# InTech®

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

DECEMBER 2023

ISA™

www.isa.org/intech

## Digital Twins for the Virtual Plant: A Bioreactor Example

## Cybersecurity Preparedness for Oil, Gas and Petrochemical Operations

## Utility Consumption Monitoring for Sustainability

## Advanced Analytics and OEE Improvement

## How Industrial Ethernet Is Reshaping Industry

## SCADA in a Water/Wastewater Capital Project

InTech
DIGITAL MAGAZINE

DECEMBER 2023

## WELCOME TO *INTECH*

As the official publication of the International Society of Automation (ISA), *InTech* digital magazine is written for engineers, managers, and other automation decision-makers. It serves ISA members and the wider automation community with practical, in-depth coverage of automation technologies, applications, and strategies that help automation professionals succeed.

*InTech* is brought to you with the support of advertisers. Click the logos on the right to go to their ads, then click through to their websites to discover information on automation hardware, software and services.

## Don't Miss a Single Issue

*InTech* is part of a family of ISA publications that keep you informed and up-to-date on industrial automation, control and security best practices, trends, new products and other advances. Subscribe to *InTech* digital magazine, InTech Plus newsletters and other resources through ISA's automation news and information subsidiary, Automation.com

**Rick Zabel, Managing Director**
*InTech, Automation.com & Events Sponsorships*
*International Society of Automation (ISA)*

ISA International Society of Automation
*Setting the Standard for Automation™*
company/internationalsocietyofautomation
InternationalSocietyOfAutomation
ISA_Interchange

## Advertisers Index

To obtain further information, please contact the advertiser using the contact information contained in their ads.

| | |
|---|---|
| ISA International Society of Automation<br>*Setting the Standard for Automation™* | Page 6, 23, 49, 69 |
| 1898 & Co. PART OF BURNS & McDONNELL | Page 41 |
| ARC Advisory Group | Page 56 |
| AUTOMATIONDIRECT.com | Page 7 |
| beamex | Page 30 |
| Endress+Hauser<br>People for Process Automation | Page 22 |
| inductive automation | Page 4 |
| MOORE INDUSTRIES WORLDWIDE | Page 13 |
| MOXA® | Page 3 |
| SIEMENS | Page 36 |
| TADIRAN BATTERIES | Page 10 |
| txOne networks | Page 31 |

Special promotion:
Now until Dec 31, 2023

# EDS-2000/G2000-EL/ELP Series

## Industrial Unmanaged Ethernet Switches

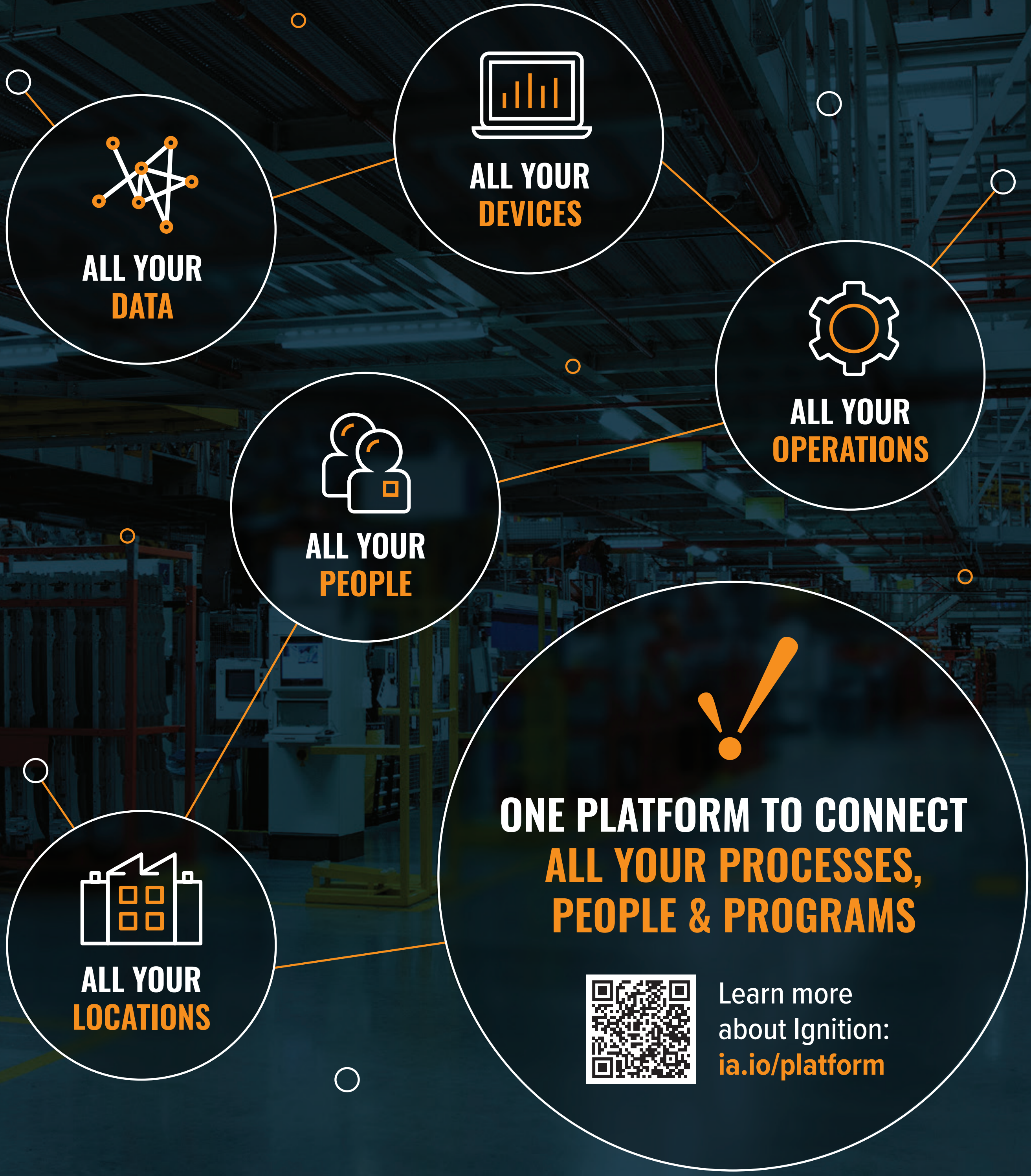
Scan the QR code
to learn more

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

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

# Connect The Dots With Ignition

## The Unlimited Platform for Total System Integration



ALL YOUR DATA

ALL YOUR DEVICES

ALL YOUR OPERATIONS

ALL YOUR PEOPLE

ALL YOUR LOCATIONS

ONE PLATFORM TO CONNECT
ALL YOUR PROCESSES,
PEOPLE & PROGRAMS

Learn more
about Ignition:
ia.io/platform

inductive
automation

InTech

Setting the Standard for Automation™

DECEMBER 2023 | VOL 70, ISSUE 6

## FEATURES

ISA

International Society of Automation

*Setting the Standard for Automation™*

# 2024

## ISA Conferences

ISA's unbiased technical conference programming provides access to worldwide experts and content on the latest technologies, trends, real-world challenges, and industry updates needed to remain competitive in today's marketplace.

### Mark your calendars and make plans to attend an ISA technical conference program in 2024!

IOT SOLUTIONS WORLD CONGRESS

**IOTSWC and Cybersecurity World Congress**
Barcelona, Spain
21-24 May

**OT Cybersecurity Summit**
Savoy Place
London, England
18-19 June

**ISA Automation & Leadership Conference**
Francis Marion Hotel
Charleston, South Carolina, USA
30 September-2 October

**Visit isa.org/events for more information.**

SCAN ME

# CAUTION VALUE OVERLOAD!

Wi-Fi

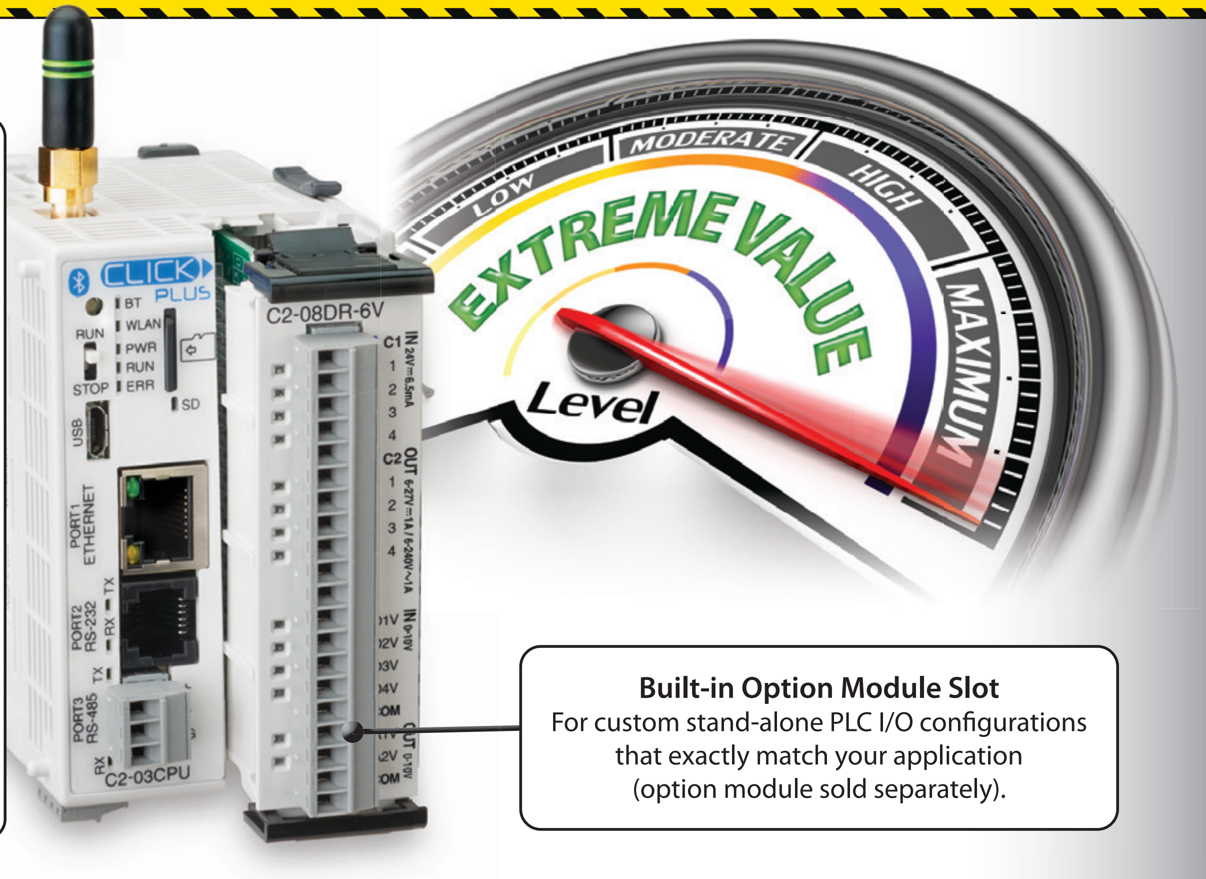
Bluetooth (provisioning only)

microSD

USB

Ethernet

Serial (RS-232 & RS-485)



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

### CPU units starting at only $97

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

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

FREE Technical Support
Located in USA

45-day Money-Back Guarantee
45 day

FREE downloadable software
for many products
see website for details

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

www.CLICKPLCs.com

TOP RATED ★★★★★ BY CUSTOMERS

Order Today, Ships Fast!

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

# InTech

DECEMBER 2023 | VOL 70, ISSUE 6

## DEPARTMENTS

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

### EDITORIAL & PRODUCTION

**CHIEF EDITOR:** Renee Bassett, rbassett@isa.org
**SENIOR CONTRIBUTING EDITOR:** Jack Smith, jsmith@isa.org
**EDITOR EMERITUS:** Bill Lydon, blydon@isa.org
Charley Robinson, crobinson@isa.org
**ART DIRECTOR:** Bonnie Walker
**DIGITAL DESIGNER:** Colleen Casper
**DIGITAL PRODUCTION MANAGER:**
Melissa Landon, mlandon@isa.org

### ISA EXECUTIVE BOARD

**ISA PRESIDENT:** Marty Bince
**ISA PAST PRESIDENT:** Carlos Mandolesi
**ISA PRESIDENT-ELECT & SECRETARY:** Prabhu Soundarrajan
**ISA TREASURER:** Steve Mustard
**ISA EXECUTIVE DIRECTOR:** Claire Fallon

### ADVERTISING & SPONSORSHIP

Rick Zabel, **PUBLISHER**
rzabel@isa.org
Chris Nelson, **ACCOUNT EXECUTIVE**
chris@isa.org
Richard T. Simpson, **ACCOUNT EXECUTIVE**
richard@isa.org
Gina DiFrancesco, **ACCOUNT EXECUTIVE**
gina@isa.org
Cathi Merritt, **ADVERTISING PRODUCT MANAGER**
cmerritt@isa.org
Matt Davis, **DIGITAL MEDIA PROJECT MANAGER**
mdavis@isa.org

2024
Media Planner

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

Editorial and advertising offices are at 3252 S. Miami Boulevard, Suite 102, Durham, NC 27703; phone 919-549-8411; email info@isa.org.

*InTech* digital magazine publishes six times per year. **ISA Members** receive *InTech* digital magazine as part of their annual membership and get access to archived issues. Non-members can **subscribe** to *InTech* and InTech Plus newsletters through ISA's automation news and information subsidiary, Automation.com. InTech and the ISA logo are registered trademarks of ISA.

Trademarks used in this digital magazine are the property of their respective owners. Opinions expressed or implied are those of the persons or organizations contributing the information and are not to be construed as those of ISA.

International Society of Automation
*Setting the Standard for Automation™*

# The Evolution of *InTech*

**By Renee Bassett, *InTech* Chief Editor**

*InTech*, in its evolving formats, has been ISA's flagship publication for more than 70 years. Last year in this same space, I let you know about our move to all-digital distribution, and about how to subscribe to the InTech Plus newsletters.

This year I have exciting news about access to *InTech* magazine issues, past and ongoing, and about the range of other ISA resources designed to keep automation professionals well-informed about our fast-moving, quickly evolving industry.

New landing pages for *InTech* digital magazine articles and ISA-related news have been set up on Automation.com, ISA's news and publications subsidiary. You can find and download *InTech* issues through the new InTech Channel on Automation.com: https://www.automation.com/en-us/intech-international-society-of-automation. You can also find additional features, ISA news and links to ISA Interchange and ISAGCA blogs through the new ISA News channel.

To have *InTech* articles and ISA news delivered to your inbox, subscribe to the bi-monthly InTech Plus newsletter. Through that link, you can also sign up for other newsletters. Automation.com's newsletters curate the top website posts each week into a variety of topical and general-interest periodicals. Automation Insights and InTech Plus are general interest newsletters; topic-specific newsletters include a new one on Industrial Sustainability, Cybersecurity & Connectivity, Factory Automation & Control, Industry 4.0 & Smart Manufacturing, and Process Automation & Control.

InTech
AUTOMATION FUNDAMENTALS
Fundamentals of PID Control
ISA-TR5.9-2-23: Achieving the Best PID
Basics of Control Valve Flow Characteristics
Industrial Computers: Robust and Ready
Remote-Site Data in Real Time: A Case Study
InTech Plus
Published by ISA
Valve Stem Sealing Best Practices
Connect Your Pressure Measurement to the Future
Deploying IIoT Sensors and Networks in Remote Locations
Future-Proofing Controls Programming for the Edge

For issue archives and much more,  ISA members get access to PubHub, the ISA content portal that  contains issues of *InTech* magazine going back to 2010.  It also contains years of other ISA technical content including ISA standards and technical reports, *InTech FOCUS* digital magazines, AUTOMATION 2024 ebooks, and select ISA book chapters, webinars, and training modules.

Automation.com has a wealth of industry news, new product information and other resources that will keep you in-the-know and up-to-date on what's happening in industrial automation. Remember that any automation professional is welcome to send content for consideration: news on themselves, news from their companies, or queries about contributing articles. Send to press@automation.com with "ISA Member News" in the subject line.

Let me know what you are using to keep up with our industry in addition to *InTech* and Automation.com. Best wishes for a happy new year.

# Remote Monitoring Key to Chilean Gold Mine Operation

**By Jack Smith**

Salares Norte is a gold and silver mining project owned by Gold Fields, in the Atacama region of Northern Chile. An enterprise-grade digital platform—Ability Genix Industrial Analytics and AI Suite from ABB—is being installed to drive efficient, sustainable, remote operations.

The gold and silver mine is located among the highest peaks of the Andes Mountain range with elevations of between 13,780 ft. (4,200 m) and 16,076 ft. (4,900 m). It is 808 miles (1,300 km) from the Chilean capital of Santiago where a remote monitoring center for the mine houses the analytics and artificial intelligence (AI) software.

With the technology, Gold Fields hopes to gain data insights that will help the mining company increase industrial productivity and operational excellence and reduce costs. Safety will be improved because remote connectivity will help reduce the number of people needed at the actual mine location.

The analytics software suite combines the power of industrial analytics and AI to integrate 25 engineering, operational, and information technology (IT) systems across different functional areas, including the mine, processing, geology and exploration, asset management, finance, legal, and human resources.

## Solution details

Starting with data capture and integrating cross-functional data, the analytics software suite connects operational, business, and engineering systems. It then collects, contextualizes, and converts data through advanced analytics into meaningful information to

The Salares Norte gold and silver mining project uses remote data capture analytics software to optimize operational, business, and engineering systems.

unlock productivity improvements by driving smart business decisions. In addition, it will help visualize and analyze information required to support Gold Fields' reporting and drive its environmental commitments, helping the company achieve its vision of becoming the global leader in sustainable gold mining.

"Salares Norte deploys a high level of digital industrial software and technology. This is critical to this project due to its remote location—the nearest town is Diego de Almagro, 180 km [112 miles] away—the altitude of the project, and adverse weather conditions, which make site access and fieldwork challenging," said Max Combes, project director of the Gold Fields mines. "It demands a solution for the remote monitoring center in Santiago that could integrate and contextualize information from many systems, including some common to Chile, as well as perform data analytics."

ABB will deliver an integrated electrification, automation, and digitalization solution to Salares Norte. Iván Villegas, hub product marketing manager for Automation in South America for ABB said, "ABB Ability Genix, set to be fully commissioned in record time, will help Gold Fields use [its] data from operations better by combining it with engineering and IT data for multi-dimensional decision making."

ABB has already deployed its ABB Ability MineOptimize solution to supply an integrated power and automation system at Salares Norte. The solution comprises six electrical rooms and a suite of process and power controls under the ABB Ability System 800xA distributed control system (DCS). The control systems include Power and Process Control Library and Camera Connect (the ABB video system embedded in the control platform for optimized process monitoring).

ABB Ability Knowledge Manager is used to manage information production through Plant Information Management System (PIMS), alongside ABB Ability Asset Vista Condition Monitoring.

ABB's Dynamic Process Simulator reviews plant control logics, which reduces commissioning times and allows Gold Fields to train operators to acquire the skills required to achieve high-quality operations.

## Looking ahead

Salares Norte is expected to produce 3.7 million ounces of gold over an initial mine life of 11 years. The operation involves drilling, blasting, loading, and hauling methods for ore extraction, and has an installed production capacity of two million tons per year.

### ABOUT THE AUTHOR

**Jack Smith** is senior contributing editor for Automation.com and *InTech* digital magazine, publications of ISA, the International Society of Automation. Jack is a senior member of ISA, as well as a member of IEEE. He has an AAS in Electrical/Electronic Engineering and experience in instrumentation, closed loop control, PLCs, complex automated test systems, and test system design. Jack also has more than 20 years of experience as a journalist covering process, discrete, and hybrid technologies.

INDUSTRY 4.0

# Digital Twins for the Virtual Plant

## A bioreactor system design example shows a way forward for plant development and process optimization.

**By Gregory K. McMillan**

We have exceptional opportunities offered by today's automation system capabilities to meet the needs and challenges of sustainable and productive plant operation. Smart instrumentation performance and intelligence and the increasing capabilities of control algorithms, data analytics, diagnostics, and simulation to deal with a wide spectrum of process situations offers incredible possibilities. This is particularly important considering increasingly prevalent control expertise retirements, tighter budgets and schedules, and equipment and professionals stressed to perform beyond original expectations.

It is increasingly difficult—in actual plants—to conduct the tests and experiments needed to develop, implement, and continuously increase plant capacity and efficiency or to prolong equipment life. The digital twin offers a groundbreaking way forward by virtue of the virtual plant.

A virtual plant is a software model that encompasses all the latest capabilities in an adaptable real-time simulation that includes the dynamic responses of the process, the equipment, and automation system. The digital twin sets up the understanding required to import the configuration and files that are used by the actual plant. The digital twin setup and use are normally within the functional realm of experienced process control engineers. Many can help improve and connect dynamic simulations. However, the models and advanced control tools related to virtual plants are more likely developed by specialists.

This article reviews the functional value of digital twins and uses a bioreactor system design example to show how digital twin modeling and simulation feeds virtual plant design and maximizes the synergy among scientists, operators, process control engineers, and control systems to enable process optimization. It is an adaptation of material from two new books that can help process control engineers learn more about virtual plants, setting up and running dynamic simulations, and optimizing the operations of existing plants using digital twin technology. This knowledge is critical for addressing the many challenges in bioprocess and pH control systems and achieving the most reliable and proficient process performance.

## Functional value

Figure 1 illustrates a digital twin's functional value, highlighting the bidirectional flows of the control system and process/equipment knowledge of process control and analysis tools, including online key performance indicators (KPIs) and real-time accounting (RTA) metrics for greater analysis and justification of improvements. The two-way knowledge flow is the key to improving the process/equipment and the control system in addition to the dynamic model and data analytics. As the fidelity of the dynamic model increases, opportunities arise for these

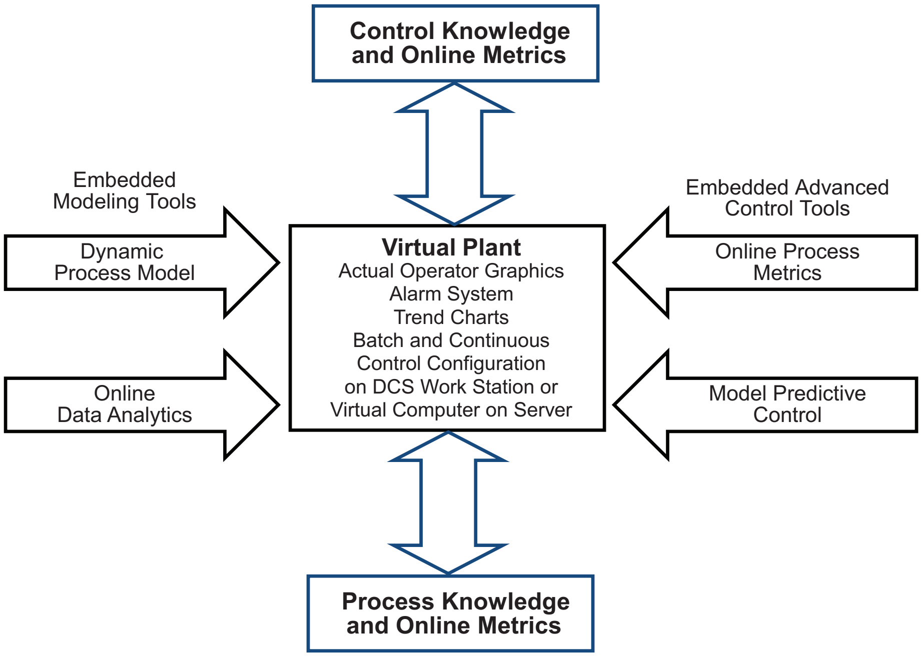

Control Knowledge and Online Metrics
Embedded Modeling Tools
Dynamic Process Model
Online Data Analytics
Virtual Plant
Actual Operator Graphics
Alarm System
Trend Charts
Batch and Continuous Control Configuration on DCS Work Station or Virtual Computer on Server
Embedded Advanced Control Tools
Online Process Metrics
Model Predictive Control
Process Knowledge and Online Metrics

**Figure 1. The two-way flow of knowledge in the digital twin between tools, models, and the actual control system is the source of the increasing synergy of knowledge between the process, control system, engineers, technicians, and data scientists.**

tools to get results from the digital twin that can be used in the actual plant. The dynamic model can be run faster than in real time with the tuning corrected by applying the speedup factors. New control functionality can be developed and included in the dynamic model for evaluation. If online metrics show significant improvements in control and process performance, the functionality prototyped can be added as new blocks or as improvements to existing blocks in the distributed control system (DCS).

The digital twin can accelerate the benefits gained by offering users the ability to use process and end point monitoring and control, continuous improvement, and knowledge management tools in an integrated manner.

The most familiar use of a digital twin is for testing and training. To check out batch sequences and train operators, it is important to be able to simulate batch phases repetitively and rapidly. The ability to stop, start, save, restore, and replay scenarios and record operator actions is critical. For first pass testing and familiarization of sequences and graphics, an automated tieback simulation may be sufficient. To test and learn about the interaction and performance of control strategies and the process, the higher fidelity dynamics offered by process models is important. It opens the door to upgrading the process and control skills of technology, maintenance, and configuration engineers who support operations. A process simulation with high dynamic fidelity is also important for testing process and control system interaction and performance.

The dynamic models often used for training operators as part of an automation project have a much wider utility that is more important today than ever is a reality that is not well recognized. There is a great opportunity to use the digital twin to maximize the synergy between the operators, process control engineers, and control systems. To start on this path, process control engineers must be given the time to learn and use a digital twin and set up online metrics for process capacity and efficiency. The digital twin offers flexible and fast exploring => discovering => prototyping => testing => justifying => deploying => testing => training => commissioning => maintaining => troubleshooting => auditing => continuous improvement showing the "before" and "after" benefits of solutions from online metrics. Figure 2 outlines the major steps in continuous improvement and maximizing innovation.

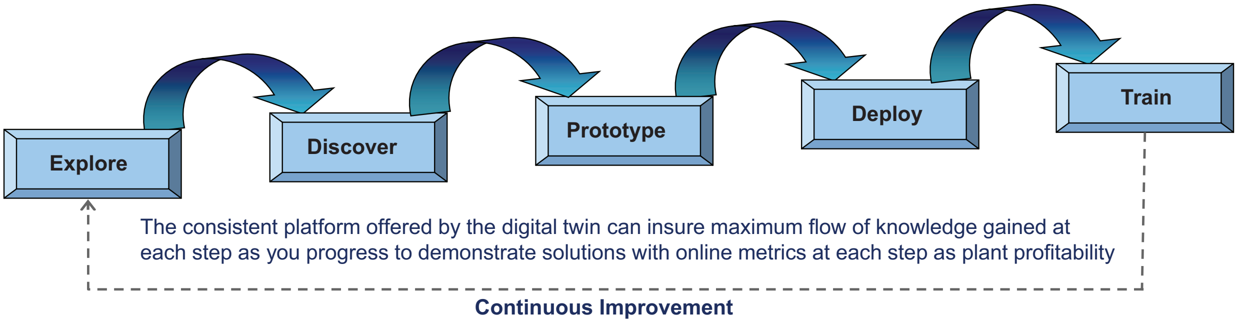

Explore
Discover
Prototype
Deploy
Train
The consistent platform offered by the digital twin can insure maximum flow of knowledge gained at each step as you progress to demonstrate solutions with online metrics at each step as plant profitability
Continuous Improvement

**Figure 2. Continuous improvement can become an inherent part of the digital twin, maximizing the synergy of operational, process, and control system knowledge.**

The capability of dynamic models to improve system performance has greatly increased, even though the use has focused mostly on training operators as an automation project nears completion. The digital twin should detail the tasks needed to address difficult situations based on the best operator practices and process knowledge and eliminate the need for special operator actions through state-based control. Advanced process control (APC) and model predictive control (MPC) can respond to disturbances and address constraints intelligently, continually, and automatically with great repeatability.

Compare this with what operators can do in terms of constant attention, deep knowledge, and timely predictive corrections considering dead time, multivariable situations, and uncertainty in human behavior. Some operators may do well, but not all operators. Then, of course, an operator can have a bad day. Automation enables continuous improvement and recognition of abnormal conditions by a much more consistent operation. A better understanding by the operator of control system functionality and process performance from online metrics greatly reduces disruptions by an operator unnecessarily taking a control system out of its highest mode and/or making changes in flows. Furthermore, procedure automation can eliminate manual operations during startup when the risk is the greatest compared to steady-state operation.

While we have singled out operators and process control engineers, the need for knowledge to attain the best performance extends to maintenance technicians, process engineers, mechanical engineers, and information technology (IT) specialists. Think of what can be realized if we are all on the same page understanding the process, operational opportunities, and the value of the best measurements, valves, controllers, and software.

**Digital twin modeling and simulation feeds virtual plant design and maximizes the synergy among scientists, operators, process control engineers, and control systems.**

Possible digital twin opportunities to increase plant knowledge and performance include:

- Cause-and-effect relationships
- Interactions and resonance
- Valve and sensor response
- Process safety stewardship
- Control system and safety instrumented system (SIS) knowledge
- Validation and regulatory support
- Code checkout
- Process and equipment knowledge
- Process equipment degradation
- Startups, transitions, shutdowns, and batch operation
- Optimum operating points.

Before the configuration even starts in the front end of a project, the process models can be used to evaluate control strategies and advanced control tools. In the past, this was done with offline dynamic simulations. Having ready access to an industrial tool set for basic and advanced control and simulations that are adapted to benchtop or pilot-plant runs offers rapid prototyping opportunities. This can lead to control definitions that have better detail and potential performance.

Benchtop or pilot-plant systems with a mini version of the industrial DCS are now available that greatly facilitate developing and scaling up the control system. Benchtop systems and pilot plants that have all the functionality of the main manufacturing systems are not yet prevalent because the development groups of these types of companies traditionally do not have the expertise (and, more importantly, the interest) to configure, maintain, and engineer these systems. The digital twin enables synergy between scientists and control engineers to make the incredible capability of DCS part of the process R&D.

## Bioreactor system design example

Digital twin use is particularly beneficial in pH and bioreactor system design. A pH system offers many orders of magnitude greater hydrogen ion concentration control precision and rangeability than any other concentration measurement. However, this is accompanied by extraordinary process gain nonlinearities and instrumentation response requirements. A digital twin can greatly increase system performance and decrease system cost as detailed in “Advanced pH Measurement and Control,” fourth edition, ISA 2023.

Bioreactors used to produce biologics for most modern-day new pharmaceuticals require incredibly tight pH and temperature control. There are exceptional digital twin opportunities to increase pH and temperature system performance but also develop innovative glucose and glutamine control systems to improve batch cycle time and yield by advanced control including batch profile and endpoint control. The digital twin offers the ability to improve batches worth more than $10 million by better process development and control without testing or experimentation

**A dynamic model can be non-intrusively adapted to improve virtual plant fidelity by matching the virtual and actual plant manipulated flows.**

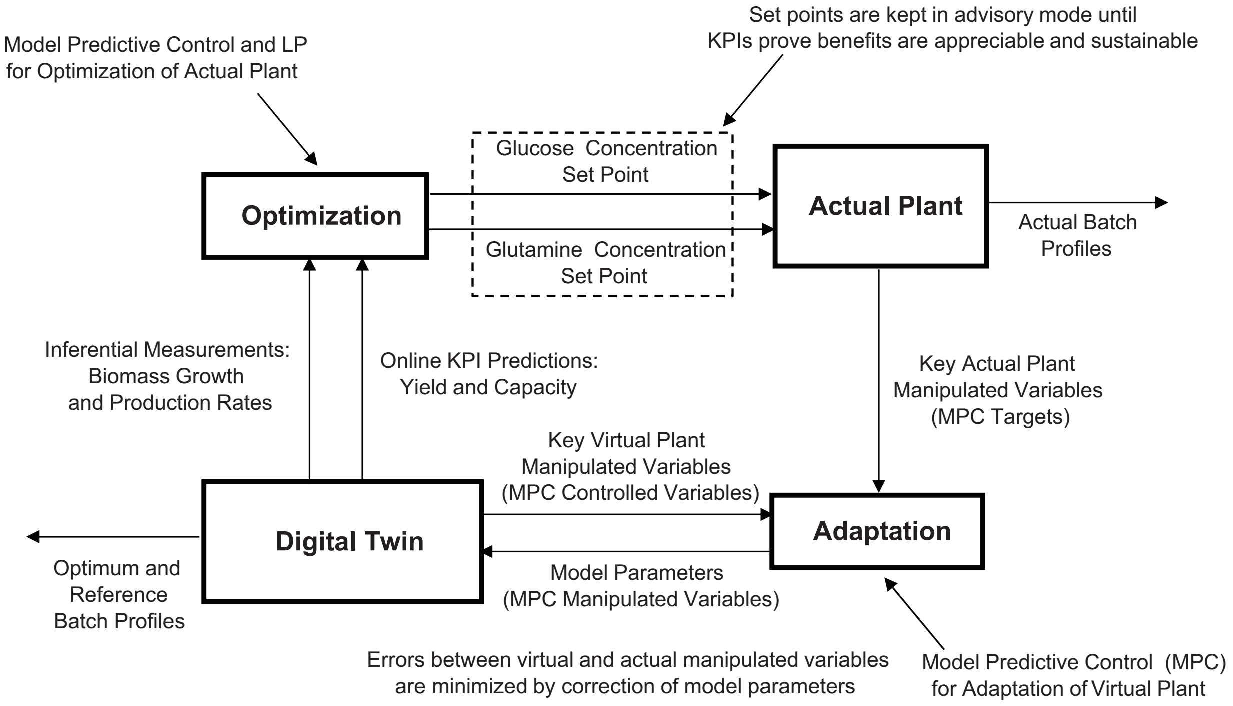

Model Predictive Control and LP for Optimization of Actual Plant
Set points are kept in advisory mode until KPIs prove benefits are appreciable and sustainable
Optimization
Glucose Concentration Set Point
Glutamine Concentration Set Point
Actual Plant
Actual Batch Profiles
Inferential Measurements: Biomass Growth and Production Rates
Online KPI Predictions: Yield and Capacity
Key Actual Plant Manipulated Variables (MPC Targets)
Key Virtual Plant Manipulated Variables (MPC Controlled Variables)
Digital Twin
Adaptation
Optimum and Reference Batch Profiles
Model Parameters (MPC Manipulated Variables)
Errors between virtual and actual manipulated variables are minimized by correction of model parameters
Model Predictive Control (MPC) for Adaptation of Virtual Plant

**Figure 3. Nonintrusive automated adaptation of model parameters to match manipulated variables with potential future optimization based on improvement in KPIs.**

within the actual plant as detailed in "New Directions in Bioprocess Modeling and Control," second edition, ISA, 2020.

In addition, a dynamic model can be nonintrusively adapted to improve virtual plant fidelity by matching the virtual and actual plant manipulated flows. This can be done by an MPC developed offline whose controlled variables are the virtual plant's manipulated flows, targets are the actual plant's manipulated flows, and manipulated variables are the corresponding virtual plant's model parameters.

The adaptation is done without affecting the actual plant because the plant's manipulated variables are being read by, but not changed by, the digital twin. It is critical that the digital twin has the same setpoints and tuning settings as the actual plant and that the digital twin is started with controller outputs initialized to match the actual plant.

Figure 3 shows a bioreactor model adaptation and consequential optimization by an MPC using inferential measurements and KPIs. The optimized setpoints from MPC with inferential measurements of growth and production rate are done in an advisory mode that does not affect the actual plant. Not shown in Figure 3 is that an MPC is run in automatic mode in another digital twin that is a duplicate of the adapted digital twin to generate and study the optimized setpoints. The setpoints are only eventually used to automatically optimize the plant if they prove more accurate, beneficial, and reliable per KPIs than an MPC with inferential measurements computed from online and at-line analyzers.

## Final thoughts

The digital twin and virtual plant provide a revolutionary opportunity to conduct the tests and experiments needed to develop, implement, and continuously improve plant capacity and efficiency or to prolong equipment life. Process control engineers need to learn more about setting up and running the dynamic simulations and how they can be used to develop new plants or optimize the operations of existing ones.

## Learn More about Bioprocess and pH Modeling and Control

Greg McMillan is co-author of the two ISA published books referenced in this article, "New Directions in Bioprocess Modeling and Control: Maximizing Process Analytical Technology Benefits," second edition; and "Advanced pH Measurement and Control: Digital Twin Synergy and Advances in Technology," fourth edition. Fellow authors of "New Directions in Bioprocess Modeling and Control" are Christopher Stuart, Rehman Fazeem, Zachary Sample, and Timothy Schieffer. Christopher Stuart, Dean Cook, Zachary Sample are co-authors of "Advanced pH Measurement and Control."

McMillan and his colleagues are well respected in the automation and the instrumentation and controls industries. He has more than 75 LinkedIn endorsements for instrumentation and automation. In addition to being an ISA Fellow, McMillan received the ISA Kermit Fischer Environmental Award for pH control in 1991. He is uniquely qualified to write and speak about the topics in this article.

In addition to the book's nine chapters, "New Directions in Bioprocess Modeling and Control" has 14 appendices—among them automation system performance; bioprocess biology; proportional, integral, derivative (PID); and charge balance to model pH—that cover a variety of topics including automation and control.

NEW DIRECTIONS IN BIOPROCESS MODELING AND CONTROL
Maximizing Process Analytical Technology Benefits
SECOND EDITION

**"New Directions in Bioprocess Modeling and Control: Maximizing Process Analytical Technology Benefits," second edition.**

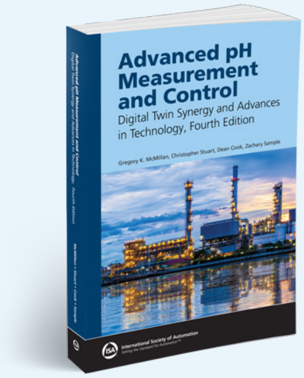
This book provides practical, comprehensive knowledge on how to use the advances in analytical measurements and advanced control to improve batch profiles and endpoint consistency. The consequential integration of measurements, models, and controls into a digital twin with recently developed blocks to provide profiles and predict endpoints enables:

- Developing dynamic models from trend charts used for experiment design, diagnosing the sources of limitations and inconsistencies, and developing and testing solutions 500 times real time without interfering with existing plant operation.
- Comprehensive views of basic process control with the possibilities of model predictive control to control and optimize batch profiles by non-intrusive development and confirmation.
- The ability to determine how to maximize the performance of bioreactors, which are often the bottleneck and the key to product quality and consistency, without tests or trials in the actual plant.

## Learn More about Bioprocess and pH Modeling and Control *(Continued)*

"Advanced pH Measurement and Control" provides knowledge of key principles and advances in electrode technology and diagnostics; a largely unrealized, simple method of computing titration curves that match laboratory curves; and the selection and implementation of the best control valves and control strategies. The results can be a significant reduction in equipment costs and a remarkable improvement in system reliability and performance.

The role of the digital twin and a first principle charge balance in design, testing, and training to provide the innovation, implementation, operability, reliability, and maintenance needed is detailed. Finally, the appendices discuss the essential fundamentals of first principles and provide guidance on using new PID features that enable greater achievements in minimizing project costs and maximizing process efficiency, capacity, and safety.



**"Advanced pH Measurement and Control: Digital Twin Synergy and Advances in Technology," fourth edition.**

Look for these titles and many others at ISA Books.

—Jack Smith, *InTech* and Automation.com

### ABOUT THE AUTHOR

**Gregory K. McMillan**, the author of more than 30 books and 400 articles, is a retired Senior Fellow from Solutia and retired principal software engineer from Emerson. He won the InTech magazine "Most Influential Innovators" award in 2003 and the International Society of Automation "Life Achievement" award in 2011.

#TeamUpToImprove

ISA GLOBAL CYBERSECURITY ALLIANCE

# Industrial Cybersecurity is a Global Imperative

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

### Get Engaged!

Johnson Controls
Honeywell
cervello
SecurityRisk ADVISORS
Cyolo

NOZOMI NETWORKS
RA Rockwell Automation
HEXAGON
ACET SOLUTIONS
SIKER

Life Is On | Schneider Electric
CLAROTY Clarity for OT Networks
FORTRESS
Chevron
FORTINET

exida
Radiflow
PURDUE UNIVERSITY Polytechnic Institute
BUREAU VERITAS 1828
NEOM
ISASecure

BR BASEROCK IT SOLUTIONS
DIGITAL IMMUNITY™ STAY PRODUCTIVE, STAY SECURE
tenable
WisePlant® Smart, Safe & Secure

LOGIIC
TiSafe
EATON Powering Business Worldwide
1898 & CO.
tdi technologies
DRAGOS

RESILTECH Technologies for Resilience
BYHON
JM Johns Manville A Berkshire Hathaway Company
asp AUTOMATION STRATEGY & PERFORMANCE
INL Idaho National Laboratory
Emerging Technology Apprenticeships

KPMG
Deloitte.
xage SECURITY
OMICRON
senhasegura by MT4

FINITE STATE
txOne networks
xylem Let's Solve Water
ENAXY
Carrier

COONTEC
RED TRIDENT INC
UL Solutions
Idaho State University
[r [redacted]

Inst MC
Peloton CYBER SECURITY
TRANE TECHNOLOGIES
PETRONAS

www.isagca.org

International Society of Automation
*Setting the Standard for Automation™*

# Utility Consumption Monitoring for Sustainability

By Cory Marcon

To optimize use of industrial electricity, water, liquid fuel and gases, operations teams need reliable measurement paired with energy management systems.

Improving operational efficiency is a long-time goal of process control and industrial applications, but today's rising utility costs and widespread eco-conscious corporate initiatives are placing a new spotlight on energy savings in production facilities across all industries. Central to both operational efficiency and energy savings are the ability to squeeze as much production or output from the smallest net input possible, while maintaining high safety, quality, reliability, and uptime.

Utilities can be broadly placed into two camps. Tier-one utilities are typically purchased directly from an external supplier, including electricity, water, liquid fuel, and various industrial gases. These are used directly to power many operational components within a facility, but additional general-purpose products are also required to run particular processes such as purging or cooling. These tier-two utilities—created from tier-one supplies—include steam, compressed air, treated water, and heat.

The use of utilities is directly correlated with profits and carbon footprint, incentivizing companies to minimize consumption, while upholding safety and quality. Utilities are a necessary expenditure, but there are almost always opportunities for savings, which can help companies reduce operational costs, increase product margins, and meet ambitious environmental stewardship targets. However, proper energy management requires accurate data capture and appropriate analysis.

None of this is possible without reliable instrumentation to monitor plant processes and utility consumption. This information empowers plant personnel to establish baselines, monitor process efficiency, identify opportunities for savings, and optimize operations.

## Reduce operational costs to become more competitive

Organizations can reduce their operating costs by saving energy wherever possible, thereby increasing competitiveness. However, many companies are still unaware of how much energy they actually consume. This and other issues can be resolved by implementing an energy management system with the right instrumentation.

There are many areas for potential savings in steam, compressed air, heating, cooling, and industrial gas usage. These are common process inputs for plant operation in many industry sectors, and vast quantities of energy are expended in the production and distribution of these utilities. This is why identifying opportunities for consumption reduction in plant processes is so critical.

**Proper energy management requires accurate data capture and appropriate analysis.**

Steam, for example, drives heat exchangers, distillation column reboilers, and similar applications because it is an efficient and controllable mechanism for delivering energy exactly where it is needed. But it is also expensive to produce and distribute, calling for careful measurement and control.

Comprehensive utility monitoring and optimization can regularly reduce energy consumption by 5 to 15 percent, but this requires establishing the right energy performance indicators (EnPIs) and making appropriate process operational tweaks or investments. All reduction opportunities depend on instrumentation that can objectively quantify energy flows, energy consumption, and process data according to ISO 50001 and ISO 50006, with related systems presenting this data in terms of EnPIs.

## Guiding standards

ISO 50001 is a universal energy management standard, specifying the establishment of EnPIs for setting up an energy management system. These indicators must be regularly reported, checked, and compared against an energy baseline (EnB) created prior to introducing measures for increased energy efficiency (Figure 1).

On the basis of this information, potential areas for savings are evaluated, and improvement measures can be initiated for single processes as well as throughout buildings, plants, or entire factory complexes.

The ISO 50006 standard provides step-by-step guidance to companies for defining robust EnPIs and an accurate EnB for later comparison. The standard also contains several real-life examples, which are helpful because it can be difficult to initially identify relevant variables in an energy system from which to determine EnPIs. Such variables include weather conditions, balance period, plant size, production variations, and energy sources, to name a few.

Common EnPI examples include:

- Total primary energy consumption (MWh/year)
- Improvement in energy intensity for the baseline year (percent)
- Adjustment for primary energy demand (MWh/year)
- Energy savings for the current year (MWh/year)
- Energy savings since the baseline year (MWh/year)
- Improvement in energy intensity for the current year (percent)

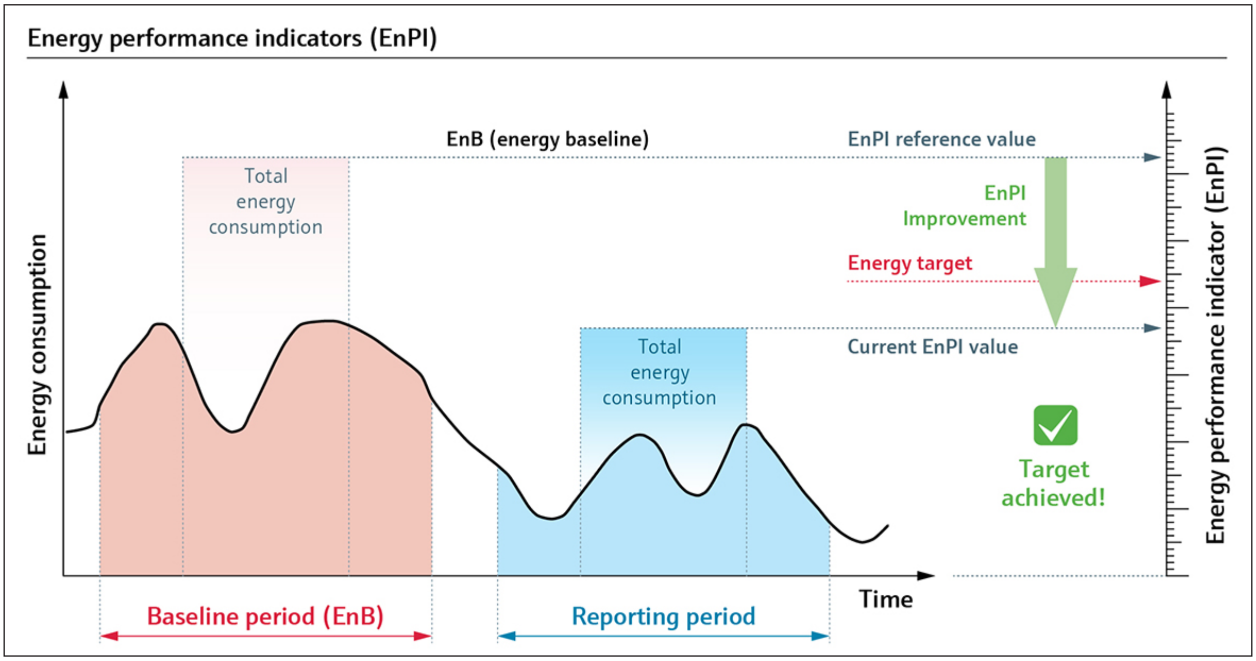


**Figure 1. Defining effective energy performance indicators and comparing results against an energy baseline enables organizations to see the results of their energy efficiency enhancements.**

- Total consumed primary energy (MJ/year)
- Electricity, water, or fuel consumption (total values, peak loads, etc.)
- Specific energy consumption, i.e., energy consumption per quantity of produced media, like compressed air (kWh/Nm$^3$), steam (MJ/t), and hot water (kW/kg)
- Efficiency of steam boilers (percent).

## Software-aided savings

Installing instrumentation across flow, temperature, pressure, and other critical measurements is key for energy management systems, but these systems are not complete without a means to visualize measured values and energy data. This element is the basis for detailed evaluation, compliant with the ISO 50006 standard.

Energy management software is used to analyze measurement data and create energy reports, and the applications on the market today typically provide access to entire plant monitoring systems via an internal intranet or the Internet. The best software packages incorporate:

- Web-based secure local or remote access
- Simple operation and easy-to-use interfaces with drop-down menus
- Automatic data import from data loggers, supervisory control and data acquisition (SCADA) systems, production systems, and building management systems
- Simple integration into existing operating data recording systems
- Modular application design for simple customization
- Simulation and calculation using multivariate mathematical functions
- Energy analysis:
  - Energy consumption monitoring
  - Efficiency assessment
  - Target/actual energy data comparison
  - Peak values identification.
- Cost analysis:
  - Create diagrams and displays.
  - Create and monitor budget plans.
  - Cost comparison.
  - Profitability calculations in terms of return on investment.
- Deviation analysis:
  - Email notifications and warnings
  - Limit value adjustment
  - Notification prioritization.
- Reporting:
  - Tailored reports via SQL Server Reporting Services
  - Cumulative curve calculation and comparative displays
  - Automatic report creation and sharing capabilities.

**These systems are not complete without a means to visualize measured values and energy data.**

## Measure to monitor

Getting started can be overwhelming, but reliable instrument installation lays the foundation for effective energy management system rollouts (Figure 2). Engaging with the right experts can ease the journey from first steps to final refinements by providing end users with high-quality instrumentation, system components, software solutions, and support.

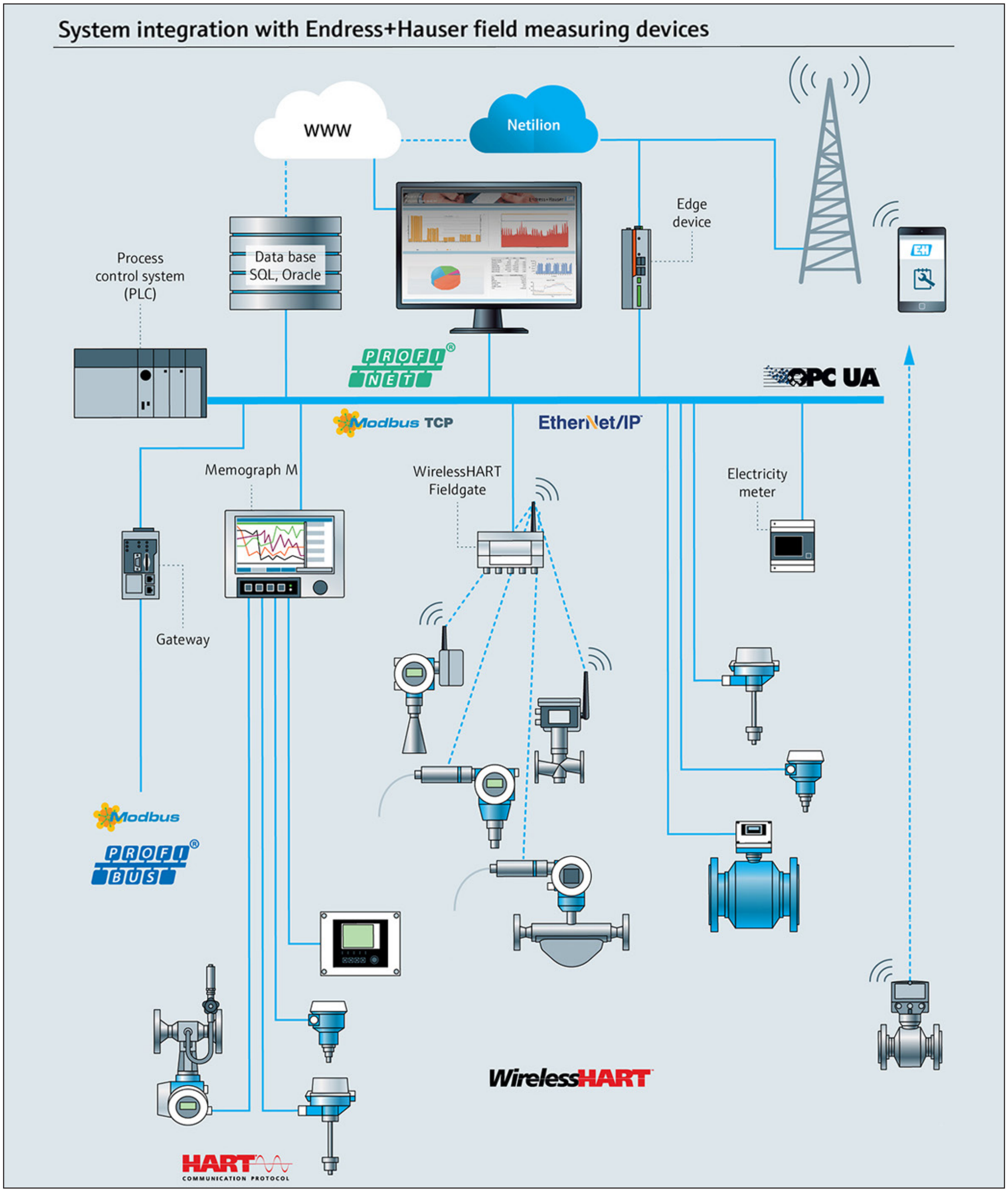


**Figure 2. An instrument portfolio like this helps companies manage their utilities reliably and save energy.**

Components and services to look for in an industry partner include:

- Robust instrumentation with high accuracy, reliability, and repeatability
- Smart devices for data logging and transfer
- EMAS- and ISO-compliant calibration services
- Professional planning, commissioning, and maintenance of energy monitoring and management systems
- Engineering and project management for single applications—e.g., boiler efficiency monitoring—and system-wide solutions
- Expert support from qualified specialists
- A wide-reaching service network.

## Looking ahead

When implementing initiatives to reduce energy consumption in industrial applications, accurate measurements are essential for making informed decisions. By generating reliable utilities data, carefully evaluating it in energy management systems, and making informed process adjustments, companies can reduce operating costs, while leading the way with energy-efficient practices for a sustainable future.

*All figures courtesy of Endress+Hauser*

### ABOUT THE AUTHOR

**Cory Marcon**, Power & Energy Industry Marketing Manager for Endress+Hauser USA, is responsible for the overall business development and growth of the company position related to traditional power generation & the energy transition. As part of his role, he serves as the US representative in the global SIG (Strategic Industry Group), helping develop education, the long-term vision, brand, and product direction within Endress+Hauser as the world actively works toward carbon neutrality. Cory is a 2012 graduate of McGill University with a decade of experience in many forms of energy, including solar, wind, and gas.

# Cybersecurity Preparedness for Oil, Gas and Petrochemical Operations

By Renee Bassett

OT cybersecurity preparedness is a journey. PETRONAS is one company using ISA/IEC 62443 Series standards to move toward maturity.

Industrial companies often pride themselves on their safety culture, but few have elevated or advanced cybersecurity activities to a similar level of visibility and prestige. Stuxnet, the first known cyberweapon, hit industrial control systems in the 2010s and, in the dozen years since, information technology (IT) professionals and industrial automation and control system (IACS) experts have worked to protect operational technology (OT) and business systems from similar threats. Unfortunately, cyber threats keep evolving, IT and OT efforts are often unaligned, and many industrial companies struggle to achieve what might be called cybersecurity maturity.

Help is available from the International Society of Automation (ISA) in multiple forms. This article highlights resources available from ISA and the ISA Global Cybersecurity Alliance (ISAGCA) including the ISA/IEC 624443 Series standards and online cybersecurity training, and reports on some research from ISA's news and publications subsidiary, Automation.com. It also reveals how Malaysia's national oil and gas company, PETRONAS, is building "institutionalized capability" in OT cybersecurity to become one of the world's most cyber mature organizations.

Increasingly frequent and often high-profile attacks like the Colonial Pipeline incident in the U.S., as well as new government regulations around the world, have spurred industrial companies to improve cybersecurity. But studies by McKinsey & Co., Gartner and others reveal that companies fall into a range of maturity levels when it comes to cybersecurity preparedness and protections.

Companies in the energy sector—including oil & gas, electric power generation, coal, renewable energy, and related systems and services—have been the most frequent target of OT cyberattacks in recent years, so it's not surprising to find a lot of cybersecurity interest and awareness in those companies. Automation.com conducted a survey in May 2023, sponsored by Fortinet, of OT professionals in oil and gas and petrochemical companies to ask their OT cybersecurity actions and perceptions.

Slightly more than half of respondents believe their companies are on par or above average compared to industry peers when it comes to securing OT systems. These companies seemed more mature in their cybersecurity posture, having completed all or most recommended tasks. The other half of respondents were notably less mature, with plans but little implemented so far.

The survey revealed that some of the concerns of process control engineers and other automation professionals were:

- The increasing risk of cyberattacks on OT systems including supervisory control and data acquisition (SCADA), industrial control, and pipeline control. Recent high-profile attacks have highlighted vulnerabilities.

**Insufficient collaboration between IT and OT teams can result in a lack of alignment between the two groups' assumptions, procedures, and motivations about cybersecurity.**

- The rapid evolution cyber threats, which require continued vigilance and adaptation from companies to detect and mitigate new attack vectors.
- Safety risks, including environmental incidents or harm to human health/safety, resulting from successful cyberattacks that disrupt industrial processes and plant operations.
- Shortage of skilled workers to properly secure systems, detect threats, and respond to incidents.

- Insufficient collaboration between IT and OT teams within organizations to ensure integrated security policies, technology, monitoring, and response.

The report suggests OT cybersecurity be made an organization-wide priority, with strong leadership, governance, training, and technological protections put in place to create robust, secure operational environments.

## ISA/IEC 62443 standards

Insufficient collaboration between IT and OT teams can result in a lack of alignment between the two groups' assumptions, procedures, and motivations about cybersecurity. The hardware and software technology used by each group can be similar, but how they are used is often very different. The convergence of IT and OT security ends up being as challenging as the integration of the systems themselves.

Seeing the need for OT-specific cybersecurity action and advocacy, ISA created the ISA Global Cybersecurity Alliance (ISAGCA) in 2020. At the time, Andre Ristaino, managing director of Global Consortia and Conformity Assessment for ISA said, "The operational technologies and control systems that automate critical infrastructure are experiencing a rapid increase in malicious cybersecurity attacks that include data breaches and ransomware. The impact is serious, affecting life, safety, environmental protection, and economic viability across sectors. ISAGCA is driving alignment and clarity across public and private sectors."

The foundation of ISAGCA's work is ISA/IEC 62443, a series of ISA-developed, consensus-based security standards for automation and control system applications. The ISA/IEC 62443 series of standards address all entities involved in the protection of operating facilities (Figure 1). Various stakeholders—including industrial product designers, system integrators, service providers, and asset owners—leverage ISA/IEC 62443 Series standards to create

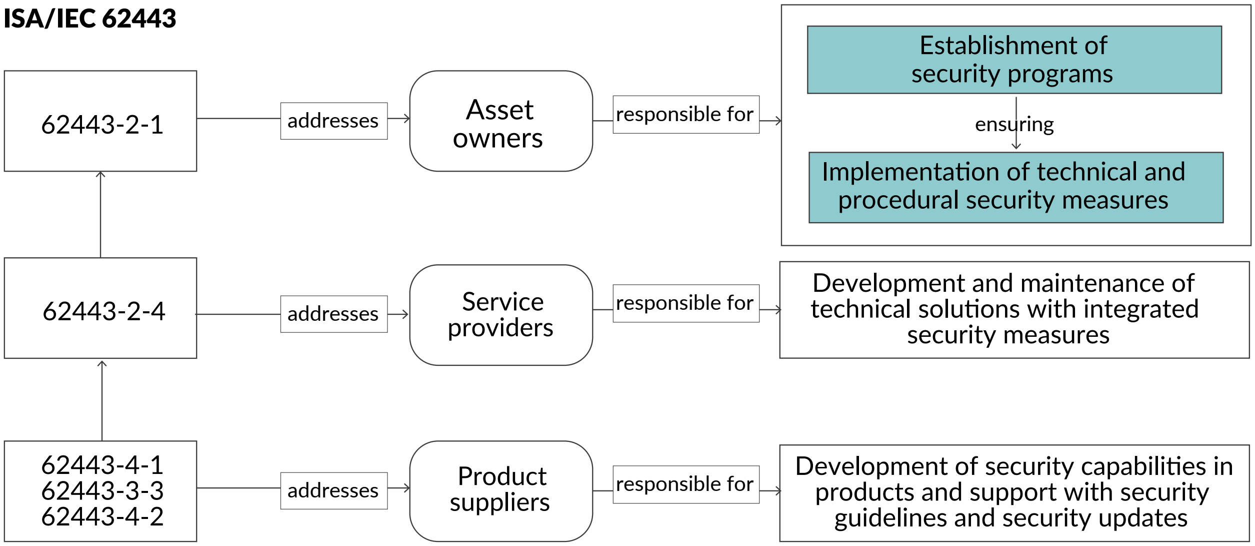

ISA/IEC 62443
62443-2-1
addresses
Asset owners
responsible for
Establishment of security programs
ensuring
Implementation of technical and procedural security measures
62443-2-4
addresses
Service providers
responsible for
Development and maintenance of technical solutions with integrated security measures
62443-4-1
62443-3-3
62443-4-2
addresses
Product suppliers
responsible for
Development of security capabilities in products and support with security guidelines and security updates

**Figure 1. The ISA/IEC 62443 series of standards addresses all entities involved in the protection of operating facilities. Visit ISA.org for the most up-to-date information.** *Source: ISA*

secure products and systems, conduct risk assessments, and much more.

"The series approaches the cybersecurity challenge in a holistic way, bridging the gap between operations and information technology, and between process safety and cybersecurity," said Ristano.

According to an ISAGCA whitepaper, "Many organizations (especially very large ones) have established policies and procedures governing the IT security in their office environment; many of these are based on ISO/IEC 27001/2 [27001] [27002]. Some have attempted to address their operational technology (OT) infrastructure under the same management system and have leveraged many IT/OT commonalities.

"Although it would be ideal to always select common controls and implementations for both IT and OT, organizations have been confronted with challenges in doing so: the locking of an OT operator screen creating unsafe conditions, antivirus products incompatible with OT equipment, patching practices disrupting production schedules, or network traffic from routine backups blocking safety control messages. The ISA/IEC 62443 Series standards explicitly address issues such as these; this helps an organization to maintain conformance with ISO/IEC 27001 through common approaches wherever feasible, while highlighting differences in IT versus OT approach where needed."

The whitepaper offers guidance for organizations familiar with ISO/IEC 27001 and interested in protecting the OT infrastructure of their operating facilities based on the ISA/IEC 62443 series. It describes the relationship between the ISA/IEC 62443 series and ISO/IEC 27001/2 and how both standards may be effectively used within one organization to protect both IT and OT.

## PETRONAS leverages ISA/IEC 62443

PETRONAS, Malaysia's national oil and gas company, is a dynamic global energy group with presence in more than 100 countries. According to Sharul A. Rashid, PETRONAS GTS head of technical excellence and group technical authority for instrumentation and control, the enterprise-wide cybersecurity program for PETRONAS started in 2018.

"A five-year roadmap toward building an institutionalized capability in OT cybersecurity was crafted and subsequently approved in 2019," said Rashid. "The institutionalized capability-building program was established mainly to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel commensurate with the risk to critical infrastructure. The organizational objectives were: responsibilities; workforce controls; knowledge, skills and abilities; and awareness."

At that time, the task force consisted of Sharul, principal instrument and control (I & C) engineers Azmi Hashim and Michael Ng Chien Han, and senior I & C engineer Ping Yang. All four men helped shape and steer the PETRONAS OT cybersecurity program.

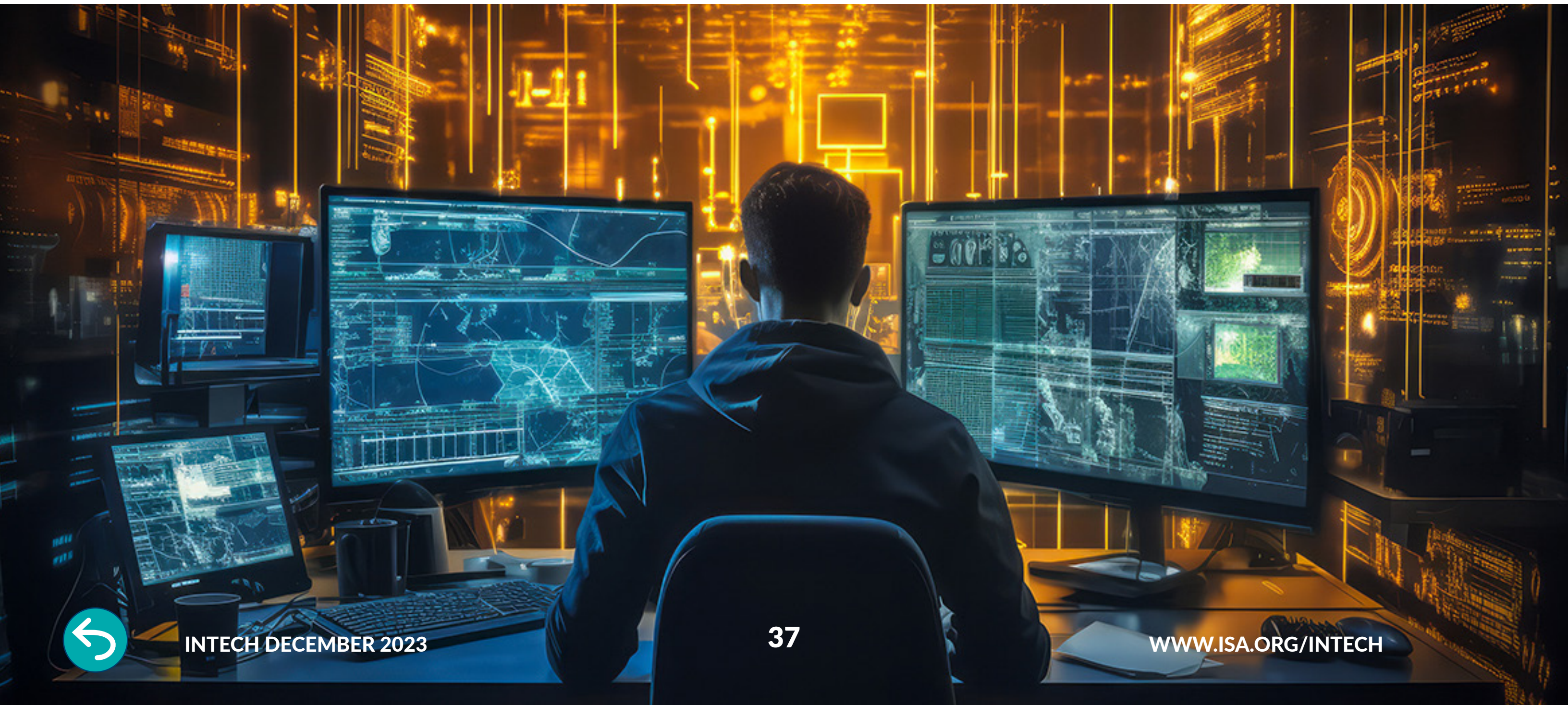
In November 2020, PETRONAS became a founding member of ISAGCA. By

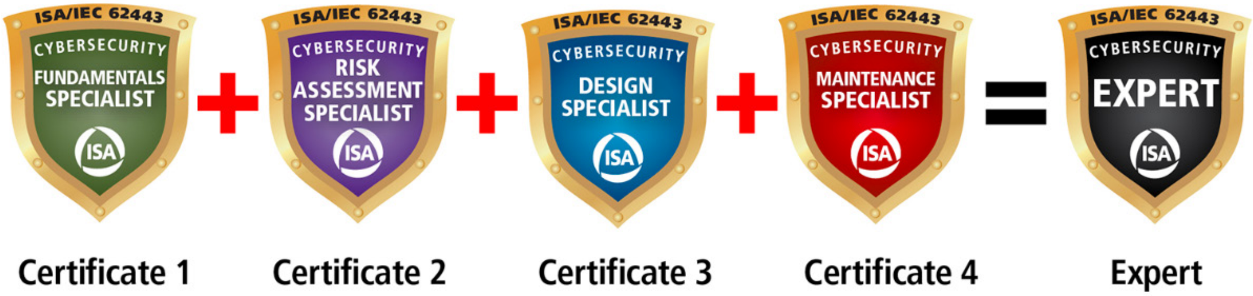
February 2021, it started attending ISAGCA Government Relations—Asia Pacific meetings. "We learned that ISAGCA aspired to designate and reference the ISA/IEC 62443 standard in a country's law and regulatory policy. So, for Malaysia, we started our efforts to support that," said Rashid.

OT Risk Management for PETRONAS is based on the ISA/IEC 624443-3-2 Standard, said Ng Chien Han.  "Cyber risk of an OT system is established by evaluating the business impact of that system, if it is compromised, and the likelihood of that compromise happening. Business impact is evaluated from the lens of how it affects people, environment and assets, as well as the company's reputation. The likelihood is established via control compliance in addressing threats from a cyber security threat register," he explained.

In September 2023, "PETRONAS reached a milestone by—for the first time—executing a cybersecurity risk assessment as part of the engineering design stage of a capital project," Rashid added. "Through the risk assessment, the Security Level Target (SL-T) of each OT system of the project was established. This exercise provided the EPCC (Engineering, Procurement, Construction, and Commissioning), OT, and OT vendors with detailed security specifications for the systems being designed. The specifications to be delivered are from the ISA/IEC 62443-3-3 system security requirements and security levels standard in addition to the PETRONAS technical standards," he explained.

PETRONAS has made good use of the wide range of cybersecurity resources that ISA offers (see sidebar). "Utilizing the ISA/IEC 62443 standards in engineering design has helped advance cybersecurity discussions with the OT vendors in delivering secured-by-design OT systems. It has also helped PETRONAS as a tool to strengthen the cybersecurity awareness and practices of its partners and collaborators," said Rashid.





**ISA offers multiple levels of OT cybersecurity training courses. Students who complete the courses and associate exams can earn certificates that demonstrate their growing cybersecurity maturity.** *Source: ISAGCA*

## Role of training and certification

Facing increasing threats of cyber-attacks, PETRONAS sought to better train its staff. "We realized that both IT and OT personnel must work together, and we applied an IT-OT convergence strategy in action," said Rashid. "We quickly built up and nurtured our best performing team in this area as a high-level, IT-OT converged cybersecurity taskforce, guided by the ISA/IEC 62443 standards' sustainable, international best practices. As part of this program, competency and capability building was one of our primary agenda points," he explained.

As part of the competency goals, PETRONAS decided that all cybersecurity task force members would be trained. The team reviewed available OT cybersecurity trainings and chose ISA online certificate courses including Cybersecurity Fundamental, Risk, Design and Maintenance courses and passed four certificate exams to earn ISA/IEC62443 Expert Certificates.

PETRONAS added other trainings, such as the PETRONAS cybersecurity project for OT, short trainings on human defense/ firewall, and more. New IT personnel "attend onboarding programs to ensure that they understand very well the criticality and priority of the OT environment. We are also extending the awareness training to the frontline, such as panel operators and boardmen who are monitoring and controlling OT assets via distributed control systems (DCS) 24/7, 365 days a year," he said.

More than 1,000 manhours were spent conducting awareness training. "Combining ISA trainings with other relevant trainings, I

**Today, an established, experienced and matured cybersecurity team is collaboratively working as a fully converged IT-OT enterprise level entity at PETRONAS.**

believe that PETRONAS is moving forward in the right direction toward our goal of enhancing our cybersecurity culture," said Rashid.

With the staff trained in ISA/IEC 62443, Rashid said PETRONAS personnel are "able to communicate our cybersecurity goals more effectively to our stakeholders and vendors. Knowledge in the standards have also helped us shape the cybersecurity governance framework of our organization."

## Addressing vulnerabilities, supporting staff

In general, OT cybersecurity incident reporting reveals more unauthorized attempts and a marked increase in malicious code attacks. Rashid believes OT systems will be subject to the same vulnerabilities as IT systems, especially as industrial control systems employ more commercial off-the-shelf (COTS) hardware and software with more embedded IT technology such as MS Windows operating system, Ethernet IP-based communication, and virtualization such as VMWare and Hypervisor.

"Common cyber incidences include blue screens, denial of service (DOS), and unauthorized remote access. Therefore, aggressive education, training, visual management, audits, and the courage to give feedback to staff on cybersecurity malpractices is surely needed," said Rashid. Rashid and Hasim published a case history article showing some of the "aggressive education," training, and visual management tools PETRONAS used to create the cybersecurity culture they wanted. See the ISAGCA blog titled, "Accelerating Cybersecurity Culture Maturity in the Workplace."

## ISASecure and Other OT Cybersecurity Work Being Done by ISA

Industrial automation and control system cybersecurity, also known as operational technology or OT cybersecurity, is one of the most critical issues facing manufacturing and industrial companies around the world today. The International Society of Automation plays a key role in helping to protect people, operating sites, products, and systems through its wide range of resources built on the ISA/IEC 62443 series of standards.

As Andre Ristaino, managing director of Global Consortia and Conformity Assessment for ISA explains, "ISA is addressing multiple dimensions of the challenge and seeking to elevate OT cybersecurity from an art to a science and ultimately to an engineering discipline."

While the ISA Education department trains and certifies personnel on the OT cybersecurity topics, for example, the ISASecure program certifies commercial off-the-shelf (COTS) devices and systems to the ISA/IEC 62443 series of standards.  This makes it easier for asset-owner companies like PETRONAS to build secure systems.

"When ISASecure becomes an integral part of an asset owner's overall security strategy and program, they can include ISA/IEC 62443 product and system conformance in their procurement specifications," said Ristaino. "That means there are fewer security mitigations needed at the operating site." The ISASecure program was founded in 2007 and has been elevating the security levels of COTS products since 2010, he added, and "some companies are now informing suppliers that they want ISASecure-compliant products."

ISASecure has developed a 3-day training class for product developers and assessors (IC47) to teach them how to develop secure products conformant to ISA/IEC 62443-4-1, 4-2, 3-3. "ISASecure is also developing a new program to certify OT systems to ISA/IEC 62443 deployed at operating sites like PETRONAS, along with a 3-day assessor training class," Ristaino said.

Other OT cybersecurity work is being done by ISA in:

**Standards development.** The ISA99 Standards committee writes and publishes the ISA/IEC 62443 standards on which all ISA OT cybersecurity activities are based. The

*Continued on next page*

"Today, an established, experienced and matured cybersecurity team is collaboratively working as a fully converged IT-OT enterprise level entity. Core to sustaining PETRONAS' cybersecurity maturity ambitions was the establishment of a cyber risk management framework. In this regard, PETRONAS has developed a standardized cybersecurity risk management program to cover both IT and OT domains," said Rashid.

"As part of an accelerated cybersecurity culture at the workplace, one must engage staff, conduct awareness training, and foster an understanding that becoming inactive and uneducated on cybersecurity risk management can lead to a major loss of business," said Rashid. "In leading the OT Cybersecurity team at PETRONAS, we engage and support staff as much as possible. We build and nurture our best performing teams with our new cybersecurity taskforce, as well as guide them using international standards and best practices on sustainable, pragmatic approaches."

*Continued from page 29*

work of this group of ISA volunteers "codifies what amounts to thousands of years of combined experience in OT cybersecurity," said Ristaino.

**Workforce development.** ISA educates more than 3,000 students per year on automation and control cybersecurity topics through its online and in-person Training courses and annual events. ISA's inaugural OT Cybersecurity Summit was held in Aberdeen, Scotland in 2023 and the 2024 summit will be held in London June 18-19.

**Credentials.** ISA's Cybersecurity Certificate programs provide credentials to OT cybersecurity professionals. "ISA offers the most comprehensive set of industrial cybersecurity certificate programming and aligned training courses in the world," said Ristaino. The programs are designed to deliver in-depth, OT-specific knowledge through a series of training courses designed to increase the cybersecurity maturity of individuals and entire organizations. It's another step in the journey toward a culture of cybersecurity.

**Advocacy.** The ISA Global Cybersecurity Alliance (ISAGCA) advocates for adoption of ISA/IEC 62443 by suppliers, asset owners, integrators, and public policy makers, and develops work products to accelerate adoption. The ISAGCA blog regularly provides information on risk assessment, compliance, education, and more.

**Incident response.** The ICS4ICS, or Incident Command System for Industrial Control Systems, is an ISAGCA effort that helps operating sites respond to and recover from attacks. It provides workforce development and credentialling for "incident commanders"—the people who must respond to industrial control system breaches and other cyberattacks. For response structure, roles, and interoperability, ISAGCA joined forces with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and cybersecurity response teams from more than 50 participating companies to adapt the Federal Emergency Management Agency (FEMA) Incident Command System. This system is used daily by first responders worldwide in emergency situations like fires, industrial accidents, extreme weather events, and other high-impact situations.

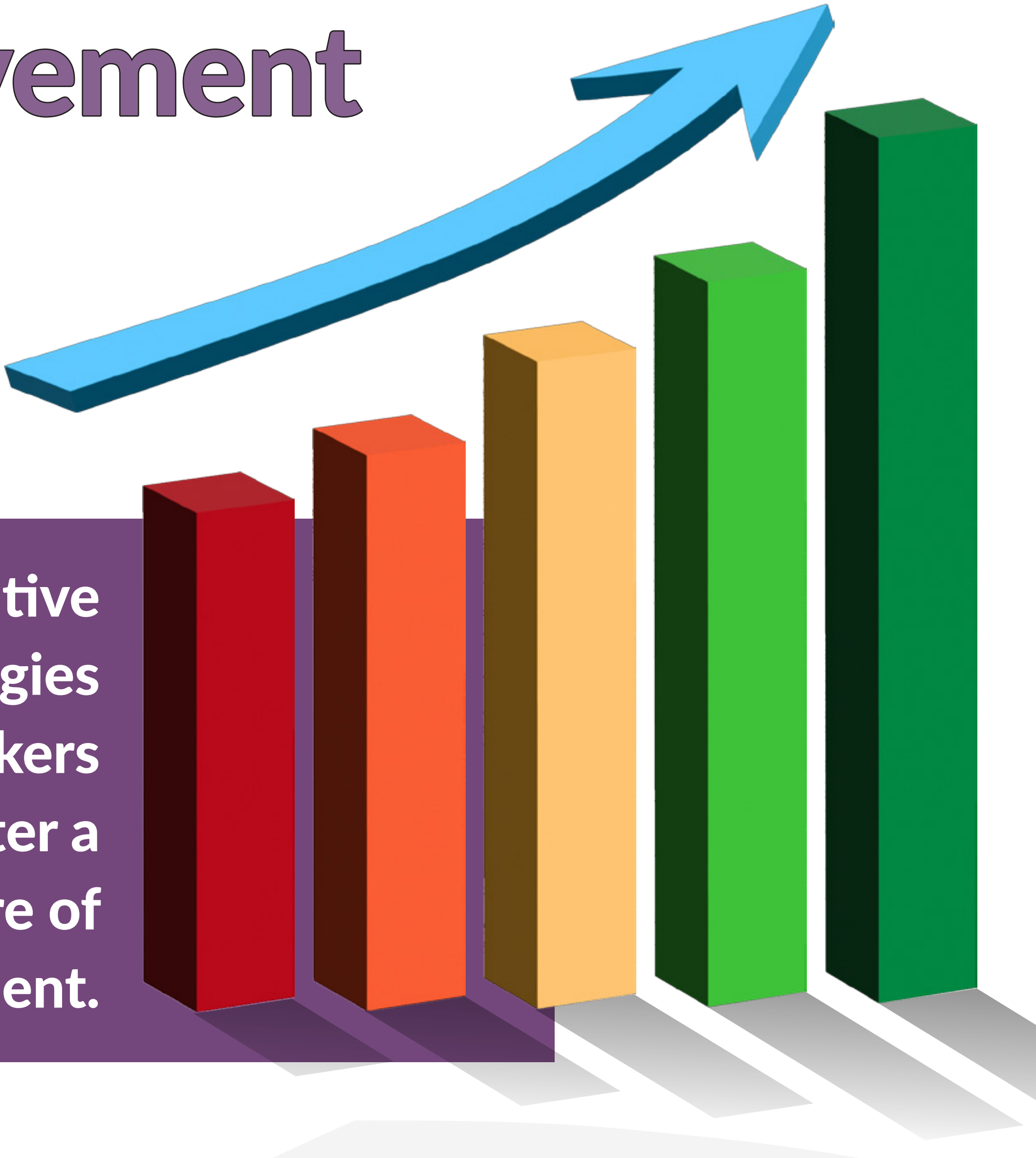
## ABOUT THE AUTHOR

Renee Bassett is Chief Editor of *InTech* and AUTOMATION 2023 digital magazines, and other publications produced by Automation.com, ISA's news and publications subsidiary. Renee is a technology journalist with more than 20 years' experience producing and managing content creation related to industrial automation, manufacturing, engineering and IT systems.

AT RESOLVED

# How Advanced Analytics Enables OEE Improvement

By Fiona Guinee



Collaborative technologies empower workers and foster a culture of improvement.

Overall equipment effectiveness (OEE) is a standardized and internationally recognized performance metric used to represent the effectiveness of a line, machine, or process. Expressed as a percentage, it quantifies the proportion of planned value-adding production time, and how much time and resources are being wasted due to unplanned availability losses, performance issues, and quality losses.

Popularized in the 1980s, OEE has evolved from a rough calculation scrawled on a shopfloor chalkboard to a critical key performance indicator (KPI), with an entire

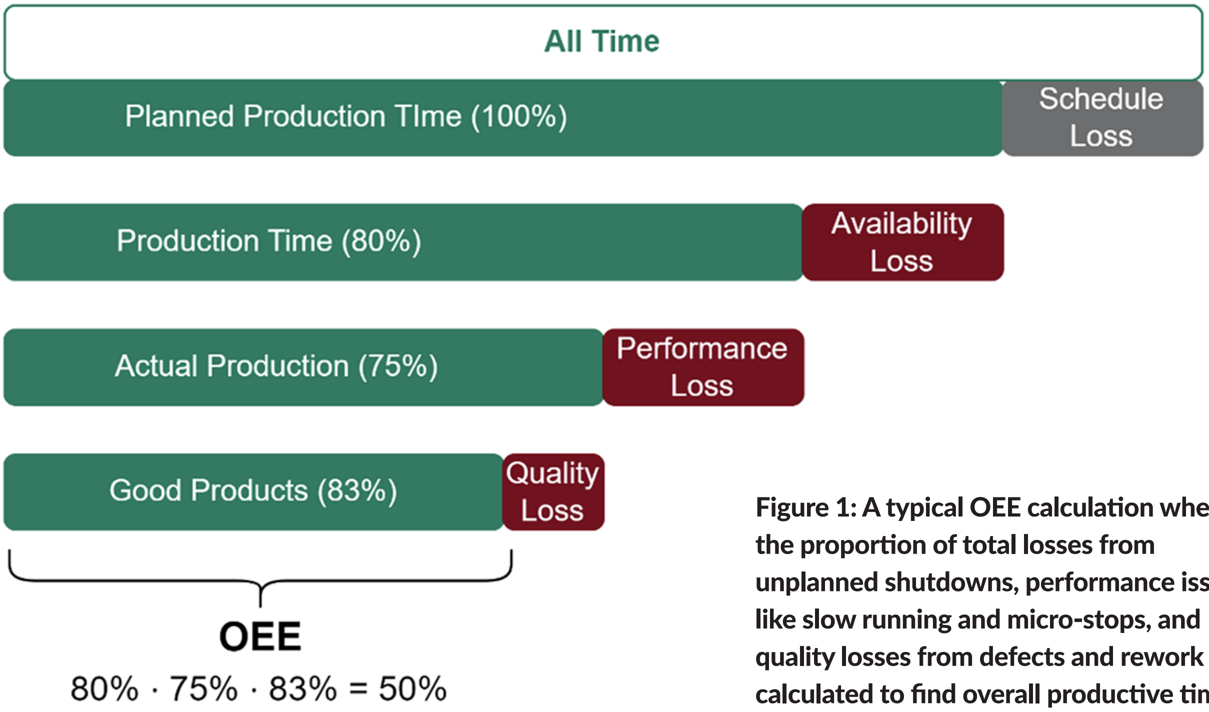


**Figure 1: A typical OEE calculation where the proportion of total losses from unplanned shutdowns, performance issues like slow running and micro-stops, and quality losses from defects and rework are calculated to find overall productive time.**

software market dedicated to digitally monitoring and enhancing its score (Figure 1).

Although the way OEE is recorded and monitored has changed, the interpretation of its results has remained the same for many companies. However, progressive companies are introducing new technologies to reframe OEE from a target for operations into a valuable source of data that can be used throughout the entire organization.

At its most fundamental level, OEE is an indication of where to invest resources. For example, if the OEE is high on a bottleneck machine and there is demand for additional products, this indicates a capacity problem, and it is a signal to invest in additional machinery. Conversely, if the OEE on the same machine is low, then this indicates an opportunity to improve the effectiveness of the machine. In this latter situation, breaking OEE into its components and categorizing the losses will highlight the most critical issues and provide a way to track the impact of continuous improvement activities.

## Limitations of OEE

With an OEE of 85 percent often touted as "world-class" or the "gold standard," this might give the misguided impression that it is the sole marker of a successful and productive operation. In reality, the situation is much more complex, and fixating on this single metric—rather than using it as a component of a broader framework—can be detrimental to a company's overall objectives and bottom line.

When OEE is treated as the singular target, there arises a potential incentive for workers to manipulate inputs to achieve their targets. For example, tweaking the ideal production rate or misclassifying production stops as planned events are two common methods for artificially inflating a machine's OEE without any meaningful increase in production or profit. This is also problematic because it decreases the quality of data collection, which ultimately causes inaccurate or misguided data-based decision-making.

OEE is focused on the local optimization of an individual unit. However, the end goal should be optimizing the entire production system. To effectively achieve this, the context of wider topics—such as market prices, energy consumption, and sustainability goals—must be considered.

Furthermore, OEE is an effective measurement for assessing the current state of operations and potential for efficiency gains, but monitoring OEE in isolation does not produce improvements. For example, knowing a machine failed because of a certain fault, or quantifying the number of micro-stops that occurred in the past week, is of limited value without the ability to pinpoint root causes, predict future events, and take corrective measures to reduce subsequent occurrences.

According to IDC Insight's 2022 Worldwide IT/OT Convergence Survey, the average cost of downtime across industries is $200 k/hr, so the benefits of even small incremental improvements are significant. When continuous improvement efforts can be accelerated or enhanced with digital solutions, like advanced analytics software, realizing return on investment occurs quickly.

## Breaking down data silos with advanced analytics

As with any data-driven decision-making, the value of the outcome largely depends on data availability, accessibility, and quality. Calculating OEE metrics tends to require very limited data, but fully addressing the underlying issues often necessitates more elaborate datasets.

When digitally mature companies implement OEE improvement strategies, data availability is rarely the limiting factor. Instead, the primary barrier is typically data accessibility, with relevant information spread throughout many different data sources such as a process historian, manufacturing execution system (MES), laboratory information management system (LIMS), or other similar systems. It is also usually in a raw format that requires significant data cleansing and contextualization to provide meaning.

This was the finding of one multinational consumer goods company looking to address the issue of frequent micro-stops in its process. Information about micro-stop events was contained within the manufacturer's MES, and configuration settings were stored in the process historian. With this data siloed in different sources, it was previously impossible to find correlations between settings and the frequency of micro-stops without complex and time-consuming data wrangling.

However, by deploying an advanced analytics solution, the company was able to access multiple data sources from one central location, empowering users to seamlessly combine and interrogate data regardless of source. This enabled a simple correlation analysis that provided users with rapid diagnostics to identify optimal configuration settings, resulting in significant performance improvements.

The other principle of data accessibility is providing all users with access to the information they need when they need it. In the past, the manual collection of data meant OEE could only be reported on days or weeks after the fact. This activity generated some interesting insights for management, but operations staff often lacked the ability to make proactive improvements. Even now, with the majority of OEE monitoring systems collecting and calculating metrics automatically, the results are often presented in a way that is more aligned with the long-term reporting method of the past, instead of near-real-time monitoring.

It is important to carefully consider the information an operations team and supporting functions need, and to provide them with relevant, real-time, and auto-updating dashboards that reflect this. For example, a world-renowned pharmaceutical company developed multiple dashboards that were designed with its operations staff in mind. One of the most impactful dashboards provided visualizations of the current duration of multi-step changeovers.

Because changeovers are a mandatory process step, they are usually categorized as a planned stop reason that does not contribute toward availability loss. However, the company was experiencing a high variability in the duration of changeovers, which was limiting the amount of finished product. By leveraging an advanced analytics solution, the company was able to accurately quantify the lowest repeatable time for each stage of the changeover and use a simple formula to split the changeover into components of planned and unplanned downtime. A custom-built dashboard then highlighted all changeover durations that were excessive as events requiring investigation (Figure 2).

This additional granularity was presented directly to the operations staff in the form of

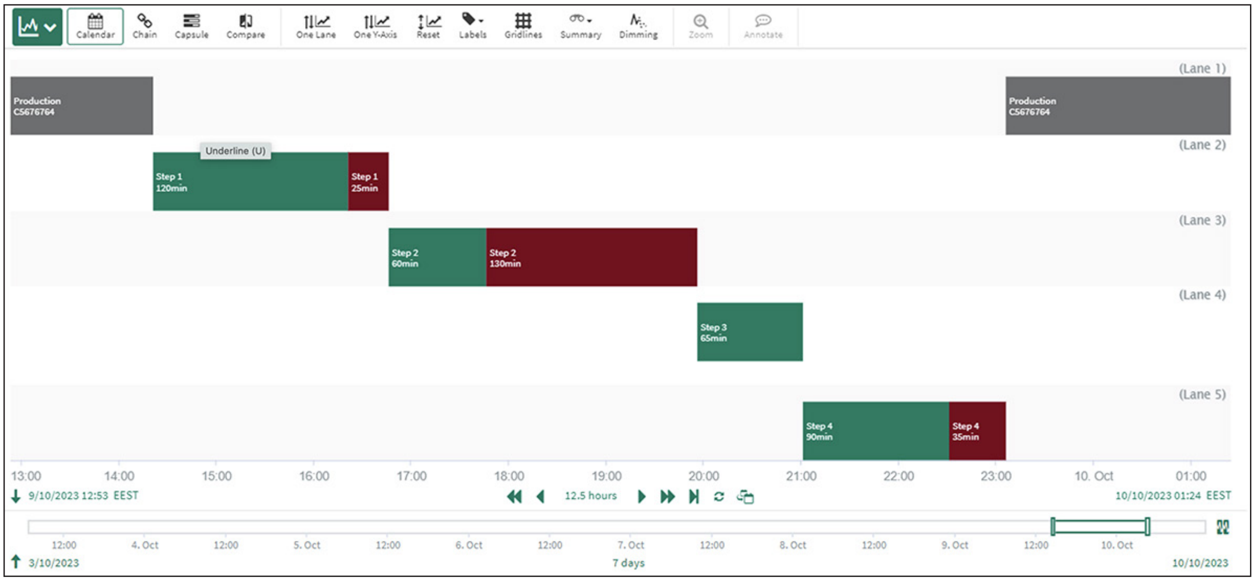


**Figure 2: OEE planned changeover monitoring.**

Some advanced analytics solutions supply access to Python and R libraries alongside their process data, providing complex algorithm generation and a new depth of operational intelligence.

a traffic-colored process flow, providing the opportunity to immediately investigate and resolve delays. These proactive investigations significantly reduced turnaround time variability, which in turn increased time spent in production.

## The power of advanced analytics

Equipped with access to live data via advanced analytics platforms, process engineers and operations personnel are no longer limited by convoluted analyses within tabular spreadsheets. These solutions are designed to work optimally with time series data, and they provide easy access to analytical tools and insightful visualizations that help solve problems quickly (Figure 3). Use cases that were previously discounted as too time-consuming suddenly become feasible, and new ideas can now be envisioned.

For example, combining event-based data about an equipment failure with related process data makes it possible to build machine performance prediction models that depict the likelihood of future failure. Engineers can train and build their own prediction models using point-and-click tools, and they can validate the prediction using built-in statistic calculations and XY plots. Reliability engineers can then better track the performance of their assets and replace time-based maintenance scheduling with optimized performance-based scheduling, providing increased equipment availability.

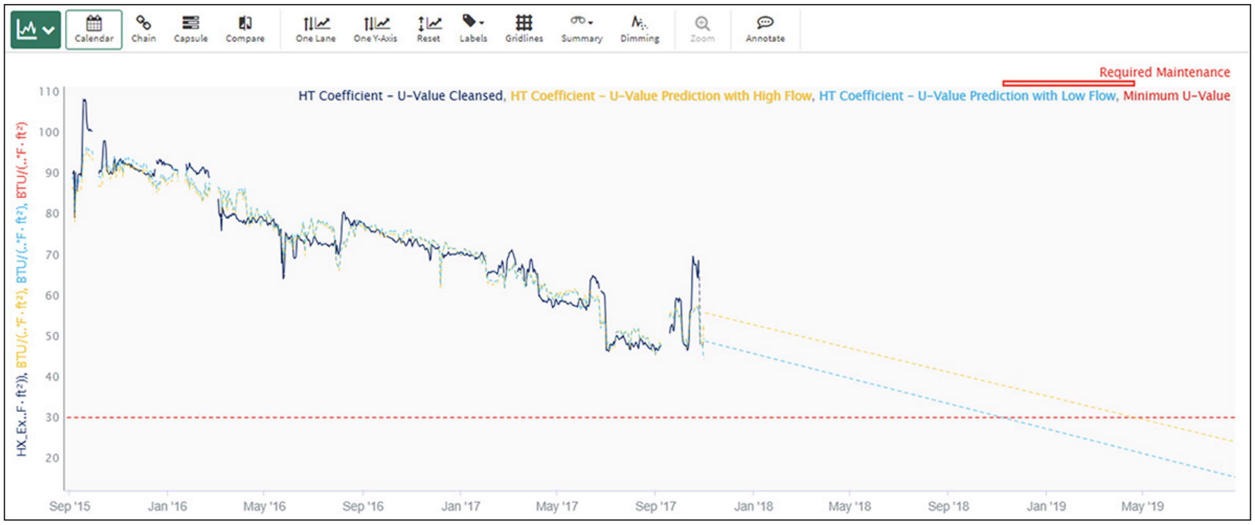
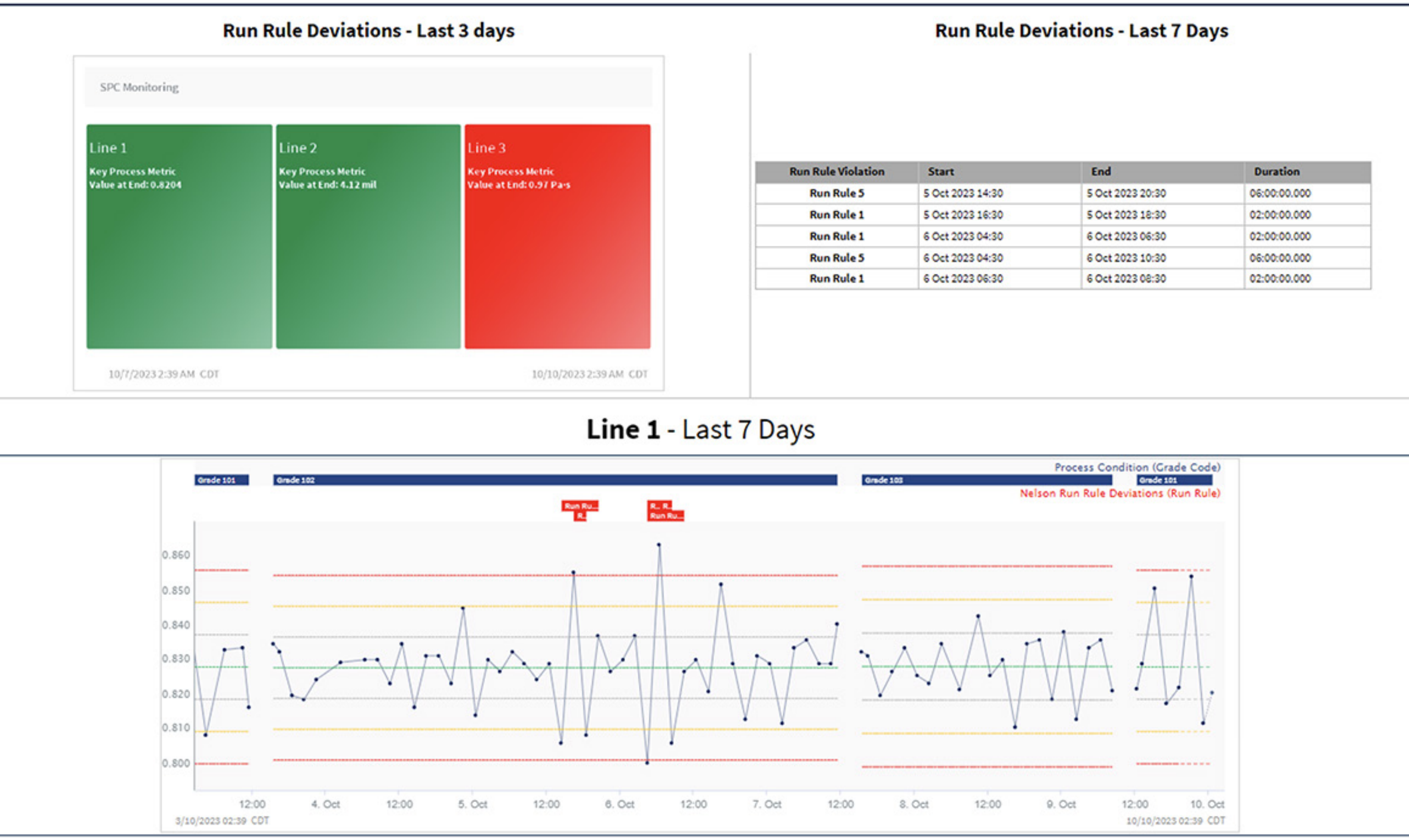


**Figure 3: A prediction model used for scheduling maintenance at optimal times**

Similarly, quality monitoring can be used to improve the control of critical parameters. For example, statistical process control (SPC) charts can be deployed with run rules to track variations in key product qualities. Based on rigorous statistical methods, the run rules accurately differentiate special cause variation—abnormal fluctuations that indicate a quality parameter is out of control—from common cause variation, which is normal fluctuation in a process. This empowers engineers to monitor and correct issues as they develop, long before defects occur (Figure 4).

Some advanced analytics solutions also supply engineers and data scientists with access to Python and R libraries alongside their process data, providing complex algorithm generation and visualization options, along with the ability to easily share insights. This provides a new depth of operational intelligence.

All these factors foster sharing best practices among various sites and business units, but to do so effectively, standardized approaches must be developed for deployment at scale. With regard to OEE, this usually means defining how it is calculated, predefining how losses should be categorized, and providing a suggested reporting template. However, as most operations are constantly



Run Rule Deviations - Last 3 days

SPC Monitoring

Line 1
Key Process Metric
Value at End: 0.8204

Line 2
Key Process Metric
Value at End: 4.12 mil

Line 3
Key Process Metric
Value at End: 0.97 Pa·s

10/7/2023 2:39 AM CDT

10/10/2023 2:39 AM CDT

Run Rule Deviations - Last 7 Days

| Run Rule Violation | Start | End | Duration |
|---|---|---|---|
| Run Rule 5 | 5 Oct 2023 14:30 | 5 Oct 2023 20:30 | 06:00:00.000 |
| Run Rule 1 | 5 Oct 2023 16:30 | 5 Oct 2023 18:30 | 02:00:00.000 |
| Run Rule 1 | 6 Oct 2023 04:30 | 6 Oct 2023 06:30 | 02:00:00.000 |
| Run Rule 5 | 6 Oct 2023 04:30 | 6 Oct 2023 10:30 | 06:00:00.000 |
| Run Rule 1 | 6 Oct 2023 06:30 | 6 Oct 2023 08:30 | 02:00:00.000 |

Line 1 - Last 7 Days

Figure 4. An SPC monitoring report identifies run-rule violations.

in flux and new constraints come and go, it is equally important for users to have the flexibility to collaborate, drill down, and perform their own ad-hoc investigations. The most successful initiatives allow for a combination of standardized template deployment at scale and custom self-service advanced analytics capabilities for individual users.

In one instance, a leading medical device company that implemented a plug-and-play OEE monitoring solution found the increased ownership and visibility resulted in significant process improvement. However, the manufacturer lacked the ability to investigate the root causes of complex issues or implement preventive measures. It was only after engineers gained access to OEE data within a self-service advanced analytics solution that the company could move from reactive monitoring to fully optimized maintenance and cleaning cycles. This yielded more production time, empowering the company to manufacture an additional 500,000 devices per year of a product they previously struggled to make enough of to meet market demand.

## Innovate to add value

Calculating and monitoring OEE remains a highly valuable metric for measuring equipment effectiveness. However, it is not sufficient to mindlessly collect and monitor the data. It must be translated and converted into meaningful, actionable information for various end users to provide business value.

By fostering improvement culture and empowering workers with collaborative advanced data analytics technologies, organizations can reach new levels of efficiency needed to remain competitive in today’s fast-paced manufacturing market.

*All figures courtesy of Seeq*

### ABOUT THE AUTHOR

**Fiona Guinee** is a senior analytics engineer at Seeq. She has an engineering background with an MEng in chemical engineering from the University of Stratchclyde. In her current role, she enjoys helping process manufacturing companies maximize value from their time series data.

# Partner with ISASecure on the New Site Assessment and Certification

The new ISASecure Site Assessment assures owner/ operators that ISA/IEC 62443 target cybersecurity levels for automation have been achieved.

Your Benefits:

- Reduce the risk of disruptions and economic loss
- Protect the health, safety, and environment of your stakeholders, including investors, employees, community, etc.
- Meet regulatory requirements

**Join forces with a growing consortium of over 40 companies to collaborate on this important industry initiative.**

ISASecure®

## Supporting Companies

Carrier

Chevron

ExxonMobil

GSK

Honeywell

Johnson Controls

Saudi Aramco

Schneider Electric

Trane

Yokogawa

Bureau Veritas

CSSC

DNV-GL

Exida

FM Approvals

UL Solutions

Ikerlan

TrustCB

TUV Rheinland

TUV SUD

BYHON

Kaizen Cyberlab

YPF

IriusRisk

Synopsys

SecurityGate

Secudea

Peloton Cyber Security

Arcadis

Amazon Web Services

WisePlant

InterStates

IACS Consulting

Armexa

Cyberprism.net

Securing Things

ZuoNet

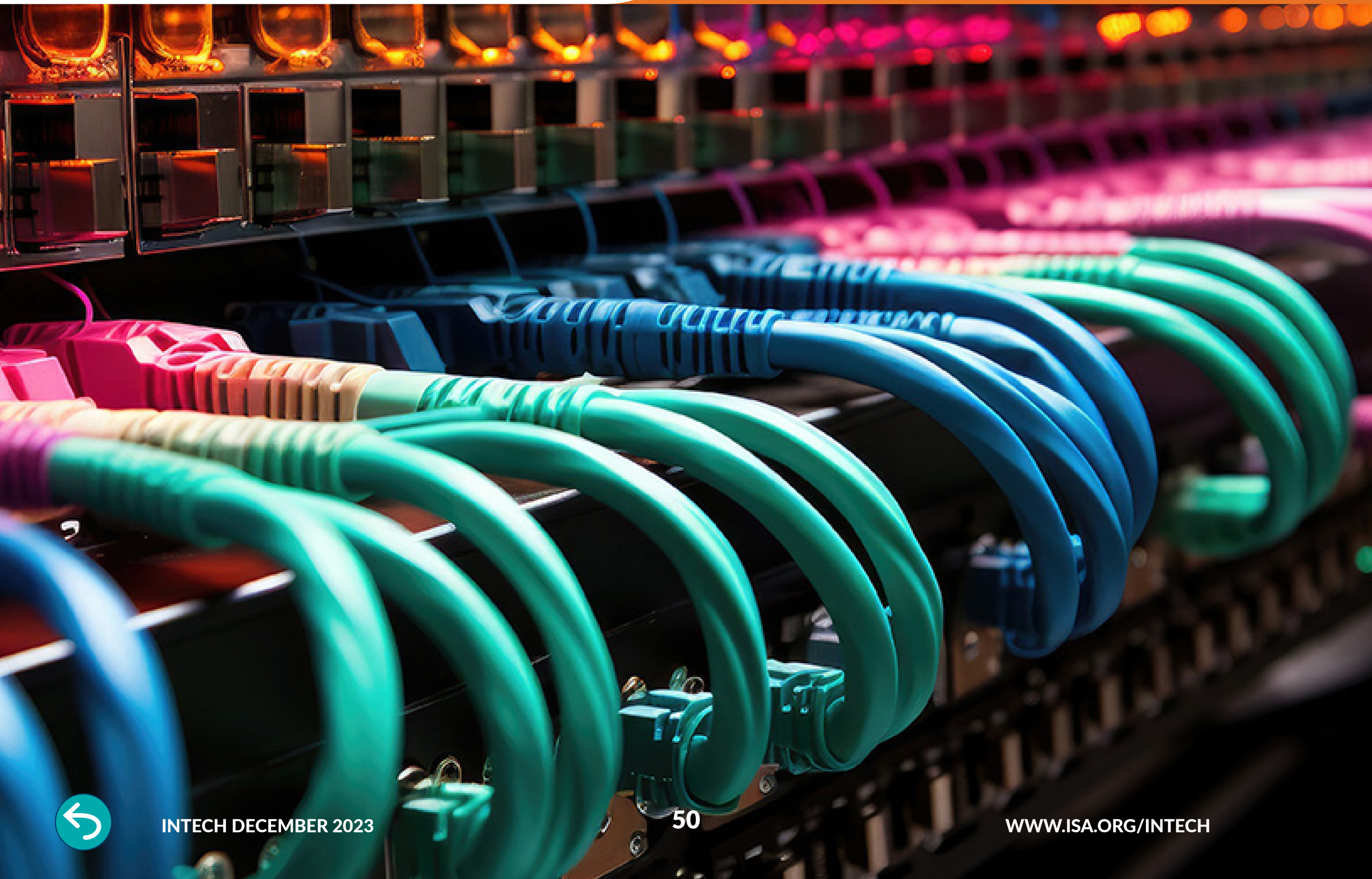
# How Industrial Ethernet Is Reshaping Industries

By Vivek Bhargava

In the era of Industry 4.0, where machines communicate, automate, and optimize processes, the need for robust and reliable networking solutions has never been more critical. Industrial Ethernet has emerged as the backbone of industrial connectivity, enabling seamless communications, enhancing efficiencies, and paving the way for advances in various sectors.

Legacy connectivity methods such as serial, twisted pair, coaxial, and other proprietary

> **Wired networks are "legacy" solutions that provide a solid foundation for mission-critical applications.**



protocols and methods, are now giving way to standards-based Ethernet. This transition is being driven by several key factors such as the need for interoperability across diverse industrial devices, higher bandwidth for data-intensive communications, better integration with information technology (IT)-driven enterprise systems, lower costs incurred in using standard rather than proprietary products, and more.

Today's Ethernet can do much more than provide high-speed connectivity at lower costs. This article presents five key areas where Ethernet-based industrial switches can power smart operations of the future.

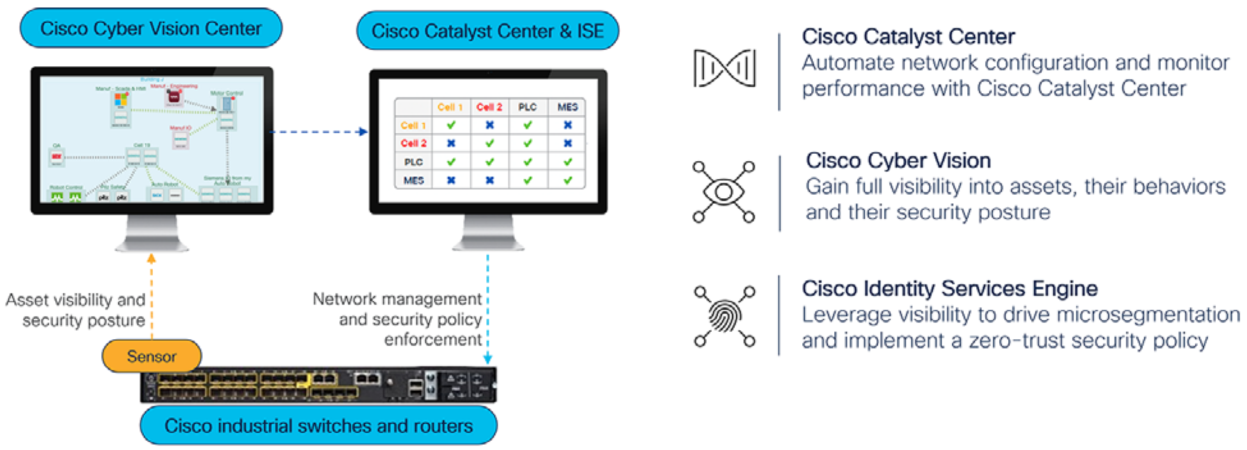
## 1. High-performance infrastructure

Industrial Ethernet helps build a highly resilient, high-performance infrastructure. More than the enterprise, industrial operations rely on continuous uninterrupted operations to meet production targets and deliver services. Network downtime or interruption can result in decreased productivity leading to significant financial losses.

Today's industrial Ethernet combines enterprise-grade performance and scalability with industrial-strength reliability and resilience. It features multi- and 10-gigabit interfaces to connect high-bandwidth devices and features high switching capacity to handle many connected devices. Industrial Ethernet also enables software-defined networking for greater flexibility, scalability, and programmability in network infrastructure.

Several Ethernet-based redundancy protocols are used in industrial networks to provide high availability and fault tolerance. These include high-availability seamless redundancy (HSR) that uses redundant paths for Ethernet frames allowing for seamless failovers in case of link or node failures.

Similarly, parallel redundancy protocol (PRP) is another standard where the transmitting mode sends duplicate frames over two independent channels and the receiving node discards any duplicates it receives, ensuring data integrity, and protecting against packet loss.


Cisco Cyber Vision Center
Cisco Catalyst Center & ISE
Asset visibility and security posture
Network management and security policy enforcement
Sensor
Cisco industrial switches and routers

| | Cell 1 | Cell 2 | PLC | MES |
|---|---|---|---|---|
| Cell 1 | ✓ | ✗ | ✓ | ✗ |
| Cell 2 | ✗ | ✓ | ✓ | ✗ |
| PLC | ✓ | ✓ | ✓ | ✓ |
| MES | ✗ | ✗ | ✓ | ✓ |

Cisco Catalyst Center
Automate network configuration and monitor performance with Cisco Catalyst Center

Cisco Cyber Vision
Gain full visibility into assets, their behaviors and their security posture

Cisco Identity Services Engine
Leverage visibility to drive microsegmentation and implement a zero-trust security policy

**Figure 1. Industrial Ethernet switches and related security tools like these enable the network to act as security sensor and enforcer.**

Technologies such as device level ring (DLR) connect devices in a ring and allow for simple and cost-effective implementation without additional switches. Resilient Ethernet protocol (REP) provides a sub-50 millisecond failover using a loop-free topology with backup paths.

## 2. Built-in cybersecurity

Cybersecurity is top-of-mind for industries. Visibility into connected devices, their interactions, and vulnerabilities is the first step in securing industrial assets. This visibility can be gained from deep packet inspection (DPI) of network traffic. Traditionally, industrial networks have duplicated traffic from their switches to feed into offboard DPI servers. However, this leads to extra cost and complexity in the network. Today's Ethernet provides a much simpler solution. Industrial switches can themselves perform DPI and obtain visibility and security insights as noted in Figure 1.

Visibility informs the second step in securing operations. Once you know the identity of assets and traffic patterns, you can define access policies that selectively allow or deny traffic between assets, control systems, and external entities. These policies segment the network and place limits around groups of assets creating zones and conduits as required by the ISA/IEC62443 security standards, restricting unimpeded flow of potential malware through the operations.

While zones and conduits can be carved through extensive placement of firewalls, it is much simpler for the industrial Ethernet switches themselves to enforce access policies, thereby avoiding the extra cost and complexity.

**Industrial organizations are starting to deploy zero trust network access (ZTNA) solutions as alternatives to always-on VPNs.**

## 3. Zero-trust network access

Industrial Ethernet can enable zero-trust network access (ZTNA). The ability to access industrial assets remotely, especially ones that may be geographically distributed, can be invaluable. Using it, operations staff, vendors,

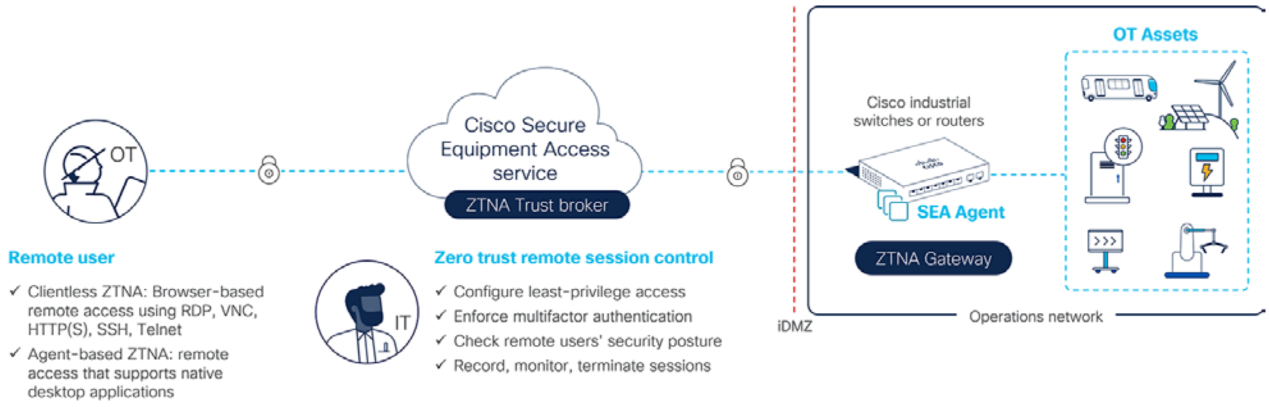

OT
Cisco Secure Equipment Access service
ZTNA Trust broker
iDMZ
Cisco industrial switches or routers
SEA Agent
ZTNA Gateway
OT Assets
Operations network
Remote user
✓ Clientless ZTNA: Browser-based remote access using RDP, VNC, HTTP(S), SSH, Telnet
✓ Agent-based ZTNA: remote access that supports native desktop applications
IT
Zero trust remote session control
✓ Configure least-privilege access
✓ Enforce multifactor authentication
✓ Check remote users' security posture
✓ Record, monitor, terminate sessions

**Figure 2. Industrial Ethernet switches like these enable Zero Trust Network Access at scale.**

or contractors can log in to those assets without costly site visits to monitor, debug, configure, or otherwise manage them.

The solution for such access has traditionally been virtual private networks (VPNs). The drawback for VPNs is that they are an always-on solution with all-or-nothing access to operational technology (OT) assets. Industrial organizations are starting to deploy zero trust network access (ZTNA) solutions as alternatives to always-on VPNs.

ZTNA is a security service that verifies users and grants access only to specific resources at specific times based on identity and context policies. ZTNA solutions consist of a trust broker, typically a cloud service, that mediates connections between remote users and OT assets by working with a ZTNA gateway onsite, responsible for creating a communication path to the assets and an outbound connection to the trust broker, as shown in Figure 2.

Existing ZTNA solutions deploy gateways in the industrial demilitarized zone (iDMZ). But in distributed field networks, there is generally no space to install dedicated gateway hardware. And in larger industrial networks, where IP addresses are often reused, many OT assets sit behind network address translation (NAT) boundaries and are not visible from the iDMZ. Industrial Ethernet switches are ideally suited to be ZTNA gateways because of their proximity to OT assets, saving the undesirable cost and burden of installing dedicated ZTNA gateway hardware in each location.

## 4. Power over Ethernet

Industrial Ethernet provides PoE and helps make operations more sustainable. Originally gaining popularity in enterprise IT settings, power over Ethernet (PoE) is becoming increasingly common in industrial settings. However, there are significant differences between the two environments.

Industrial environments can be harsh, with extreme temperatures, dust, and vibrations. Both Industrial Ethernet equipment acting as power sourcing equipment (PSE) and powered devices (PD) must be ruggedized, allow for higher power levels, adhere to stricter safety standards, and be more resistant to

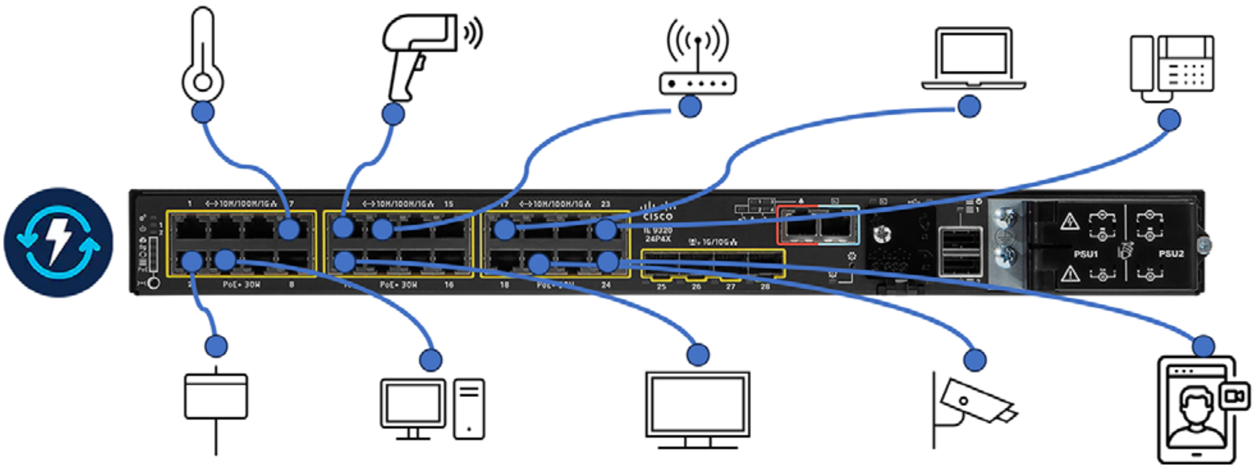


Figure 3. Industrial Ethernet switches can provide PoE up to 90 W per port and up to 720 W per switch.

electrical noise and interference from electromagnetic fields.

Finally, power to critical devices in industrial environments must be maintained to avoid downtime or safety issues, and therefore the PSE must be able to prioritize power to specified ports, maintain power through reboots, and be able to report outages or overdrawn conditions for corrective actions.

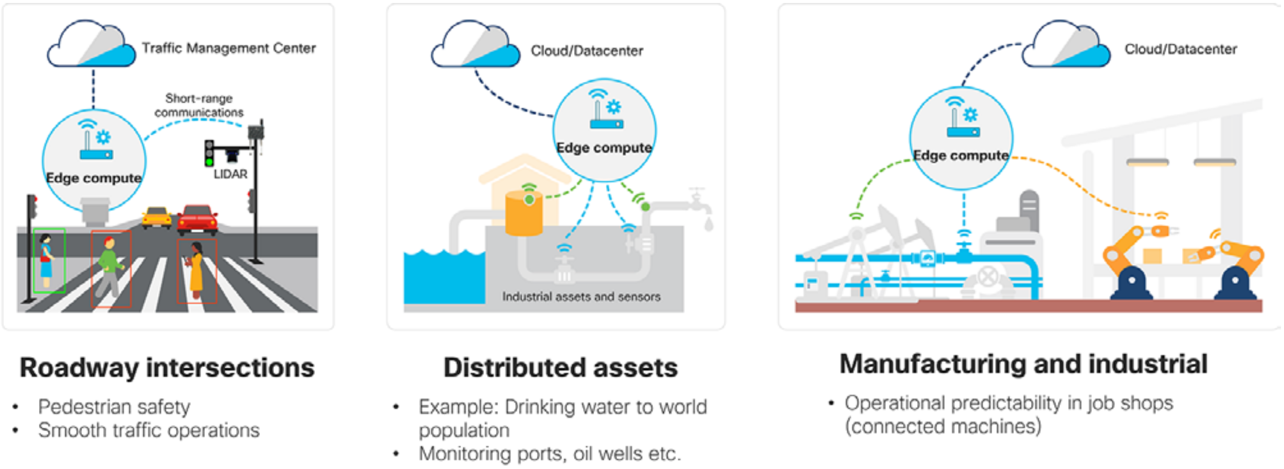
Advances in IEEE PoE standards that define power supply levels from 15.4 W to 90 W have allowed an increasing array of devices that can be powered from sensors, IP-phones, surveillance cameras, POS systems, and laptops; to high-wattage and high-bandwidth devices such as Wi-Fi 6/6E access points, digital signage, LiDAR equipment, 4KUHD PTZ cameras, and displays.

Because of its importance to operations continuity, deploying PoE in industrial environments comes with important considerations. These include provisioning power backups and redundancies, heat dissipation and cooling, power management and monitoring and more.

Industrial Ethernet switches must be able to provide relevant telemetry to a central analytics dashboard to visualize the deployment, obtain insights, and resolve potential issues before they disrupt operations.

**Industrial Ethernet, as the conduit for network traffic, can extract relevant data, transform it in the required format, and securely transfer it to these applications.**

Industrial Ethernet with PoE can also help in sustainability of operations. Not only does it eliminate the need to run extra copper cabling and steel conduits to each PD, but it also avoids ac-dc conversion at the device—which could save up to 20 percent of energy that would otherwise be lost. Power can also be more easily controlled by programmatic suspension of power to nonessential devices when not in use. Finally, ruggedized industrial Ethernet


Traffic Management Center
Short-range communications
Edge compute
LIDAR
Cloud/Datacenter
Edge compute
Industrial assets and sensors
Cloud/Datacenter
Edge compute

**Roadway intersections**

- Pedestrian safety
- Smooth traffic operations

**Distributed assets**

- Example: Drinking water to world population
- Monitoring ports, oil wells etc.

**Manufacturing and industrial**

- Operational predictability in job shops (connected machines)

**Figure 4. Industrial Ethernet helps data-driven decision making and achieving Industry 4.0 benefits.**

equipment can be placed in non-climate-controlled environments, saving cooling costs.

## 5. Enabling Industry 4.0

Industrial Ethernet enables Industry 4.0. Industry 4.0 promises to transform operations by integrating advanced technologies such as the Industrial Internet of Things (IIoT), artificial intelligence (AI), big data analytics, cloud computing, and robotics into industrial processes. It can help increase productivity and improve product quality through real-time data-driven decisions.

However, all this is possible only when accurate, timely process data is made available to the software applications in the data centers and cloud. Industrial Ethernet, as the conduit for network traffic, can extract relevant data, transform it into the required format, and securely transfer it to these applications.

Industrial Ethernet assists in faster data-driven decision-making. While applications in the data center and the cloud, fed by data from operations, can help derive insights and make operations decisions, there are time-sensitive use cases where these decisions need to be made on the spot.

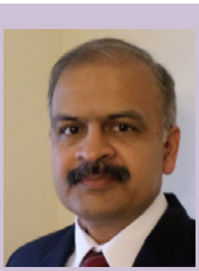
For example, in autonomous vehicles, faster capabilities can enable the real-time processing of data from sensors and cameras to make instant decisions and respond quickly to changes in environment. It can also support various smart city applications such as intelligent traffic management, public safety systems, environmental monitoring, etc.

In industrial settings, processing data locally can help monitor and control machinery and optimize processes. Traditionally, industrial PCs have been deployed to process data. However, edge-computing capabilities within Industrial Ethernet equipment can analyze data more efficiently, saving money, complexity, and delays incurred in transit to offboard applications.

## Industrial transformation

Industrial Ethernet has proven to be a critical component in driving transformation in various industries. Its ability to provide fast, reliable, and secure communication has resulted in increased productivity, improved efficiency, and enhanced decision-making processes. Industrial Ethernet has enabled the adoption of advanced technologies such as IIoT and Industry 4.0. This transformative power has led to optimized operations, reduced downtime, and ultimately, significant cost savings for businesses across the globe.

*All figures courtesy of Cisco Industrial IoT.*



### ABOUT THE AUTHOR

**Vivek Bhargava** is product marketing manager at Cisco Industrial IoT. Working in the industrial IoT marketing group, Bhargava focuses on industrial switching, industrial security, and the manufacturing sector. In this role, he works to raise awareness of how Cisco IIoT networking and security solutions form the critical backbone of the modern industrial enterprise, and why such solutions are essential for realizing the promise of Industry 4.0.

PRESENTING THE 28TH ANNUAL ARC INDUSTRY LEADERSHIP FORUM

# Accelerate Transformation in the Age of AI, Cybersecurity, and Sustainability

**FEBRUARY 4-8, 2024 • ORLANDO, FLORIDA**

For industrial sectors, it is a time of uncertainty. Market disruption abounds and change is inevitable. For companies that can make fast, effective decisions, change presents significant opportunity and not just existential risk. Industrial leaders deal with this by leveraging transformational technologies such as generative AI to evolve business models, focusing on competitive and operating excellence, anticipating changes to the workforce and work itself, establishing cyber-resilient operations, and driving energy transition and sustainability into core business strategies. Join us to discover what your peers and industry leaders are doing today and what steps they are taking to prepare for the future.

- Digital Workforce and Culture
- Cybersecurity and Safety
- Industrial AI
- Asset Performance Management
- Supply Chain Digitalization
- Energy Transition and Sustainability
- IT/OT/ET Convergence
- Automation Innovations
- Industrial IoT Platforms and Edge Devices
- Digital Twins and Connected Smart Machines

***Is your organization successfully evolving to be a digital organization?***

Go to www.arcweb.com/events/arc-industry-leadership-forum-orlando/ or call 781-471-1000

*Visit digitaltransformationcouncil.com for more on ARC's Digital Transformation Council*

ARC Advisory Group

Co-Sponsored by *Intech*

VISION, EXPERIENCE, ANSWERS FOR INDUSTRY, ENERGY, & INFRASTRUCTURE

# Managing SCADA During a Municipal Water/Wastewater Capital Project

By Graham Nasby and John Robert Davis

**Building critical infrastructure is a team effort that requires many types of skilled personnel working together.**

Automation continues to play an increasing role in providing critical infrastructure including public water and wastewater facilities. Gone are the days of operators driving from site to site to turn valves and start or stop pumps as part of normal operations. Instead, we now use sophisticated supervisory control and data acquisition (SCADA) systems to automatically control and monitor the wide range of facilities that provide the drinking water and wastewater services we all depend on.

Building this critical infrastructure involves much planning, design, and resources, not to mention many people with a wide variety of skillsets. This article provides an overview of the typical workflow involved with designing and building a municipal water/wastewater capital project, and the role that automation professionals play.

## It's a team effort

Good projects are always a team effort. No matter what methodology is used—traditional design-bid-build, design-build, design-bid-build-operate, etc.—the common element is a wide variety of individuals and skillsets that need to come together to execute a successful project. Obviously, having a common goal, ensuring all parties work together, and ensuring the plant works—as well as ensuring everyone gets paid—are all of paramount importance.

The coordination of these efforts is usually undertaken by a group of project managers: One acting for the owner, one acting for the design team, and another acting as part of the construction team. It is the project managers who oversee the overall timeline and do the important tasks of controlling the schedule, scope, cost, and quality aspects of the project. Historically, most project managers at this level come from a civil engineering/construction background. Civil engineers are generally not specialists, but typically will have a broad background that allows them to have a deep understanding of what is needed for each phase of the project and who will be needed to carry out the work. The project managers will then bring in various specialists as needed during the duration of the project. If a project involves SCADA in any way—which is pretty much a foregone conclusion these days—automation professionals will be needed throughout the project.

## Scoping the project

Most municipal water/wastewater projects start with a study to confirm the need and timing for the upgrade (or new facility). The study is typically followed by securing funding, and then the development of a charter to define the project.

**If a project involves SCADA in any way, automation professionals will be needed throughout the project.**

Once a project charter has been developed, the first task for the utility is to develop a detailed scope of what the project will include (and not include) and the intended plan for staging the work. To do this, a terms of reference (ToR) document

### Fast Facts about SCADA

- In the municipal water/wastewater sector, automation systems are referred to as SCADA systems and typically include instrumentation, signal wiring, programmable logic controllers (PLCs), motor control centers (MCCs)/motor starters, actuated valves, the control network, servers, workstations, and alarm callout systems.
- SCADA systems can be implemented in the municipal water/wastewater sector using a variety of technologies including PLCs with human-machine interface (HMI) software, distributed control systems (DCSs), Industrial Internet of Things (IIoT), and proprietary controllers.
- Once installed, SCADA equipment in the municipal water/wastewater sector is expected to have a service life of 20 to 30 years, which is considerably longer than many other industries.

is typically created for each of the major project teams. For a traditional design-bid-build project, the ToR will provide a task-based overview of what aspects the design team will be handling. The design team will, in turn, develop the builder's scope in the form of contract drawings and specifications.

From the design team's perspective, the ToR document will outline the design goals and provide a list of the deliverables and services the owner is expecting. A typical ToR includes task descriptions such as collecting background information, developing a design brief, preliminary design, various detailed design stages (e.g., 50 percent, 75 percent, 90 percent), and creating a ready-for-construction set of drawings and specifications, as well as administering the construction contract. In effect, the ToR for the design team forms the basis for many of the stages of a typical municipal infrastructure project. A summary of typical project stages is listed in Figure 1.

Once written, the ToR is typically accompanied by a copy of appropriate design standards or templates the owner wants included as part of the design. From a SCADA perspective, it is essential that the utility include SCADA design standards, such as guidelines, templates, and work examples, as part of the ToR. If the project involves upgrading, replacing, or adding onto an existing facility, it is also essential that documentation about the existing facility (usually in the form of drawings and documentation) is included as part of the

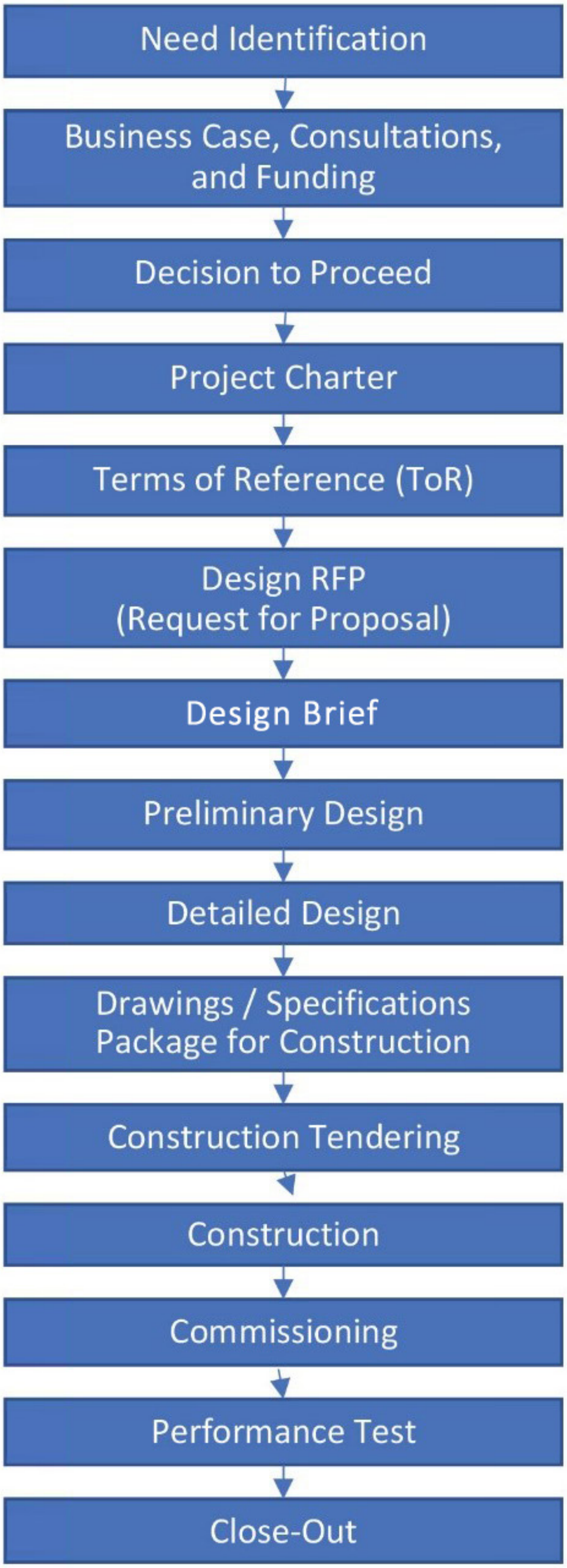


**Figure 1. Typical stages of a municipal infrastructure project.**

ToR so the design team can have a clear picture of what they will be working with.

The ISA112 series of SCADA systems standards, currently in development, will provide guidance on how these various facility-owner SCADA design guidelines, templates, and examples can be organized into a set of SCADA design standards. A committee of 300 automation professionals are working on the ISA112 standards and Part 1 is on track to be published in late 2024. A draft SCADA Systems Management Lifecycle diagram is downloadable now; excerpts are shown in Figures 2 and 3.

## Background stage

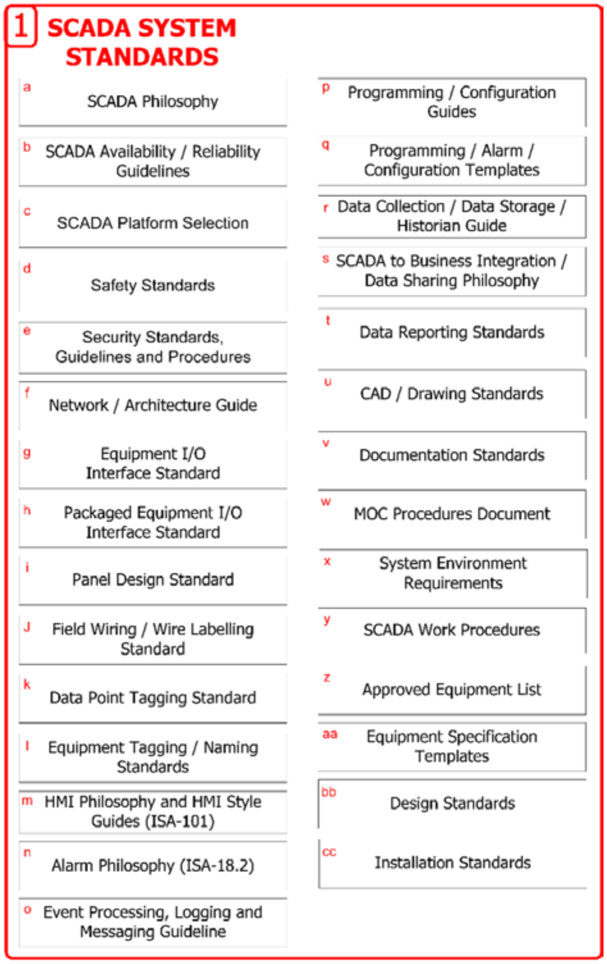
Once the design team has been selected, the next step is to conduct a detailed survey of the existing conditions and legacy systems that must be incorporated (or replaced) by the new design. If it is a legacy site, this includes gathering historical documentation about the facility. From a SCADA perspective, this should include, at a minimum, a set of up-to-date piping and instrumentation diagrams (P&IDs), site layouts, floor plans, and electrical drawings.

Ideally, electrical drawings will include not only power distribution drawings, but also drawings for programmable logic controller (PLC) panels, controller panels, motor starters, field wiring, input/output (I/O) signals, control system networks, and any other control system wiring. Some utilities will even pay a third-party engineering firm to make a set of as-found electrical drawings, P&IDs, and floor layouts, so these can be provided to the main project's design team as part of the background information.

## Design brief

Once the design team has a good understanding of the project scope and background information, they will develop a short report that outlines their proposed design solution. This is typically called the "design brief," which can range from a few pages to more than 100. The design brief usually includes conceptual drawings. Sometimes the design brief is referred to as the "conceptual design phase" or a "10 percent design."

From a SCADA perspective, the design brief must also include a short section about the proposed automation hardware and how it will work.



1 SCADA SYSTEM STANDARDS

- a SCADA Philosophy
- b SCADA Availability / Reliability Guidelines
- c SCADA Platform Selection
- d Safety Standards
- e Security Standards, Guidelines and Procedures
- f Network / Architecture Guide
- g Equipment I/O Interface Standard
- h Packaged Equipment I/O Interface Standard
- i Panel Design Standard
- J Field Wiring / Wire Labelling Standard
- k Data Point Tagging Standard
- l Equipment Tagging / Naming Standards
- m HMI Philosophy and HMI Style Guides (ISA-101)
- n Alarm Philosophy (ISA-18.2)
- o Event Processing, Logging and Messaging Guideline
- p Programming / Configuration Guides
- q Programming / Alarm / Configuration Templates
- r Data Collection / Data Storage / Historian Guide
- s SCADA to Business Integration / Data Sharing Philosophy
- t Data Reporting Standards
- u CAD / Drawing Standards
- v Documentation Standards
- w MOC Procedures Document
- x System Environment Requirements
- y SCADA Work Procedures
- z Approved Equipment List
- aa Equipment Specification Templates
- bb Design Standards
- cc Installation Standards

**Figure 2. Recommended end-user-specific SCADA standards.** *(Source: ISA112 SCADA Systems standards committee)*

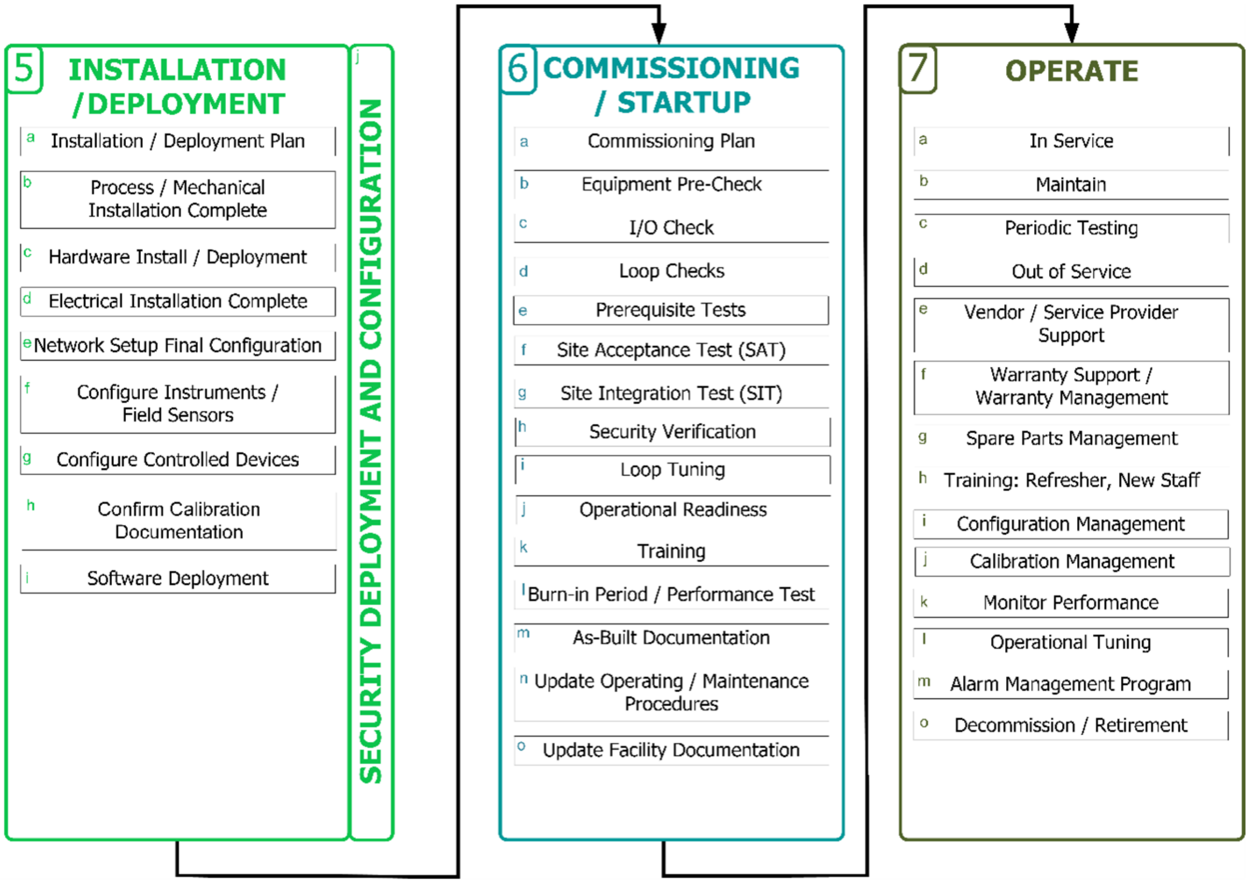

5 INSTALLATION /DEPLOYMENT
a Installation / Deployment Plan
b Process / Mechanical Installation Complete
c Hardware Install / Deployment
d Electrical Installation Complete
e Network Setup Final Configuration
f Configure Instruments / Field Sensors
g Configure Controlled Devices
h Confirm Calibration Documentation
i Software Deployment
j SECURITY DEPLOYMENT AND CONFIGURATION
6 COMMISSIONING / STARTUP
a Commissioning Plan
b Equipment Pre-Check
c I/O Check
d Loop Checks
e Prerequisite Tests
f Site Acceptance Test (SAT)
g Site Integration Test (SIT)
h Security Verification
i Loop Tuning
j Operational Readiness
k Training
l Burn-in Period / Performance Test
m As-Built Documentation
n Update Operating / Maintenance Procedures
o Update Facility Documentation
7 OPERATE
a In Service
b Maintain
c Periodic Testing
d Out of Service
e Vendor / Service Provider Support
f Warranty Support / Warranty Management
g Spare Parts Management
h Training: Refresher, New Staff
i Configuration Management
j Calibration Management
k Monitor Performance
l Operational Tuning
m Alarm Management Program
o Decommission / Retirement

**Figure 3. Recommended SCADA installation and commissioning work processes.** *(Source: ISA112 SCADA Systems standards committee)*

## Preliminary design

After the design brief has been reviewed by the utility and relevant stakeholders, the next step is to carry out the preliminary design. This stage is often called the "30 percent design." There is usually a considerable amount of design effort that must be spent at this stage, as this is when the overall project plan is fully developed and the important question of "Will it all work?" must be sorted out. The preliminary design stage should result in a preliminary design report that outlines the various features of the proposed design and the rationale behind them, and it should be accompanied by a set of preliminary drawings.

From a SCADA perspective, the preliminary design package should include a high-level diagram of the automation equipment to be used, a process flow diagram, floor plans, and a list of hazardous areas that may require equipment with special electrical ratings. Many preliminary designs also include preliminary lists of electrical loads, pumps, major valves, and instruments. Preliminary design is also when SCADA "proof-of-concept" testing should be carried out as needed on proposed automation equipment.

## Detailed design phases

Once the preliminary design has been reviewed by the utility and feedback has been gathered, the next step is to proceed to detailed design. A commonly used progression of detailed design stages is 50 percent, 70 percent, 90 percent, and construction ready. The decision of how many detailed design stages will be used and if supporting technical memos are to be developed will have been defined in the ToR at the start of the project.

At the end of each detailed design stage, an increasingly detailed package of drawings and specifications will be provided to the utility for review. At each design phase, the number of drawings and length of the specifications will increase as well. For example, at 50 percent design, the specifications section will usually only consist of a table of contents, whereas at 90 percent, it is not uncommon for a specifications section to consist of hundreds, if not thousands, of pages organized into numbered sections.

## The SCADA team's role during detailed design

From a SCADA perspective, the main goal during detailed design is to ensure that all the various aspects of the design have been properly coordinated with each other, and that the utility's SCADA design standards are being followed. The overall process systems, and the SCADA system that controls and monitors them, will only be able to function effectively if all the various aspects of the design have been well designed, coordinated, and sized properly for all operating modes.

Operating modes include startup, shutdown, online, offline, normal operation, and abnormal situations. Thus, both the utility's and the design team's SCADA staff need to be able to review all the drawings and specs together, not just the SCADA-specific sections, so they can check the overall design coordination.

## Common SCADA and process design issues

Common SCADA and process design issues that are often encountered on municipal water/wastewater infrastructure projects include:

- **Improperly sized flowmeters:** Flowmeters should be sized based on the expected flow rate, not the pipe size leading to them. If a flowmeter that's too large is installed, it can read unreliably or suffer from sludge/sediment buildup due to flow velocities being too low.
- **Poor locations for instrument taps:** Well-designed tap points for instruments are accessible and are clearly shown in the drawings. Good practices include having full port shutoff valves on each port for isolation, having spare ports, and locating tap points so they won't be prone to fouling/sediment.
- **Sample lines that are too long:** Long sample lines, or sample lines that are poorly sized, can result in long dead times for the sample to pass from the sampling point to where the analyzer will see it.
- **Chemical dosing lines that are too long:** Long chemical dosing lines create the same problem as long sample lines. Long dosing lines can make it difficult (or impossible) for chemical dosage adjustments to affect the process as desired.

- **Misplaced or missing air relief valves:** Not having enough air relief valves installed in the high points of piping systems and on pump discharges can result in problems with trapped air in pipes, vapor locking, and erratic flow behaviors.
- **Inappropriate use of valve types:** Butterfly valves should not be used as control valves, as they do not effectively control flow, and if used as control valves, they can rapidly deteriorate due to cavitation.
- **Improperly sized control valves:** Improperly sized control valves will never work properly, no matter how sophisticated the software-based control scheme is. For example, control valves should be sized based on an appropriate valve coefficient (Cv) rather than just the line size.
- **Missing pressure testing instructions in contract documents:** When no guidance is provided in the contract documents to the construction team, mistakes can easily happen. This can include rupturing instrumentation and diaphragm seals, incomplete testing, or missing test documentation.
- **Missing SCADA and/or network details:** Incomplete process control narratives, missing PLC hardware details, or no clear instrumentation and controls (I&C) wiring guidelines are a recipe for delays and extra costs during construction.

These are only a sample of the many potential design issues that can happen when the detailed design of a municipal water/wastewater facility is rushed by a design team. The important takeaway here is this: Use a team approach to ensure that enough QA/QC is done on the design package to catch potential problems at the design stage, when they are much cheaper to resolve, rather than during the construction stage. Often, when a problem is not fixed during design, it can cost 10 to 20 times more to resolve during construction.

## Construction phase

Once the construction project has been awarded, a construction kick-off meeting will be held, followed by regular construction meetings between the utility, the design team, and the construction team. The construction schedule will be reviewed and details relating to the construction will be coordinated as needed.

As part of the construction process, the contractor issues shop drawings that consist of specification sheets and other submissions for the various products the

The upcoming ISA112 series of standards will provide guidance on how various SCADA design guidelines, templates, and examples can be organized into a set of SCADA design standards.

contractor proposes to install along with information about how they propose to install them. These will be reviewed by the design team and the utility as needed prior to installation.

The shop drawings must be reviewed by the various design disciplines that are impacted by them including the utility's SCADA team. Most SCADA professionals will want to review the shop drawings for automation equipment, instrumentation, and any other equipment that "has wires" attached to it, to ensure the automation aspects of the project are properly coordinated.

## SCADA construction aspects

While the physical construction is taking place, a system integration team works on the offsite SCADA aspects of the project. This typically involves PLC panels, instrumentation, and automation programming. Depending on how the project is structured, these three aspects may be handled by one team or may be split up among several teams that coordinate with each other.

A series of factory acceptance tests (FATs) will be held for the various pieces of automation/SCADA equipment and software. These are typically reviewed by the design team and the utility's inhouse SCADA team prior to installation. Depending on the aspect, they will also be reviewed by the utility's operations and maintenance team as well. As with any fabrication/development phase, it is best to resolve problems as early as possible to avoid costly rework later.

## Commissioning

Commissioning is the step where the various pieces of installed equipment, software, and support systems onsite must work together as a system for the first time. Best practice is for a detailed plan to be developed and followed for the commissioning stage as it will involve a lot of people to start up the various pieces of equipment and support systems. Most commissioning teams maintain a commissioning logbook and ensure that all tests are documented and signed off as the plant commissioning proceeds. Commissioning can be very time consuming so it is important that is it carefully planned out and coordinated.

Commissioning usually starts by individually checking each piece of equipment before attempting to run it together. These individual checks usually start with visual inspections, configuration checks, test runs, and testing various auto-shutdown conditions. Only after individual checks are complete can the entire system be tested together.

Also, equipment, systems and subsystems should always be tested in manual mode before attempting to run them under automatic control. Commissioning can be very time consuming because all the possible operating modes, and issues must be carefully checked, and adjustments made as needed, for all aspects of the facility.

From a SCADA perspective, commissioning usually involves power-on checks, I/O wiring checks, loop checks, and informal testing, followed by formalized site acceptance tests, and site integration tests.

## Performance test

After all the commissioning tests are complete, the facility enters a performance test period in which it is expected to run with few, if any, adjustments. It is not unusual to see a seven-, 14-, or even 21-day performance test run specified in the construction contract for a municipal water/wastewater facility.

## Close-out

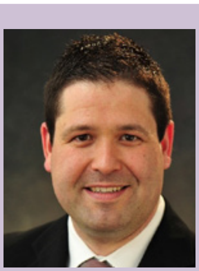
The successful completion of the performance test does not signal the end of the project. The design and construction teams must now document what has been built in a series of submittals into various project closure documents which will include operations and maintenance (O&M) manuals and as-built documentation.

A typical contractor-provided O&M manual will include the specifications and manuals for every component installed in the plant, along with copies of the associated approved shop drawings, and copies of the configuration settings and commissioning reports that were used for commissioning it.

The system integrator will provide an O&M and as-built package that consists of backups of any automation code and documentation on how the various automation systems work. Finally, as part of the ToR's scope of work, the design team will provide an O&M submission for how the plant is intended to operate from an operations point of view, plus a full set of as-built drawings to reflect how the plant was built.

## Final thoughts

Building critical infrastructure is a complex process with many moving parts. It is a team effort that requires personnel who have a wide variety of skillsets working together during all the various project phases for the result to be a successfully operating facility. Because of the prevalence of automation, automation professionals are an essential part of this team effort. By being involved at every step of the process, automation professionals continue to make the world a better place with automation when it comes to critical infrastructure.



ABOUT THE AUTHOR

Graham Nasby, P.Eng., PMP, CAP, CISSP, CISM, is a professional engineer who has more than 20 years of experience working with SCADA, operational technology (OT), and industrial automation systems. He is currently the co-chair of the ISA112 SCADA Systems Standards Committee.

**John Robert Davis** is a retired instrumentation and automation professional located in Oldsmar, Fla. After working in both the industrial and municipal water/wastewater sectors for more than 50 years, he is now writing technical articles to share his working experiences.

# HMIs Are Not iPhones: HMI Upgrade Considerations

By Greg Philbrook

HMI suppliers will offer a consolidated portfolio of popular sizes that maintain installation sizing, such as the CM5 generation of AutomationDirect C-more HMIs shown. Source: AutomationDirect

In the consumer world, each year ushers in phones, televisions, and other technologies that are progressively better, and often cheaper. At the very least, users expect a generally improving price/performance ratio. These same trends track in the industrial automation world, although usually at a slower and delayed pace. But because industrial HMIs share similarities with the smartphones and tablets used by consumers every day, and represent a main way operators interact with equipment, these devices undergo an additional degree of scrutiny by users.

Industrial automation specifiers are right to consider at what point diminishing returns indicate a product has reached peak maturity. For industrial products, new and convenient features can be interesting, but users tend to be concerned more with certain basics such as ease-of-use, cybersecurity, and a future-proof path forward.

Operators used to frequent updates to their personal consumer electronics should understand how industrial HMI upgrade strategies are different. Specifiers looking for next-generation human-machine interfaces for their machinery and manufacturing equipment will find that advances are still being made both in the foreground and behind the scenes, making industrial HMIs easier to use and better in tangible ways.

## Deciding when new is better

Typical consumer electronic hardware is progressively improved with better displays, increasingly capable processors, faster execution, and more memory. These result in more responsive operation, and the ability to run software with increased functionality. Due to constantly improving manufacturing methods, sometimes performance advantages are realized in conjunction with a price decrease. Therefore, consumers frequently upgrade their personal electronics.

While performance benefits are also an important part of the reasoning for upgrading industrial HMI solutions, there are other factors to consider, and HMI suppliers need to carefully address certain issues specific to industrial use, such as those associated with form factors and longevity.

For example, while it may be fine to change the size of a next-generation phone or TV, an HMI specifier is building equipment that lasts years or decades, so they need the physical form factor to remain consistent. HMI suppliers can support this need for standardization by ensuring the overall bolt-in form factors remain largely the same to the greatest extent possible, regardless of changing display size.

There can are challenges with this approach, such as when common displays transitioned from a 4:3 ratio to a more modern ratio like 16:9, or when users are demanding smaller and larger sizes than have been previously available. However, experienced HMI suppliers listen to their users and will offer a consolidated portfolio of the most popular sizes, while maintaining uniform installation sizing.

Other hardware upgrades are welcome additions for new designs, while not impacting older retrofits. This is especially the case when additional Ethernet and USB ports are added, providing more design options to segregate networks for security or to add external devices. Other hardware features that users have come to accept as standard must be preserved, such as NEMA 4/4X ratings, 12/24VDC power inputs, serial ports, and SD card ports.

Many other developments are vitally important, but they may not be immediately or easily recognized.

## Behind the scenes improvements

The display size, look-and-feel, and responsiveness of an HMI are immediately noticeable by users. But there are a host of crucial details which must be incorporated into software and firmware to fully modernize an HMI which are also very important. In particular, secure remote connectivity is a top feature many users now require. This can take many forms, such as an HMI that can host displays via web browser connections, a dedicated mobile device app able to connect with the HMI, FTP data transfer, and email.

**Because industrial HMIs share similarities with consumer smartphones and tablets, they get an additional degree of scrutiny from equipment operators used to new features and frequent upgrades.**

Other features of modern HMIs include:

**Compatibility.** Users require software to remain significantly compatible with older versions so they can avoid costly coding and configuration rework. This can be tricky to do well because balancing support of legacy code with the need for new functionality and forward-looking flexibility is difficult.

**Cybersecurity.** Some vendors may try to add modern cybersecurity provisions as superficial patches, but best practice is to incorporate cybersecurity at the fundamental development level, which requires deploying updated firmware and software.

**Network Time Protocol (NTP).** As HMIs are being called upon to do more, such as provide accurately timestamped alarm and event logging, NTP is necessary to provide proper synchronization among all connected devices.

**Secure communications.** Connectivity among multiple on-premises and cloud-based resources has become extremely useful for many applications. Updated platforms need to support secure versions of popular communications protocols, including SMTPS, HTTPS, and MQTTS.

**Networking.** Many HMIs include drivers to communicate with a variety of PLCs, but fewer can perform more advanced functions, such as acting as a data bridge between different PLCs, or aggregate data from multiple HMIs, instead of adding communications load to the source PLCs.

**Configuration and programming advances.** A modern integrated development environment will support user libraries, project migration, database import/export, simulation, and more to minimize designer effort.

## HMI upgrades that provide real benefits

For completely new "clean sheet" projects, most designers are free to choose the latest HMI offerings. But for anyone performing a retrofit or an automation upgrade, or supporting a legacy installation, the choice of how and when to upgrade an HMI becomes more relevant.

Designers will be considering the following attributes, in a priority order suitable for their application:

- Selection: A concise yet comprehensive range of sizes covering small to large, with the ability to retrofit into existing cutouts where possible.
- Capability: Improved processing speed, more memory, upgraded visualization, and added performance characteristics.
- Easy-of-use: Free software, with numerous tools and drag-and-drop options, to simplify the development, migration, simulation and deployment of applications.
- Industrial internet of things (IIoT): Modern HMIs with built-in cybersecurity provisions are the right answer to take advantage of the latest communication protocols and methods in a secure fashion.
- Value: While the preceding technical points are of great importance, part of any HMI decision will always rely on a favorable price/performance ratio.

Industrial HMIs are a relatively mature part of the manufacturing and process automation landscape. However, experienced suppliers are working to make the upgrade path straightforward and secure to deliver maximum value and performance.

*All figures courtesy of AutomationDirect*

**ABOUT THE AUTHOR**

**Greg Philbrook** is a product manager at AutomationDirect. He is responsible for product strategy, specifications, and development for HMI and communications products. In Philbrook's 25+ years with the company he has worked in several roles including technical sales, support, engineering, and development.

International Society of Automation
*Setting the Standard for Automation™*

# 2024 Executive Board

The International Society of Automation is pleased to introduce the 2024 Executive Board.

President
**Prabhu Soundarrajan**
Service by Medallion Inc.

President-elect Secretary
**Scott Reynolds**
Johns Manville

Past President
**Marty Bince**
EECOL Electric

Treasurer
**Ardis Bartle**
Apex Measurement and Controls LLC

Executive Director
**Claire Fallon**
International Society of Automation

**Soliman Almadi**
Saudi Aramco

**Colleen Goldsborough**
United Electric Supply

**Maxym Lachance**
BBA

**Jagdish Shukla**
Servilink Systems Ltd.

**Dean Bickerton**
The Reynolds Company

**Vivek Gupta**
DCM Shriram Ltd

**Edward Naranjo**
Honeywell International

**Sujata Tilak**
Ascent Intellimation

**Francisco Diaz-Andreu**
Repsol-ISA

**Eddie Habibi**
Zenzero Investments

**Megan Samford**
Schneider Electric

**Jeff Winter**
Hitachi Solutions

**Nick Erickson**
AWC, Inc.

**Shank Iyer**
Amazon Web Services

# Enabling Kubernetes at the Edge

By Jack Smith

Kubernetes is an open-source container orchestration system for automating software deployment, scaling, and management. Originally designed by Google, the technology is now maintained by the Cloud Native Computing Foundation (CNCF). Many who are building cloud-native software are using Kubernetes to deploy these apps in the cloud or data center.

Given its suitability for running and managing large cloud-native workloads, Kubernetes is being widely adopted in data centers and multiple distributions of this platform—from independent software vendors (ISVs) and major public cloud vendors—are available. With so many industrial automation and control systems moving to the cloud, operational technology (OT) practitioners need to understand it.

Kubernetes was a big topic at the recent Ignition Community Conference (ICC) 2023 put on by Inductive Automation in September. Lead software engineer Kevin Collins explained that Kubernetes involves multiple computers to form a cluster. It is organized into a control plane for managing everything and a data plane for running workloads. It handles deployment, scaling, and management of containerized applications, which is its intended purpose.

"It gives us a standardized set of resources, a common application programming interface (API) for most of the typical things we do in application development," Collins said.

Although Collins' presentation focused primarily on how to deploy Ignition on Kubernetes, it also provided insight into the inner workings of the technology and how it behaves both on-premise and in cloud deployments. He said Kubernetes is very modular, much like Linux. Its modular construction facilitates everything from how containers execute to how the networking is configured. Users have a wide variety of potential places to use Kubernetes, everywhere from the edge all the way up into massive cloud cluster deployments.

**Regardless of the edge deployment objective, first address the inherent challenges of edge computing before devising a plan to implement Kubernetes.**

The technology is not limited to Inductive Automation's Ignition platform, however. For example, ZEDEDA recently announced its ZEDEDA Edge Kubernetes Service, a fully managed Kubernetes service for the distributed edge. According to ZEDEDA, in a little longer than a decade, with the continually evolving edge as a backdrop, organizations have gone from using a virtual machine as their application form factor to containerizing just about everything.

## Containerization advantages

Containerization offers several advantages, not the least of which are ease of development and ease of deployment, according to ZEDEDA. As the frontrunner of containerization technology, Kubernetes has already helped countless organizations successfully run and manage the full lifecycle of their containers in a variety of environments. The CNCF estimates that more than 5.6 million developers are using Kubernetes today;  its recent survey revealed that 96 percent of organizations are either using or evaluating Kubernetes—a substantial increase from 83 percent in 2020 and 78 percent in 2019.

ZEDEDA contends that organizations are likely to be evaluating Kubernetes through one of two lenses:

1. Users who may have recently invested a lot of resources and capital into developing Kubernetes in cloud or data center environments. They are now looking to capitalize on those investments by applying them to the edge.
2. Users who have already deployed Kubernetes in the cloud or a data center, but they are just starting deployment at the edge. They realize they need to safeguard legacy workloads and modernize their assets, hardware, and applications, while closely investigating the potential for any risks at the edge.

Regardless of the edge deployment objective, users should first address the inherent challenges of edge computing before devising a plan to implement Kubernetes. These challenges include everything from hardware and operating system diversity, network connectivity, and safety and security to diverse and remote environments and a lack of skilled resources in the field. Once these challenges are adequately resolved, users can plan for the deployment of a long-term Kubernetes edge solution.

## Final thoughts

Running Kubernetes at the edge has very little to do with Kubernetes itself, and everything to do with how to enable Kubernetes at the edge. The biggest challenge is how to orchestrate Kubernetes environments at the edge, how to secure them, how to manage them, and how to monitor them at scale.

### ABOUT THE AUTHOR

**Jack Smith** is senior contributing editor for Automation.com and *InTech* digital magazine, publications of ISA, the International Society of Automation. Jack is a senior member of ISA, as well as a member of IEEE. He has an AAS in Electrical/Electronic Engineering and experience in instrumentation, closed loop control, PLCs, complex automated test systems, and test system design. Jack also has more than 20 years of experience as a journalist covering process, discrete, and hybrid technologies.