latency or have regulatory data residency requirements must stay on-premises. However, leading public cloud vendors enable cloud services on shared infrastructure or provide dedicated hardware to extend the cloud to your premises. The examples are AWS Outpost, MS Azure Stack and Google Anthos.

Each model offers varying degrees of control, which allows manufacturers to select an approach that aligns with their strategic and operational application objective.



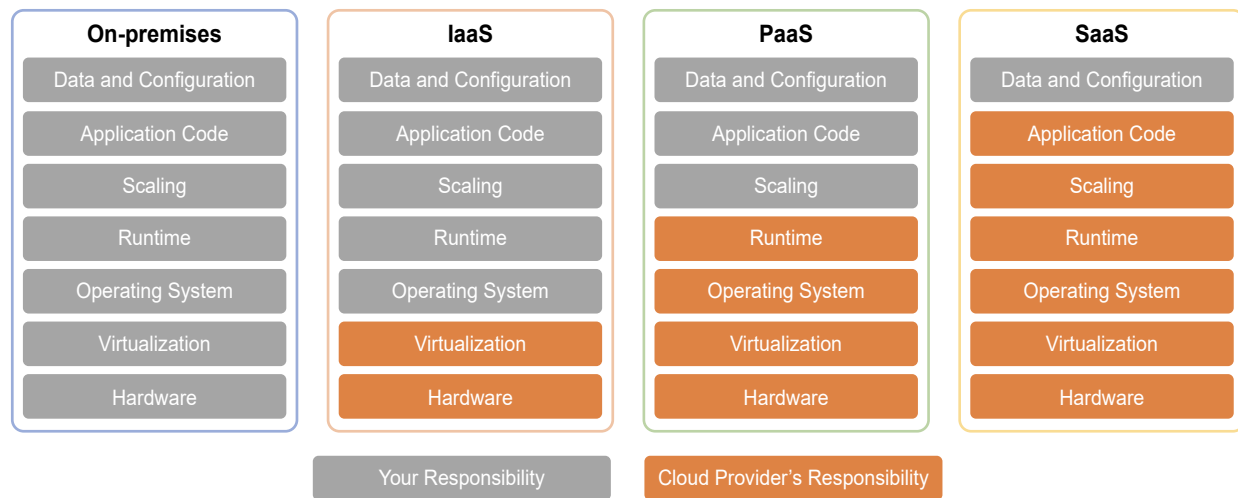


Figure 2: Cloud computing access model. Image inspiration: Google Cloud.

Cloud Computing access models

Users can access cloud resources in a few ways that depend on the exact nature of the use case (Figure 2). The main models for offering cloud computing are infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

IaaS. This access model provides manufacturers with on demand access to cloud resources such as physical and virtual servers, storage and networking. With this model, manufacturers provision and manage these services according to their needs.

PaaS. This access model offers a complete cloud-based environment for developing, managing and deploying applications. This model enables manufacturers to create and use software applications tailored to their operational needs without the complexity of building and maintaining the underlying infrastructure.

Software as a service (SaaS). This access model gives manufacturers access to a range of applications hosted online, which they can

use on a subscription basis. These applications spread across the manufacturing value chain—from inventory management to manufacturing systems to relationship management (CRM). These applications are available over the Internet and are maintained by the SaaS providers.

A manufacturer may use all types of models in different proportions simultaneously for diverse use cases.

Cloud computing and Industry 4.0

Cloud computing is a critical enabling technology for Industry 4.0, the fourth industrial revolution focused on interconnectivity, automation, machine learning and real-time data. By providing on demand network access to a shared pool of computing resources, such as servers, storage, applications and services, cloud computing allows businesses to provision resources rapidly, deploy applications and scale services as needed. This agility and flexibility support the data-driven, highly connected systems central to Industry 4.0.

With cloud computing, manufacturers can leverage IoT sensor data, analyze it in real time using advanced analytics and integrate it with enterprise applications and machines on the factory floor. The cloud's scalability also allows manufacturers to apply computing-heavy capabilities such as AI and machine learning for optimizations and predictive maintenance.

Leading cloud providers

All large public clouds provide a variety of services for manufacturing and industrial companies, which facilitates advances in industrial IoT, factory automation and supply chain optimization. Their solutions support a connected infrastructure that enables real-time data collection and analysis from factory equipment. Machine learning and analytics services empower predictive maintenance and operational insights. For supply chains, they offer services that enhance visibility and forecasting, which contributes to more resilient operations. These tools allow manufacturers to harness the power of data to streamline processes, innovate and maintain competitiveness in the modern industrial landscape. Due to their ability to provide extensive scalability, their public clouds are also referred to as "hyperscalers."

Each cloud hyperscaler—Azure, AWS and GCP—varies in range and specialization and differentiates its services. This offers unique strengths across various aspects of IoT, automation and supply chain management to cater to distinct manufacturing needs.

MORE HYPERSCALER INFORMATION

For detailed information on how hyperscaler cloud providers support these industrial use cases, please visit each provider's web page:

- **Amazon Web Services (AWS):** [AWS for Industrial](#)
- **Microsoft Azure:** [Microsoft Azure Industry](#)
- **Google Cloud Platform:** [Google Cloud for Manufacturing](#)

For more study on hyperscalers by independent analyst:

- [Gartner Magic Quadrant for Strategic Cloud Platform Services](#)
- [The IoT Cloud](#)

Case studies

The following sections are case studies about how the aforementioned hyperscalers were of benefit to manufacturers.

AWS case study. Global biopharmaceutical company, Merck, leveraged AWS to enhance the efficiency of its manufacturing operations through a centralized data and analytics platform named "MANTIS." By migrating its legacy data platform to AWS, Merck achieved a threefold increase in performance and a 50% reduction in operating costs. The platform unifies data from more than 120 manufacturing systems that provided real-time insights into more than 3,000 users, which significantly improved decision making, reduced data ingestion time and increased supply chain visibility. This transformation enabled Merck to become more data driven by optimizing manufacturing processes and ensuring timely delivery of high-quality medications.

Source: [AWS - Merck Case Study](#)

Microsoft Azure case study. Husky Injection Molding Systems used Azure IoT Hub for its digital solution “Shot Scope NX,” which dramatically improved the monitoring and operation of their injection molding machines. This implementation led to a notable increase in operational efficiency that offered real-time insights for proactive maintenance and enhanced customer service. By adopting Azure IoT Hub, Husky experienced significant advances in machine uptime and operational productivity, thereby revolutionizing their manufacturing process and customer support.

Source: [MS Azure – Husky Case Study](#)

Google Cloud case study. AB InBev, the world’s largest brewer, collaborated with Pluto7 and Google Cloud to enhance its demand forecasting. By leveraging Google Cloud’s AI and machine learning capabilities, they achieved a 95% accuracy rate in demand forecasting, which led to more efficient inventory management and a significant waste reduction. This advanced forecasting model provided AB InBev with deeper insights into consumer behavior, which enabled more effective and sustainable business decisions.

Source: [GCP – AB InBev Case Study](#)

Risks and challenges

While using the cloud offers benefits to manufacturers, it does not alleviate the risks and challenges such as data security, compliance and network reliability.

Data security. When using cloud services for IT infrastructure, data travels through external networks to remote data centers,

which introduces additional security risks. Ensuring data security in the cloud involves several measures such as authentication, authorization, encryption, identity, access management and more.

The division of security responsibilities between the cloud provider and the user can be complex. The chosen deployment and access models also influence who is responsible for different security tasks. Cloud providers often use a shared responsibility model to define these roles clearly. Users must recognize and understand their security responsibilities when using cloud services. This awareness should guide decisions regarding selecting service and deployment models in the cloud.

Compliance. Compliance with various local, national and international regulations such as ITAR, GDPR and HIPAA is mandatory in manufacturing. When transitioning workloads to the cloud, meticulous due diligence is crucial to maintain compliance. Although cloud providers may offer support for most regulations and compliance laws, the user is ultimately accountable for ensuring that their applications adhere to these legal requirements.

Network reliability. Manufacturing plants—often located in remote locations and spread across vast areas—face challenges with network connectivity, which is crucial for cloud computing. A comprehensive assessment of network infrastructure and related risks is necessary to make informed decisions on deployment models, edge computing needs and balancing latency, performance, cost and other system parameters. To mitigate connectivity

risks and maintain business continuity, options such as redundant network paths and offline capabilities should be considered.

Other risks. When transitioning to cloud computing, it's crucial to recognize risks such as data loss, vendor lock in and fluctuating costs. Mitigating data loss risks involves regular data backups and archiving critical data. It is vital to examine service agreements to achieve an optimal balance between cost and flexibility. Cloud pricing—typically based on a pay-as-you-go model—can vary with multiple tiers, usage-based discounts and options for long-term contracts. Implementing cost management strategies that suit specific use cases is essential. A careful analysis of these risks when designing cloud architecture allows a strategic approach that maximizes the cloud's benefits.

Challenges. As manufacturers embark on the cloud transformation journey, there will be many milestones to celebrate success, yet the journey is not without challenges. There can be different challenges at different stages of this journey.

- **Pilot purgatory.** Research and study reports indicate that many manufacturers embark on a cloud transformation journey but are stuck in “pilot purgatory.” It means the projects do not scale beyond initial pilots despite heavy upfront investment with expectation that they would scale. Manufacturers must secure leadership support to prevent such pilot purgatory. Leadership support must envision and ensure business benefit realization and align stakeholders.
- **Other challenges.** A study named [“Clearing the air on cloud”](#) by McKinsey & Company

on cloud adoption in the discreet manufacturing industry indicates that approximately two-thirds of industrial firms use cloud solutions. Yet, a minority fully capitalizes on their advantages. The focus often mistakenly rests on infrastructure hosting and IT savings rather than the fully native cloud solution and their ability to boost operational efficiency and market agility. About 74% of cloud projects miss their targets due to complexities and budget excesses. The cloud's value extends beyond just IT Infrastructure saving into manufacturing, supply chain and procurement, which offers substantial business transformation opportunities.

Preparing for cloud migration and modernization

When users embark on the journey to migrate to the cloud and modernize their operations, it is vital to reduce risks and tackle the aforementioned challenges. For this journey, users can use valuable insights from best practices derived from various sources and successful manufacturing transformation case studies. Users should adopt specific steps to fit their organization's unique situation.

Leadership alignment. For any manufacturer to succeed in cloud migration, their leadership including CXOs must be aligned and understand the benefits of the cloud, support training and adoption efforts.

Assessment. Begin by evaluating the current IT environment. Inventory all IT assets and understand their roles, importance and dependencies.

Prioritization. Prioritize workloads for migration based on factors like criticality, security and readiness. Start with less critical systems for a proof of concept.

Platform evaluation. Identify the cloud provider (e.g., AWS, Azure, Google Cloud) that best suits your needs; consider functionality, security, compliance and pricing.

Migration plan. Create a phased migration plan with timelines. Include planning, testing, configuration and migration activities; allow room for issue resolution.

Cloud governance. Establish cloud management and governance processes including security policies, monitoring, access controls and financial management.

Software/configuration updates. Make necessary software or configuration changes to adapt applications for the new cloud environment. This will enable them to use cloud-native services.

Execution. Execute the migration plan systematically by moving systems from on-premises to the cloud while continuously testing functionality and dependencies.

Optimization. After the initial migration, focus on optimizing cloud usage and realizing ongoing benefits. Consider modernizing applications for improved performance and flexibility.

Acquiring cloud skills

As users begin their journey into cloud computing transformation, it is essential to have the right skills within your team. Different individuals in the organization require varying expertise

and skills that depend on their specific roles and interactions with cloud technology.

General awareness. General awareness is the minimum requirement, regardless of your role in the organization. It would be best if you had a fundamental understanding of cloud computing, that you could participate in discussions, understand what cloud computing meant to you and benefit from organization-wide efforts.

In-depth technical training. Users should take a deep dive into technology if their roles require interacting technically with cloud services. Users can equip themselves with the right skills to manage and use cloud resources effectively.

Certifications. Pursue cloud certifications—especially those offered by providers like AWS, Azure or GCP—to validate expertise and commitment to cloud technology. An organization should also incentivize the training and certification of its employees. It motivates employees to invest in their professional development and contribute to the organization's cloud adoption and innovation goal. Manufacturers can partner with their cloud provider and leverage their training resources. Cloud providers often offer comprehensive training programs and material that aligns with their specific platform.

IMPORTANT LEARNING RESOURCES INCLUDE:

- [AWS Skill Builder](#)
- [Microsoft Azure Skills](#)
- [Google Cloud Training](#) [The IoT Cloud](#)

Looking ahead

According to the reports by Deloitte on [Manufacturing Industry Outlook](#) and [Smart Factory](#), 86% of participants believe that smart factory solutions will be the primary driver of competitiveness in five years, and 83% believe they will transform the way products are made in five years. Cloud computing plays perhaps the most crucial

role in digital transformation and industry 4.0 initiatives by enabling big data processing, high-performance computing and more. The manufacturers who stay ahead of the curve in adopting emerging technologies will have competitive advantages.

*A [version of this article](#) originally appeared in the *International Journal of Engineering Research and Technology (IJERT)* on March 21, 2024.*



ABOUT THE AUTHOR

[Ravi Soni](#) is a smart manufacturing and transformation leader with more than 22 years of experience in manufacturing, digital transformation and consulting. He is a dedicated member of the International Society of Automation (ISA), serving on the Smart Manufacturing and IIoT ([SMIIoT](#)) Division board and chairing its GenAI Committee. He has also been a speaker at ISA division and chapter-level events on smart manufacturing. As a principal in strategic design consulting at Infosys, Soni empowers global manufacturers to drive innovation and achieve digital excellence through technologies like manufacturing execution systems (MES), IoT, AI/ML, digital twin and more. He holds fellowships with the British Computer Society and APICS, senior memberships with IEEE and ASQ, and certifications such as Six Sigma Black Belt, PMP, TOGAF, SAFe and AWS Architect.



2025 Executive Board

The International Society of Automation is pleased to introduce the 2025 Executive Board.



President
Scott Reynolds
Johns Manville,
A Berkshire Hathaway
Company



President-elect
Secretary
Ashley Weckwerth
P.E.
Burns and McDonnell



Past President
Prabhu Soundarrajan
Kingston Capital



Treasurer
Ardis Bartle
Apex
Measurement
and Controls



CEO and Executive
Director
Claire Fallon
International
Society
of Automation



Dr. Soloman Almadi
Saudi Aramco



Marco Ayala
MITRE



Alan Bryant
P.E., PMP
Occidental



Alexa Burr
NEMA



Francisco Diaz-Andreu
Repsol



Nick Erickson
AWC, Inc.



Colleen Goldsborough
CPSC
United Electric Supply



Sherry LaBonne
Rockwell
Automation



David Lee
C.Eng, FIChemE
User Centered
Design Services



Robert E. Lee
Dragos



Edward Naranjo



Mary Riedel
Martin Control
Systems, Inc.



Megan Samford
Schneider
Electric



Sujata Tilak
Ascent
Intelligence



Jeff Winter
Critical
Manufacturing

2025

Modernize Your Automation Systems

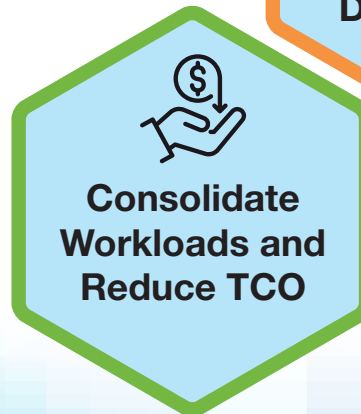
Moxa's new lineup of industrial PCs with advanced x86 architecture delivers a higher level of connectivity, intelligence, and performance for automation. Build a solution fit for any scenario with a comprehensive range of options.



SCAN OR CLICK
TO LEARN MORE



**Rapid and
Cost-effective
Deployment**



**Consolidate
Workloads and
Reduce TCO**



**Improve
Security and
Manageability**



BXP Series
Box Computing
Platform

DRP Series
DIN-Rail Computing Platform

RKP Series
Rackmount
Computing Platform

GET IN TOUCH

+1-888-MOXA-USA
+1-714-528-6777

info.us@moxa.com
www.moxa.com

MOXA[®]

Edge Computing Fundamentals

Edge computing supports Industry 4.0, smart manufacturing and digital transformation.

In the realm of information technology (IT), edge computing is a concept that has revolutionized the way data and computing tasks are processed. Traditionally, these tasks were processed in a centralized location on a local server. Edge computing has decentralized this process, which moves resource-heavy computing tasks to the cloud while using the edge devices on the network for simple calculations and data orchestration. This shift has been enabled by the Internet of Things (IoT) using sensor data and cloud computing, which are becoming more cost effective.

By Ryan Treece and Sujata Tilak

Edge computing brings the power and advantages of computing closer to where data is created and acted upon. This proximity improves efficiency, security and reduces bandwidth requirements. Edge devices and sensors, which are the sources of data generation and collection, often lack the compute and storage resources needed to perform advanced analytics. This is where edge computing comes into play, which can handle real-time data processing for important smart factory applications like predictive maintenance on premise in facilities.

Cloud computing, on the other hand, is performed in a remote environment hosted by public cloud companies like Microsoft, Amazon or IBM. This environment supports more data-intensive and less time-critical processes. Public cloud providers increasingly focus on a hybrid cloud model, according to Forbes. This model allows manufacturers to store and analyze their proprietary internal process information locally on their own servers, while offloading resource-intensive applications like machine learning to a public cloud to take advantage of scale and cost efficiencies.

Edge computing supports Industry 4.0/smart manufacturing

Edge computing is a pivotal architecture in supporting Industry 4.0 and smart manufacturing initiatives. Factories that deploy edge platforms experience faster network speeds and low latency, which significantly contribute to better decision making and production optimization. This ultimately improves return on investment.

By using edge and cloud computing, manufacturers improve productivity and identify revenue opportunities from the efficiencies and capabilities of smart systems. In particular, real-time overall equipment effectiveness (OEE) visualization tools provide full visibility into every aspect of a factory's efficiency.

OEE—a key performance indicator (KPI) calculated to measure machine and overall manufacturing performance—was invented in the 1960s by Seiichi Nakajima, the founder of

the Total Productive Maintenance (TPM) system. It is not a static, individual measurement of success, failure or mediocrity, but rather a living metrics combination that points operational technologists to the levers they must pull to improve business performance.

The first and most common challenge for an effective OEE implementation is data collection. Good data analytics start with good data availability. For manufacturing environments that use hundreds of types of machines and gather data from multiple industrial protocols, real-time data collection from machines is critical.

Advanced industrial IoT (IIoT) data management edge platforms provide this. Most offer core capabilities that include real-time access to operational data, data rationalization to identify relevant points, data transformation into usable formats and speedy delivery for ingestion by cloud and middleware (operational technology (OT) and IT systems).

Edge computing is performed at or near devices and offers more security, lower latency and more bandwidth capacity and reliability than cloud services. The most efficient IIoT edge platforms for data management include a large library of protocol converters that enable machine data collection using open and private protocols such as OPC UA and OPC DA, Modbus, MTConnect, BACnet, EtherNet/IP and Profinet for networked machines. The edge solution makes data collection a simple process, particularly for choosing the driver and appointing it to the IP address. All the tags are auto enumerated.

For machines requiring analog or digital input/output (I/O) data collection or external instrumentation, edge platforms can collect data from sensors or from a hardware adaptor for legacy machines. With the machines connected, algorithms can be set up by mapping the variables to a trigger. The logic was previously written in traditional programming languages. However, newer platforms provide a low- or no-code environment for a visual logic workflow to facilitate application creation, maintenance and calculations. OEE calculations can be done machine by machine and consolidated by line, shift and plant level to improve management visibility.

Alarm functions for monitoring specific machine and process conditions can be added and customized to automated actions.

With robust OT/IT edge integration software, it is possible to automate machine setup and reduce setup time, as the software's low latency is critical to avoid hidden downtime in the machine. With improved process visibility, managers have better information for planned stops and can calculate the machine OEE and schedule maintenance based on machine information.

Every manufacturer knows that unscheduled downtime is expensive. If one machine component fails, it can halt the entire production system, which could result in the loss of production time, raw materials and more.

Edge platforms can be deployed to learn expected machine behavior and fully automate preventive maintenance with triggers that identify anomalies in the production cycle such

as power consumption, vibration and noise and temperature. Given that the most common challenge for smart factories is usually interoperability with infrastructure implementation, it is well worth prioritizing IIoT architecture that uses edge intelligence to integrate legacy machines and sensors into IT systems.

Use cases

As previously mentioned, the fundamental purpose of edge computing is to collect data from edge devices or "things." But an edge computing platform offers several other use cases as well such as:

- **Executing business/application specific logic:** As edge software runs near the devices, it makes sense to execute logic that uses data generated at the edge and makes real-time decisions. This ensures fast response and less resource usage compared to sending all data to cloud for decision making. The logic itself depends on the application. For example, consider a scenario where a chiller provides coolant to all shop floor machines. Edge software will decide chiller output level based on current load and send commands to the chiller.
- **Local visualization:** Edge software can provide local visualization such as a human-machine interface (HMI) for plant people. Examples include:
 - Viewing production information
 - Viewing output of logic executed on edge
 - Viewing operator-provided downtime reasons.
- **Sending control commands:** Control commands can originate from following sources:

- As a result of logic executed in edge software.
- As a result of logic executed in cloud server such as data analytics.
- User-initiated commands such as starting or stopping a pump.

One of my favorites is the “machine interlock” feature. If a machine is down for more than a defined threshold, edge software will switch on an interlock output that prevents the operator from starting the machine unless they have entered a downtime reason.

- **Generating alerts:** Edge software can generate alarms/alerts by evaluating data for various purposes. For example, perform continuous condition monitoring of devices and generate alerts for maintenance team.
- **Data transformation:** Perform data transformation based on defined rules and send

processed data to the cloud rather than raw data. This reduces data volume sent to the cloud and conserves bandwidth and cloud storage. For example, send average rather than raw data of parameters.

- **Send data to a third-party server:** Sometimes data generated on the edge must be shared with third-party servers. The edge software is ideally suited for this purpose. It can do required data transformation and send data to the third-party server. For example, report emissions data to regulators.

Edge software architecture

The next decision is how the edge software should be architected, for example, what components it should offer one or more of the aforementioned use cases.

Figure 1 shows components in typical edge software. Each installation of the same edge

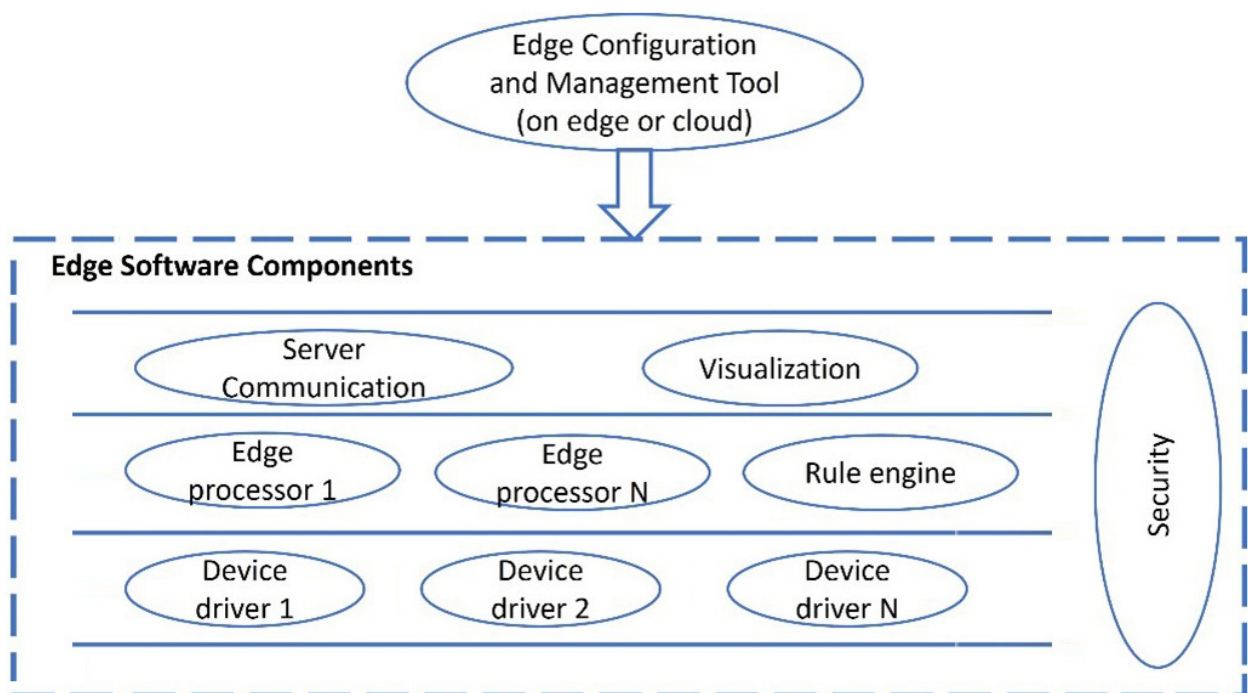


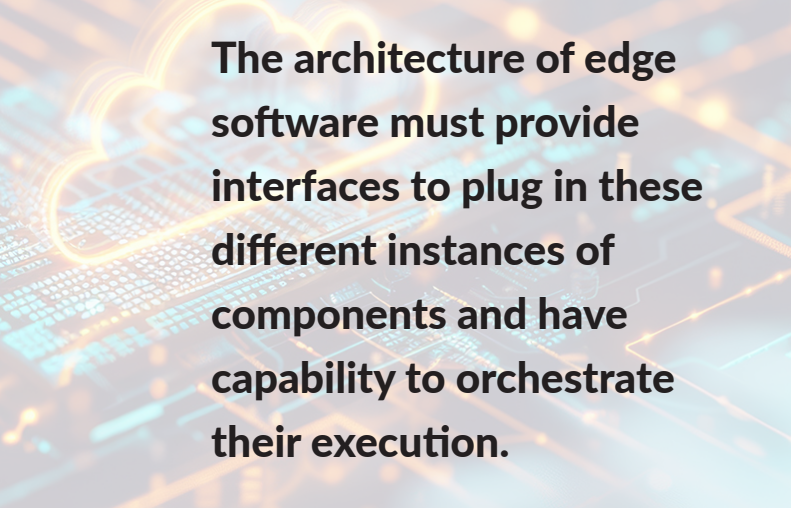
Figure 1: Components in typical edge software.

software will have different components.

Consider these examples:

- Installation A uses OPC UA, EtherNet/IP drivers and edge processor 1.
- Installation B uses Modbus TCP, Modbus RTU and OPC UA drivers; edge processor 1 and edge processor 2; and sends data to a 3rd party server.

Architecture of edge software must provide interfaces to plug in these different instances of components and have capability to orchestrate their execution. This is very critical. The individual instances of compo-



The architecture of edge software must provide interfaces to plug in these different instances of components and have capability to orchestrate their execution.

nents will be developed using a base design or may be parameterized in some cases. An edge configuration tool allows users to define components that will go in a specific instance and configure them. The configuration tool normally runs in the cloud with a part of it running on the edge. This tool or a separate component handles device management and provisioning including over the air (OTA) updates. A key requirement is to ensure that edge software runs 24/7.

Edge computing in Industry 4.0

According to IoT Analytics, the number of connected IoT devices is expected to reach 14.4 billion by the end of 2022. Allied Market Research states that the global value of IoT in manufacturing products was \$198.25 billion in 2020, with predictive maintenance applications commanding the largest share. Thanks in large part to advances in smart sensors and virtual and augmented reality, the demand for real-time asset monitoring will boost the overall value to \$1,495.65 billion by 2030, at a compound annual growth rate of 22.6 percent from 2021.

With exponentially more IoT devices collecting, analyzing and processing more data and information, the need for edge computing can only increase in an effort to reduce latency and increase speed. With the edge orchestrating, aggregating and trimming data on the fly, companies will rely on the cloud for long-term storage and cost-efficient compute. The toughest decision corporations will face is choosing which data points are worth real-time analysis on premise, which need long-term storage and analysis in the cloud and, most importantly, which data needs no analysis at all.

The future of edge computing and Industry 4.0

Many experts believe enterprises will deploy edge platforms and 5G wireless communications together in the coming years. A recent article from The Enterprisers Project indicates that the “next big thing” will be private 5G

networks. 5G adds ultra-reliable, low-latency communication (URLLC) that has previously only been offered on Class-C Ethernet technology.

With increased data transfer speeds, decreased latency and higher capacity of 5G technology, factories will be able to scale without relying on proprietary industrial Ethernet protocols via standard wired network infrastructures. Combining edge computing with 5G will allow more flexibility in on-premise deployments by extending the

range and reach of data collection to assets normally unreachable through wired deployments or bandwidth constraints.

Artificial Intelligence (AI) solutions depend on edge computing and will continue to require an IoT platform to integrate legacy equipment into new and developing solutions. The importance of device level data acquisition will continue to be critical in scaling solutions across this heterogeneous mix of complex IT and OT protocols in manufacturing and industrial environments.



ABOUT THE AUTHOR

[Ryan Treece](#) is the head of ISA's Edge & Cloud Technical Committee under the [SMIIoT division](#). He brings 15 years of experience to his role as the Global Business Development Manager at [FreeWave Technologies](#), where he leads IIoT solutions in edge intelligence and remote connectivity cloud. Treece has been instrumental in driving technological innovation at industry-leading companies by leveraging advanced technologies to create unique solutions addressing complex challenges in manufacturing.



[Sujata Tilak](#) is a thought leader and recognized expert in IIoT and IT/OT convergence. An instrumentation and control engineer from the College of Engineering, Pune, Tilak has more than 30 years of experience in industrial automation, environmental monitoring, smart manufacturing and digital transformation. She is the co-founder and MD of Ascent Intellimation. Under her leadership, AIPL conceptualized and developed an innovative IoT platform called PlantConnect, and various products based on this platform. She is an ISA volunteer leader and currently serves on the ISA Board of Directors. Tilak is a member of ISA's SMIIoT Division.

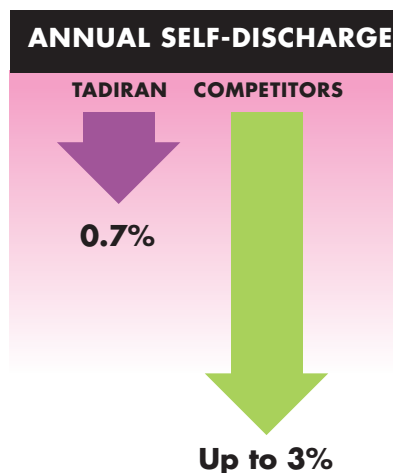
IIoT devices run longer on Tadiran batteries.

PROVEN
40
YEAR
OPERATING
LIFE*



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

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



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



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

www.tadiranbat.com

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

We bring color into view!

Compact pressure sensors and switches with 360° custom-color status display



256 colors

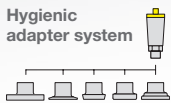
Individually selectable:

- Measurement in progress
- Sensor switching
- Process malfunction

Compact design



Hygienic adapter system



IO-Link



Adjustment via smartphone



\$535

VEGABAR 39 Clamp 1"



www.vega.com/vegabar

VEGA HOME OF VALUES



Secure Data Access for Industrial AI

By Xavier Mesrobian

Accessing production data through a DMZ can be done with well-designed tunnel/mirror software.

The year 2025 shows no signs of slowdown for industrial artificial intelligence (AI).

Early adopters are forging ahead, and those who took a wait-and-see position are now scrambling to catch up. At whatever point you find yourself on the AI adoption curve, it is important to keep your process data secure. Thankfully, there are ways to establish secure, real-time connections from the

plant to an AI system running in-house or on the cloud.

The best approach, mandated by the NIS2 Directive and NIST CSF 2.0, is complete network segmentation. The operational technology (OT) system should be fully isolated from the Internet and any cloud system. This is best done using a demilitarized zone (DMZ), which keeps the production network behind closed firewalls.

Protocol challenges

Moving production data to a cloud-based AI system in real-time through a DMZ requires two steps, plant-to-DMZ, and DMZ-to-cloud. However, two of the most popular industrial protocols, OPC UA and MQTT, were not designed for this type of data transfer. Although often used in Industrial Internet of Things (IIoT) and Industry 4.0 systems, they were conceived in the early 2000s, long before people were thinking of secure ways to access industrial data from outside the plant.

The OPC UA protocol by itself is simply too complex to reproduce well in a daisy chain across multiple servers. Information will be lost in the first hop. The synchronous multi-hop interactions required to pass data across a DMZ would be fragile on all but the most reliable networks and would result in high latencies.

MQTT, on the other hand, can be daisy-chained but it requires each node in the chain to be individually configured and aware that it is part of the chain. The quality of service

(QoS) guarantees in MQTT cannot propagate through the chain, which makes data at the ends of the chain unreliable. Therefore, MQTT is best used as the last step only to move data from the DMZ to the cloud.

Getting data securely from the plant to the DMZ is the challenge. Using OPC UA for that step has a serious pitfall: It requires opening a firewall on the production network. Any OPC UA client on the DMZ would need to connect through the firewall to the OPC UA server in the plant. Opening a firewall into the plant for this is far too risky. Most security administrators will not allow it.

Tunnel/mirroring

Since neither OPC UA nor MQTT alone, or together, are sufficient for passing data through a DMZ, another approach is needed—one that integrates well with both protocols. Secure tunnel/mirroring software with a unified namespace provides a solution (Figure 1). It can make the connections at both ends and pass the data along the daisy-chained connections necessary for DMZ support.

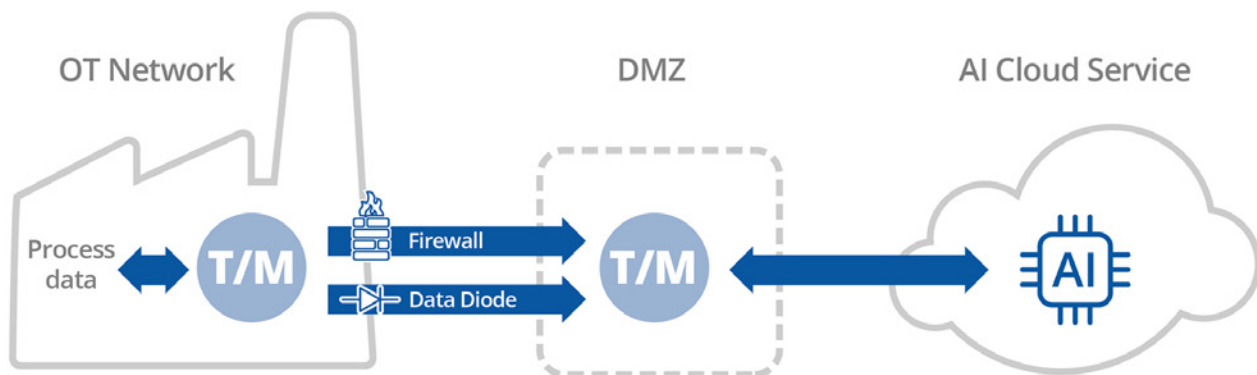


Figure 1. Secure tunnel/mirroring software with a unified namespace can make the connections at both ends and pass the data along the daisy-chained connections necessary for DMZ support.

AI implementations may call for bidirectional data flow to enable hands-off supervisory control or similar data inputs back into the production system.

The tunnel/mirror software connects to MQTT, OPC UA or other industrial protocols at the production facility, and mirrors the full data set to a similar component on the DMZ. Ideally, both components should be able to maintain the data in a unified namespace. This way, the data can be converted to MQTT for sending to the AI cloud service from the DMZ. The mirroring capability of the tunnel/mirror software keeps that data consistent between the original data source, the DMZ and the AI system.

Firewalls and data diodes

As mentioned previously, all inbound firewall ports on the production system must be kept always closed. The tunnel/mirror system must be able to make outbound-only connections from the production network to the DMZ. Going a step further, some high-security, critical infrastructure applications require a hardware data diode to ensure that not a single data packet gets back to the industrial

network. The tunnel/mirror system would need to provide data diode support for that level of secure architecture.

Other AI implementations may call for bidirectional data flow to enable hands-off supervisory control or similar data inputs back into the production system. The tunnel/ mirror technology should be flexible enough to support that, if needed. In any case, there should be no access to data beyond what the AI system uses. Plant engineering staff must have full control over which data will be made available.

To optimize production systems, many companies today are turning to industrial AI. The challenge they face is accessing the data they need without compromising security. This is difficult, but not impossible. You can have a zero-attack-surface OT network and still provide data to AI systems. The security is provided by a DMZ. Accessing production data through a DMZ can be done with well-designed tunnel/mirror software.



ABOUT THE AUTHOR

Xavier Mesrobian is on the Board of Directors at [Skkynet](#), a global leader in industrial data connectivity. With more than 25 years in the industry, Skkynet software and services are used in more than 29,000 installations in 86 countries including the top 10 automation providers worldwide.

Custom Tailor Batteries for Maximum Performance

By Sol Jacobs

Expert recommendations can help maximize the power supply of remote wireless devices to suit specific remote applications.

When it comes to powering remote wireless devices, there are no one-size-fits-all solutions. Choosing a battery should be like visiting a custom tailor shop, where an expert with decades of experience sizes you up for a beautiful garment that highlights your strengths and disguises your weaknesses. Similar expertise is required for specifying the optimal power supply solution that combines reliability, durability and long-term cost savings while minimizing tradeoffs.

Inexpensive off-the-shelf solutions may work for certain consumer electronic devices powered by alkaline or lithium-ion batteries,

especially in situations where the batteries are easily replaceable and operate in moderate environments. However, consumer batteries rarely serve the needs of industrial applications involving hard-to-access locations, extreme environments or large-scale installations where multiple simultaneous battery failures could be highly disruptive—and expensive.

Expert fitting is necessary when specifying an ultra-long-life lithium battery. Thorough due diligence is required to develop a clear understanding of the power requirements and challenges specific to each application. The entire selection process can be streamlined

with the help of a qualified applications engineer who—with the help of proprietary data intelligence—can help you identify the optimal power supply solution that delivers the biggest bang for the buck.

Know your application

Too commonly, a one-size-fits-all mentality is followed throughout the battery specification process, as the power supply is often seen as an afterthought rather than an integral step toward optimal product performance. By thoroughly understanding your power requirements, and then eliciting outside expertise to validate your choice of battery, you will be far more likely to ensure that your device will operate reliably for long-term deployments in remote or extreme environments, where battery replacement can be impractically expensive or impossible.

Design optimization begins with a thorough understanding of each application's unique performance requirements. Certain fundamental questions must be answered. For example, is the device being used as a backup power source or as the main power supply? Does the application require an extended shelf life? Is the amount of average current being drawn high enough to demand the use of an energy-harvesting solution combined with an industrial-grade rechargeable Li-ion battery to store the harvested energy?

Answers to these and other pertinent questions can vary significantly throughout the Industrial Internet of Things (IIoT), including applications such as supervisory control

and data acquisition (SCADA), process control, industrial robotics, memory backup, asset tracking, safety systems, environmental monitoring, machine-to-machine (M2M), machine learning (ML), wireless mesh networks and many more.

Typical factors that require consideration when specifying a battery for a low-power remote wireless application include electrical, environmental and size and weight requirements.

Electrical requirements. The ideal starting point is to know your specific requirements for maximum, nominal and minimum (cut-off) voltage, keeping in mind that a higher voltage battery could enable the use of fewer or smaller batteries. The math is simple: It takes at least two 1.5 V cells to deliver the same energy as a 3.6 V cell.

The total capacity of the battery, measurable in Ampere-hours (Ah), is also vital because it establishes the maximum theoretical life of the battery based on its calculated annual energy consumption. High capacity along with high energy density are essential to battery miniaturization.

Another important consideration is the average amount of current expected to be drawn as it allows you to calculate expected annual losses in available capacity. You must also factor in the potential need for high pulses to facilitate two-way wireless communications or other advanced functionality. High pulse requirements vary in their size, duration and frequency. When predicting expected capacity losses, you must also factor in the expected

amount of time the battery will spend in storage where available capacity will be consumed by self-discharge.

Environmental requirements.

Environmental factors can significantly influence overall battery performance. For example, long-term exposure to extreme temperatures can compromise battery performance by reducing available capacity, which causes voltage drops and delays, and by accelerating the battery’s self-discharge

rate. Certain battery chemistries are far better adapted to operate reliably in extreme temperatures (see Table 1).

Understanding the operating environment is especially important for remote wireless devices designed for long-term deployments in extreme environments you must calculate the expected maximum, average and minimum temperatures while in operation and during storage, including the percentage of time spent in each phase.

Primary cell	LIS ₂ CL ₂ Bobbin-type with hybrid layer capacitor	LIS ₂ CL ₂ Bobbin-type	LI METAL OXIDE Modified for high-capacity	LI METAL OXIDE Modified for high power	LIFES ₂ Lithium iron disulfate (AA-size)	LIMNO ₂ Lithium manganese oxide
Energy density (Wh/Kg)	700	730	370	185	335	330
Power	Very high	Low	Very high	Very high	High	Moderate
Voltage	3.6 to 3.9 V	3.6 V	4.1 V	4.1 V	1.5 V	3.0 V
Pulse amplitude	Excellent	Small	High	Very high	Moderate	Moderate
Passivation	None	High	Very low	None	Fair	Moderate
Performance at elevated temp.	Excellent	Fair	Excellent	Excellent	Moderate	Fair
Performance at low temp.	Excellent	Fair	Moderate	Excellent	Moderate	Poor
Operating life	Excellent	Excellent	Excellent	Excellent	Moderate	Fair
Self-discharge rate	Very low	Very low	Very low	Very low	Moderate	High
Operating temp.	-55°C to 85°C, can be extended to 105°C for a short time	-80°C to 125°C	-45°C to 85°C	-45°C to 85°C	-20°C to 60°C	0°C to 60°C

Table 1. Numerous primary lithium battery chemistries are available.

The widest temperature range of all (-80°C to 125°C) is provided by bobbin-type lithium thionyl chloride (LiSOCl₂) batteries, which are unrivaled in their ability to operate in extreme environments while delivering the highest capacity and energy density, potentially resulting in the use of fewer or smaller cells. Bobbin-type LiSOCl₂ batteries are also ideally suited for surviving humidity, shock and vibration.

Size and weight requirements. Allowable size and weight restrictions can have a major impact on the battery selection process. Many remote wireless devices need to be miniaturized for ease of transport, ergonomics or to accommodate severe space and weight restrictions. Reducing the size and weight of the battery also can mitigate the rising cost of transporting

hazardous goods while meeting increasingly stringent UN and IATA shipping regulations.

Maximizing battery operating life

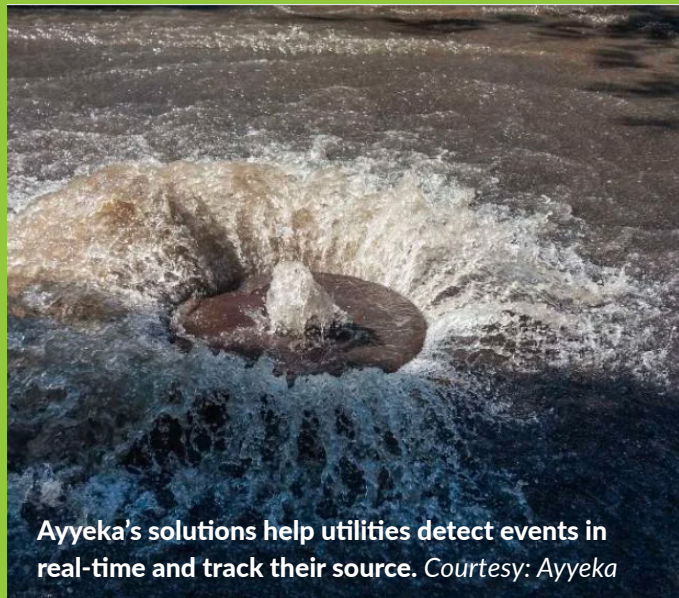
The longer a device can operate maintenance-free on its original battery, the higher the return on investment. Expected battery life can be calculated based on numerous factors, principally the cell's total capacity, energy consumed while in operation and, most importantly, the cell's annual self-discharge rate.

All batteries experience some amount of self-discharge, as chemical reactions consume small amounts of energy even when the device is not in use or is disconnected. Self-discharge can be significantly minimized by controlling the passivation effect, which involves a thin

Water/Wastewater Application

Ayyeka is a developer of remote monitoring technologies that provide digital transformation for critical infrastructure. The company's technology embeds edge AI into field assets. With its combination of edge, Internet of Things (IoT), and AI/machine learning (ML), it propels the critical infrastructure space, enabling infrastructure stakeholders to create, manage, and use remote field assets data.

Ayyeka's AI-enabled smart sensors monitor sensors used in solid waste and wastewater management, public utilities, transportation, energy exploration and distribution, smart cities, environmental monitoring, and other hard infrastructure. Tadiran bobbin-type LiSOCl₂ batteries power two-way wireless communications to maximize operating life, detect unusual events, enable predictive maintenance and repairs, and counter cyber security threats.



Ayyeka's solutions help utilities detect events in real-time and track their source. *Courtesy: Ayyeka*

film of lithium chloride (LiCl) that encircles the anode of an unused battery to limit its chemical reactions. Passivation is a repeating phenomenon. Whenever continuous current is drawn from an unused cell, there is an initial period of high resistance combined with a temporary drop in voltage until the protective layer begins to dissipate, also known as depassivation. This phenomenon occurs whenever an LiSOCl_2 cell remains dormant for extended periods.

Passivation varies based on many variables including the cell's current discharge capacity, the length of storage, storage temperature, discharge temperature and prior discharge conditions, as partially discharging a cell and then removing the load will lessen passivation over time.

Competing bobbin-type LiSOCl_2 batteries vary significantly in terms of their ability to harness the passivation effect, thus impacting their self-discharge rate. For example, the highest quality LiSOCl_2 batteries can feature a self-discharge rate as low as 0.7 percent per year, retaining nearly 70 percent of their original capacity after 40 years. Conversely, inferior quality LiSOCl_2 cells can have an

annual self-discharge rate of up to 3 percent per year, causing roughly 30 percent of the cell's available capacity to be consumed every 10 years, making 40-year battery life unachievable. If the application demands an ultra-long-life battery, this becomes a critical consideration.

High pulses drive wireless communications

Certain low-power remote wireless devices require high pulses of up to 15 A to initiate and power two-way wireless communications. Standard bobbin-type LiSOCl_2 cells cannot generate such high pulses due to their low-rate design. As a result, a hybrid solution

Structural Integrity Applications

Resensys provides a powerful platform for remote monitoring of strain (stress), vibration (acceleration), displacement, crack activity, tilt, inclination, temperature, and humidity. The company developed a global network to protect infrastructure systems against aging and malfunction. It supplies its high precision, durable, and reliable structural monitoring solutions to customers monitoring bridges, tunnels, buildings, dams and cranes.

Resensys wireless sensors are mounted beneath bridge trusses to measure structural stress. These locations are highly inaccessible and the use of a bobbin-type LiSOCl_2 battery serves to maximize return on investment by maximizing the operating life and increasing product reliability in extreme temperatures.



Structural stress sensors mounted beneath bridge trusses use extended-life bobbin-type LiSOCl_2 batteries to reduce the need for the costly and dangerous work or replacing them.

Courtesy: Resensys

is required that combines the use of a standard bobbin-type LiSOCl₂ cell that delivers low-level base current along with a patented hybrid layer capacitor (HLC) that generates pulses of up to 15A. As cell capacity starts approaching its end-of-life, the patented HLC experiences a unique voltage plateau that can be measured and interpreted to deliver “low battery” status alerts.

Consumer devices often use supercapacitors for similar purposes. However, supercapacitors are ill-suited for most industrial applications due to serious limitations such as short-duration power, linear discharge qualities that do not allow for the use of all available energy, low capacity, low energy density and very high self-discharge rates up to 60 percent per year. When linked in series, supercapacitors also require the use of bulky and expensive cell-balancing circuits that drain additional current, which further reduces battery operating life.

An expert can help

The ideal battery-powered solution should last for the entire lifetime of the device, thereby eliminating the need for costly battery change-outs. This is especially important for ultra-long-life deployments.

However, short-term test data is often inaccurate in predicting long-term battery performance, which makes it difficult to distinguish a higher quality cell from a lower quality battery. This is where the advice of an experienced applications engineer becomes advantageous to making an informed choice. An experienced applications engineer can assist you in performing thorough due diligence by reviewing your power requirements, then recommending the solution that best suits your application. The applications engineer can also help you interpret the test data, bearing in mind that the most reliable predictor of expected battery life is in-field test data derived from similar devices operating under equivalent loads and environmental conditions.

Final thoughts

Choosing the ideal battery for a low-power remote wireless device involves numerous considerations including potential trade-offs. Therefore, it pays to have a qualified applications engineer assist you when performing your due diligence. This collaborative approach can result in a custom-tailored solution that serves to extend battery life, increase reliability, and maximize your return on investment.



ABOUT THE AUTHOR

Sol Jacobs is the vice president and general manager at [Tadiran Batteries](#).

Enhancing Power Grid Resiliency

By James Haw

The U.S. electrical grid must significantly expand its capacity to meet growing demands from electrification and renewable energy sources. Studies, such as those from the Department of Energy and Princeton University, [estimate](#) that by 2050, the grid's transmission capacity will need to increase between two to five times its current levels. Specifically, grid transmission expansion is expected to require a 60 percent to 100 percent increase in capacity by 2035 to support the shift to a zero-carbon grid, as per President Biden's 2035 clean energy goals. This expansion will be crucial as economies and lifestyles shift toward greater electrification and connectivity, i.e., the adoption of electric vehicles, rapid data center growth, etc., but also to support the adoption of renewables like wind and solar, given that these sources introduce unique challenges and requirements to grid infrastructure.

Expanding the grid requires not only building new infrastructure but also upgrading existing systems to meet modern demands. This includes adding thousands of miles of high-capacity transmission lines to efficiently

New technology improves grid reliability and safety through early fault detection.

connect renewable energy sources to demand centers, which will be central to increasing grid capacity. Equally important is enhancing current infrastructure with advanced technologies—such as reconductoring with high-capacity conductors and implementing predictive analytics—to reach capacity goals while minimizing the need for entirely new lines. This balanced approach helps preserve existing assets while supporting a more resilient and efficient grid.

Ensuring that existing infrastructure remains reliable and resilient is essential to optimizing grid efficiency and minimizing unnecessary expenses on reactive maintenance and emergency repairs. By proactively maintaining and modernizing the current transmission network, the high costs associated with unexpected failures and outages can be avoided, and those cost savings can be redirected to the expansion of the grid.

This assurance of maintaining a resilient infrastructure also supports uninterrupted power delivery, which is crucial for public safety, especially during extreme weather events. Investing in preventive technologies and grid-enhancing measures, such as advanced sensors and fault detection systems, reduces both the frequency and severity of outages and extends the life of existing assets, which maximizes the value of limited funding sources.

This article details how IND Technology's early fault detection (EFD) provides a groundbreaking solution to strengthen grid reliability and resilience, which supports the achievement of critical energy infrastructure goals.

Supporting federal initiatives

To help address this challenge, the U.S. government has introduced crucial initiatives to enhance grid modernization and security. Key among these are the Grid Resilience and Innovation Partnerships (GRIP) program and the Advancing Grid-Enhancing Technologies (GETs) Act of 2024. The GRIP program, initiated by the U.S. Dept. of Energy (DOE), supports the development and deployment of technologies that increase the resilience, reliability and flexibility of the nation's power grid. Through funding aimed at both large-scale grid modernization projects and community-based initiatives, GRIP fosters innovation that directly addresses vulnerabilities within current transmission and distribution networks.

Complementing GRIP, the GETs Act of 2024, introduced by Senators Peter Welch and Angus King, specifically targets the implementation of technologies that can optimize grid performance without necessitating extensive new construction. This legislation encourages investments in tools that expand grid capacity,

Ensuring that existing infrastructure remains reliable and resilient is essential to optimizing grid efficiency and minimizing unnecessary expenses on reactive maintenance and emergency repairs.

enhance operational efficiency and improve reliability, with incentives to encourage the adoption of such technologies. With a focus on solutions like dynamic line ratings (DLR), power flow control and advanced sensor systems, the GETs Act aims to bridge existing infrastructure gaps as the nation moves toward increased electrification and renewable integration. If enacted, the bill would catalyze investments projected to yield a [tenfold return](#) by 2030 by significantly reducing annual energy production costs and enhancing overall grid efficiency.

EFD technology provides a robust and compelling solution to enhance the Grid Reliability Improvement Program (GRIP) and Grid Enhancing Technologies (GETs) initiatives. EFD combines advanced sensors and software to identify potential faults early, thereby enabling proactive maintenance and repair measures that boost both grid reliability and safety. It also enhances the effectiveness of other grid technologies.

For example, traditional line ratings have typically been conservative and set to accommodate worst-case environmental scenarios such as high temperatures or low wind speeds. Dynamic line rating (DLR) was developed to allow utilities to adjust transmission capacity in real-time based on actual environmental and operational conditions, thereby maximizing efficiency. However, DLR increases line current based solely on environmental data without considering the physical condition of the grid. While valuable, this approach could inadvertently overstress grid components with hidden vulnerabilities,

which could lead to faults or outages. Integrating EFD with DLR provides utilities with added security; they can safely increase power flow knowing the grid's integrity is intact, thereby reducing the risk of outages from unaddressed weaknesses. EFD not only optimizes but also safeguards power transmission, which makes it a key component in advancing a resilient and efficient power grid.

This proactive approach not only aligns with the GRIP program's goals to enhance resilience against extreme weather events but also fulfills the GETs Act's requirements for technologies that optimize grid capacity and efficiency. Additionally, EFD contributes to environmental safety by detecting and addressing vegetation encroachment, which is a frequent cause of outages; and worse, grid-related fires. Through these capabilities, EFD represents a vital step toward a more resilient, efficient and safe grid infrastructure that supports the broader goals of both GRIP funding and GETs legislation.

Advanced sensors impact on grid resilience and reliability

EFD technology enables utility providers to better manage rising energy demands by ensuring that existing power lines operate at full capacity while reducing the frequency and cost of unplanned outages. With advanced systems, utilities can prevent congestion and downtime to ensure more consistent power delivery to meet growing electricity needs across the country.

This is accomplished through the deployment of advanced sensors that detect and pinpoint

defects and/or vulnerabilities (within an accuracy of 30 feet) before they develop into electrical faults that can result in damage to infrastructure, customer outages and safety threats (Figure 1) such as downed wires and wildfires.

As shown in Figure 1, system anomalies (incipient failures) are detected via RF signals picked up by the EFD data collection sites that are situationally spaced based on the monitored circuit. Data is continuously collected and transmitted to IND.T's cloud infrastructure via LTE cellular infrastructure. Once an early fault is detected, i.e., actionable data is delivered via IND.T's analysis software to the utility in the form of energy, activity, location and other metrics for visual discovery and repair/resolution.

EFD units proactively report on an array of common anomalies such as broken conductors, damaged insulators, crossarm failures and loose clamps, etc. This allows the utility

time to proactively address these issues before they escalate. These capabilities align with the GETs Act's objectives by enhancing grid reliability and resilience, which exemplify the goals outlined in the act. As EFD identifies potential issues within the transmission infrastructure before they lead to faults, it effectively contributes to "grid reliability, resilience and efficiency." By mitigating the likelihood of failures, EFD directly supports the Act's emphasis on "building a power grid that can sustainably integrate renewable energy sources while minimizing disruptions."

Proactive versus reactive maintenance and cost reduction

EFD transforms the traditional maintenance approach by shifting it from a reactive to a proactive model. Rather than responding to unexpected outages or damage, utility providers using EFD can address issues before they evolve into costly failures. This proactive

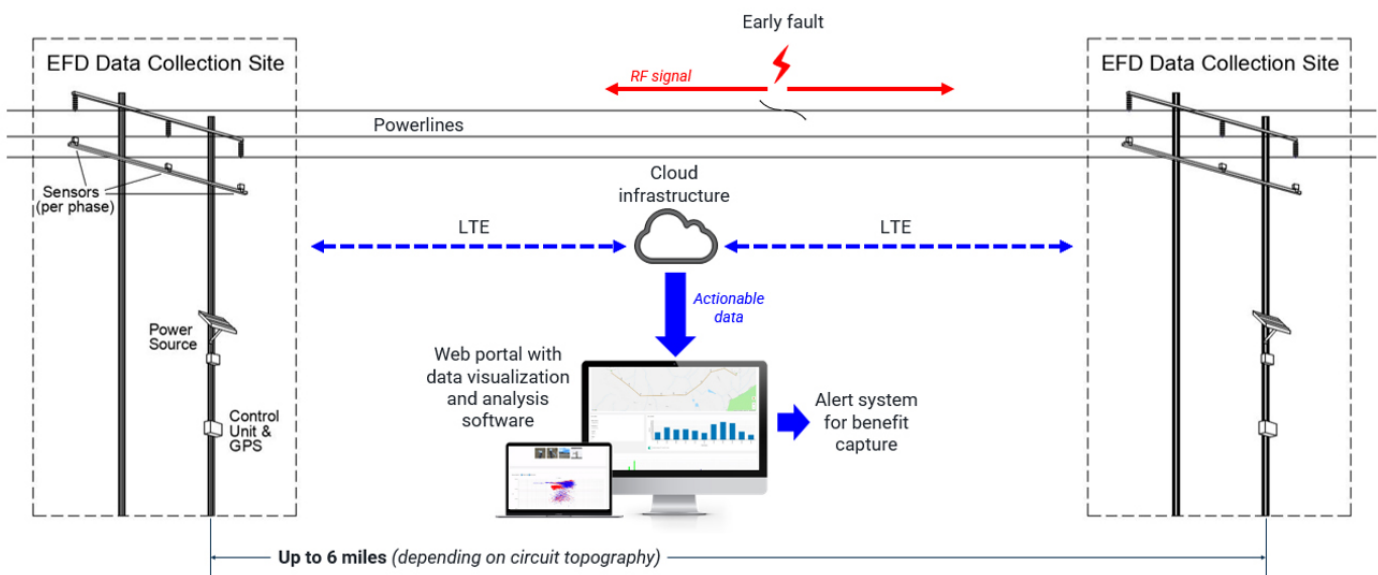


Figure 1. Advanced sensors detect and pinpoint defects and/or vulnerabilities before they develop into electrical faults that can result in damage to infrastructure, customer outages and safety threats.

approach leads to considerable cost savings by reducing or even eliminating emergency repair needs. Maintenance can be planned during off-peak hours, which minimizes disruption and lowers labor costs. The long-term financial benefits for utility companies are substantial, as the reduction in emergency repairs and downtime translates to a more efficient allocation of resources.

Environmental and customer impacts

According to the latest estimates, the U.S. government spends more than \$3 billion annually to fight wildfires, which are estimated to result in losses of hundreds of billions each year in economic costs and property damage. Over the last decade, wildfires have become a more pressing and prevalent problem in the U.S., where larger fires in greater numbers and with more extreme fire behavior seem to have become more commonplace.

While statistically more than 50 percent of the total acreage affected by wildfires in the last 15 years has occurred in just five states—Alaska (15 percent), California (14.6 percent), Oregon (8.8 percent), Idaho (8 percent) and Texas (7 percent)—no state is immune. The most recent fire in Hawaii occurred in a somewhat unexpected place since the region affected was assumed to be too “lush” for wildfire to spread so quickly and to any great degree. But it happened—and it happened quickly—destroying more than 2,700 structures and killing 102 people. The cause of the fire has been determined to be the result of an electrical fault followed by mismanaged extinguishing efforts.

From a much broader perspective, it is estimated that around 10 percent of wildfires are caused by damaged or aged/degraded electrical power systems worldwide. Ten percent may seem like a low number. But when climate change is considered, i.e., where hot and dry conditions are becoming more commonplace and severe, which leads to vegetation drying out and landscapes becoming more flammable, coupled with the fact that electrical distribution/transmission systems are rather ubiquitous in our ecosystem, the impact of that 10 percent can be enormous.

As climate conditions persist, proactive identification of weaknesses in the grid can serve to reduce or eliminate the threat of electrically induced wildfires, which will, in turn, lower costs significantly, protect the environment (including public and private infrastructure) and save lives.

All electrical utility companies are required by the U.S. government to include vegetation management as a key element of their wildfire mitigation plan. Traditionally, this involves crews performing manual inspections, which is a time-consuming and labor-intensive (high-cost) process. Although technologies such as drones exist to inspect and monitor vegetation encroachment, these technologies provide situational and intermittent awareness, not continuous awareness. In other words, they report on the condition of the vegetation for a specific place on a specific date/time and don't report on it again until the specific place recurs in the inspection rotation.

To that point, the EFD units constantly report on system health and are capable of reporting on vegetation encroachment when vegetation gets to within 24 inches of the lines—well before it touches the conductor. EFD reports on the condition of vegetation encroachment every second of every hour of every day using proprietary high-frequency monitoring technology. This capability is especially critical in fire-prone areas where vegetation contact with power lines can spark devastating wildfires. By ensuring that transmission corridors remain clear, EFD contributes to environmental conservation and reduces the risk of fires that would otherwise lead to significant ecological damage.

The impact of EFD technology on customers is equally profound. By preventing faults before they lead to power outages, EFD improves the customer experience by ensuring a more reliable energy supply. Reduced outages mean fewer disruptions to daily life and business operations, which contributes to an enhanced quality of life and economic stability. Additionally, frequent outages during

extreme weather conditions—whether high heat or cold—pose safety risks to customers. Reliable power access is essential to maintaining safe indoor temperatures, especially for those most vulnerable to extreme weather conditions. The capacity of EFD to prevent such outages addresses these concerns and enhance customer safety and welfare.

Looking ahead

The EFD solution is poised to play a transformative role in the modernization of the U.S. power grid. Through advanced sensing capabilities and proactive fault detection, EFD aligns closely with the objectives of the GETs Act of 2024. This innovative technology not only enhances grid reliability and reduces wildfire risks but also lowers maintenance costs, minimizes environmental impact and improves customer satisfaction and safety. As the U.S. continues to adopt clean energy sources and address the challenges of a modernized grid, this new technology offers a promising path forward for a resilient and efficient energy infrastructure.



ABOUT THE AUTHOR

James (Jim) Haw is a seasoned electrical engineer with more than 35 years of experience across the paper, plastics, electrical utility and oil and gas industries. He recently joined IND Technology as the director of business development for North America. Haw has served the International Society of Automation (ISA) at the local, regional and national levels. He was recognized for pioneering the concept of the “born digital” industrial facility with a 2023 Excellence in Technical Achievement Award from ISA for his contributions to a new plastics recycling facility. Haw has a BSEE from the University of Arkansas at Fayetteville and is a licensed professional engineer in Texas. He is also a Certified Maintenance and Reliability Professional (CMRP) and a Project Management Professional (PMP).



Seven ISA Fellows Named for 2025

By Renee Bassett

The International Society of Automation recognized these professionals for their accomplishments and service.

The esteemed Fellow member grade is one of the highest honors ISA can bestow. It recognizes only those senior members who have made exceptional contributions to the automation profession, in practice or in academia. This year, ISA has elevated seven individuals to the status of Fellow. They join dozens of other [distinguished professionals](#) recognized by ISA since the 1960s.

Fellows often play an outsized role in furthering the organization, whether through active leadership positions or by volunteering to speak at conferences, write articles, or lead committees. 2025 Fellow Steve Mustard will speak in Brussels at the OT Cyber Summit,

while 2025 Fellow Marco Ayala is on the program committee. Several 2025 Fellows also have speaking slots at the ISA Automation Summit & Expo in September—an excellent place to meet and talk with these accomplished professionals.

“ISA is proud to acknowledge these distinguished achievers who have made a positive impact on the automation industry with their exceptional contributions,” said ISA President Scott Reynolds. “We appreciate those who made nominations and congratulate those who are being elevated to Fellow. It is my honor to recognize them.”



Marco (Marc) Ayala: MITRE Corporation

As a respected ISA cybersecurity course instructor, a member of the program committee for the OT Cyber Summit and AMSC Cybersecurity Chair. Ayala is president of the InfraGard Houston Members Alliance, serving as Maritime Domain Sector Chief for ports and terminals. Professionally, Ayala is Senior Principal Advisor for Energy, Oil, and Gas at The Cyber Infrastructure Protection Innovation Center (CIPIIC) for MITRE. He's made many [contributions](#) to the ISA Interchange and ISAGCA blogs.

In a post on LinkedIn, Ayala said, "I am deeply honored to have been named an ISA Fellow.... This recognition is not just a personal milestone but a testament to the collective effort of everyone who has supported and collaborated with me throughout my journey in the automation and cybersecurity fields. [Crossing off a massive bucket list item! IYKYK]. My drive has always been to enhance the safety, efficiency, and security of our critical infrastructure, particularly in the sectors of oil, gas, chemicals, and maritime. Being recognized as an ISA Fellow underscores the importance of our work in industrial control system automation and security, pushing the boundaries to ensure our systems are resilient against the ever-evolving cyber threats."



Dr. Jayesh Barve: GE Vernova Advanced Research Center

Dr. Jayesh Barve was named an ISA Fellow for his exemplary academia-plus-industrial R&D contributions in advanced controls optimization. His work addresses energy transition and global energy access challenges via an innovative "lab-scale steam-generator" research-prototype ("agile" power-plant boiler-controls R&D) and a "microgrid-in-box" with integrated an IIoT-edge-cloud solution pilot product ("viable" rural electrification solution). He is based in Bangalore, India.



Dr. Harvinder Singh Gambhir: Council of Vibration Specialists (CVS)

Dr. Harvinder Singh Gambhir was elevated for his contributions to the field of automation in process instrumentation and controls used in oil & gas, refinery, and petrochemicals. He is also a former section president of the ISA Mumbai section.



Steven Pflantz: CRB Engineers and Consultants

Steven Pflantz was elevated to Fellow for the creation, execution and success of a unique and inclusive automation mentorship process utilizing real-time issues and considerations. Pflantz is based out of Wilmington, North Carolina, USA and has contributed many [articles](#) to ISA blogs over the years.



Dr. Brian P. Romano: The Arthur G. Russell Co., Inc.

Dr. Brian P. Romano was rewarded for his development of automation curricula and for teaching the art and science of control systems engineering. Romano spoke at the 2024 Automation Summit & Expo and has contributed many [posts](#) to the ISA Interchange blog. In a post on LinkedIn, he said, "I am beyond thrilled and deeply honored to share that I have been elevated to the prestigious level of ISA Fellow in 2025! I am incredibly grateful for this acknowledgment and excited to continue

advancing and sharing my passion for our field. Thank you to the International Society of Automation (ISA) community and everyone who has supported me on this journey!"



Steve Mustard: au2mation

Steve Mustard was nominated for leading efforts to ensure the U.S. NIST Cybersecurity Framework included ISA/IEC 62443 and for successfully implementing a practical approach to cybersecurity based on the ISA/IEC 62443 standards across multiple industry sectors. Mustard is a prolific contributor to ISA, and has had articles published on the ISA [Interchange](#) blog, - <https://blog.isa.org/author/steve-mustard> AND the [ISACGA](#) blog and Automation.com.

In a post on LinkedIn, he said, ISA Fellow "Marco (Marc) Ayala and I had a great time this week at ConocoPhillips delivering the International Society of Automation (ISA) IC32 and IC33 training courses to a great group of people from all over the world. As always, we learned just as much by sharing knowledge and experience, which is exactly what ISA is all about!"

RECOGNITION



Dr. Ravindra Thamma: Central Connecticut State University

Fellow status was bestowed on Dr. Ravindra Thamma for pioneering the

first ABET-accredited robotics and mechatronics curriculum, harmonizing academic training with industry demands, and advancing early research in internet-based control systems and Industry 4.0 paradigms.

Look for opportunities to meet these Fellows at ISA events and read their work throughout the year on Automation.com. ISA members can [nominate](#) 2026 Fellows now.



ABOUT THE AUTHOR

Renee Bassett is chief editor of *Automation.com Monthly* digital magazine and Automation.com, both official publications of the International Society of Automation. Bassett is an expert content creator, media manager, and journalist with 25 years of experience. Bassett is based in Nashville, Tennessee, and can be reached at rbassett@isa.org.

PLAN TO ATTEND

OT Cybersecurity Summit

Radisson Grand Place,
Brussels Belgium

18-19 June 2025



**AUTOMATION
SUMMIT & EXPO**



ISA Automation Summit & Expo

Disney Coronado Springs,
Lake Buena Vista, FL, USA

5-7 October 2025



International Society of Automation
Setting the Standard for Automation™



Association News

News and resources from the International Society of Automation. Information from International Society of Automation leadership and staff, including the latest news, standards updates and technical resources. Find the latest at <https://www.automation.com/en-us/news-by-company/international-society-automation-news-articles>

Update to ISA/IEC 62443 Standards Addresses Organization-Wide Industrial Cybersecurity and Operations

ISA has announced the publication of [ANSI/ISA-62443-2-1-2024](#) *Security for Industrial Automation and Control Systems*. It is the latest update to ISA/IEC 62443, the widely used global consensus-based automation and control systems cybersecurity standards.

Addressing cybersecurity on an organization-wide basis can be a daunting challenge for companies that rely on industrial automation and control systems (IACS) in their manufacturing, processing and critical infrastructure operations. While no one-size-fits-all set of security practices can meet the widely varying security needs across the global industry, ANSI/ISA-62443-2-1-2024 addresses the complexity by setting forth requirements for establishing, implementing, maintaining and continually improving a security program intended to reduce IACS security risks to tolerable levels.

The requirements are written to be implementation-independent, allowing asset owners to select approaches most suitable to their needs. This update of the

2010 version provides significant technical changes including a revision of the requirement structure into security program elements, and a maturity model for evaluating requirements.

The standards are developed by the ISA99 Standards Committee as American National Standards, with simultaneous review and adoption by the Geneva-based International Electrotechnical Commission. ISA99 draws on the input of cybersecurity experts across the globe in developing the standards, which apply to all industry sectors and critical infrastructure in providing a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in IACS.

“Security is a balance of risk versus cost, and each situation will be different,” said ISA99 Co-Chair Eric Cosman of OIT Concepts. “In some, the risk can be related to health, safety and environmental factors rather than purely economic impact — presenting the possibility of an unrecoverable consequence instead of a temporary

financial setback. Thus, a predetermined set of mandatory security practices could be overly restrictive and costly—or else insufficient to address the risk. This newly updated standard provides the flexibility to reach the right level of risk versus cost for a given operation.”

To learn more about the ISA/IEC 62443 series of standards, [visit www.isa.org/62443standards](http://www.isa.org/62443standards).

Keynotes, Tracks Announced for OT Cybersecurity Summit



ISA has announced the conference tracks and keynote speakers for the 2025 OT Cybersecurity Summit.

Held in Brussels, Belgium, from June 17-19, the event focuses on strategic, industrial operations cybersafety using ISA/IEC 62443 standards and offers various technical tracks, training courses and even a cyber escape room.

Day 1, 18 June, will feature Lauren Neal, project manager with BP UK. She will be speaking on protecting capital assets with a robust cybersecurity plan. Day 2 features

John Fitzpatrick, founder of Lab539, speaking on “proven resilience: trusting in OT’s own path to cybersecurity.”



Lauren Neal
British Petroleum UK

Conference track 1 is on Threat Intelligence: Transforming Business and Driving Progress. Threat Intelligence plays a crucial role in the ongoing advancement of automation by enabling the development of more sophisticated, adaptive, and efficient systems.

As automation technologies continue to evolve, integrating advanced intelligence capabilities, such as machine learning, artificial intelligence and predictive analytics, is becoming increasingly important. These technologies enable automation systems to learn from experience, adapt to changing conditions, and make more informed decisions, ultimately driving greater efficiency, productivity, and accuracy.



John Fitzpatrick
Lab539

Conference track 2 is on Securing the Supply Chain: Strategies for Mitigating Risk.

As the industrial landscape rapidly evolves, ensuring the security of operational technology (OT) systems is paramount. A critical component of this is safeguarding the supply chain, which has become a prime target for cybercriminals seeking to exploit vulnerabilities. With the rise of interconnected systems and the growing reliance on third-party vendors, organizations must develop a comprehensive approach to protecting their

critical infrastructure and understand the implications of supply chain security for their overall cybersecurity posture.

To learn more or to register, visit the event page: <https://otcs.isa.org/>.

ISA Announces 2025 Society Leadership

ISA—the leading professional society for automation—has announced its Society leadership for the term beginning Jan. 1, 2025. These individuals have demonstrated their strong commitment to ISA and to envisioning the role that the Society plays in the future of the global automation community. Members of the 2025 Executive Board include:

- President: Scott Reynolds, Johns Manville, A Berkshire Hathaway Company
- President-elect Secretary: Ashley Weckwerth, P.E., Burns and McDonnell
- Past President: Prabhu Soundarrajan, Kingston Capital
- Treasurer: Ardis Bartle, Apex Measurement and Controls
- CEO and Executive Director: Claire Fallon, International Society of Automation
- Dr. Soloman Almadi, Saudi Aramco
- Marco Ayala, MITRE
- Alan Bryant, P.E., PMP, Occidental
- Alexa Burr, National Electrical Manufacturers Association (NEMA)
- Francisco Diaz-Andreu, Repsol
- Nick Erickson, AWC, Inc.
- Colleen Goldsborough, CPSC, United Electric Supply
- Sherry LaBonne, Rockwell Automation

- David Lee, C.Eng, FIChemE, User Centered Design Services
- Robert M. Lee, Dragos
- Edward Naranjo
- Mary Riedel, Martin Control Systems, Inc.
- Megan Samford, Schneider Electric
- Sujata Tilak, Ascent Intellimation
- Jeff Winter, Critical Manufacturing.

“I am honored to welcome this new slate of exceptional professionals to ISA leadership,” said Mr. Reynolds. “I am delighted to see such a wide array of experience across ISA and the industry sectors our Society serves. I look forward to working with this group to continue the growth trajectory of ISA and empower our global community of automation professionals.”



In case you missed them, here are the top 20 highest-performing posts from 2024 on the ISA Interchange blog.

20. [How Much Does Rework/Repair Really Cost?](#) (Grant Vokey, published May 21, 2024)
19. [How to Validate Your Knowledge of the ISA-95/IEC 62264 Standards Framework](#) (published Sept. 3, 2024)
18. [Achieving the Best Cascade Control](#) (Greg McMillan for “Ask the Automation Pros,” published Dec. 6, 2024)

Onward and Upward to 2025: Proud of a Great Year at ISA

By Prabhu Soundarrajan

As my year as president of the International Society of Automation (ISA) comes to a close, I wanted to take a moment to reflect and celebrate all the great things the International Society of Automation (ISA) has achieved in 2024. I am so grateful to everyone at ISA for their hard work and strong support of big, member-generated ideas, and I am so proud of where ISA is headed. ISA is undergoing transformational change to meet the future, and I am honored to have served during such a pivotal year.

This article is a follow-up to the [first blog post I wrote](#) in early 2024 outlining my plans as the incoming ISA president. I'm pleased to report that our strategies paid off—we met and exceeded our goals and set us up for an amazing 2025.

2024 ISA highlights

We certainly had an eventful year! ISA continued to make massive strides forward in 2024. Here are just a few highlights:

- The publication of [ISA-5.1-2024](#), an update to ISA's oldest and most widely used standard
- The launch of a much-requested certification program for [ISA-95/IEC 62264](#)
- Release of the world's first SL3 certifications by the [ISASecure®](#) cybersecurity certification program
- Two conferences—the OT Cybersecurity Summit in London and the Automation

17. [Intelligent Automation: Overcoming Challenges for Seamless Implementation](#) (Amol Kakade, published Feb. 20, 2024)
16. [ISA Landmark Turnaround Fuels Future Growth](#) (ISA President Prabhu Soundarrajan, published Oct. 8, 2024)
15. [An Interview with Béla Lipták, Author of "Controlling the Future: Preventing Climate and Other Disasters"](#) (published Feb. 8, 2024)
- 13 (tie). [AI in Oil: Unleashing a New Era of Efficiency and Innovation](#) (Emily Newton, published Jan. 19, 2024)
- 13 (tie). [2024 Will Be a Remarkable Year for Automation Led by ISA](#) (ISA President Prabhu Soundarrajan, published Jan. 30, 2024)
12. [When Are We Modernizing Control Systems?](#) (Greg McMillan for "Ask the Automation Pros," published Jan. 22, 2024)
11. [ISA Technical Content Available at Pub Hub](#) (published June 14, 2024)
10. [Social Learning in the Automation Profession: 7 Benefits You Can't Ignore](#) (published Aug. 16, 2024)
9. [Meet ISA's 2024 Executive Board Members, Part 1](#) (published Aug. 2, 2024)
8. [ISA Business Academy: A Mini-MBA for Automation Industry Leaders](#) (published March 11, 2024)
7. [Sustainability, Automation and Cybersecurity: Partners to Drive Growth and Governance](#) (ISA President Prabhu Soundarrajan, published July 9, 2024)

THE LATEST

Summit & Expo (ASE) in Charleston, S.C.—drew hundreds of automation professionals to network and learn about standards, training, certification and membership opportunities

- The addition of several new sections including Minas Gerais (Brazil), Bahrain, the United Kingdom and Sacramento (CA)
- The growth of [Podomation](#), ISA's official podcast, to include listeners from 46 countries
- Acknowledgement of ISA as a 2024 Top-Rated Nonprofit by GreatNonprofits.

All of these accomplishments took incredible amounts of time and effort from committee members, staff and volunteers alike. It's clear that ISA is on an upward trajectory as a direct result of these efforts.

I'd also like to point to a couple of recent projects that illustrate how much we are changing as a society and how we are laying the groundwork for an inspiring future.

Membership growth. In 2024, ISA grew significantly—I'm proud to report that, as of December 2024, ISA membership now includes more than 17,000 automation professionals from all over the world. That's record membership growth for our society of 15.78%. This is a major turnaround from years past, representing the highest numbers we have seen since 2013.

2024 ISA strategic plan. The following elements contributed to the fulfillment of the 2024 ISA Strategic Plan. Here are a few highlights:

- We developed the ISA corporate engagement program, attracting and engaging

6. [Understanding Data Mesh and the Modern Smart Factory](#) (Sukanta Kumar Rout, published Jan. 3, 2024)
5. [Key Takeaways from My Year as ISA President](#) (ISA Past President Marty Bince, published Jan. 12, 2024)
4. [Symptom vs. Cause vs. Root Cause](#) (Grant Vokey, published Feb. 6, 2024)
3. [Taking a Look at the Virtual PLC Technology Stack](#) (Daniel O'Duffy, published Sept. 24, 2024)
2. [How Can We Improve or Eliminate Split Range Control?](#) (Greg McMillan for "Ask the Automation Pros," published March 5, 2024)
1. [Getting to Know MimoSM, ISA's Large Language Model Trained on ISA Content](#) (published July 26, 2024).

Contributing to the ISA Interchange blog can be a great way to build your reputation as a thought leader. If you'd like to share your knowledge of the automation profession in 2025, we would be excited to read your work. [Contribute your articles for consideration here.](#)

new companies in the breadth of ISA programs, products and services. Many of these companies have offered their testimonials on what ISA means to them across a number of program areas, including standards, training, events and the ISA Global Cybersecurity Alliance (ISAGCA).

- We continued to foster discussion around evolving and emerging technology, processes and business practices related to

THE LATEST

ISA's mission, developing guidance and content around industrial AI, OT cloud and cybersecurity resilience as well as elevating our voice on resilient supply chain, energy transition, digital deglobalization and ethical sourcing.

Celebrating Mimo. [MimoSM](#), an artificial intelligence-powered large-language model trained on ISA-exclusive content, launched this summer with full access granted to ISA members. Mimo provides its answers to user-generated questions by learning from all things ISA-related including ISA standards, training, technical reports, white papers, articles and presentations.

During the first full month of Mimo's wide release this summer, [Mimo answered roughly 4,000 prompts](#). According to [Betty Bot](#), ISA's partner in building Mimo, that's eight times the prompts a typical association knowledge assistant can expect to see upon launch. Mimo has also answered questions in at least eight languages. It's a runaway success story that has become a case study on

how associations can create a useful knowledge assistant for their members.

That's a wrap

It's been a phenomenal year, and I must reiterate how proud I am to have served this wonderful society that means so much to automation professionals around the world. As I hand the reins to incoming 2025 ISA president Scott Reynolds, I can do so knowing that ISA met and exceeded our goals this year. I have been so impressed by our extraordinarily dedicated volunteers, staff and Executive Board, and I know ISA will continue to reach new heights with everyone working together.



Prabhu Soundarrajan (kneeling) is shown with other members of ISA leadership including ISA CEO and Executive Director Claire Fallon (far left).

Technology Update

A monthly magazine can't keep up with all news, insights and inspiration automation professionals need. Stay informed with [Automation.com](https://www.automation.com), the publication platform of the International Society of Automation. New articles are published daily under six broad categories encompassing a range of automation, control and cybersecurity topics. Search for new products and whitepaper resources in all categories. You can also [subscribe](#) to the Automation Weekly newsletter or one of the topic-specific newsletters to get news, new products and other technical resources delivered to your inbox.—*Melissa Landon, Senior Content Editor*

Digital Transformation - What the cool kids are doing

Better Insights Lead to Better Manufacturing

Management

Changing core processes while managing the daily demands of the business is seldom easy. Introducing new technology to a



100+-year-old manufacturer is even more challenging. Here's how that manufacturer navigated its digital transformation.

Smarter Factories: Manufacturing in 2025 and Beyond

A survey from the Institute for Supply Management showed that 60% of manufacturers anticipate increased revenues in 2025. Manufacturers can prepare for success by creating smart factories using AI and decentralized manufacturing methods.

Safety & Cybersecurity - Protecting people, plants and the environment

Digital Innovations Are Making Industrial

Facilities Safer

Although regulations are important to promote safety, industrial facilities also need safety technologies such as AI, automation and software tools. Connecting the dots between new safety technologies and existing workflows should be a strategic imperative for industrial organizations.

What Does the Future of Zero Trust in OT Look Like?

The irreversibility of IT/OT convergence and the pervasiveness

and effectiveness of zero trust in enterprise IT systems give clear signaling that OT networks will adopt it, eventually. So what, exactly, will zero trust look and feel like in the future? And when will it happen?



Enterprise Architecture & Networks - How things fit and communicate

How eSIM, IoT and Connectivity Security Are Powering Industry 4.0

eSIM eliminates the limitations of traditional SIM cards by allowing secure over-the-air provisioning and updates, making it easier for businesses to manage large-scale deployments across multiple regions.

2025 IoT Breakthrough Awards Announced

More than 100 awards were given in 13 categories to celebrate innovative IoT companies, products, services and people. The awards honor an industrial IoT company, solution and innovator of the year, digital twin solutions, predictive maintenance solutions, smart manufacturing solutions, and more.

Operations & Management - Managing the business

The Future of Energy Storage with AI-driven Technologies

As the world becomes increasingly focused on renewable energy and reducing carbon footprints, the need for advanced energy



storage systems is growing significantly. The integration of artificial intelligence is helping to make them more reliable, efficient and cost-effective.

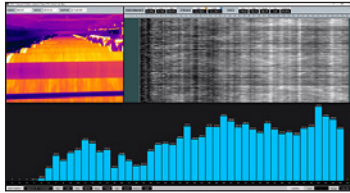
The Role of AI in Lean Manufacturing

Lean manufacturing aims to reduce waste, enable continuous improvement and enhance customer value. Artificial Intelligence supports lean manufacturing by offering accessible personalization for high-end items, analyzing factory processes to find improvement opportunities and boosting productivity.

Automation & Control - Running the plant

Case Study: Visualizing the Pathway to Better Papermaking

Industrial Video Solutions Inc., a US-based specialist in automation for the papermaking industry, is leveraging infrared (IR) thermal cameras



to get data from paper machines that can be used to boost machine-control efficiency.

Motion Controls Market Declines as Over-Ordering Results in DeStocking

Marked by low manufacturing output and a significant “destocking” event, 2024 was a rough year for makers of motion control products. However, the market has begun to stabilize and the long-term compound annual growth rate remains largely unchanged.

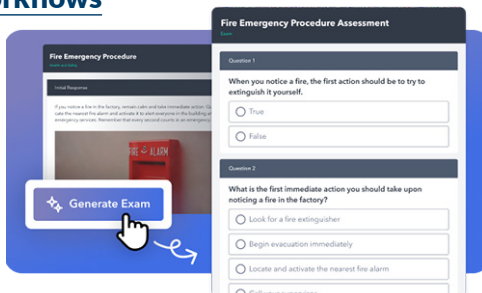
New Products - Hardware and software solutions

Yokogawa Releases OpreX Quality Management System

The cloud-based system can accelerate the digital transformation of quality assurance processes for the manufacturing of pharmaceuticals and food & beverages.

knowledge on the shop floor, these innovations address critical challenges in workforce efficiency, training and communication. The toolkit will provide new benefits to workers on the shop floor, from video-based work instructions to multilingual translation and smarter search functions.

Poka Introduces AI Toolkit for Manufacturing Workflows



Poka has added AI-powered features to its Connected Worker Platform. Designed to transform the way manufacturers create, share and access

ABB Strengthens Roller Table Motor Offering for Global Steel Industry

The motors, designed specifically for rolling mills, have up to 20-year lifespan and have been shown to slash operating costs.



Advantech IoT Edge Device Is Pocket-Size Industrial Gateway

The compact device delivers powerful edge computing capabilities with second-stack expansion options for diverse industrial applications.



A MESSAGE FROM THE EDITOR

ISA's Magazine Continues to Digitally Transform

February 2025 marks the debut of the latest iteration of the International Society of Automation's magazine, *Automation.com Monthly*. This nine-times-a-year periodical, published in PDF and Web formats, will expand the society's mission of empowering the global automation community through standards and knowledge sharing.

ISA purchased Automation.com in 2014 and this year the website is celebrating its 25th anniversary. The site's strong domain name and digital presence—including an audience of more than 123,000 industry professionals—give ISA a global reach beyond its 17,000 members. Visitors to Automation.com get access to thousands of curated automation resources from ISA and the wider automation community: news, new product announcements, technology trends, technical deep dives, whitepaper reports, and more.

Automation.com's digital magazine, most recently called *AUTOMATION 2024*, is being consolidated with ISA's *InTech* digital magazine to become *Automation.com Monthly*. Anyone can [subscribe](#) to the magazine or the range of newsletters covering specific topics like industrial cybersecurity and safety. Like other business-to-business magazines, the "cost" to subscribe is a valid email address and other professional information.

InTech has transformed multiple times since its inception in 1954 as *ISA Journal*. The print magazine was renamed *Instrumentation Technology* in 1967 and became *InTech* in 1978. Access to digital versions of *InTech* magazine began in 2016; in December 2023, ISA mailed its last print issue of *InTech* and began digital-only access alongside the other information resources of Automation.com.

Automation.com's strong domain name and digital presence give ISA global reach and ISA members access to thousands of curated automation resources.

ISA's strong commitment to producing automation content for its members and in service to the wider automation community continues. The new magazine will contain the same high-quality technical content from ISA subject matter experts and volunteers that *InTech* has been known for, as well as expert-authored articles from other automation professionals. Submissions from ISA members take precedence, and potential authors are encouraged to reach out to me via ISA Connect or [email](#).

Renee Bassett Chief Editor,
Automation.com Monthly