

June 2021

InTech[®]



OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

OPC FLC reaches milestone

Tech-driven asset management

Cybersecurity: from standards to practices

Batch processing digitalization

Controller Redundancy Under the Hood

www.isa.org/intech

CLICK PLUS

Simple PLC control ...on STEROIDS!

NEW!

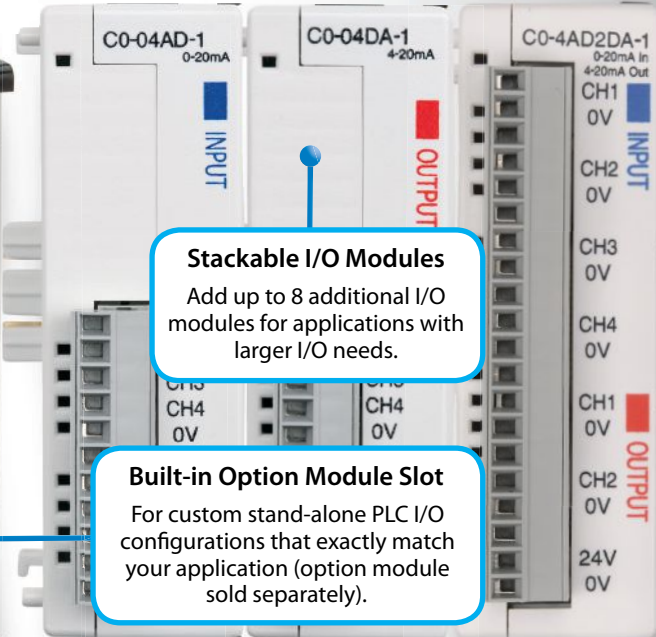
-  Wi-Fi
-  Bluetooth (provisioning only)
-  microSD
-  USB
-  Ethernet
-  Serial (RS-232 & RS-485)

(antenna sold separately)



Stackable I/O Modules
Add up to 8 additional I/O modules for applications with larger I/O needs.

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



CPU unit starting at only **\$89**

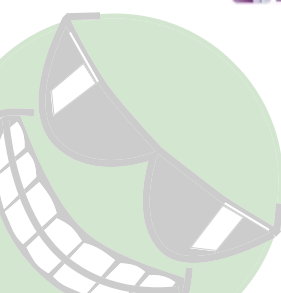
We've taken our most practical, most popular PLC family and supercharged it with features you wouldn't expect from a simple low-cost controller. Data logging, Wi-Fi connectability, MQTT communication and increased security measures are just a few of the impressive features offered with the new CLICK PLUS PLC series. With a starting at price of only \$89.00 and free easy-peasy programming software, CLICK PLUS PLCs are a "must have" for simple, affordable control...with a kick!



Check out what puts the "PLUS" in CLICK PLUS in this quick intro video:
www.go2adc.com/CPVID

MQTT EtherNet/IP Modbus

www.CLICKPLCs.com




Order Today, Ships Fast!



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

*See our Web site for details and restrictions. © Copyright 2021 AutomationDirect, Cumming, GA USA. All rights reserved.



We understand you need insightful process information to help you run your plant efficiently.

MEASURED VALUE + ADDED VALUE

You make confident decisions backed by process data and a complete portfolio of services and solutions to support you.

100%

of **Reference Standards** traceable to Nationally Recognized Standards.

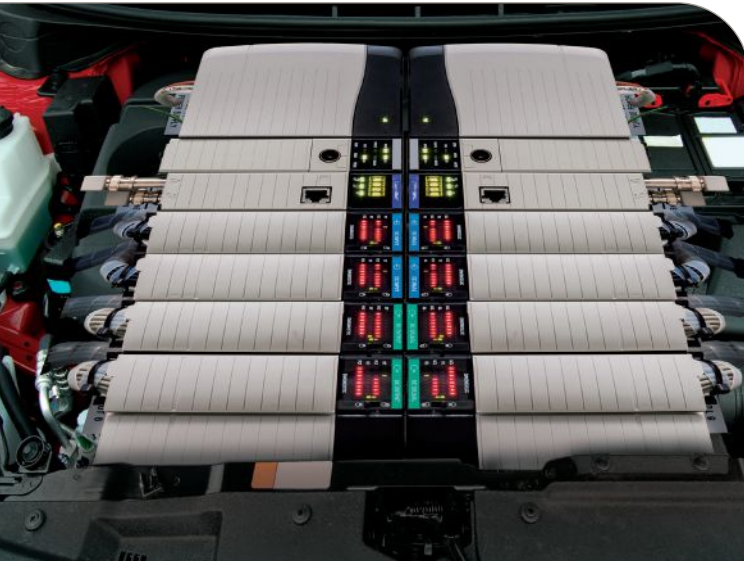
Ensure compliance and increase process uptime with optimized services

- Lab and field accredited calibrations (A2LA) and verification capabilities for flow, pressure and temperature instruments
- Patented, industry-expert methods to optimize your calibration plan
- We are a leading manufacturer of process instrumentation – uniquely qualified to verify and calibrate
- Our global, harmonized calibration standards provide consistent service quality

Do you want to learn more?
www.us.endress.com/calibration-usa

Endress+Hauser 

People for Process Automation



FACTORY AUTOMATION

16

Controller Redundancy Under the Hood

By Vibhoosh Gupta

Understanding the details behind industrial controller redundancy implementations is important. Industrial controller redundancy improves system availability, but only if it is implemented with the right capabilities. All redundant industrial controllers do not behave exactly alike, and implementation design choices can affect performance, timing, and supportability.

DIGITAL TRANSFORMATION

22 OPC UA – From Automation Pyramid to Information Network

By Peter Lutz

The OPC Foundation Field Level Communications work has made good progress, despite COVID-19 and the associated restrictions. The goal is horizontal and vertical communications throughout industrial automation and control architecture, which is essential to achieve the goals of Industry 4.0 and IT/OT convergence.

PROCESS AUTOMATION

26 Technology-driven Asset Integrity Management Perspectives

By Sugata Bandyopadhyay and Shalini Bandyopadhyay

Adopting best practices and redefining asset configuration and health are necessary to be responsive to continuously changing requirements. IIoT-enabled APM can consolidate disparate data and help build useful models to improve equipment uptime.

CYBERSECURITY AND SAFETY

30 Automation Systems Cybersecurity: From Standards to Practices

By Eric C. Cosman

Improving the state of cybersecurity in critical infrastructure should be considered an important aspect of improving system resilience. Standards, guidance, and direction are available from several sources, but surveys and anecdotal reports have shown that many still struggle with how to turn this information into effective programs.

www.isa.org/InTech

DEPARTMENTS

- 8 Industry Update**
BioPhorum Plugfest, Colonial Pipeline Attack, Digital Twin Consortium, Intel AI Speeds Papermaking, FDT Group Changes DTM Certification with FDT 3.0, and more
 - 35 Standards**
ISA's Relationship to IEC Standards
 - 36 Association News**
ISA Fellow John Sorge, In Memoriam, Certification, and more
 - 40 Digitalization Diaries** ★ **NEW**
Specialty Chemicals Manufacturer Achieves Consistently Reliable Batch Processing
 - 43 Workforce Development**
'Understand the Full Process': Tips for Automation Career Success
 - 44 ICS Cyberwatch** ★ **NEW**
Cybersecurity Using ICS ATT&CK
 - 47 Products**
Focus on Cybersecurity
 - 48 Jobs on isa.org**
 - 49 Index of Advertisers; Datafiles**
- COLUMNS**
- 7 Talk to Me**
Do You Do Digitalization?
 - 12 IIoT Insights**
OPC UA: IIoT Enabler and Conqueror of the Cloud
 - 14 Executive Corner**
If AI Is So Awesome, Why Aren't You Using It?
 - 50 The Final Say**
Electric Vehicle Success Requires Automation Professionals



InTech Plus is ISA's online eNewsletter that connects automation professionals to all things automation. *InTech Plus* has technical content, educational training and videos, industry-related Q&A excerpts, and the latest and greatest on industry technology and news. *InTech Plus* focuses on a variety of topics, such as fundamentals of automation and control, certification, safety, cybersecurity, the Internet of Things, wireless devices, human-machine interface, pressure, level, temperature, and batch. All editorial content comes from a variety of sources, including ISA books, training course videos, and blogs and bits from ISA's cast of subject-matter experts. *InTech Plus* is powered by Automation.com, ISA's premier electronic publisher of automation content. Automation professionals can subscribe to *InTech Plus* at www.automation.com/subscribe.



© 2021 InTech

ISSN 0192-303X

InTech, USPS # 0192-303X, is published bimonthly in Research Triangle Park, NC by the International Society of Automation (ISA), 67 T.W. Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709.

Volume 68, Issue 3

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

Subscriptions: ISA Members receive *InTech* as part of their annual membership. Become an ISA Member at: <http://www.isa.org/join>. Other subscribers: 175 USD in North America; 235 USD outside North America. Single copy and back issues: 20 USD + shipping.

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

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

Printed in the U.S.A.

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

For permission to make copies of articles beyond that permitted by Sections 107 and 108 of U.S. Copyright Law, contact Copyright Clearance Center at www.copyright.com. For permission to copy articles in quantity or for use in other publications, contact ISA. Articles published before 1980 may be copied for a per-copy fee of \$2.50.

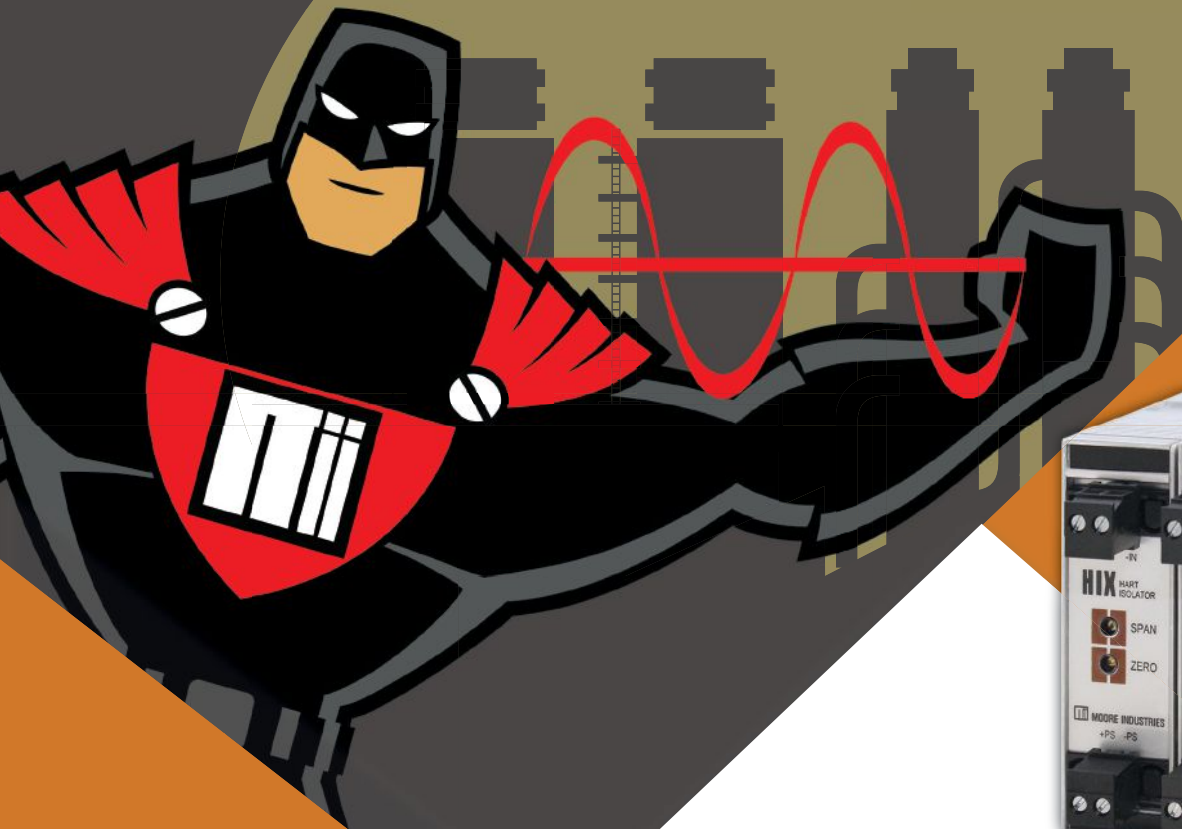
To order REPRINTS from *InTech*, contact Jill Kaletha at 1-800-428-3340 x149 or jkaletha@mossbergco.com.

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



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

When You Need to Pass HART Data, Get a Little Super Hero



HART® data is extremely useful but when you have to isolate your loops in order to share key process signals or keep your systems safe from power issues, HART data can be stripped off and blocked by most isolators. This prevents your critical HART data from reaching your to asset management systems, programming devices or host systems.

HART Isolators from Moore Industries can save the day. With built-in HART pass-through technology you can rest assured that when your loops use HART transmitters, critical and valuable HART diagnostic, process, and calibration information can be read on either side of the Moore Industries HART Isolators.

 **MOORE**
INDUSTRIES
WORLDWIDE
Demand Moore Reliability



To learn more about
HART Isolators from Moore Industries
Call 800-999-2900
or visit www.miinet.com/HART-Isolators

Do You Do Digitalization?



By Renee Bassett, *InTech* Chief Editor

How's your digital transformation going? I don't mean the creation of your personal hologram or Internet avatar; that kind of "digital twin" is outside the scope of *InTech* magazine. I mean, how is the tech-driven transformation of your plant going? Have you integrated your manual processes with your automated ones? Have you dabbled in the darlings of digitalization, the killer apps of industrial computing: namely, the virtual models of physical objects and systems known as digital twins?

If not, maybe it's time. If so, care to tell me about it?

Digital twins are popping up all over to help automation professionals build

Have you dabbled in the darlings of digitalization, the killer apps of industrial computing known as digital twins?

new products, monitor existing assets, optimize maintenance, reduce downtime, and more. There are scores of examples and more coming out every day. The models being built are increasingly robust and benefit from an abundance of IIoT data. (See p. 26 for what ISA members from Tata Consulting are doing to use modeling and sensor data to enable technology-driven asset integrity management.)

The technology has gained a lot of traction in the past few years due to an acceleration of digitalization in general. *InTech* magazine has been monitoring the trend and will now cover it through our new department called Digitalization Diaries (p. 40). This showcase for case

studies and first-person essays is being created in conjunction with Automation.com, the subsidiary of ISA for which I am also the chief editor.

Automation.com is the leading online publisher of automation-related content, including industrial and commercial automation news and case studies. The information available through its website, newsletters, ebooks, and webinars helps automation professionals improve production efficiencies, secure and optimize facilities, and digitally transform their manufacturing and industrial businesses.

Digitalization Diaries seeks to capture and convey, via the pages of *InTech*, the real-world challenges and successes of digital transformation being experienced by members of ISA and the larger automation community at companies large and small; we start this month with the story of a small chemicals batch processor.

As digitalization rises, so too does attention to cyberattacks and cybersecurity. While we regularly cover OT cybersecurity in our features (see p. 30 for a look at how standards become best practices), another new department will provide a more regular outlet: Find ICS Cyberwatch on p. 44.

InTech magazine only publishes six times per year, but Automation.com publishes continuously; you can learn the latest on OT cybersecurity developments, digital transformation, and more in Automation.com newsletters and ebooks. Subscribe at www.automation.com/newslettersubscription.

So how have Industry 4.0 technologies and digitalization improved your plant and operations, made your work life more efficient, or made your products even more praise-worthy? I hope you'll tell me about it. ■

CHIEF EDITOR
Renee Bassett
rbassett@isa.org

CONTRIBUTING EDITOR
Bill Lydon
blydon@isa.org

CONTRIBUTING EDITOR
Charley Robinson
crobinson@isa.org

PUBLISHER
Rick Zabel
rzabel@isa.org

PRODUCTION EDITOR
Lynne Franke
lfranke@isa.org

ART DIRECTOR
Lisa Starck
lstarck@isa.org

GRAPHIC DESIGNER
Bonnie Walker
bwalker@isa.org

ISA PRESIDENT
Steve Mustard

PUBLICATIONS VICE PRESIDENT
Joao Miguel Bassa

EDITORIAL ADVISORY BOARD
CHAIRMAN
Steve Valdez
GE Sensing

Joseph S. Alford PhD, PE, CAP
Eli Lilly (retired)

Joao Miguel Bassa
Independent Consultant

Eoin Ó Riain
Read-out, Ireland

David W. Spitzer, PE
Spitzer and Boyes, LLC

Dean Ford, CAP, PE
IB Abel, Inc.

David Hobart
Hobart Automation Engineering

Smitha Gogineni
Midstream & Terminal Services

James F. Tatera
Tatera & Associates

ADVERTISING & SPONSORSHIP
<https://tinyurl.com/ISA-InTechMediakit2021>

BioPhorum Plugfest Tests Plug-and-Play Equipment Interoperability

At the annual BioPhorum Module Type Package (MTP) standard Plugfest, held in May, biopharmaceutical users and vendors collaborated to move toward the goal of achieving plug-and-play equipment interoperability. The user and vendor participants were highly professional and focused on positive outcomes, and their progress was farther along than one might expect. The success of the remote testing methods used, caused by the realities of the pandemic, was also impressive.

BioPhorum participants—over 108 member companies with more than 3,700 leaders and subject-matter experts participating—pursue a variety of collaborative initiatives. This Plugfest, named PP05, focused on the development of guidelines for MTP files to be used with modular equipment commonly found in biopharmaceutical processing. The three-day event was a successful series of tests to help the plug-and-play workstream build toward the commercial launch and use of plug-and-play capability.

Achieving plug-and-play interoperability of biopharmaceutical manufacturing equipment would dramatically reduce engineering labor, lower project execution time, and increase product quality. At the heart of the idea is the VDI/VDE/NAMUR 2658 standard that defines the module type package. The objective of BioPhorum's plug-and-play concept is to effortlessly integrate intelligent unit operations into the ISA-88 procedural batch engine of the overlying supervisory automation system of a facility compliant with good manufacturing practices.

The MTP focuses on creating standardized nonproprietary descriptions of modules for process automation. This advances the concepts of the ISA-88 and ISA-95 standards into open-vendor, independent, plug-and-produce models that include attributes such as alarm management, safety and security, process control, human-machine interfaces, and maintenance diagnostics. OPC UA is used to

communicate MTP data between systems. MTP also addresses common user complaints that disparate pieces of equipment do not directly and intelligently communicate, requiring significant investment in hardware, software, and application engineering to create necessary interfaces.

Plugfest results. The goal of the PP05 tests was to run multiple bioreactor services on process equipment assemblies (PEAs)—such as single-use bioreactors, chromatography, and filtration unit skids from three different bioreactor suppliers—and stress test. Each set of services was controlled from three different process orchestration layers (POLs). A total of six executions of the services were run simultaneously on two PEAs.

The three POL testing participants were Emerson, Rockwell Automation, and Siemens. Each hosted virtual testing on three separate days. The PEA testing participants were Cytiva, Merck KGaA (Life-Science), and Pall.

Outputs from PP05 include completed test specification records, MP4 recordings of the test sessions, and a list of conclusions and next steps. Some issues were identified and documented that will be worked out, and this is exactly the value of having a Plugfest. The next goal is a physical face-to-face meeting as soon as possible, with simultaneous meetings in the U.S. and Europe.

Having been involved in various industry organizations and standards groups over the years, I find the use of dedicated, professional, BioPhorum facilitators to be an innovative approach to achieve goals. As I observed the three days of the Plugfest, I was impressed by the process and by BioPhorum PP05 facilitator Julian Goy's skills and experience.

Given pandemic-related travel restrictions, I also was impressed by the group's use of virtual tools and remote connections to communicate and verify operations of equipment in different physical locations. Past Plugfests have been held in a single plant. ■ —By Bill Lydon



Litmus Awarded CESMII Smart Manufacturing Project

Litmus, an intelligent edge computing company, has been awarded a contract from CESMII – The Smart Manufacturing Institute. Litmus was chosen from 28 request-for-proposal responses.

The Litmus project, titled, “Machine and Process Health Monitoring,” will connect Litmus Edge software to CNC machines at Bray International, a manufacturer of flow control and automation products and accessories. The project has three projected outcomes: create a smart manufacturing profile for a valve-manufacturing CNC machine, expose key performance indicators (KPIs) to optimize Bray International maintenance routines, and expose KPIs to optimize Bray International machine uptime and part quality.

Litmus was chosen because its project “directly aligned with our specific areas of interest for applying smart manufacturing principles to real-world manufacturing processes and operations challenges,” said John Dyck, CEO of CESMII. “These projects are vital to a global transformation of the manufacturing industry.”

Litmus will meet the CESMII Innovation Project requirements to rapidly solve a challenging manufacturing use case for processes and equipment (approximately 3–6 months) in a cost-effective, reusable, secure, scalable, and repeatable manner. ■

DIGITAL TRANSFORMATION
Virtual Conference

31 August
9:00 a.m. – 5:00 p.m. ET

Register: <https://isaautomation.isa.org/virtual-events-program>

Colonial Pipeline Attack Started in IT Systems, Highlights SCADA System Vulnerability

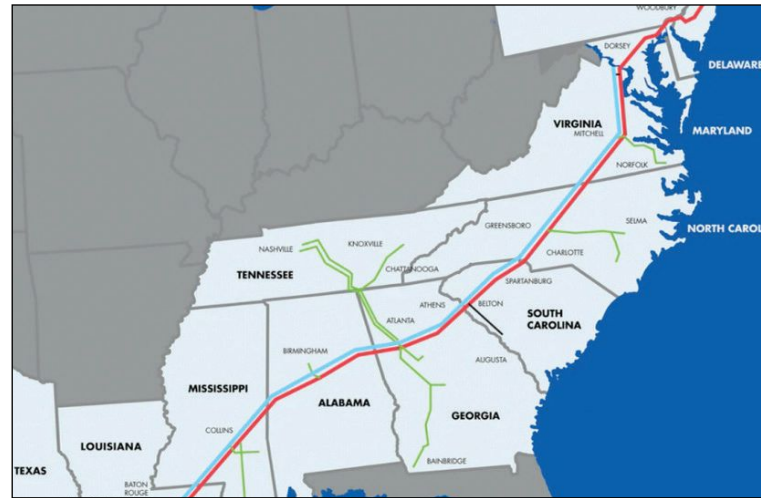
Colonial Pipeline, which operates a major pipeline system that transports fuel across the East Coast, fell victim to a ransomware attack in May that halted all pipeline operations while it dealt with the incident, company officials said. Colonial Pipeline did not say what was demanded or who made the demand. Ransomware attacks are typically carried out by criminal hackers who seize data and demand a large payment in order to release it.

“Cyberattacks are a real and present danger to critical infrastructure around the world and, by extension, every single consumer. If reports are accurate, the Colonial Pipeline incident has all of the markings of a possible ransomware attack that began in the IT environment and, out of precaution, forced the operator to shut down operations,” said Marty Edwards, vice president of OT security at Tenable and the longest-serving director of the Department of Homeland Security’s ICS-CERT.

“I’m surprised that it took this long for a major incident to happen for a pipeline operator,” said Dewan Chowdhury, chief executive and founder of security provider MalCrawler. “I have spent 20+ years securing and responding to cyberattacks on [the] OT-ICS/SCADA environment [and] have worked with dozens of large pipeline operators globally and dozens of the DNG [downstream natural gas] operators who help distribute natural gas.”

Edwards said, “I have responded to nation-state cyberattacks on pipeline infrastructure in the past, and I can tell you that the attackers had the resources to include human assets on the ground to help facilitate a cyberattack. Therefore, when responding to the pipeline cyberattack, we would know by the level of sophistication [if] these attacks were conducted by groups that have the resources to plan a sophisticated cyberattack.”

“We should not underestimate these groups,” Edwards added. “Many of them now have help desks, technical support, payroll processing, and subcontractors. They are essentially



full-fledged criminal corporations operating in the digital world. While it’s unknown how this attack played out, it’s yet another reminder of the increasing threats to critical infrastructure we all rely on.”

John Cusimano, vice president at aeCyberSolutions, the Industrial Cybersecurity division of aeSolutions, said pipeline cybersecurity is far behind that of other energy sectors. “A common gap in the pipeline industry is the lack of segmentation of the pipeline supervisory control and data acquisition [SCADA] networks . . . [Once] someone gains access to the SCADA network, they have access to every device on the network.” This was one of his greatest concerns when he first learned of the SolarWinds attack, he added.

In the SolarWinds attack, hackers inserted malware into a service that provided software updates for the SolarWinds Orion platform, which is a suite of products used to monitor the health of its IT networks.

Colonial Pipeline said its ransomware attack affected some of its IT systems, and the company moved proactively to take certain systems offline, halting pipeline operations, according to a report by The Associated Press. In an earlier statement, it said it was “taking steps to understand and resolve this issue” with an eye toward returning to normal operations. The company also said it hired a cybersecurity firm to investigate the nature and scope of the attack. ■ —By Gregory Hale

Digital Twin Consortium Forms Open-Source Collaboration Community

Digital Twin Consortium (DTC) announced an open-source collaboration community to accelerate the adoption of digital twin-enabling technologies and solutions. Consortium members and nonmembers can collaborate on open-source projects, code, and collateral and become part of the DTC ecosystem.

To participate, candidates complete a project application that is reviewed by

the DTC Technical Advisory Committee. Approved contributors upload their projects or related content to the DTC Open-Source Collaboration GitHub site. The site contains project files and revision history, and enables participants to collaborate on digital twin-related content and projects.

“Open-source collaboration will encourage innovation in digital twin solutions,” said DTC steering committee member Said Tabet, PhD, who is also distinguished

engineer, chief architect emerging technology and ecosystems, CTO office of Dell Technologies.

Open-source projects are more flexible and respond more rapidly to market demands than closed counterparts,” said Dan Isaacs, CTO, DTC. “Our Open-Source Collaboration Community initiative will substantially expand the DTC ecosystem and facilitate the adoption of digital twin and digital twin-enabling technologies.” ■

Intel AI Helps Speed Papermaking Process in Europe

Intel and byteLAKE are collaborating on a new artificial intelligence system to automate wet- and dry-line management during the papermaking process. The system helps paper mills avoid costly disruptions during paper production. The wet line detector from byteLAKE is commercially available and has been successfully implemented in paper mills across Europe.

Paper production is a multiphase process during which a natural phenomenon called “wet line” (sometimes “dry line”) is observed. The wet line must be carefully monitored to avoid losses and expensive breaks in production. It is a highly tedious process where an operator must visually inspect the machine and adjust settings to avoid any issues.

“Many companies still perceive the application of AI in their business as an addition, not its foundation,” said Krzysztof Jonak, EMEA territory sales director at Intel. “The application of the Intel Distribution of OpenVINO toolkit in byteLAKE’s tool shows not only that AI works well as an actual tool for optimizing company opera-

tions, but also that this combination reduces the barrier of necessary upgrades to IT infrastructure in the company to an additional computer forming the basis for the whole system. This is a breakthrough in looking at AI and its implementation in companies that are able to see the potential in joining the ‘Industry 4.0’ family of businesses.”

The wet line detector for paper mills is a dedicated AI model designed and trained specifically for the role of wet-line detector. It can work in real time and perform ongoing analysis of the frames from closed-circuit television. AI algorithms examine the surface where the weave is formed and detect the wet line. Additionally, the algorithms measure and estimate the location of the wet line and its width. This information is then presented to the paper-machine operator, who can react appropriately and adjust the settings as needed. ■



AspenTech Expands Application of Industrial AI

Aspen Technology, Inc., has extended industrial artificial intelligence (AI) across its asset optimization solutions to improve profitability and sustainability in customer operations. In addition, the company’s Industrial AI Workbench will enable data scientists to collaborate with domain experts to develop AI apps based on enterprise-wide data.

With first principles–driven hybrid models, AI is directly embedded into Aspen HYSYS and Aspen Plus process simulations, so engineers can easily build operations-ready models calibrated with relevant plant data. Reduced-order hybrid models can be shared across engineering, planning, and dynamic optimization solutions to improve the accuracy and predictability of these applications. Deep learning APC can provide more accurate

and sustainable models that cover a broad range of operating conditions.

“Using the hybrid model, we were able to create a model that can reproduce real plant data more accurately than the conventional reformer model. We were able to create a highly accurate model in a short period of time,” commented Takuto Nakai, production department, Nissan Chemical Corporation.

This latest version of aspenONE V12.1 also includes new models that enable customers to optimize biomass processing, hydrogen production, carbon capture, and carbon emissions more accurately and systematically to reduce environmental impact. New analysis and visualization capabilities also can help to reduce measurable waste and energy use throughout the process from lab to production. ■

TASI Group Acquires Mission Communications



The TASI group of companies, makers of flow control and instrumentation products, has reached an agreement to acquire Mission Communications in Norcross, Ga. Mission will be organized into TASI’s largest business segment, TASI Flow, to complement TASI Flow’s existing asset management and wireless connectivity strategy. Forrest Robinson will continue to lead Mission on its growth track as president of Mission.

TASI CEO John McKenna said, “TASI is committed to providing cost-effective, wireless connectivity to our customers, helping them to monitor and manage their valuable assets.” TASI Flow president John Norris added, “Using TASI Flow’s global footprint we are excited to support Forrest’s vision of expansion beyond North America” and bring a strong presence in the water/wastewater market. ■

2021 Virtual Conference
CYBERSECURITY SERIES

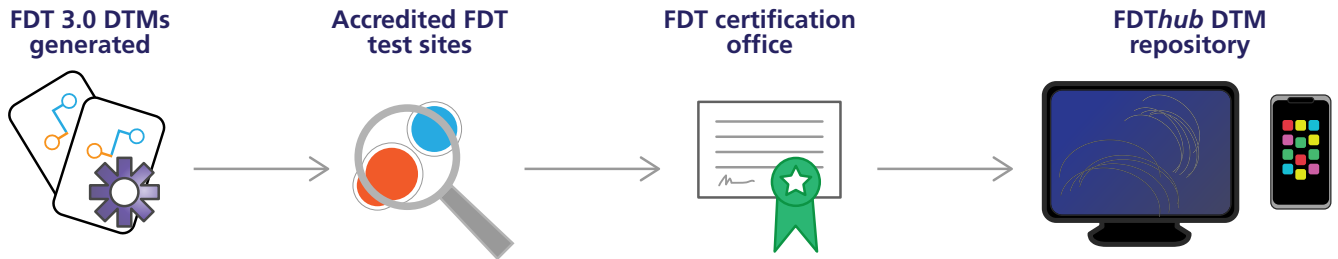
Cybersecurity Standards
Implementation Virtual Conference

19 October
9:00 a.m. – 5:00 p.m. ET

Register: <https://isaautomation.isa.org/virtual-events-program>



FDT Group Changes DTM Certification with FDT 3.0



FDT Group, which has developed and maintained an open standard for enterprise-wide network and asset integration in the process, hybrid, and factory automation markets, announced changes to its certification of a core component of the FDT standard: device type managers (DTMs).

“The organization’s new, forward-looking FDT 3.0 standard is accelerating its evolutionary journey into the Fourth Industrial Revolution. The technology’s FDT IIoT Server platform holds the key to unlocking universal device integration,” according to James Loh Chia Woon, FDT test and certification chairman.

DTMs contain the user interface and the application software that defines all the parameters and capabilities included in field instruments. DTMs encapsulate all device-specific data, functions, and business rules such as the device structure, its communication capabilities, internal dependencies, and its human-machine interface (HMI) structure.

Open access to intelligent devices

As part of FDT Group’s comprehensive DTM testing process, accredited test sites test DTMs against the current FDT specifications. DTMs that are compliant with the specifications allow open access to intelligent devices and the myriad of information available from those devices, networks, and plant and factory processes.

Recent updates to FDT Group’s test tools and certification procedures are aimed at optimizing the efforts of DTM developers and helping them bring new products to market, while at the same time improving the experience of automation end users around the world. The new steps in FDT 3.0 DTM certification are streamlined for a better overall experience.

Key to the development of FDT-compliant DTMs is the use of FDT Group’s Common Components toolkit, says Woon. It provides a fast way for development teams to view DTMs in an FDT hosting (desktop or server) application and understand

the communication flow between them. With FDT 3.0, DTMs are now OPC UA-ready and offer data through the natively integrated FDT OPC Unified server. This eliminates a significant amount of effort on the part of developers, who can implement FDT 3.0 using the common components and then rely on the toolkit’s clear guidance to support interfaces within the standard, says Woon.

Mandatory UI style guide

The FDT 3.0 Industrial Internet of Things (IIoT) ecosystem development environment, intended to simplify the transition to IIoT and Industry 4.0 solutions, includes an updated FDT 3.0 Style Guide empowering a standardized, responsive-by-design web user interface (UI) for new solutions developed by the supplier community. With the FDT 3.0 standard, DTM testing and certification has been broadened to include compliance with the FDT 3.0 DTM Style Guide. This requirement was not in effect with FDT 2.0, which allowed instrumentation suppliers to make their own decisions regarding style guide compliance. FDT 3.0 DTMs must now pass both conformance and style guide tests to receive certification.

A critical aspect of the FDT 3.0 DTM Style Guide is ensuring a uniform UI with the same look and feel, presenting information in a consistent fashion across different vendors, devices, and applications. This is especially important with new mobile systems being deployed in industrial facilities. As such, compliance with the NAMUR NE-107 recommendation is now required within the FDT 3.0 Style Guide.

While developers did not receive the DTM Style Guide test tool as part of FDT 2.0 certification—this functionality was only available to the test center—the style guide tool has been embedded in the FDT 3.0 dtmINSPECTOR5 tool version.

For more information about developer tools and certification, visit www.fdtgroup.org/development. ■

Rockwell Adds Cisco Cyberthreat Detection Services

Rockwell Automation is adding Cisco’s Cyber Vision to its existing LifecycleIQ Services portfolio of cybersecurity threat detection offerings. The two companies have been working together for more than a decade to offer jointly developed architectures, services,

and products to help build a Connected Enterprise.

Because a deeper integration between IT, cloud, and industrial networks creates security issues that become digitization obstacles, Cyber Vision provides visibility into industrial control systems to build secure in-

frastructures and enforce security policies. The addition of Cyber Vision to the LifecycleIQ Services threat detection offerings provides a unique switch-based architecture for customers with existing Cisco solutions, greenfield networks, or those updating their Cisco network infrastructure. ■

OPC UA: IloT Enabler and Conqueror of the Cloud

By Jim Redman



ABOUT THE AUTHOR

Jim Redman (jredman@ergotech.com) is president of ErgoTech Systems, Inc. Redman and ErgoTech were delivering what has become “IloT” systems back in 1998. The company’s MISStudio suite reflects his holistic vision to provide a single tool for integration and visualization from sensor to artificial intelligence, and from tiny IloT to worldwide cloud.

Exchanging data between Industrial Internet of Things (IloT) devices and the cloud presents a bewildering array of options. Cloud providers, Amazon Web Services, Microsoft Azure, Google IO, and many others each advocate for their own technique for IloT data interchange. But operational technology (OT) applications have a very long life, and, in the fast-moving world of cloud IT, some solutions are likely to be orphaned. IloT “standards” such as MQTT, AMQP, REST, and Kafka compete to serve as pipelines to move data across the network. At the same time, custom OT implementations from IloT/edge/cloud software and hardware vendors can cause “vendor lock,” limiting your choices and flexibility. The answer is OPC UA.

OPC UA makes using the cloud easy and safe. You already know OPC and can create secure, robust cloud and IloT applications. Moving application data to the cloud lets you do your job better while saving costs and lowering security risks. A vendor-independent, widely implemented standard ensures long-term support and protects your investment in a rapidly changing cloud environment.

OPC UA is a collection of specifications. The primary specification, and by far the most widely implemented and recognized, is the Data Access specification. Others gaining industry support include the Historical Data Access (OPC HDA) specification, which extends the OPC server to include reading and writing historical data, as well as real-time transfers.

A recent addition to the OPC specifications is the “publish-subscribe” model. This provides features

similar to the Data Access model with some additional performance and lower overhead. This further enhances the benefits of OPC UA in the cloud.

OT data security

OPC has always been targeted at automation data—a continuous stream of values that we need to share between applications to populate user interfaces and trends and from which we need to extract alarms and anomalies. OPC reflects the reality of the OT environment. Each tag or data point has descriptive metadata including valuable text descriptions of the point, units, ranges, and locations. Critical for good OT data management are a quality indicator and the time stamp of the actual reading—not the time it was uploaded. As obvious and vital as all these requirements are for OT data, many widely adopted protocols and custom cloud/IloT solutions do not include these essential aspects.

Security is always a priority whenever data is passed across a network. OPC UA security is based on state-of-the-art IT best practices, but you do not have to understand the intricacies to deliver a secure solution. Security is an integral part of the standard and is part of all OPC UA clients and servers.

OT professionals, with reasonable care and understanding, can ensure a secure OPC system end-to-end—indeed, if you have already installed and configured any OPC UA solution you know the procedure. OPC UA, like legacy OPC, supports subscriptions and on-data-change notifications. Clients can subscribe to the server and receive notification of tags that have changed in real time. This service has been enhanced so that on-data-change notifications are queued at the server. If there is a short network outage, the server will maintain the notifications for the client and deliver them in order when the client can receive them.

Another addition to the standard is the “HistoryRead” service. Clients can request data starting from a particular date and time, allowing data notifications that were missed during a more major network issue to be retrieved once the network connection is reestablished.

You already know OPC and can create secure, robust cloud and IloT applications. OPC UA makes using the cloud easy and safe. ■

A version of this article first appeared in AUTOMATION 2021 Vol.1, IloT & Industry 4.0, from Automation.com.



DOES THIS MAKE SENSE?

Aliens travel faster than the speed of light but have not invented clothing



PROVEN
40
YEAR
BATTERY
OPERATING
LIFE*

DOES THIS MAKE SENSE?

Upstart battery manufacturers with little experience are claiming their products can last for decades. We've produced over 2.2 billion industrial grade lithium cells since 1975.



Don't use batteries that are alien to you.



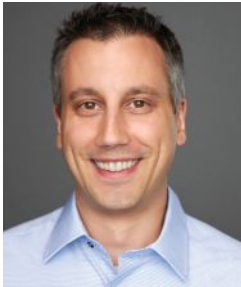
* Tadiran LiSOCL2 batteries feature the lowest annual self-discharge rate of any competitive battery, less than 1% per year, enabling these batteries to operate over 40 years depending on device operating usage. However, this is not an expressed or implied warranty, as each application differs in terms of annual energy consumption and/or operating environment.

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

www.tadiranbat.com

If AI Is So Awesome, Why Aren't You Using It?

By Jeff Winter



ABOUT THE AUTHOR

Jeff Winter (www.linkedin.com/in/jeffreywinter) is the senior director, strategy & marketing, for Grantek Systems Integration. Winter is also part of the leadership committee of the Smart Manufacturing & IIoT Division of ISA, a contributor to IEC as a member of TC 65, on the board of directors with the Manufacturing Enterprise Solutions Association (MESA), and benchmarking chair with Control System Integrators Association.

If you pay attention, even remotely, to tech news, you cannot avoid hearing about artificial intelligence (AI). It's everywhere! It dominates articles, events, podcasts, discussion boards, videos . . . you name it. I believe this is because of a combination of two notions:

- AI is extremely versatile in its application; it spans every industry and impacts nearly every job function—from entry level all the way up to the CEO.
- AI has a mysterious science-fiction allure that captivates peoples' imaginations and curiosity.

At its core, AI is basically the combination of techniques, practices, and technologies designed to mimic the function of the human mind. This results in a system that is capable of self-learning, self-evolving, and self-improvement.

The idea of artificial intelligence isn't new. In fact, it has been around since ancient times, when people imagined "beings" who were capable of intelligent decision making and who were controlled by a "master craftsman." It has only been the past decade or so when the fantasy of AI has become palpable, understandable, and capable of truly being utilized. IBM's Deep Blue supercomputer in 1997 was famously known for beating chess grandmaster Gary Kasparov using early forms of AI.

Nearly 15 years later in 2011, IBM used the Watson computer system on *Jeopardy!* to showcase its improvements. In 2020, we live in a world where visual and auditory "deep fakes" are shockingly easy to produce. No matter how you look at it, technology and ingenuity have led this charge and brought us to 2021 where AI is on everyone's minds. And why wouldn't it be? The promises of AI are powerful, inspiring, and ever growing.

According to the Center for Data Innovation, in a 2016 article called "The Promise of Artificial Intelligence," the technology will fundamentally change our lives through seven primary applications (figure 1). Any one of these applications would have tremendous positive impacts on reducing administrative managerial work, improving decision making, reducing operational costs, or reducing waste.

With all these universal applications and clearly understood benefits, the writing appears to be on the wall: AI is the wave of the future, and if you are not using or planning on using AI soon, you will be history! Software, platforms, and technologies are already out there, yet adoption appears to be slow. Financial justification and benefits analysis seem to be

no-brainers, yet no one is out rushing to make improvements. Why is that?

State of the AI industry

Surprisingly, market research back in 2015 on AI was far and few between, so unfortunately, it is hard to make useful prediction comparisons over time. One 2016 study by UBS pegged the global AI industry at roughly \$5 billion in 2015 with plans to grow to around \$120–\$180 billion by 2020. Today, there are many more market studies related to AI, but none of them put the industry close to even the low end of \$120 billion that UBS predicted. Grandview Insights indicates AI was less than \$40 billion in 2019, but projects it to grow to around \$740 billion by 2027, representing a 42 percent compound annual growth rate.

So, although AI has been steadily growing, it seems we keep predicting this massive growth that does not happen. According to a 2018 study by McKinsey, only 21 percent of companies say their organizations have embedded AI in several parts of the business, and barely 3 percent of large firms have integrated AI across their full enterprise workflows. For such an exciting technological advancement in how we live our lives, those numbers are not very impressive.

Electricity and the Internet: A similar story

In 1893, the world was mesmerized by the infamous illumination of Chicago during the World's Fair by President Grover Cleveland simply pushing a button. The entire world was inspired and captivated, fully believing electricity would change everything. The problem was that no one really knew how. According to *The New York Times*, it took nearly 30 years until 50 percent of U.S. homes adopted the technology, and roughly another 30 years to achieve close to 100 percent adoption. In 1989, the World Wide Web was invented with a similar story, albeit with faster adoption. According to Pew Research, it took until 1995 to get 14 percent of U.S. adults to use the Internet. The same study showed that by 2014, there was only an 87 percent adoption rate. Living in 2021, it is hard to imagine life without the Internet or electricity—especially when trying to work from home during a pandemic!

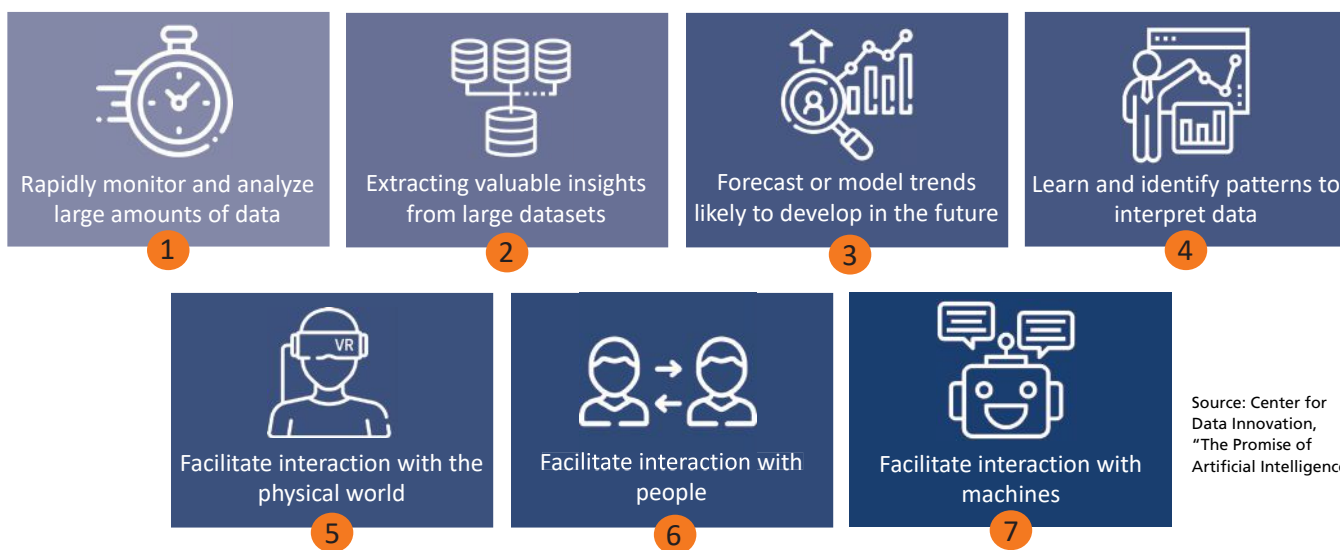
Today both of these technologies are considered a utility—something necessary to allow other things to function. When rapid growth by companies occurred as a result of these utilities, they did not attribute their success to electricity or the Internet. Even companies

like General Electric, with electricity in the name, were not promoting their products under the slogan “look what electricity can do for you.” Rather, GE and other successful companies took advantage of the utility of electricity to create a bunch of products that solved people’s needs, such as the light bulb, the washer and dryer, the refrigerator, and the TV.

The point is: Electricity by itself was too vague and intangible. It was the products that take advantage of electricity that changed the world and drove recognizable benefits to the way we live our lives. More than 100 years later, it is impossible to imagine a life without electricity. It is used to support nearly everything we do and everything we create (from a manu-

bunch of pilot projects. Instead, you, along with everyone in your entire company, need to change the way you think.

You need to start every decision process with the idea that there is this “thing” (artificial intelligence) already out there that is smarter, faster, more accurate, and more reliable than you in making a decision. By letting that guide your thought process, you will automatically start to include the idea of AI into everything you do, everything you decide, and every action you take. You will end up identifying and capitalizing on the “appliances” (to tie back to the electricity analogy) that AI allows for, rather than thinking about AI itself. And going one step further, if your company makes



Source: Center for Data Innovation, “The Promise of Artificial Intelligence”

Figure 1. Any one of these applications could have tremendous positive impacts on reducing administrative managerial work, improving decision making, reducing operational costs, or reducing waste.

facturing perspective). The same can also be said for the Internet.

The inevitable boom

The same can also be said for artificial intelligence. AI will inevitably be used to assist, offset, and even replace tasks we do today, just like the Internet and electricity did many years ago. AI will permeate every part of our personal and professional lives. It will be used to help us grow our businesses and eventually be used in nearly every electronic product companies make. So, what can you do today to take advantage of AI?

The answer is surprisingly simple in concept, yet requires a huge, concerted effort to pull off effectively. You do not need to go out and do tons of research on AI technology, understand the details of how it works, investigate all the existing platforms, or even launch a

electronics of any kind, your product development cycle will naturally start to include AI into the very things you create!

You will notice that this is much different from the traditional technology adoption model, where you either look for a new product on the market that can solve your existing problem or where you discover a new product that can make an incremental improvement on something you already have or do. No, AI is far more fundamental and pervasive. If it is treated like a “product,” it will be siloed, underutilized, and haphazardly applied. It will not ever be fully used in a way necessary to transform the entire foundation of a company.

Let AI channel your left brain’s creative tendencies to get you to think differently. AI is here to stay. Don’t be a laggard! ■



Controller Redundancy

Under the Hood

By Vibhoosh Gupta

Industrial controller redundancy improves system availability, but only if it is implemented with the right capabilities.

In many cases, conventional wisdom tells us that if one is good then two are better. This concept extends to the design of industrial automation systems. Even though industrial programmable logic controllers (PLCs) are very reliable, they are a single point of failure susceptible to onboard faults, as well as external problems with power or networking. For critical applications, designers must consider how to address this issue, usually by implementing a secondary backup or redundant PLC.

A more general and encompassing discussion is how to achieve high availability (HA) for industrial automation platforms. Providing an HA system requires eliminating as many single points of failure as possible. Redundancy, either as parallel systems or as multiple systems that can take over for failed systems, is a primary strategy for HA designs. And if redundancy can be easily and cost effectively accomplished while preserving the necessary performance level, it becomes useful and desirable for many more machine automation applications. While the primary goal of redundancy is usually around-the-clock availability, many users rely on redundancy to help them perform maintenance during normally scheduled operating hours without affecting production.

It is tempting to assume that all factory automation redundancy solutions provide the same benefits, but upon inspecting the details it soon becomes clear that all solutions are not the same. For controllers and control systems used for factory and machine automation, attention to controller redundancy implementation details is crucial to understanding their effectiveness.

All redundant industrial controllers do not behave exactly alike. There are many implementation design choices affecting the performance, timing, and supportability of redundant controller solutions, and end users must carefully weigh these details before committing to a deployment.

Edge to enterprise redundancy

Redundancy at all levels of automation is justified by the return on investment (ROI). Users must recognize any costs of equipment, setup, commissioning, and maintenance versus the benefits of operational availability, flexibility of maintenance scheduling, and better diagnostics (figure 1).



Redundant systems are generally preferred over nonredundant (simplex) systems, with a few caveats. Some redundant implementations increase complexity, driving up the design, hardware, and operational costs beyond what is justified. Also, some redundancy methods compromise various aspects of performance and are therefore unsuitable.

When considering a redundancy solution for any application, multiple automation disciplines must be evaluated in relationship with each other to ensure the expected performance will be delivered:

- power distribution
- instrumentation
- fieldbus networks
- industrial controller
- on-site PCs
- information technology (IT) networks
- cloud connectivity
- cloud computing.

Figure 1. For critical equipment and processes, redundant PLC processors with the right level of performance are often justified.

FAST FORWARD

- Controller redundancy provides many benefits as part of any high-availability strategy for factory automation and machine control.
- Traditionally, controller redundancy schemes introduced performance limitations and were complex and expensive—so they were used for only the most crucial applications.
- Today's technologies offer a much better controller redundancy price/performance ratio, but users must understand the implementation details to ensure they receive the expected ROI.

Redundant devices powered from a single fallible circuit do not have the best reliability. Redundant instruments provide more data but raise the question of which signal is correct. Fieldbus and IT networks in a ring configuration are a good redundancy choice, if designers route the cabling carefully so a physical break opens the ring in only one location. Many cloud resources have redundancy features, but poor connectivity can compromise them.

This article focuses on HA redundancy factors for industrial controllers, such as programmable logic controllers and edge controllers. These controllers interact in several ways with other devices, connecting:

- down to lower-level field devices and instruments

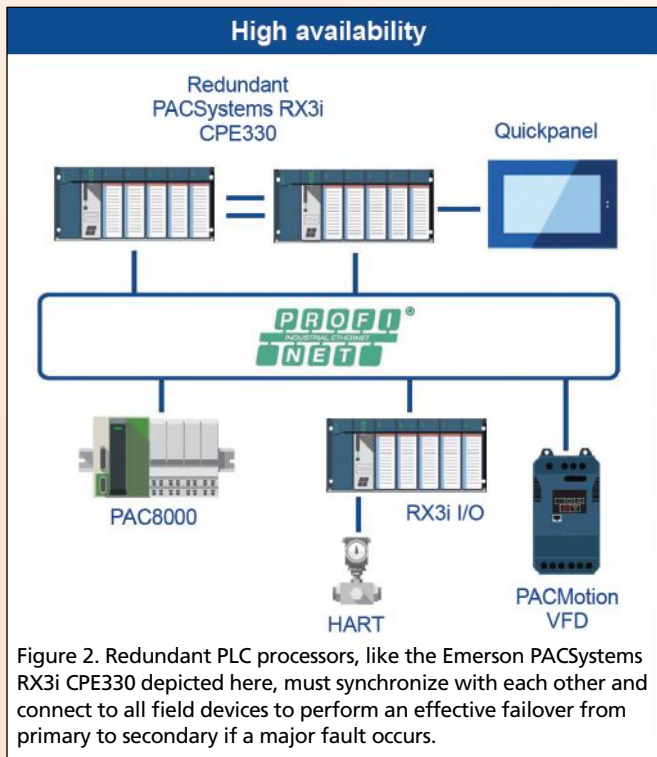


Figure 2. Redundant PLC processors, like the Emerson PACSystems RX3i CPE330 depicted here, must synchronize with each other and connect to all field devices to perform an effective failover from primary to secondary if a major fault occurs.

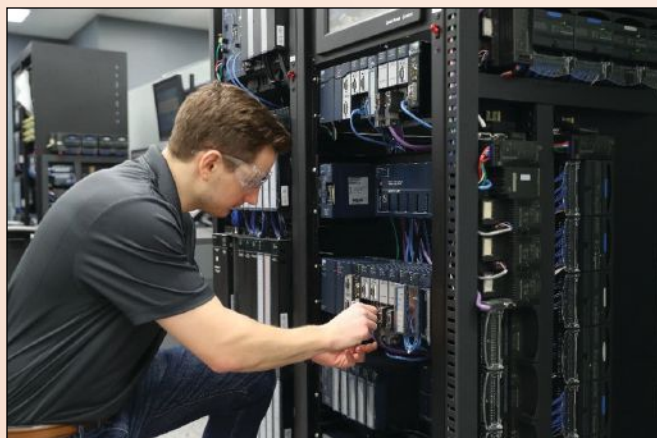


Figure 3. Not all redundancy schemes are created equally. PLC redundancy implementations should ensure deterministic and secure performance, maximizing uptime in operation and during maintenance activities.

- up to higher-level human-machine interface (HMI) and supervisory control and data acquisition (SCADA) systems
- laterally to other peer controllers.

Due to expense and complexity, industrial automation redundancy has largely been reserved for only the most critical processes in past years. However, advances with hardware, software, and networking have made it far more practical to incorporate controller redundancy into machine automation applications of all types.

Basic controller redundancy architectures

Controller redundancy architectures for delivering HA typically involve paired controllers, although more controllers are possible for the most crucial applications. One controller is the *primary* or *active* device, while the other is the *secondary* or *standby* device. Usually, but not always, these roles can be exchanged at will.

The primary controller operates the input/output (I/O), and it executes control logic and communication tasks. Physical I/O and other smart devices are arranged on one or more fieldbus network ring for access by both processors (figure 2).

Also, the primary controller must continually update or mirror itself to the secondary regarding the I/O status, memory values, and any program changes, so the secondary is ready to assume control seamlessly if needed (figure 3).

In the event of a major fault—such as a power failure, cut cable, rack fault, or processor error—the primary controller switches over to the secondary, which should seamlessly continue with operation. This action is known as *switchover* or *failover*. The most preferable architecture for switchover is *hot standby*, where the primary controller constantly synchronizes to a powered secondary controller, which is available to take over at any time. However, the amount of time required for failover, and whether it is fast enough for the application at hand, is of great importance. Some schemes may take a bit of time, while others can be accomplished within a single control execution logic sweep making them effectively bumpless on failover.

Another scheme called *warm standby* indicates that a secondary controller may be installed, powered, or at least preloaded, but may not be synchronized and may require user intervention to initiate a switchover. This introduces significant delay and might only be acceptable for simpler systems. For instance, if a production line has many machines in parallel, the loss of one line for a short time may not be debilitating.

The lowest performance redundancy scheme, although perhaps the most typical real-world scenario, is a spare controller on the stockroom shelf, which requires significant technician effort to access, install, and load. This is sometimes called *cold standby*.

Key redundancy considerations

End users investigating HA and controller redundancy must ensure that any solution satisfactorily addresses four key areas:

- deterministic switchover
- geographically diverse controller installation locations

- ability to upgrade hardware and firmware revisions without downtime
- secure native communications.

Deterministic switchover: Deterministic switchover guarantees that the transition from a failed primary controller to an available secondary controller not only happens within a maximum defined time, but also occurs seamlessly.

Geographic diversity for controllers: Many applications, especially those aboard ships and vehicles, or for very large sites, provide improved reliability if they locate each member of a redundant controller pair as far apart from each other as practical. With this arrangement, a physical failure (like a fire or flood) at one controller location is less likely to impact the other controller location.

Upgrades without downtime: Users need to periodically perform system-level upgrades, such as changing out hardware or updating firmware. Any so-called redundant system that cannot be updated without a shutdown is not truly redundant.

Secure native communications: Security is related in part to the previous upgrade item, because it is almost a certainty that systems will need periodic firmware updates to address cybersecurity issues. Operating systems and software libraries are complex; control and communications functions are more extensive; and system lifetimes are expected to be 10 to 20 years. A redundant controller system can be more cybersecure than a simplex system, but it must rely on secure native communications to safeguard against outside attacks.

Real-world implications

A successful failover can never be too fast. While some processes can withstand disruption or a “hold last state” condition for a few seconds or longer, many machines must failover within milliseconds to preserve acceptable operation. Applications for the management, backup, and distribution of power are prime examples requiring fast failover.

Following are some successful ways that specific redundancy technologies and implementations can meet key requirements, and also some ways they often fail to do so.

Synchronization

Optimal redundancy implementations fully synchronize all data and I/O memory every single scan (figure 4). However, many PLC platforms attempt to synchronize by exception in an attempt to optimize normal operating performance at the expense of allocating enough resources to handle a worst-case event properly. This approach can lead to variable performance on failover and even more drastic cascade-failure problems due to too much data changing at once. Some PLCs must restrict the amount of usable memory by up to one half in order to carry out sync functions.

Similarly, primary and secondary PLC logic solving should be executed in synchronized lockstep for fast, consistent, and reliable failover. Operating asynchronous redundant PLCs can lead to unexpected application behavior, and those requiring special program arrangements to group I/O for bumpless handling can be difficult to configure.

For the best performance, the synchronization should be carried out over a dedicated network. Some schemes attempt to use the I/O network for the sync task, and therefore compromise performance for both functions. A dedicated sync network may use copper media, but fiber optic media is often available and offers high bandwidth and electrical noise immunity. It can also extend great distances for applications where the controllers are installed far apart.

Full synchronization is certainly critical for robust I/O control, but it also plays a role for supervisory systems. It allows HMIs and SCADA to continue communications with little or no interruption during failover. Some PLC redundancy schemes exhibit an “HMI blind time” during failover where supervisory systems are unable to read/write PLC tag data, an inferior approach.

Communications

For redundant systems, separate I/O networks are rings themselves, both for high availability and so each controller of the redundant pair can interact with all devices. These fieldbuses, such as PROFINET, should be natively available within the PLC or edge controller ecosystem because relying on a gateway introduces an additional failure point.

The communication protocol from redundant PLCs to higher-level systems is also important. OPC UA has emerged as the preferred choice in this role for several reasons:

- Redundancy provisions: OPC UA includes two types of redundancy in the specification.
- Industrial capability: OPC UA is extensible and incorporates features for contextualizing data, making it a universal language for communicating between all sorts of industrial devices.

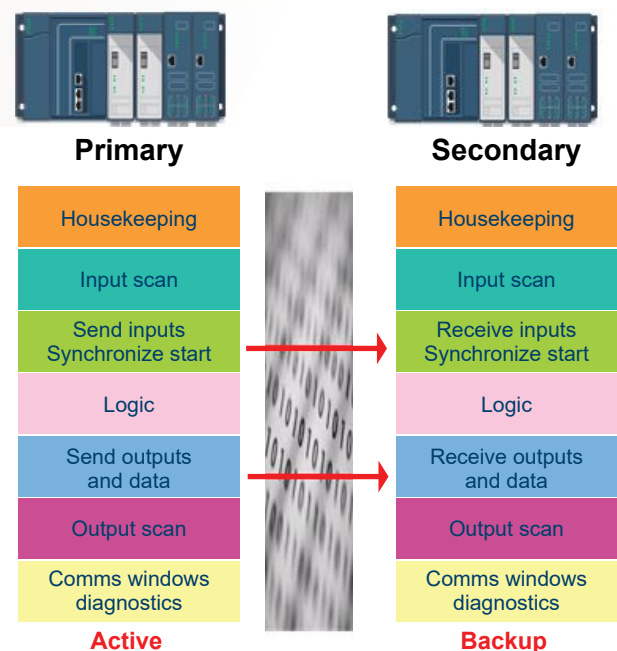


Figure 4. Emerson’s redundancy strategy transfers all synchronization data every PLC scan, so the standby controller always has the same dataset as the active unit for consistent performance.

- Security: OPC UA provides security in the form of encryption and authentication to help protect industrial systems from outside influences.

However, some PLCs do not support OPC UA in redundant systems and therefore lack these benefits.

Maintenance

It is one thing to experiment with a redundant configuration on the workbench, and quite another to deploy one to the field where it needs to run nonstop for decades. In the real world, parts sometimes need replacing, connections fail, and firmware must be upgraded.

The last point is more important than ever. In past years, many PLCs were installed and never upgraded again as long as they remained functional, a feasible approach because they were largely standalone islands of automation. However, today's PLCs are heavily networked to external systems, exposing them to cybersecurity threats. Periodic firmware upgrades are more necessary than ever to update systems and improve their cybersecurity, and to provide other features.

Redundant PLC platforms are easiest to maintain if the hardware, firmware, and software versions are not specifically required to match. Unfortunately, many redundant PLC implementations require exact matches, even to the extent of needing a system shutdown to perform firmware upgrades, or in the worst case, triggering a shutdown upon mismatches.

The right controller redundancy combination

As with any effort, the costs of designing, procuring, implementing, and supporting a redundancy solution must be tallied. Certainly, a second controller is necessary, although this is often costed into the work as a spare part anyway. Redundant controllers require additional power supplies, networking cards, cabling—and even entire control panels in some cases. Design and installation efforts can escalate.

Beyond these relatively straightforward costs, users need to consider the impacts on software, licensing, and configuration labor. Some implementations require specialized software versioning, additional licensing costs, and careful programming practices to function. Other systems may only require a few configuration clicks to add redundancy at any time, even after a simplex system is already deployed (figure 5).

Many vendors offer basic HA redundancy by just adding one more controller, where only the changes are synchronized and there may be a nondeterministic failover time. This is the case for many types of basic PLCs and edge controllers. Some redundancy schemes may place limitations on the number of I/O, field devices, or tag counts.

A more robust configuration incorporates the following characteristics:

- Primary and secondary controllers.
- Each controller in its own rack or location, with a dedicated synchronization communication card using fiber optics, allowing the racks to be located as far as 10 km apart.
- Each rack powered with an independent UPS or other HA power provision, to provide power diversity.
- Complete primary-to-secondary memory synchronization every scan, providing deterministic failover and avoiding HMI blind time.
- Some field device count limitations are acceptable, but full memory and I/O counts must remain available.
- Availability of native use ring-based fieldbus for I/O, such as PROFINET.
- Availability of native secure OPC UA for connectivity to higher-level HMI and SCADA systems.
- Check-box configuration to enable redundancy, with no special PLC or HMI programming needed.
- Ability of users to mix and match hardware, software, and firmware versions at will, and perform upgrades as needed (although maintaining consistent versions is always recommended). The key is to have a matching data synchronization list on both controllers.

Redundant PLC solutions as described in the bullet points above are available and are the best way to deliver true HA for industrial automation platforms. Unfortunately, not all solutions have these capabilities, so buyers must beware.

Comprehensive redundancy is a reality

Industrial controller redundancy has been available for many years, but cost and complexity reserved it for only the most demanding applications. Controller redundancy can

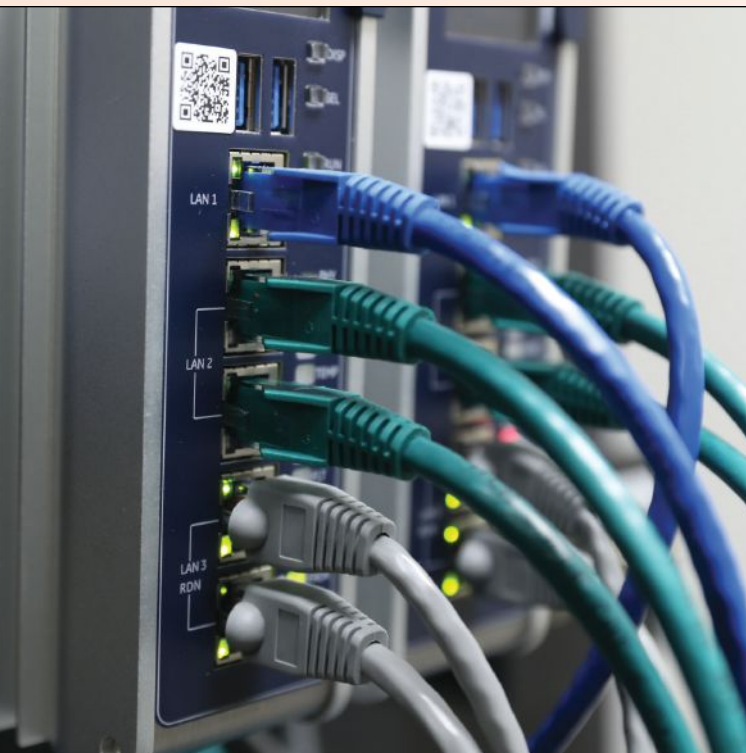


Figure 5. Although redundancy requires extra hardware, users will find that integration effort can vary greatly; some implementations are performed with just a few configuration clicks.

now be implemented simply and cost effectively, making it feasible and practical for many more factory automation and machine control applications.

But simply choosing redundant-capable products is not good enough, because there are many implementation details that can erode effectiveness. Nondeterministic failover schemes and nonsecure communications are not suitable for many applications. In particular, if a redundant system must be stopped for any length of time to upgrade user applications, hardware, or firmware, then the promise of HA is broken.

Once users understand critical controller redundancy design details and strategies, they can make an informed decision and select PLC hardware, software, and networking technology to overcome these challenges and deliver a comprehensive HA controller redundancy experience. With minimal additional hardware investment, sometimes nearly equivalent to the amount of spares that would be ordered anyway, end users can select and easily configure a controller redundancy platform that has the best possible performance. ■

All figures courtesy of Emerson.

ABOUT THE AUTHOR



Vibhoosh Gupta is a portfolio leader for Emerson's machine automation solutions business unit. He manages its portfolio of automation system, operator interface, industrial PC, and Industrial IoT software and hardware products for industrial automation.

RESOURCES

"Edge analytics speed optimization cycle times"

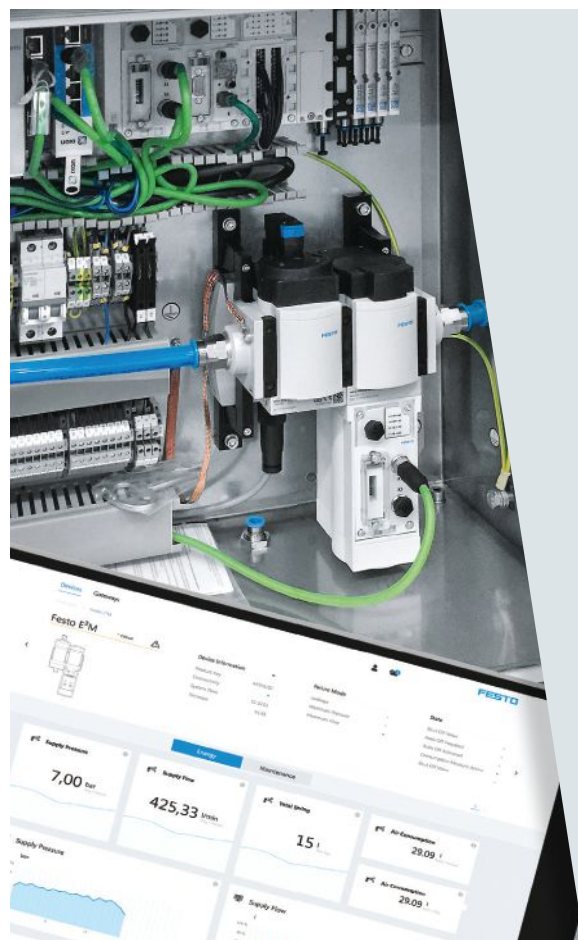
www.isa.org/intech-home/2020/july-august-2020/features/edge-analytics-speed-optimization-cycle-times

"Solving big data problems with a little data approach"

www.isa.org/intech-home/2020/march-april/columns/solving-big-data-problems-with-a-little-data-appro

"Better performance begins at the edge"

www.isa.org/intech-home/2020/january-february/features/better-performance-begins-at-the-edge



FESTO

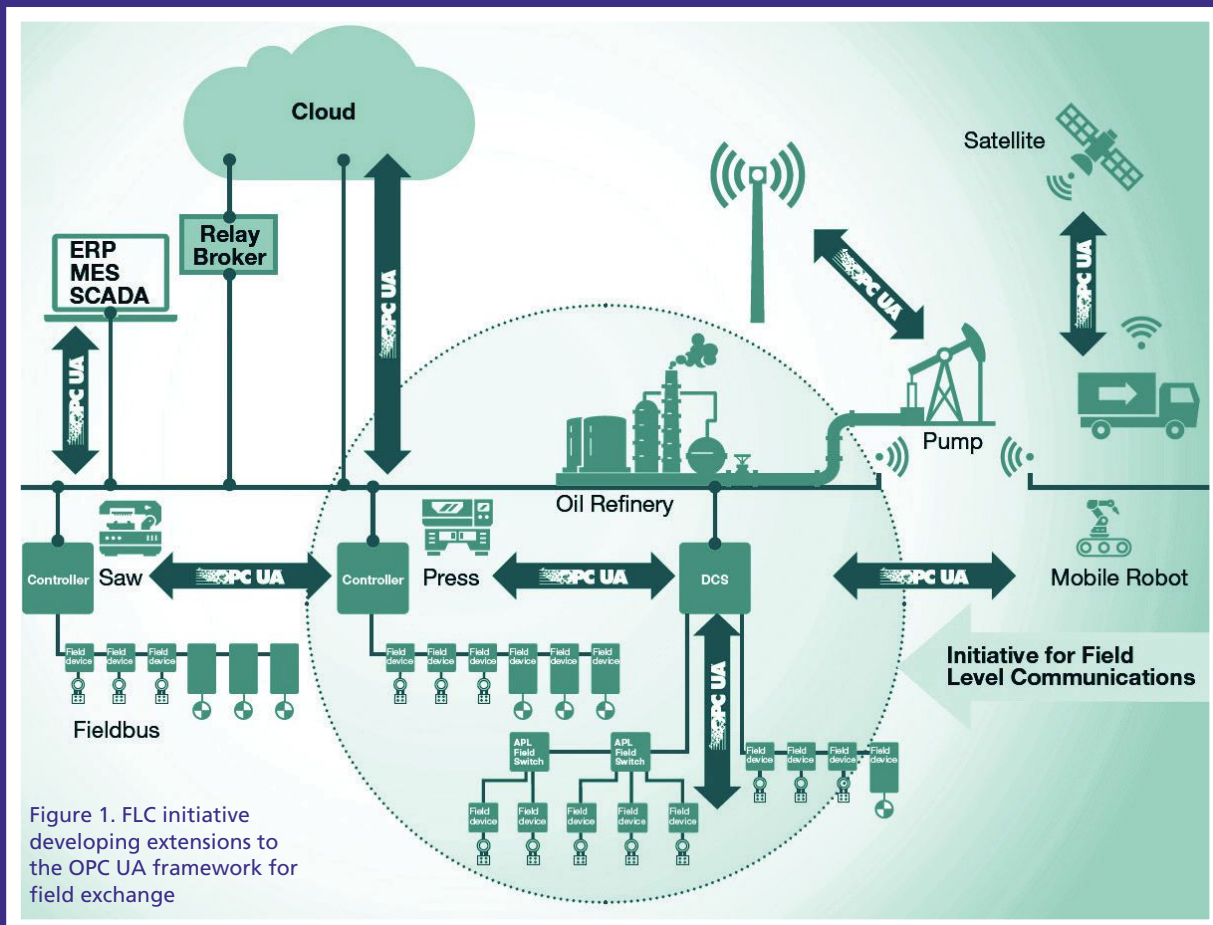
Smart IoT Compressed Air Device Delivers Advanced System Diagnostic and Energy Efficiency

Saving energy is easier than ever before thanks to the MSE6-E2M. Achieve your energy efficiency and sustainability targets while optimizing process equipment performance. Intelligent assembly features include:

- Zero compressed air consumption in standby mode
- Monitors the system for leaks
- Ensures maintenance in the event of leaks
- Enables effective real-time monitoring of relevant process data

www.festo.us

OPC UA – From Automation Pyramid to Information Network



OPC UA including APL, TSN, and 5G for the field: The Field Level Communications initiative reaches a major milestone.

By Peter Lutz

A little over two years after its launch, the Field Level Communications (FLC) initiative of the OPC Foundation has completed the first release candidate (RC1) supporting horizontal communication between shop floor systems. It includes the exchange of real-time and safety-critical data between controllers (e.g., programmable logic controllers and distributed control systems) in a vendor-independent way. This is an important milestone to further develop OPC UA as a uniform and manufacturer-independent interoperability solution for industry that fully scales from field to cloud, including communication and information exchange at the

control and field level (figure 1). For this, OPC UA is taking advantage of enabling communication technologies, such as Ethernet Time-Sensitive Networking (TSN), Ethernet Advanced Physical Layer (APL), and 5G mobile networks.

FLC initiative – Goals and achievements

In November 2018, the FLC initiative was founded under the umbrella of the OPC Foundation. A total of 27 companies, including the largest automation manufacturers in the world, have joined the initiative's steering committee and support it financially as well as with labor and technical know-how (figure 2). The common

goal is to expand the scope of OPC UA to the field level and to establish OPC UA as a uniform and consistent communication standard in factory and process automation. In the technical working groups, which are open to all members of the OPC Foundation, a total of over 300 experts from more than 60 companies are currently working to develop appropriate concepts and specifications.

Work on the first version of the specification has made good progress—despite COVID-19 and the associated restrictions. The basic concepts for the use case controller-to-controller (C2C) have been developed and have been incorporated into a first set of specifications. The initial release candidate has been completed. This so-called RC1 is now used to implement prototypes and to execute interoperability testing to validate the specifications. At the same time, test specifications are being generated. They will later be converted into corresponding test cases for the OPC UA Compliance Test Tool (CTT).

In a second version of the specification, the already developed concepts will be extended for the use cases controller-to-device and device-to-device, so that OPC UA can then be used as a uniform and consistent communication solution for vertical and horizontal integration. This includes field, edge, and cloud (figure 3). This opens up completely new possibilities, especially with regard to the different Industry 4.0 application scenarios and information technology/operational technology (IT/OT) convergence.

Extending OPC UA to the field level

OPC UA framework

The field extensions specified by the FLC initiative are based on the OPC UA framework (IEC 62541), which enables a secure and reliable, manufacturer- and platform-independent information exchange (figure 5). Controllers and field devices support both the connection-oriented client/server communication model and the publish/subscribe extensions, which are indispensable for communication at the field level due to the corresponding requirements for flexibility, efficiency, and determinism. The security mechanisms specified

FAST FORWARD

- The basic concepts for the use case controller-to-controller have been developed and have been incorporated into a first set of specifications and the initial release candidate completed.
- Test specifications are being generated that will later be converted into corresponding test cases for the OPC UA Compliance Test Tool.
- A second version of the specification will be extended for the use cases controller-to-device and device-to-device, so OPC UA can be used for uniform and consistent communication for vertical and horizontal integration.

in OPC UA are also used, which, among other things, support authentication, signing, and encryption of the data to be transported. They can be used for both client/server and publish/subscribe communication relationships.

OPC UA FX – Extensions for field exchange

The initial release candidate of the FLC initiative, completed in November 2020, consists of four specification parts (OPC UA Parts 80–83, figure 4) and focuses on C2C communication for the exchange of process and configuration data by means of peer-to-peer connections and a basic diagnosis. These parts are labelled with OPC UA FX (field exchange):

- Part 80 (OPC UA FX 10000-80) includes an introduction and provides an overview of the basic concepts for expanding OPC UA for communication with and at the field level.
- Part 81 (OPC UA FX 10000-81) specifies the basic information model for controllers and field devices (automation components) and the communication concepts to meet the various use cases and requirements of factory and process automation.
- Part 82 (OPC UA FX 10000-82) describes network services such as topology detection and time synchronization.
- Part 83 (OPC UA FX 10000-83) describes the data structures for the exchange of information



Figure 2. The member companies of the steering committee of the OPC Foundation's FLC initiative

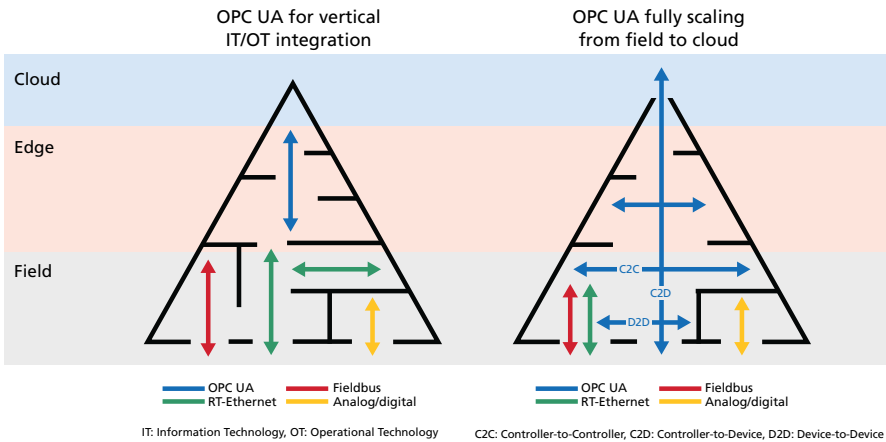


Figure 3. Evolution of OPC UA driving convergence and harmonization in industrial communication

required for offline engineering using descriptors and descriptor packages.

In addition, a 40-page technical paper was published. It explains the overall vision and the technical approach.

OPC UA Safety – Fail-safe communication based on Profisafe

Work on the safety solution for OPC UA (OPC UA Safety) is also very advanced. A joint working group with Profibus & Profinet International (PI) developed a first OPC UA Safety specification based on client-server mechanisms. It was published in November 2019 (Part 15, OPC 10000-15). A revision of the OPC UA Safety specification will be available soon. It will describe the extensions for OPC UA pub/sub and the parameterization of safety devices, including controller-to-device (C2D). OPC UA Safety supports a maximum user data length of 1500 bytes, the creation of any network topology (e.g., star, line, grid), hierarchical safety IDs for simplified management of series machines, and dynamic connection setup with changing partners, such as modular machines, autonomous guided vehicles, autonomous moving robots, and tool changers.

OPC UA Motion based on Sercos and CIP Motion

Progress can also be reported with regard to OPC UA Motion. In mid-2020, a working group started to develop an OPC UA-based motion solution comprising motion control functions for various types of motion devices, such as controllers, standard drives, frequency converters, and servo drives. The FLC steering committee has agreed to base the work on the CIP Motion and Sercos specifications and to adapt them to the OPC UA information modeling and system architecture, considering the relevant Industry 4.0 and Industrial Internet of Things (IIoT) use cases. As with safety, existing concepts and specifications are being used, so the specification work can be significantly accelerated.

OPC UA with TSN, APL, and 5G

OPC UA is much more than a protocol. It is an industrial framework that is fundamentally transport-agnostic, and therefore it can be easily adapted to different transport layers depending on the application-specific requirements and use cases. Key technologies for

bringing OPC UA to the field level are Ethernet Time-Sensitive Networking and the Ethernet Advanced Physical Layer. For OPC UA FX, two communication profiles are defined. One is mapping the OPC UA protocol (UADP) to UDP/IP. The other one is directly mapping UADP to Layer 2 of conventional Ethernet (non-TSN), but also to Ethernet TSN. The latter option is being used to reduce the protocol overhead and to increase the protocol efficiency for demanding automation applications, such as motion control or high-speed I/Os.

By using a universal quality-of-service (QoS) modeling concept, which includes real-time communication capabilities with guaranteed bandwidth and low latencies, information and services can be easily mapped to different underlying transport protocols and physical media. But OPC UA applications using deterministic communication will not be bound to Ethernet TSN only. Wireless communication standards, such as 5G or Wi-Fi 6, support similar QoS guarantees and therefore will also be supported in the future.

The combination with TSN

Using Ethernet TSN facilitates deterministic data transmission via OPC UA, which is particularly indispensable for demanding automation applications. In addition, TSN allows different applications and protocols to be operated using a standardized hardware and a common network infrastructure. This enables the implementation of convergent industrial automation networks in which various IT and OT protocols can coexist. A working group of the FLC initiative is currently identifying which TSN substandards are mandatory for OPC UA-based end devices and infrastructure components to meet the specified requirements for performance, flexibility, and ease-of-use. The OPC Foundation has given a clear commitment to the TSN-IA (Industrial Automation) profile, which the IEC/IEEE 60802 working group is developing. For this reason, the OPC Foundation has entered into liaisons with the standardization bodies IEC SC65C and IEEE 802.1.

| | | | |
|---|--|--|---|
| <p>OPC 10000-080</p> <p>OPC Unified Architecture Field eXchange (UAFX)</p> <p>Part 80: UAFX overview and concepts</p> | <p>OPC 10000-081</p> <p>OPC Unified Architecture Field eXchange (UAFX)</p> <p>Part 81: UAFX connecting devices and information model</p> | <p>OPC 10000-082</p> <p>OPC Unified Architecture Field eXchange (UAFX)</p> <p>Part 82: UAFX networking</p> | <p>OPC 10000-083</p> <p>OPC Unified Architecture Field eXchange (UAFX)</p> <p>Part 83: UAFX offline engineering</p> |
|---|--|--|---|

Figure 4. Initial specifications for OPC UA FX

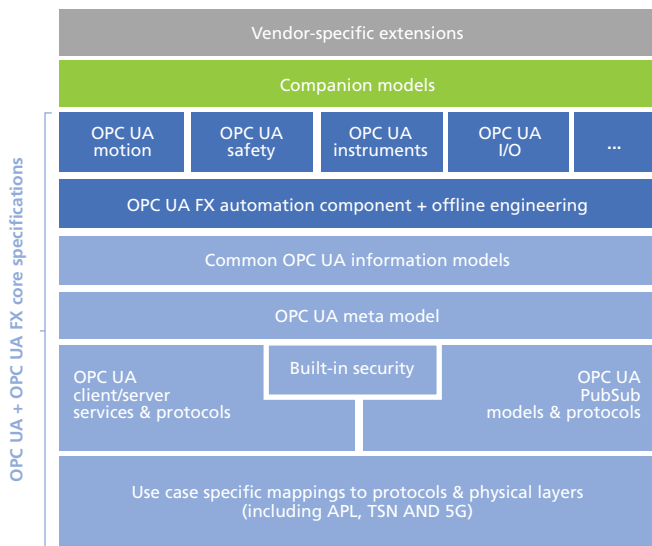


Figure 5. OPC UA framework with extensions for FX using QoS mapping to support different transport options

The combination with APL

Ethernet APL describes a physical layer for Ethernet that was specially developed for the requirements of the process industry. Ethernet APL enables data transmission at high speeds over long distances; the supply of energy and data via a common, twisted two-wire cable; and protective measures for safe use in hazardous areas. This makes Ethernet APL the enabling technology for the use of OPC UA and other Ethernet-based protocols in the process industry.

Due to the special importance of this technology, the OPC Foundation joined the APL project group in June 2020 to develop and promote APL to-

gether with other nonprofit organizations and various industrial partners.

The combination with 5G

Data exchange via OPC UA is not limited to wired or wireless Ethernet communication. Support for the 5G mobile communications standard is also on the OPC Foundation’s roadmap. For this, the OPC Founda-

tion has been working on concepts to include 5G in its quality of service modeling concept to enable the seamless integration of 5G into the existing OPC UA architecture. Furthermore, a cooperation with the 5G Alliance for Connected Industries and Automation (5G-ACIA) has recently been established. The entities will identify and leverage the synergies of combining OPC UA with 5G with the goal of supporting Industry 4.0 and IIoT applications with a reliable yet flexible communication solution.

Information at the data source

The OPC UA (IEC 62541) framework with the extensions for field exchange (OPC UA FX) specified by the FLC initiative,

in combination with underlying communication technologies such as APL, TSN, and 5G, offers a complete, open, standardized, and interoperable solution. It not only fulfills the requirements of industrial communication, but also enables consistency and semantic interoperability from the field level to the cloud and vice versa (figure 6). With this approach—and by adopting additional device companion specifications that numerous organizations all over the world develop—information is made available with standardized semantics directly at the data source, if possible. A flowmeter, for example, offers directly standardized “OPC UA flow measuring data” as soon as the APL cable is plugged in. And analogously, servo drives directly process standardized “OPC UA drive set points” and provide standardized “OPC UA actual drive values” as soon as they are integrated into a machine network with Ethernet TSN. ■

ABOUT THE AUTHOR

Peter Lutz (peter.lutz@opcfoundation.org), director of the Field Level Communication Initiative, OPC Foundation, leads the development of the initiative and specifications. He has led various international projects, initiatives, and consortia that developed and promoted innovative technologies for the benefit of users and suppliers in the industrial market. In his recent past role as managing director of Sercos International, Lutz was responsible for designing, specifying, standardizing, and promoting the company’s automation bus.

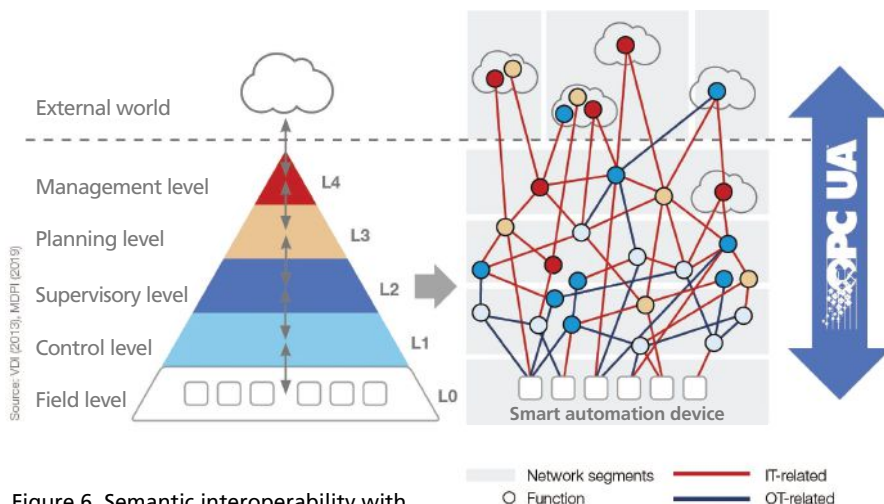


Figure 6. Semantic interoperability with OPC UA from the sensor to the cloud

RESOURCES

FLC initiative

www.opcfoundation.org/flc

FLC initiative technical paper

<https://opcfoundation.org/wp-content/uploads/2020/11/OPCF-FLC-Technical-Paper-C2C.pdf>

APL white paper

https://opcfoundation.org/wp-content/uploads/2020/06/Ethernet-APL_Ethernet-To-The-Field_EN.pdf



Technology-driven Asset Integrity Management Perspectives

Image courtesy of AAEngineering Group, a Bentley Systems
Going Digital Award Winning Digital Twin Project.

By Sugata
Bandyopadhyay
and Shalini
Bandyopadhyay

Business in the twentieth century was driven by unprecedented challenges from continuously changing requirements, more competition, and enhanced regulations for health, safety, and the environment. Thus, aging assets require a recasting of the retrofit methodology to achieve sustainability. This methodology requires a structured approach toward defining the process in line with the new opportunities rolling out. Today is characterized by concepts adopted from Industry 4.0 and 5.0, which have defined the use of a technology-driven methodology to configure the way a sustainable business works. Adopting the best practices and redefining the asset configuration and health is the requirement of the day.

Defining a proper understanding of an asset and addressing approaches for a long-term sustainable business, ISO 55000, 55001, and 55002 have come out with a structured process of managing risks, plant availability, safety, environmental regulations, and financial returns. The standard advocates requiring:

- considerations for continual management of the asset across the life cycle
- risk assessment and management of risk for sustainability
- creating increased value for investment and ensuring financial returns
- creating visibility of the asset across the life cycle
- asset availability and efficient operation
- compliance to regulatory standards
- improved branding.

To ensure a sustainable solution, Industry 4.0 and 5.0 have introduced a package of cutting-edge

technologies, providing visibility across the operation and connecting the plant process, logistics, and supply chain, so all the stakeholders can make proper decisions and act at the right time.

The various approaches introduced by Industry 4.0 and 5.0 may be summarized as:

Cyber-physical systems that connect the world: Connecting people, machines, information, and the organization for integrated operation.


New technology: Adopting disruptive technologies to help adapt products to changing requirements.

Digital twins: Simulation and testing before actual implementation to ensure precision in products and services and faster execution without bottlenecks and delay.

Asset performance management: Used for real-time plant and equipment diagnosis to predict and plan convenient maintenance schedules and eliminate unplanned shutdowns for visibility of the process and equipment.

Product life-cycle management: Integrating and simulating the compatibility of all components/stages of a value-added product in real time and planning for a successful launch. On the other hand, management of an asset from conceptualization, planning, construction, operation and maintenance, upgrading, and demolition, are planned with total visibility across the life cycle.

Total automation driven by Industrial Internet of Things (IIoT): Integrating plant, logistics, and supply-chain management with the process to plan and produce optimally, matching the supply and demand without creating surplus unsalable products.



Sustainable business model for age-old assets in the present decade.

Human-machine collaboration: Collaborative robots enable better precision, faster execution, personalized products, and minimized waste.

Cybersecurity: Ensuring a risk-free cyber-physical platform with continuously upgraded and strong security standards for data integrity for individual organizations and secured data access from public domain or paid sites.

Digital transformation: Enabling a connected process between plant, supply chain, original equipment manufacturers (OEMs), customers, and all other stakeholders to ensure quality, availability of products, a proper feedback system, and customization of products, so there is continuity and a sustainable process with visibility throughout.

Industries need to head toward digital transformation within the footprint of Industry 4.0 and 5.0. The transformation then creates more opportunities in other emerging domains, like industry upgrades by customizing the production path to address better safety, reduced labor, better environmental standards, improved energy efficiency, benchmarked utility consumption, eliminated leakage losses, and 360-degree automation with robotic process automation. Thus, organizations need to focus on asset integrity management to create a sustainable business from all the operating assets by addressing customized requirements; rules for safety, health, and the environment; and other regulatory compliances.

Because greenfield projects require big funds and the volatile situation in the market is delaying long-term forecasts for sustainable business, there are fewer decisions for greenfield projects.

FAST FORWARD

- It is important to have a strategy for generating long-term sustainable business through structured processes for plant assets adopting Industry 4.0 and 5.0 methodologies.
- Use fast-track disruptive technologies comprehensively to drive digitization, digitalization, and creation of digital landscape.
- You need a customizable framework for AIM work processes for civil and structural assets that have surpassed their design lives.

On the other hand, investments are being pumped into the operating industries. They face challenges from nonperforming assets, unsafe conditions, the introduction of more stringent environmental standards, energy efficiency needs, the plugging of leakage losses, etc., which adversely affect technical and commercial viability. As a result, there are enormous opportunities for asset integrity management (AIM) of old assets to create more value.

Goals and objectives of asset integrity management

To establish a structured approach for AIM, the following considerations are necessary, aligning with the guidelines spelled out in ISO 55000, 55001, and 55002:

- asset management across the entire life cycle with total visibility of the asset
- improved availability and elimination of unplanned downtime
- reduced environment, health, and safety risks and adherence to stringent regulations
- enhanced sustainability
- energy efficiency, elimination of leakage losses, and a better bottom line
- better branding.

AIM for plant equipment

Many plants are not performing at the best efficiency, due to issues like aging and using phased-out technology, which cause uneconomic consumption of power and utilities and unexpected trips that disrupt production. The other challenge faced is the requirement of new environmental emission standards, which put an embargo on the operation of much of the polluting equipment and lead to the adoption of changes to combat the same. Through AIM, planned and phased engineered solutions are implemented to address these issues to make the process sustainable from techno-economic considerations.

Apart from refurbishment by adopting technical replacement, AIM adopts an IIoT-based solution, with asset performance management (APM). APM ensures the plant and equipment are more available, with visibility into the health and performance of the whole plant and its equipment and utilities.

This makes the plant not only viable but also more predictable and future proofed.

The APM is IIoT enabled and works on a special algorithm to consolidate disparate data, building a data analytic model and executing condition monitoring of a variety of mechanical equipment and processes, resulting in:

- Web-based access for visibility of the process condition and the asset health and performance of all equipment.
- Asset reliability by analyzing asset status and the evolving maintenance strategy to eliminate unplanned shutdown.
- Working on big data analytics and risk-based strategies to identify critical assets, identifying areas of improvement on the chain of assets based on past trends and minimizing leakage loss, reducing production loss, and ensuring improved efficiency.
- Elimination of human error and equipment malfunction by using expert system tools.
- Root cause analysis on all events applicable for production, environment, health, safety, security, quality, and customer feedback.

Often the process modification is done to adapt to the latest process technology for better performance and sustainability, and adoption of APM creates more predictable performance and availability.

The culture brought by APM creates enhanced product quality, improved efficiency, minimized downtime, better reliability and safety, an improved environment, and customer delight.

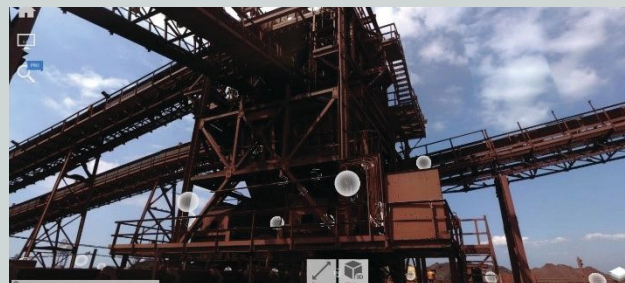
AIM through automation

Today, reduced human intervention has become the driving factor when configuring the automation system. For this, more visibility into the process is needed, including the health of the equipment, the inflow and outflow of raw material, and intermediate and final products, to optimally run the plant. Thus, IIoT-driven, web-enabled field instruments (edge devices), communication media, a secured cyber-physical network, the creation of big data, and a data analytics-based approach give both predictable and the most-efficient plant performance, ensuring better returns.

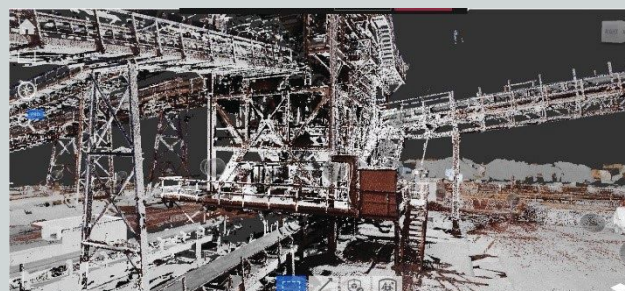
Introducing a robotic interface for carrying out plant operation and construction activities brings better precision, faster operation, and less human intervention. Presently, collaborative robots (cobots) are gradually being deployed across the industries with remarkable results. The construction approach is further automated using laser precision, automated welding, testing, and CCTV-based monitoring of the process and operation. Technology-driven investigations also limit human interventions with lesser execution time.

While designing plant automation, considerations are for a holistic approach for total connectivity, remote control and monitoring, inbuilt fail-safe conditions, and predictability. Plants want to create improved operation with benchmarked data for all plant and equipment through cloud-based access to big data, data analytics from OEMs, and other similar models. Automation also integrates the in-house process, plant logistics, supply chain management, customer connections, demand-

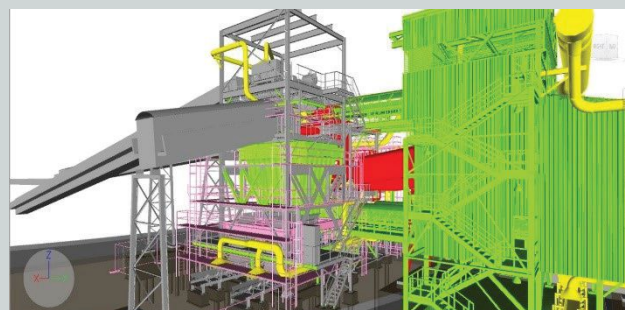
A pictorial representation of the various stages of the project



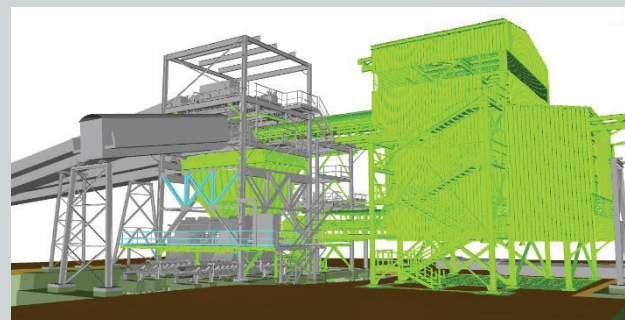
Asset site photograph



Three-dimensional laser scan data of asset



Engineered model created from 3D laser scan adding scaffolding plan and safety fencing



Engineered 3D model depicting completed work

supply analysis, and optimized operation.

The integrated network ensures plants meet all safety standards, environmental guidelines, and applicable statutory processes. Further, automated event reporting and autocorrection are implemented for any deviations from the benchmarked data based on artificial intelligence-enabled expert systems with continuous machine learning by tracking the ever-changing

process and requirements.

Thus, AIM is a necessity and not a choice in the present competitive environment. The most pressing challenge is for personnel to have an ever-changing mindset to stay ahead of the changes. The workers need to upgrade themselves with newer technology-relevant skill sets to create better opportunities. Continuous training and workforce development will bridge gaps between available talent and the most pressing requirement for skilled resources.

AIM for civil and structural assets

The civil and structural part of an asset does not contribute directly to daily production and, as a result, does not receive as much attention for continuous maintenance. During their life cycles, these assets pass through cyclic or continuous stress, corrosive and dusty environments, and often face accidental impacts, causing issues such as corrosion-driven section loss, delamination of structural elements, damaged sections, spalling of concrete, and deterioration of base plates and foundation bolts. This renders the overall asset risk prone. Depending on the severity of the risk, classification of risk becomes necessary to ascertain whether immediate or delayed action for corrective measures is necessary.

As information about the old running plants is not always available, companies are adopting a technology-based approach to capture data and transfer it to a digital platform. A 3D-based engineering solution is carried out for the retrofitting work.

Strategic approach for AIM work process

While deciding on the work methodology to retrofit an existing asset, the stakeholders need to evaluate the asset with respect to its present health conditions, its ability to perform with the planned upgrade (maintaining safety and abiding by all environmental and regulatory compliances), and its ability to generate sustained revenue. If the asset does not meet any of the above requirements, considerations to adopt alternative technology by upgrading or replacing some part of the main equipment may be necessary. The stakeholders need to evaluate the investment versus return for sustainability. Further, while planning for the work, issues like constructability, occupational safety in a running plant, deployment of specialized construction tools, hazardous waste detection, and management need to be given prime attention.

AIM work methodology

Phase 1: Comprises inspection of assets, identification of defects based on the severity of damages, classification of risk, and the creation of a risk register.

Phase 2: Includes hazardous material (e.g., asbestos, lead) identification and creating a process for elimination.

Phase 3: In addition to physical surveys, includes a detailed investigation based on 3D-laser scans, drone-based data collection for unapproachable areas, and underground mapping. The information is transferred to the “as is” condition of the asset (digital twin) in a 3D-engineering platform. For major plant equipment, evaluation of performance, efficiency, reliability, and trip history are analyzed to classify the type of retrofitting to be

done. There is also a study of the visibility of the process operation and major equipment health monitoring, level of automation, and possibility of introducing advanced automation to minimize human intervention and increase efficiency. Equipment and devices using phased-out technology and those with the possibility of introducing energy-efficient processes are also explored.

Phase 4: New constructions and items to be retrofitted are identified by color based on the “as is” condition and the risk register report creation of an engineered solution in the 3D platform. The temporary works, such as scaffolding, crane access, safety netting, safety fencing, electrical isolation, and grounding, are all depicted.

Phase 5: The 3D model depicts the completed status of the asset. Also, the construction drawings, including the structural fabrication drawings and the reinforced cement concrete bar bending schedule, are created. The mechanical, electrical, and automation construction drawings are also formulated. The 4D sequencing video is to align stakeholders with the sequence of execution of the job in an audio-visual platform.

Phase 6: The documentation part of the project submittals includes the project overview, various site investigations, all safety risks, asbestos or lead-based paint identification and isolation, enabling activities, waste management, instruction to the bidder and also to the selected contractor, cost estimate, project execution schedule, the deployment for construction equipment and tools, requirements for personal protective equipment and safety gears, and the construction sequences and maintenance regime.

There is a Quality 4.0-compliant checking process at each phase that adheres to regulatory provisions and safety, health, and environmental regulations to ensure international standard compliance. This gives construction agencies a comprehensive roadmap for retrofitting the damaged assets.

The entire conglomeration of project submittals creates visibility into the tangible and intangible investment benefits and the roadmap for project implementation. ■

Acknowledgement: Thank you to Tata Consulting Engineers for giving us the platform to carry out the work.

ABOUT THE AUTHORS

Sugata Bandyopadhyay (sbandyopadhyay@tce.co.in), consultant and engineering manager (asset integrity management), Tata Consulting Engineers Limited, has 41 years of experience in automation and multidisciplinary project management and execution. He holds BSc, BTech, and ME degrees, is a Fellow at Institute of Engineers (India), and is a Senior Member of ISA. Bandyopadhyay is a visiting professor and member of board of studies in various engineering colleges. His interest areas are Industry 4.0 and 5.0, IIoT, and digital transformation and application.

Shalini Bandyopadhyay (shalinir@tce.co.in), senior manager (civil), Tata Consulting Engineers Limited, has primarily worked as a civil and structural engineer for the past 13 years. She is the lead engineer in AIM assignments and holds a B.E. (civil) from Jadavpur University, an MBA (finance) from ICFAI University, Tripura. She is presently pursuing an MTech (environmental engineering) from BITS Pilani.



Automation Systems Cybersecurity: From Standards to Practices

From first steps to a sustained response.

By Eric C. Cosman

Improving the state of cybersecurity in critical infrastructure has been a well-understood imperative for many years. Even without evidence of deliberate attacks, this should be considered an important aspect of improving system resilience. Although challenges have existed since the earliest days of using commercial-off-the-shelf (COTS) technology in industrial automation systems, it was not until the early 2000s that significant attention was given to potential compromises to system security. Since then, there has been significant progress in this area, but there is still much to be done.

Standards, guidance, and direction are available from several sources, but surveys and anecdotal reports have shown that many still struggle with how to turn this information into

effective programs. Suppliers have a clear imperative to improve their products, but asset owners often struggle with how to get started.

Awareness is there

Considerable effort has gone into raising awareness of the potential risk that comes with increased connectivity and the use of popular operating systems and networking technology in the monitoring and control of critical infrastructure. This conversation was initially confined largely to the engineering and operations community, but it expanded quickly, first to the community of cybersecurity experts and ultimately to the popular press. Significant attacks and events continue to get broad coverage.

Those responsible for automation systems in

critical infrastructure and other industrial sectors are now generally aware of the potential risk. Unfortunately, it is common to place more emphasis on the threat and vulnerability components of risk than on possible consequences. While general statements can be made about such consequences, only the asset owners can identify these for their specific situations.

Standards available

Increased awareness has led to the development of a variety of standards and associated practices for industrial cybersecurity. Some of these are specific to individual industries or sectors, while others are more broadly focused. Unfortunately,

the form of cases studies. Whenever possible a selective or incremental approach is preferred. All elements of the guidance should be categorized as essential or optional.

It may sound obvious, but guidance must also be actionable. While standards may state what must be achieved without too much regard to the methods used, guidance should address not only the outcome and applicable metrics but suggest suitable methods. Assuming that metrics are available, there must also be a means for measuring and reporting progress. Of course, there are several sources of useful guidance already available from various sources. None of these are suitable for all situations, so some

Standards and practices are necessary, but not sufficient. Essentially, they should be considered as reference material and not step-by-step instructions.

as with any other technical subject, specialized expertise is often required to understand these standards. They are seldom written to be used by those without such expertise. Compounding the challenge, the requirements for establishing and maintaining a secure configuration can be quite complex, addressing a combination of technical capabilities, processes, and procedures.

Fully understanding these requirements and applying them to a specific configuration is often beyond the capability of the asset owners, requiring them to purchase professional services. Purchasing such services or creating projects to improve security requires that the necessary resources be justified in business terms.

Practical guidance required

Standards and practices are necessary, but not sufficient. Essentially, they should be considered as reference material and not step-by-step instructions. They capture effective and proven engineering practices, often employing clear use cases. They are certainly not prescriptive, as they must be written in a manner that allows for the broadest possible application and are developed on a timeline that is far too long for most people.

Practical guidance is somewhat different and must be based on the requirements and performance levels defined in standards. To be applied, it must be reasonable from the perspective of those applying it. This is a somewhat subjective measure, but in general it means that it should be possible to apply it without excessive complexity or effort. Guidance is often described in

selection and evaluation are required.

Perhaps the most well-known example is the NIST Cybersecurity Framework (CSF). It has a step-by-step approach to addressing cybersecurity with an implicit assumption that it is being done in response to an anticipated or actual attack or event. Another common request is for a “checklist” that contains simple steps that should be taken to improve security. Several of these have been developed, but perhaps the most popular is the “Top 20.” Such lists do not constitute a comprehensive response, but they do cover several simple and valuable measures that almost anyone can take. There are also several sector-specific sources of guidance of effective cybersecurity. Examples include NERC CIP for the energy sector and Responsible Care® for the chemical industry.

Why not more progress?

Given that several standards have been developed and practices are available, it would be

FAST FORWARD

- For several years there has been a strong focus on the development of standards by several organizations. While certainly essential, they are not sufficient.
- There has also been considerable attention given to threat identification and vulnerability disclosure and mitigation. Again, this is necessary but not sufficient.
- Practices will ultimately be determined by asset owners. Absent regulation, they will be motivated by proof that consequences are worse than the effort expended.

reasonable to ask why there has not been more progress in securing critical systems. There are likely as many answers to this question as there are circumstances, but there are some common themes.

Just as with any proposed project or initiative, cybersecurity programs must be supported with a solid business case. Those building such a case encounter several common questions. Perhaps one of the first of these is whether a cybersecurity program should be the responsibility of the information technology (IT) function or assigned to operations or engineering. The “either/or” premise of this question is flawed, because the reality is that experience, resources, and expertise will be required from these and other organizations.

Even if the organizational alignment and accountability is clear, there will still be the fundamental question of why cybersecurity improvements must be made, or why now. This is best answered with a risk assessment, described in more detail below.

How to start?

Gaining general support for a cybersecurity program or response is only the first major hurdle. Once resources are available, those charged with designing and implementing such a program often find it difficult to find the best approach. A common question is “How or where do we start?” This requires a simple and direct response that spells out a step-by-step approach with suitable metrics at each stage.

There is often a temptation to structure the response as a project, but this will only be effective until the basic processes are in place. From that point on, cybersecurity must be conducted as an ongoing program. Although the response must be long term, these costs may be managed, just as they are for programs like quality improvement or safety.

Before you can secure a system or set of assets, it is first necessary to have complete information about those assets. All must be not only identified, but also described in terms of a defined set of relevant attributes. These include the obvious ones like name, location, and network address, as well as others that may not be so easily available.

Asset owners seldom have the time or resources required to maintain a comprehensive system and component inventory. Depending on size and complexity, the first response may be to retain a services company to collect the necessary information. Even in medium-sized systems, manual collection is impractical unless it includes provisions for detecting and recording changes. In all but the smallest and simplest installations it is problematic or even impossible to collect this information manually. This is one of the first opportunities addressed by new and existing suppliers.

The next step is a risk assessment that identifies possible consequences, as well as threats and vulnerabilities. Even after accepting that threats and vulnerabilities exist, many will be tempted to say, “it won’t affect me.” While it may be true that a particular facility may be an unlikely target, this does not mean that it cannot become “collateral damage” in an untargeted attack. There are many different approaches and methodologies for conducting risk assessments. In some cases, principles and techniques have been adapted from those used in other disciplines, such as functional safety.

Some of the earlier attempts to assess cybersecurity risk were developed by service providers. In many cases, these were initially viewed as proprietary or a source of competitive advantage. This eventually began to change with the release of textbooks, guides, and standards. Even with a clear methodology, the process for risk assessment may be difficult to replicate on a large scale.

Then what?

It is at this stage that many programs stumble and fail to achieve the support and momentum to make them sustainable over the long term. There are likely many reasons for this, but a common one is that the focus does not shift from the decision makers to those who must execute the program. This cannot be limited to IT staff but must include those who are ultimately accountable for operations availability, reliability, safety, and performance. Those responsible for program execution must know where to go to get guidance and have their questions answered. They must trust these

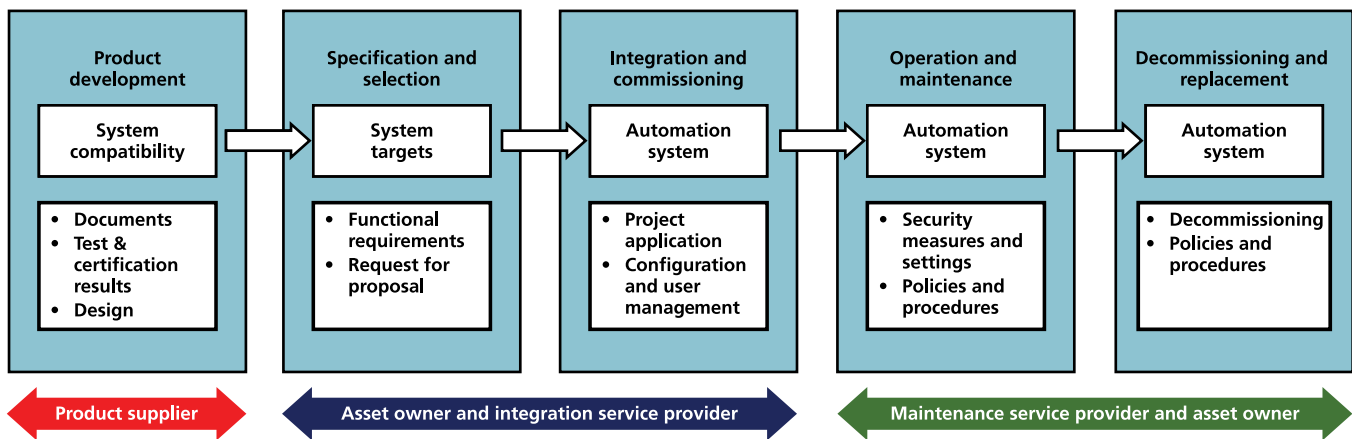


Figure 1. Life cycle

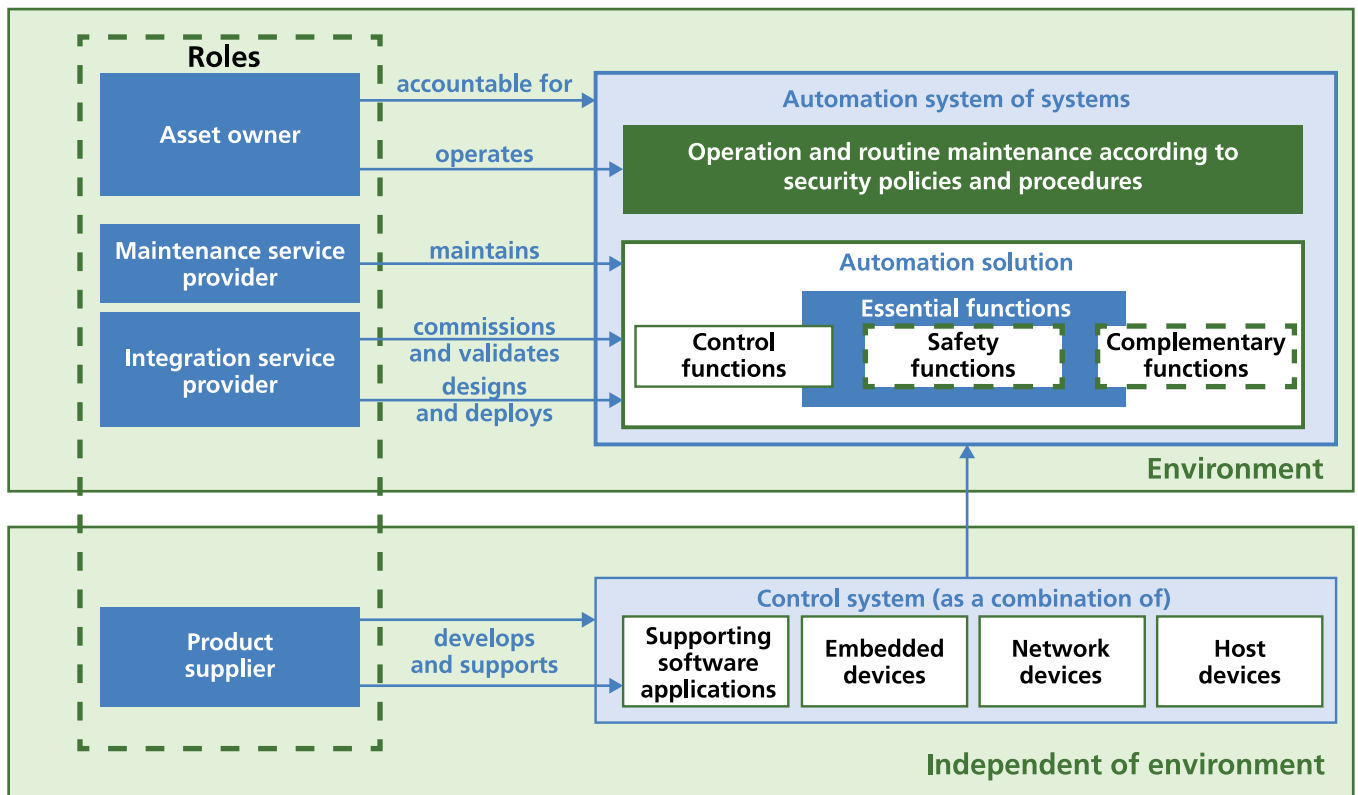


Figure 2. Principal roles

sources as being knowledgeable and appreciative of the constraints and realities that are inherent to their environment.

Answers, rationale, and explanations must also be delivered in terms that operations personnel can understand. Security experts must be able to check their complex jargon at the door, shifting to language that makes sense for the environment. Along with using appropriate language, it is also important to avoid rationale that appears to be based on a theoretical view of ideal security. Balances will have to be struck, and compromises made.

Finally, the detailed requirements spelled out in standards and practices should be seen as a source of reference and subject to some level of interpretation. They are used as references in developing more detailed policies and procedures that are tailored for the specific situation.

It is at this point that several of the questions posed earlier tend to reemerge. One of the first reactions may be to challenge the reality of the risk. Further analysis and explanation may be necessary to convince decision makers.

In all but the simplest configuration there will also be an inevitable question about how to prioritize imperatives and sequence the response. The results of the risk assessment are a major component of this analysis, but other factors may also have to be considered, such as the age and supportability of installed components and devices and the criticality of the application.

Focus on fundamentals

While there is no single approach or method when establishing a cybersecurity program that guarantees success,

there are some fundamentals that are both common and essential.

Life cycle

The first of these is the use of a clear life cycle of the system under consideration, stretching from conception and specification through operation and support. The purpose is to provide a framework for the identification and definition of the required processes and those who execute them.

There are many models that could be used to describe such a life cycle, but standards such as ISA/IEC 62443 have adopted a “system of systems” approach that is adapted from the IEC 24748 standard.

This model shows the life cycle of automation systems as consisting of several steps or phases, beginning with product conception and requirement specification and ending with eventual decommissioning and replacement. At each step there must be clear accountability and responsibility and also well-defined conditions for proceeding.

Principal roles

For each life-cycle phase, it is essential to define the scope and specific responsibilities required for the situation. Although detailed role definitions will vary from one situation to another, standards can also be used to identify the principal roles required in a generic sense. The ISA/IEC 62443 standards have identified the principal roles shown in figure 2.

This diagram shows the primary responsibility of each of these roles with respect to each of the components of the system and its environment. It is also very important to understand and appreciate that the cybersecurity response is part of a much larger program of asset protection.

For installed systems, the asset owner has principal accountability for the automation system. This role is also responsible for the operation of this system. The integration and maintenance service providers are responsible for execution of the processes in their respective phases of the life cycle. The product supplier is accountable and responsible for the execution of the processes used to specify, conceive, and develop the automation systems and associated products.

The standards describe each of the life cycle stages and roles in more detail, as well as how they provide the foundation of an effective program. Examples and derivative case studies will also be used to give more practical guidance.

Resources

Regardless of the life-cycle phase or the specific roles involved, it is important to consider all possible approaches to providing the necessary resources. Depending on the situation, roles may be assigned to internal staff, contracted contingent staff, or delegated using purchased services.

Resource availability is of course always an important factor to consider. All resources are limited, whether they are financial or human.

Taking all the above into account, it should be apparent that the exact approach used must be tailored to the environment. The approach should draw from practices proven to work for general purpose information security while adapting them as required for an environment where protection of information may not be the primary concern. There are several elements to consider in formulating this response.

In all but the simplest of cases, the approach must be both scalable and repeatable. The number of automation and other operations systems in a company may be very large and widely dispersed geographically. In such cases, there may also be a desire to be able to compare performance and needs across a fleet or facility.

Effective cybersecurity

The challenge of establishing an effective cybersecurity response may be complicated, but it is not intractable. Just as with any continuous improvement program (e.g., safety, quality, preventative maintenance), the first step is to define the scope in terms of inventory and level of improvement required. Standards define what is required, and guidance provides examples of how to proceed. Security experts are available to provide program definition as a service. Asset owners must first focus on defining potential consequences as the basis for their business case. ■



ABOUT THE AUTHOR

Eric C. Cosman (eric.cosman@oitconcepts.com) is the founder and principal consultant of OIT Concepts LLC, providing advisory services in the management of information technology solutions in operations and engineering. The 2020 ISA president, Cosman was also the vice president of Standards and Practices and an executive board member at ISA. He is an industry

leader in the development of standards and practices for industrial control systems security. He co-authored the American Chemistry Council strategy for cybersecurity and is a founding member and current co-chair of the ISA99 committee on industrial automation and control systems security.

RESOURCES

NIST Cybersecurity Framework

<https://www.nist.gov/cyberframework>

The “Top 20” Checklist

https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense

IEC 24748 standard

<https://www.iso.org/standard/72896.html>

ISA's Relationship to IEC Standards

ISA actively participates in the world's primary international standards system as sanctioned by the United Nations and operated by the Geneva-based International Electrotechnical Organization (IEC) and International Organization for Standardization (ISO). This relationship with IEC and ISO adds a layer of complexity to what many already find to be the sometimes-confusing world of standards.

Much of the confusion stems from the fundamentally different member structures of ISA standards development as opposed to IEC/ISO. Participation in ISA standards is based strictly on individuals—and is open to automation professionals from any country (not just the U.S.). IEC and ISO programs, in contrast, are based on participation by and through countries acting as single members.

That difference means that ISA cannot participate directly in the IEC/ISO systems, but rather must channel its input through a specific country to do so. That country is the U.S. by way of the American National Standards Institute (ANSI). ISA is accredited by ANSI to develop consensus industry standards following approved processes that ensure openness and balance. ISA is one of more than 250 standards-developing organizations based in the U.S. (such as ASTM, ASME, UL, and others) that are accredited in this way by ANSI.

In relation to the IEC and ISO, ANSI serves as the official "national standards body" of the U.S. That is, ANSI acts as the official representative ("National Committee") to the IEC and ISO of those 250+ accredited U.S.

standards developers. Similarly, other IEC and ISO members are the national standards bodies of participating countries such as Brazil (ABNT), U.K. (BSI), Japan (JISC), Canada (SCC), Germany (DKE), and so forth.

Per the topic division between the IEC and ISO, ISA's primary areas of standards development are covered by the IEC. Through

tween ISA and IEC—but not the only one, because occasionally ISA standards committees decide, through review and voting, that existing IEC standards are suitable for adoption (sometimes with modification) as ISA standards. For example, in 2018 the ISA84 committee adopted IEC 61511-2016 (which had been developed by IEC com-

ISA is accredited by ANSI to develop consensus industry standards following approved processes that ensure openness and balance. ISA is one of more than 250 standards-developing organizations based in the U.S. that are accredited this way.

ANSI as the "U.S. National Committee to the IEC," several major series of standards developed by ISA have been submitted to the IEC to become major IEC series of standards with the same titles, including:

- IEC 62682: Management of Alarm Systems for the Process Industries (ISA-18)
- IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector (ISA-84)
- IEC 61512: Batch Control (ISA-88)
- IEC 62264: Enterprise-Control System Integration (ISA-95)
- IEC 62443: Security for Industrial Automation & Control Systems (ISA-99)
- IEC 62734: Wireless Systems for Industrial Automation (ISA-100)
- IEC 63303: Human-Machine Interfaces for Process Automation Systems (ISA-101)

This development of ISA standards into IEC standards is the primary relationship be-

mittee SC65A with substantial input from ISA84 members) as ISA-61511.

Adoption of an IEC standard by an ISA committee in this way can create another source of confusion for ISA members. A major attraction and benefit of ISA membership is free viewing of ISA-copyrighted standards: www.isa.org/free-viewing-by-members. However, when ISA standards committees decide to adopt an existing IEC standard as an ISA standard (such as the example of ISA84 and IEC 61511), the controlling copyright of the adopted standard (ISA-61511 in the example) remains with the IEC. For that reason, ISA members do not have free viewing access to IEC standards that have been adopted by ISA. This restriction, which applies only to the small number of standards that ISA has adopted from the IEC, is driven by copyright law. ■

IEC Study Group Issues Ethics AI/AS Recommendations

In 2019, the IEC launched a study group, Standardization Evaluation Group 10, to identify ethical and societal issues and make recommendations relevant to IEC technical activities involving autonomous systems (AS) and artificial intelligence (AI) applications.

The resulting report, issued in early May, includes a primary recommendation that the IEC form an oversight committee on ethics—but one not focused on ethics of AI/AS alone, but the impact of ethics in all areas of IEC standardization. AI and AS will be key concerns, however. The oversight committee is expected to begin by developing an IEC guide, "Ethical Aspects for AI – Guidelines for their Inclusion in Standards," to provide guidance on how to identify potential issues of ethical concern and minimize or mitigate the ethical risks that may result from the use of AI/AS.

If you are interested in joining an ISA or IEC standards committee or have any related questions, please visit www.isa.org/standards or email crobinson@isa.org. ■

Meet 2020 ISA Fellow John Sorge

Until his retirement, John Sorge was principal research engineer in Southern Company's Research and Development organization. He has been an active member of the electric power generation instrumentation and control (I&C) community for more than 37 years.

Sorge began his journey into the instrumentation and control research realm by earning a degree in mechanical engineering at the University of Alabama. His linear control design professor, Dr. Youngblood, who later became his advisor, encouraged him to focus on design and simulation. "Dr. Youngblood worked with the Air Force, and I assisted him on a couple of contracts involving air-to-air missile guidance optimization," he said. "Due to his encouragement and connections, I obtained summer employment doing control V&V [verification and validation] studies on space shuttle main engineer controllers then undergoing testing at NASA's Stennis test facility."

Later in his career during the late 1980s and 1990s, Sorge became an integral member of the research effort that led the industry in the U.S. Department of Energy's Clean Coal Technologies demonstrations of NO_x reduction technologies. These demonstrations influenced the rulemaking and the eventual deployment of these technologies by utilities.

Sorge served as Southern Company's advisor to the Instrument, Controls and Automation program of the Electric Power Research Institute (EPRI) from its inception in the late 1990s until his retirement in late 2018. He also served as utility chair of that program for more than 10 years during that period. In collaborating with EPRI, Sorge participated in demonstrations of many varied technologies, including advanced controls, simulators, wireless sensors, and

fleetwide monitoring, as well as demonstrations of Southern Company's Monitoring and Diagnostic (M&D) Center.

Sorge became an ISA member in 2009. "I participated in the ISA Power Industry Division [POWID] almost every year through my retirement in 2018," Sorge explained. He served on standards committees; developed conference technical sessions; served as program chair for the annual POWID Symposium; and authored or coauthored more than 75 technical papers. "Most of my standard engagement has been with ISA-77.22, *Power Plant Automation*, and ISA-100, *Wireless Systems for Automation*," he said.

In recognition of his contributions toward the development of engineering concepts in the field of instrumentation and controls for the advancement of electric power generation, POWID recognized Sorge in 2016 with its Achievement Award. POWID also recognized him in 2018 with a Service Award. That year, the ISA Birmingham Section nominated him for the Engineering Council of Birmingham Engineer of the Year award, which he received in February 2019.

Sorge said he is proud that he had the opportunity to work on interesting topics with his colleagues over the years. "I hope that I was able to return, in some part, the favor by providing guidance to student interns and colleagues who were in the initial stages of their careers," he said. Now, he said he would advise young engineers that "if an opportunity for interesting and rewarding work makes itself available, consider it and take the risk." ■ —By Melissa Landon



In Memoriam: Samuel M. Herb



Samuel Martin Herb, PE, passed away peacefully in his sleep at home in New Britain, Pa., on 3 May 2021. He was 82. Born in Philadelphia on 29 November 1938, Herb held a BS/EE from Drexel University, was a senior life member of ISA, served six years on the faculty of Spring Garden College, Pa., and consulted with several companies. An author of dozens of journal articles

and technical papers for a variety of professional societies and technical publications, he developed and presented talks, seminars, and courses in instrumentation for more than three decades.

He was a member of the ISA95 committee, developed five online courses and CDs on control systems, and received the ISA Eagle and Distinguished Society service awards, as well as the Donald P. Eckman award for education excellence. His ISA publications include co-author of the textbook *Understanding Distributed Process Control*, author of chapters in *Practical Guide Series*

on *Continuous Control*, and author of the textbook *Understanding Distributed Processor Systems for Control*, from which seven "mini-books" were developed.

Herb worked in the utility and process controls industries for nearly five decades and was the owner of JAOMAD Consultancy. He had previously worked at Invensys Process Systems, Honeywell, Leeds & Northrup, Moore Process Automation, and Siemens. His background ranged from design and testing of components within instrumentation to responsibility for overall product line viability. For more than a quarter century, he was involved with microprocessor-based distributed process control systems.

He was most recently adjunct professor of process technology at Salem Community College in N.J. and was deeply involved with his faith and his church. Boy Scouts were also central to his life, as was a lifelong passion for trains. He was the son of the late Samuel F. and Mildred V. Herb, the oldest of four siblings, husband to the late Judith A. (Oeach) and companion to Mary Anne Devine, and the father of four children and grandfather of six. ■

ISA Virtual Conference Explores Evolution of Process Analyzers and More with JD Tate Keynote

Speaking via computer to a virtual room full of process engineers and instrumentation professionals, JD Tate, PhD, kicked off the ISA Analysis Division Virtual Conference (<https://virtualad.vfairs.com/en/hall>) with a presentation containing classic truisms, current challenges, and the continuing evolution of process analyzers that he dubbed an “unfinished revolution.” The virtual event, part of ISA’s Process Control & Instrumentation Series, was a pandemic-era extension of what had been a successful live conference and tradeshow in years past.

Tate’s long career as senior technical leader for Dow Chemical’s Process Analytical team—one of the largest of its kind in industry—made him perfectly suited to present the keynote speech for this virtual event that, on 23 March 2021, brought speakers from Dow, Insight Analytical Solutions, Informetrix, COSA Xentaur Corporation, and others to discuss the state of the art of online analyzers and the people who run them.

“We are all here to make money and to do it safely and responsibly,” said Tate. “You must manage all these competing constraints. The trend is to install more measurements, not less.”

What’s driving change in industry is something many will recognize,” he added. “At Dow we started off with about 15,000 analyzers in 2003, and [we have] more than 22,000 in 2020. Our assets have gone up. The resources used to support these assets have been cut by 75 percent. Expertise and resources have gone down, and there’s a limitation on how efficient you can be supporting those assets. Something has to change.”

Many of the crackers used in the industry are relatively old, so users face the challenge of retrofitting them—upgrading their capabilities

in the current paradigm. Though the current practice involves sending someone into the field to check the health of the equipment, the future will involve digital systems that allow a person to check on the health of the system from anywhere in the world, Tate said.

“It used to take an act of Congress” to add something with wireless capabilities to a plant, “but today, most facilities have whole teams to manage wireless capabilities,” Tate said.

However, the move to wireless assets comes with its own set of problems. For example, production, shipping, installation, operational security, data security, and reliability—as well as finding the expertise to troubleshoot issues relating to new devices. These devices are complicated, and they are all different, Tate said. They are not like cars that all operate similarly. Unfortunately, many process instruments have lots of moving parts, are expensive to install, are highly customizable, and require skilled experts to maintain.

Tate predicts that automated self-diagnostics, preventative maintenance, and remote support will help inform the new model for online process instruments. Hopefully, as we work to standardize online process instruments, there will be a focus on building on modern open protocols, creating platform-agnostic tools that are not dependent on environment, maintaining a security mindset, and prioritizing ease of use, he said.

Other presentations and papers in the virtual conference covered spectroscopy, chromatography, electrochemistry, and sample handling, focusing on how to succeed in today’s challenging environment. Register to view the entire program on demand via <https://isaautomation.isa.org/virtual-events-program>. ■

—By Melissa Landon

In Memoriam: William L. Mostia, Jr.



William (Bill) L. Mostia, Jr., PE, passed away on 5 May 2021.

He lived in League City, Texas and, following a military funeral, was laid to rest on 12 May 2021. Mostia was named an ISA Fellow in 2013, had been a member of the ISA84 committee since 1987, and was a signatory of the two versions of that standard. He was also a member of several other ISA standards

committees. In 2018, he won the Raymond D. Molloy Award for his book, *Troubleshooting: A Technician’s Guide, Second Edition*, which outsold all other ISA books published in 2017.

“Bill contributed the new motor shutdown annex for the upcoming edition of ISA-TR84.00.02, and he had a practical, field-proven belief in maintenance that supported the ISA-TR84.00.03 effort from its earliest edition,” according to Angela Summers, president of SIS-

TECH Solutions, LP. “He contributed the extensive instrumentation fundamentals appendix in CCPS’s *Safe Automation of Chemical Processes* book, covering field sensors through final elements, [but] his interests and contributions were broader than these topics. He published many papers on various control system topics over the years and had become very interested in artificial intelligence and IIoT. Bill mentored many of us on this committee over the years.”

Mostia had more than 45 years of experience in the process industries, primarily at petrochemical companies including BP, Amoco, Texas Eastman, and Dow Chemical Co. He had extensive experience in process safety, safety instrumented systems, electrical safety and grounding, cybersecurity, instruments in hazardous areas, and PLCs.

In addition to his book on technician troubleshooting, he contributed to books such as ISA’s *A Guide to the Automation Body of Knowledge, Third Edition*. Mostia was a registered Professional Engineer in the State of Texas (1982) and had a BSEE degree from Texas A&M University (1977). ■

Student Section Develops a Women's Safety App

Archit Kohli is the president of the ISA Mukesh Patel School of Technology Management and Engineering (MPSTME) student section in Mumbai, Maharashtra, India. The ISA MPSTME section aims to create meaningful networks between students and institutions, with the goal of increasing student participation and interest in automation and related fields.

Most recently, Kohli and other members of the MPSTME student section set their sights on developing an app to address women's safety in India. ISA sat down with Archit to discuss the specifics of building this app—and the MPSTME section's plans for the future.

ISA: What inspired the ISA MPSTME section to develop a women's safety app?

Archit Kohli: The issue of women's safety has been a hot topic of discussion around the world for as long as one can remember. When the pandemic started, the world witnessed some shocking events that brought to light dangers that women face daily. Our goal is to do our part to help make India, and the world, a safer place for women.

ISA: Can you discuss the process of building the app?

AK: There were three main stages we went through in the development of this app. The first was the planning stage, which allowed us to zero in on the actual problem we wanted to tackle: the issue of women's safety. The pandemic has forced people to work from home and online, which meant that an app was our best option. We started by asking the most important question involved in developing an app for women's safety: what makes a "good" women's safety app? This meant using surveys, which we conducted across the country via Google Forms. We reached out to women of different backgrounds and asked for their opinions on what would make the app foolproof.

We used the responses in the second stage, which was the building stage. We filtered and chose the best or most relevant ideas, which could be converted into working algorithms and implemented into a working module. This led us to the third stage, or the implementation stage. We believe this app is a very viable solution to assist authorities in matters pertaining to women's safety. The biggest challenge, however, is reaching out to the correct audience. It becomes a waste if a solution exists for someone who doesn't even know of its existence. Informing the masses is a long process that we are still working on, but I am confident that we will be able to accomplish this herculean task.

ISA: What are the main features?

AK: The app is called "Eve" and has the following standout features:

- SOS mode, which allows audio and video recording; sends a pre-written SMS to preset emergency contacts along with Google Maps location links; locks the screen and prevents perpetrators from ending specific vital background processes; and allows the user to make a call to the nearest police station based on location data.

- Location ratings. Areas around the users will be given a safety rating based on the presence of landmarks and data from the National Crime Records Bureau.
- Safest route shows users the safest path from their location to their destination based on the location rating.

ISA: What happens now that the app has been developed?

AK: With Eve scheduled to launch on the Google Play Store, we are now focusing our efforts on reaching out to as many women as possible to inform them about this app and encouraging them to try it out. Additionally, we are working on developing it for the iOS platform. Our main goal is to ensure that women see Eve as an option to ensure their safety. The most important thing we can have is their trust in our app. Once the presence and benefits of this app have been established in India, we aim to expand it globally.

ISA: Any advice for other ISA student sections who might want to do something similar?

AK: Firstly, I want to encourage other ISA sections to take up social initiatives. We are fortunate enough to be blessed with the life we have today. As the generation that will lead the future, it is our moral duty to ensure the existence of a safer and more sustainable environment. The only thing I request any other section do when taking up social initiatives is to thoroughly understand the background of the particular issue they aim to solve before they move ahead. Just knowing the problem is never enough. Familiarizing oneself with the origin of the problem and its causes is the only way of ensuring that a strong foundation is built upon which the problem can be tackled. If any section wants to collaborate with us in our social efforts, I encourage them to reach out to us via the official ISA MPSTME social media handles, and we will be more than happy to help. ■

—By Christina Ayala

Subscribe to ISA Interchange at <https://blog.isa.org/subscribe> to read more.

Register Now: ISAGCA Webinars

Assessing and Managing Cybersecurity Risk: Part 1
20 May | 1:00 p.m. ET

Assessing and Managing Cybersecurity Risk: Part 2
12 August | 1:00 p.m. ET

ISAGCA Security Strategies: Detailed Pros and Cons to Different Approaches
11 November | 1:00 p.m. ET

Register for upcoming and on-demand webinars online:
<https://isaautomation.isa.org/virtual-events-program>

ISA Certified Automation Professional (CAP)



Certified Automation Professionals (CAPs) are responsible for the direction, design, and deployment of systems and equipment for manufacturing and control systems. For more information, visit www.isa.org/training-and-certification/isa-certification/cap.

CAP review question

A project is underway to provide an automated safety interlock for a door to a barrier around a rotary mixing drum. Which of the following credentialed engineering roles would be most helpful in defining the requirements for this system?

- A. Certified Control System Technician (CCST)
- B. Process engineer with a master's degree
- C. Certified Functional Safety Engineer (CSFE)
- D. Microsoft Certified Systems Engineer (MCSE)

CAP answer

The answer is C, "Certified Functional Safety Engineer (CSFE)." Certified Functional Safety Engineers are tested to ensure that personnel performing SIS life-cycle activities are competent as required by the IEC 61508, ISA/IEC 61511, and 62061 standards. The other engineering roles listed may be important to the overall project, but only CSFEs are trained to provide guidance and expertise for the develop of functional/machine safety projects.

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

ISA Certified Control Systems Technician (CCST)



Certified Control System Technicians (CCSTs) calibrate, document, troubleshoot, and repair/replace instrumentation for systems that measure and control level, temperature, pressure, flow, and other process variables. For more information, visit www.isa.org/training-and-certification/isa-certification/ccst.

CCST review question

When predictive maintenance practices indicate an upcoming problem, preventive maintenance can be:

- A. Put off until two or more additional factors consistent with an impending failure are seen
- B. Budgeted for the next fiscal quarter as to not disrupt cash flow
- C. Considered as one of many possible remediation measures
- D. Scheduled to avoid system/component failure

CCST answer

The answer is D, "Scheduled to avoid system/component failure." Predictive maintenance is aimed at preventing unplanned downtime. When the predictive maintenance process identifies a problem, maintenance on the item should be scheduled at the earliest possible time to prevent the small problem from becoming a much larger issue.

Predictive maintenance techniques are designed to help determine the condition of in-service equipment to estimate when maintenance should be performed.

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

New CAPs and CCSTs

The following individuals have recently passed either ISA's Certified Automation Professional (CAP) exam or one of the three levels of Certified Control Systems Technician (CCST) exam. For more about either program, visit www.isa.org/training-and-certification/isa-certification.

Certified Control System Technicians Level 1

- Scott William Tack, U.S.
- Donald F. Schroeder, U.S.
- Jan Di Pierro, U.S.
- Carl W. Jensen, U.S.
- Larry Guth, U.S.
- Jason Van Buren, U.S.
- David Halter, U.S.
- Paul Kaczorowski, U.S.
- Seth Young, U.S.
- John Gowder, U.S.
- Danny Cooper, U.S.
- Brian D. Akins, U.S.
- James Frye, U.S.
- Andrew Parker, U.S.
- Jerry Lillard, U.S.
- Jason McLaughlin, U.S.
- Ian Follette, U.S.

Level 2

- Reagan C. Ruiz, U.S.
- David L. Trumbull, U.S.
- Todd J. Braun, U.S.
- Brandon Weibley, U.S.
- Carl W. Jensen, U.S.

Level 3

- Omar H. Abu Jadouo, U.S.
- Todd D. Erwin, U.S.

Certified Automation Professionals

- Asif Iqbal, Saudi Arabia
- Junghak Shin, Canada
- Linnea Lubke, U.S.
- Fahad F. Al Furaih, Saudi Arabia
- Ian Loke, Singapore
- Quang M. Tran, U.S.
- Jesus Andres Tous Tejada, Colombia
- James Hess, U.S.
- Sudheer Prabhakaran, Saudi Arabia
- Stephen Byl, Canada
- Mark Anthony Meso, Australia

Specialty Chemicals Manufacturer Achieves Consistently Reliable Batch Processing

An ISA-88-based layered batch management package and other software minimizes human error while improving quality and productivity.

By Chris Kourliouros

When chemical processors—including those creating plastic, polymer, or rubber products—use batch reactors, following the recipe from batch-to-batch and plant-to-plant is critical to reliably and cost-effectively manufacture high value-added materials to spec. This typically involves charging the reactor, manipulating operating conditions to meet processing criteria, and shutting down and emptying the reactor.

Even when certain procedures and processes are standardized and automated, numerous key steps in and around the automation may still depend on operator input or manual intervention. Unfortunately, when the operator is interrupted to handle other tasks or when responses vary from operator to operator, off-spec product can result. This can cause costly corrective steps or wasted product that must be disposed.

As a solution, some chemical producers are automating their standard operating procedures (SOPs) while providing operators with greater control and visibility. This helps chemical processors perform

more consistently reliable batch processing to spec, which enhances quality, productivity, and profit.

Batches of biomass-derived specialty chemicals

Kraton Corporation develops, manufactures, and markets biobased chemicals and specialty polymers worldwide and has more than 800 customers across a diverse range of end markets in more than 70 countries. The company is also a global producer of styrenic block copolymers and pine chemicals. In January 2016, Kraton Corporation completed the acquisition of Arizona Chemical, a global producer of high-value performance products and specialty chemicals derived from nonhydrocarbon, renewable raw materials.

Renewable biomass derivatives from paper production (referred to as “soap”) are used to produce a variety of specialty chemicals for 3M, HB Filler, and other clients: rosins used in inks, adhesives, road paint, construction, packaging, personal care, and other applications. The pro-

cess displaces petroleum dependence for equivalent products, but in so doing must account for the inherent variability in biomass feedstocks to their process.

Kraton operates a network of nine manufacturing facilities in North America and Europe, but its Savannah, Ga., facility was producing too many out-of-spec batches and required correction. Although the issue could not be pinpointed to a certain product or work shift, the previous automation system consisted of a series of programs that still required operator intervention at key junctures. For example, an automated procedure could charge a reactor with a particular product, but it might still require the operator’s manual attention to start and stop heating.

Optimize execution of manual tasks

After a thorough review, the Kraton team determined that product quality could be significantly improved by optimizing the execution of manual tasks. Operators would be interrupted or become busy with other tasks. For example, they would be unable to hold a material at a certain steady melt point, because they had to unstick a valve by running steam into a line to free it up.

Natural human variability in operator response was also causing inconsistencies, for instance, in starting and stopping heaters and in other time-sensitive procedural steps. While the resulting off-spec product could be corrected, making the necessary adjustments took extra time, labor, material, and line capacity, which reduced productivity and profitability.

Kraton uses three different distributed control system (DCS) platforms to filter, centrifuge, and distill the feedstocks into resin precursors. To control its reactor processes, Kraton uses the D/3 DCS from Owings Mills, Md.-based NovaTech LLC Process Division. The D/3 system was chosen for three main reasons: the company’s expertise in batch process automation; the flexibility of the Sequence and Batch Language (SABL) that the D/3 controllers use; and for an ISA-88-based layered batch management package called FlexBatch.

The NovaTech D/3 operator interface displays real-time process information

and makes it easy for the operator to control the process, enter information, and interact with sequence programs. In addition to the real-time process graphics and the FlexBatch interface, operators had access to standard operating procedures in standard document .doc and .pdf formats, which were embedded within graphics or in Help menus. For manual tasks, operators could type answers to enter values, such as which vessel was used to supply the materials to produce a given product.

“I have not seen any DCS that can handle nearly as many loops and as much programming per controller as the D/3,” explained Gregg Cox, the senior controls engineer who designed the operator interface. “We run about 3,000 I/O points on five process control modules here, and we could probably do it on two.”

Paperless procedure automation

Kraton added a layered procedural automation software package, Paperless Procedures (PLP) from NovaTech, to the D/3. The software solution allowed manual tasks and automated tasks to be seamlessly integrated into the same SABL batch programs, an innovation that NovaTech patented.

PLP provides operators with an intuitive SOP-like checklist interface that merges manual and automated tasks in real time,

that adapts dynamically to real-time process data, and that can be viewed from any PC, tablet, smartphone, or other device. PLP also provides secure, time-stamped records of every procedure step to support compliance requirements and continuous improvement efforts. The combination of tools has allowed Kraton to achieve more accurate, consistent, and repeatable batches.

“The final product is completed with scheduled campaigns on FlexBatch that



Software allows manual tasks and automated tasks to be integrated into the same batch programs.



Eliminating some of the burden on operators to interpret the process has resulted in batch cycles that are more consistently executed.

are completed with batches run with PLP,” explained Cox. “This hybrid approach has improved product quality while reducing batch cycle times.”

With this approach, the operator can modify recipe parameters, recipe procedures, production schedules, batch start rules, and equipment utilization, or scale batch amount at any point during recipe development and execution. Recipe values are automatically entered into the system, and the operator only needs to select the reactor and which vessel to pull from. This safer, more intuitive approach speeds the process because the operator selects all the equipment to be used before starting the procedure.

“We are basically eliminating some of [the] burden on operators to interpret the process,” Cox said. “This has resulted in batch cycles that are more consistently executed with the proper timing and procedure. As a result, we can begin looking at the overall design of our processes and

SUBMIT CASE STUDIES

InTech magazine’s new Digitalization Diaries department is created in conjunction with Automation.com, a subsidiary of ISA. Automation.com is the leading online publisher of automation-related content—industrial and commercial automation news, insights, new-product information, and case studies. Through its website, newsletters, ebooks and webinars, Automation.com helps automation professionals improve production efficiencies, secure and optimize facilities, and digitally transform their manufacturing and industrial businesses. See publication guidelines online at <https://www.automation.com/en-us/submit-content> and submit your success story to content@automation.com.



engineer out some of the ‘wiggle room’ that had to be there to account for operators’ varying interpretations of what to do next and when.”

According to Cox, filling in the gaps in the system’s automation process ultimately brings higher yields, reduced errors, improved safety, and greater profitability. Kraton can capitalize and expand its operations over both petroleum-based and other biosourced competitors. ■

ABOUT THE AUTHOR



Chris Kourliouros is the VP of product marketing of NovaTech LLC Process Division, www.novatech-web.com, which specializes in continuous control system architecture.

New From ISA!

Learn how to increase efficiency and improve process control *before* the plant goes online

Explore the advantages of using experimental and first-principle models for process monitoring and control. This reference guide is ideal for process design, quality control, information systems, or automation engineers who want to maximize efficiency.

Order your copy today at www.isa.org/bioprocess

International Society of Automation
Setting the Standard for Automation™

From ISA Publishing

Situation awareness + situation assessment + successfully managing abnormal situations = Situation Management

Operators must be able to monitor operations, understand the data, and plan and actualize necessary changes. This book discusses the technology and tools, as well as effective methodologies for safer and more productive control room operations through situation management.

Order your copy today at www.isa.org/situationmgmt

International Society of Automation
Setting the Standard for Automation™

‘Understand the Full Process’: Tips for Automation Career Success

By Bill Lydon

Every year, I embrace the opportunity to attend the Pharmaceutical Automation Roundtable (PAR) meetings as the only outside observer. PAR meetings highlight one of the most knowledgeable groups of automation professionals gathered in one place, at any one time, to discuss automation issues. The 2019 PAR meeting, held pre-pandemic in October 2019 at a Novo Nordisk facility, revolved around the results of the group’s most recent survey.

Survey respondents were asked questions related to the digital plant maturity model, automation challenges and solutions, and more. A significant portion of the survey also focused on workforce development issues, and the results are useful to both career individuals and managers of automation professionals.

First, some survey respondent demographics: Approximately 100 automation professionals from 19 pharmaceutical companies completed the survey. About 60 percent of respondents were from North America; 30 percent from Europe; 8 percent from Asia; and 2 percent from South America. Fifty-three percent were between the ages of 35 and 50; 30 percent were older than 50; and about 17 percent were younger than 35.

Respondents were asked to rank the skills necessary for a successful career in automation, from most to least important. Averaging the responses produced this ranking:

1. Understanding the equipment and the processes
2. Strong communications skills
3. Understanding software development and programming
4. Creative thinking and detail orientation
5. Equipment troubleshooting skills
6. Ability to perform complex system tests.

At the meeting, members discussed these and other results. Comments indicated how important it is for automation engineers to understand the full process, get on-the-job training when they are new to the field, and understand the content and applications regardless of what new tools and technology are available. One PAR member commented, “Developing troubleshooting skills poses a real learning challenge. We see automation engineers going through troubleshooting to learn from problems.”

Survey respondents were asked what type of

college technical courses and content they would like to see student engineers learn, in addition to automation fundamentals. The following are respondents’ top picks, from most to least desired:

1. Software development techniques
2. Networking technologies
3. Cybersecurity
4. Advanced analytics
5. Robotics.

Survey respondents ranked the importance of specific training and development activities. Twenty-nine percent of respondents indicated that involvement in automation projects is the most important training and development activity. Sixteen percent of respondents said peer interactions on the job are most important. Notably, 20 percent of respondents who were younger than 35 said that formal training (outside of school, not vendor) is most important, while only 7 percent of those between the ages of 35 and 50, and 2 percent of those older than 50 chose that answer.

These are the three professional development courses respondents thought were most important: (1) automation, instrumentation, and traditional control technical content; (2) quality, qualification, and computer system validation; and (3) leadership. Many comments from survey respondents indicated people do not have spare time for personal training and development.

Read more about other parts of the PAR survey at <https://www.automation.com/en-US/Articles/March-2020/2019-PAR-Insights-Automation-Workforce-Development>. ■



ABOUT THE AUTHOR

Bill Lydon (blydon@isa.org) is an *InTech* contributing editor with more than 25 years of industry experience. He regularly provides news reports, observations, and insights here and on Automation.com.

About PAR

The Pharmaceutical Automation Roundtable was founded more than 20 years ago by Dave Adler and John Krenzke, both from Eli Lilly and Company. At the time, its purpose was to provide a means of benchmarking and sharing best practices for automation groups among peer pharmaceutical companies. Lead automation engineers from around the world attended this user-only, two-day event. The participating companies in the 2019 PAR included Abbvie, Amgen, Baxalta, Biogen, Bristol-Myers Squibb, Boehringer Ingelheim, ImClone Systems, Lilly, Merck, NNE Pharmaplan, Novo Nordisk, Perrigo, Pfizer, and Sanofi Pasteur.

Cybersecurity Using ICS ATT&CK Strategies

By Jacob Chapman

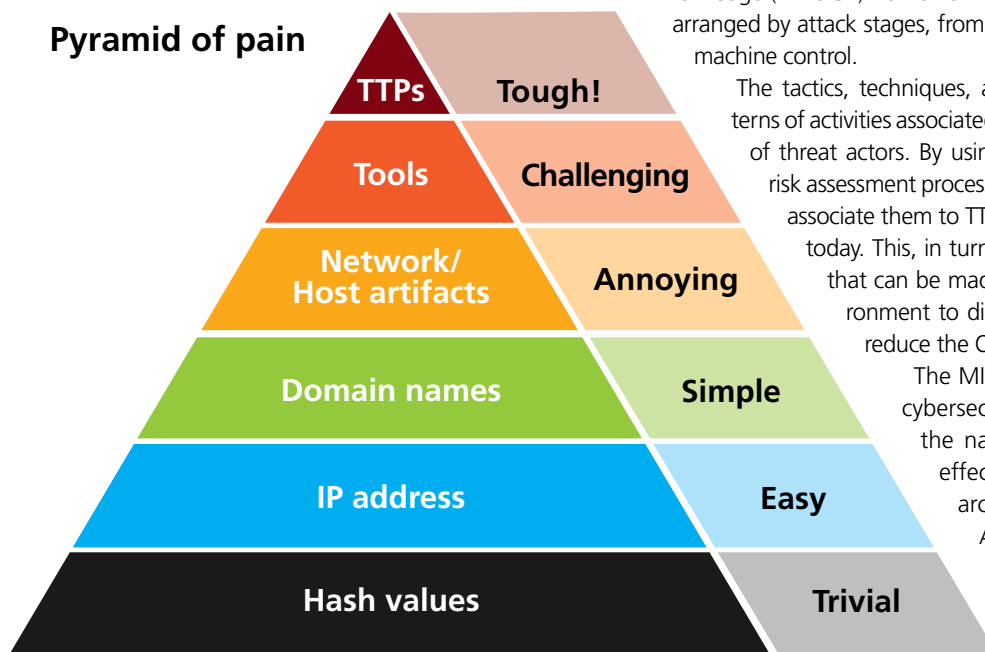
Protect smart manufacturing and IIoT systems using a security framework that presents information in matrices arranged by attack stages.

Risk assessments and mitigation are commonplace activities in the manufacturing environment, but as the number and type of cyberattacks increase in all industries, and connectivity continues to increase between information technology (IT) and operational technology (OT), it is necessary to take a practical, targeted approach to cybersecurity risk management of smart manufacturing and Industrial Internet of Things (IIoT) systems. The industrial control system (ICS) adversarial tactics, techniques, and common knowledge (ATT&CK) framework presents the information in matrices arranged by attack stages, from initial system access to data theft or machine control.

The tactics, techniques, and procedures (TTPs) describe patterns of activities associated with a specific threat actor or group of threat actors. By using the ATT&CK framework within a risk assessment process, organizations can identify risks and associate them to TTPs that adversaries are actually using today. This, in turn, helps identify the specific changes that can be made to the systems and network environment to disrupt those attacks and significantly reduce the OT environment's risk level.

The MITRE Corporation's federally funded cybersecurity R&D center helps to provide the nation's business infrastructure with effective and practical cybersecurity architectures and solutions. The ICS ATT&CK matrix is a knowledge base of adversary actions that focuses on adversaries whose goal is disrupting ICSs. This open-sourced/community-driven knowledge base is accessible at <https://collaborate.mitre.org/>

Pyramid of pain



This diagram shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause your adversaries when you are able to deny those indicators to them. Source: David J. Blanco, personal blog

attackics/index.php/Main_Page.

In the ICS ATT&CK matrix, disruptive tactics are mapped against mitigation techniques to give manufacturers practical actions to help prevent each type of threat. Information is also provided about adversary groups. Experts should know how to use the ATT&CK framework to create a roadmap that prioritizes mitigating the largest risks to an organization's smart manufacturing and IIoT systems.

Applying ATT&CK to risk management

Applying ICS ATT&CK to risk management involves identifying cybersecurity risks, determining the potential effect and likelihood of risk occurrence, and then determining the best way to deal with each risk with the resources available. Assessing this information helps manufacturers deploy the most efficient, cost-effective risk control and mitigation strategy and controls in a targeted way to reduce the most likely or highest-impact cybersecurity risks first.

In the typical risk assessment methodology, an estimate of risk probability is required. Unfortunately, there is no simple yet consistently accurate way to measure probability (likelihood of risk occurrence). Rather than relying on elaborate mathematical models or falling back on a guesstimate approach, ICS ATT&CK is a more practical approach. Some aspects of this include looking at localized data relevant to the specific environment. Risk assessment is more about prioritization than probability, so it is important to evaluate local attack vectors. It is also important to use facts and measurable data applicable to the facility's configuration and assets to estimate business impact rather than guessing or generalizing. Understanding the impact of a risk occurrence is more critical than its probability.

However, for a risk assessment to be effective, it is important for manufacturers to have a complete understanding of the assets involved in their industrial control systems and the network topology in manufacturing areas. Legacy equipment, security patches applied or lacking, and connectivity to business systems with more threat exposure must all be considered when evaluating cybersecurity risk. Typical steps involved with threat modeling and risk management are shown in the diagram figure 1.

Practical approaches to preventing cyberattack

The use cases of the ICS ATT&CK model assume that a breach will occur; thus planning and performing preventive maintenance is required to fortify an enterprise's perimeter and internal network to mitigate an attack. Proactive maintenance is always less costly than reacting after the fact, when time is of the essence and additional action may be needed to undo the damage caused by an intrusion. Risk assessment typically consists of three phases.

Phase 1 – Gather information on systems environment

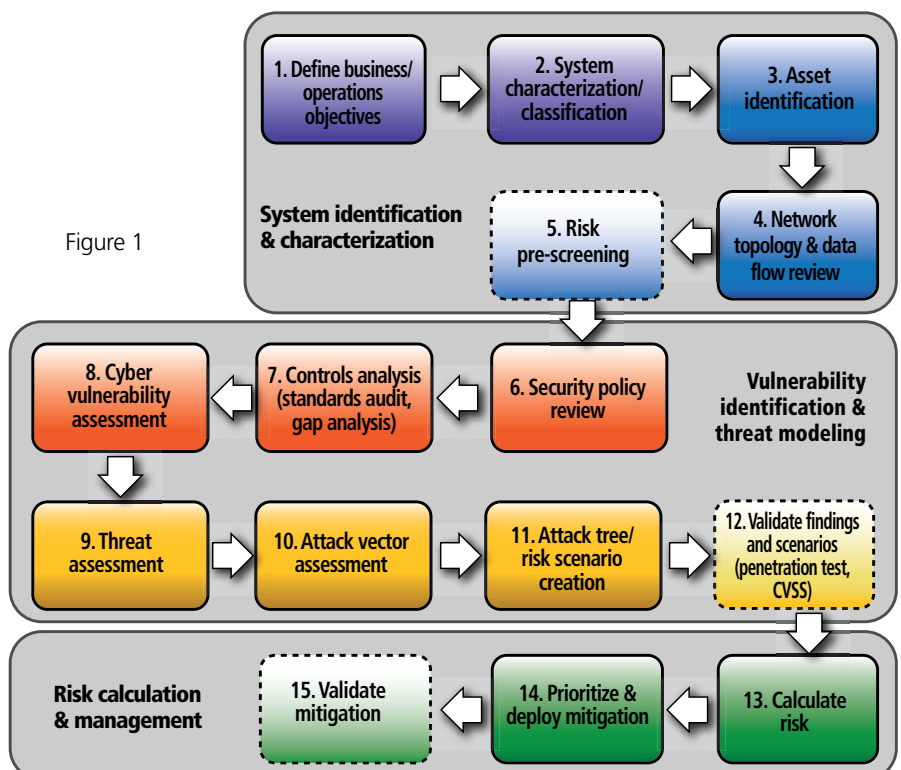
System owners should evaluate the smart manufacturing and IIoT system assets as well as the ICS environment as a whole, including links to networks outside of manufacturing; software/firmware installed on each workstation, controller, or other equipment; and user permissions, with consideration for other factors such as corporate expansion plans or equipment upgrades. Figure 2 is an example presenting simplified findings of phase 1.

Phase 2 – Create IIoT system attack tree using ICS ATT&CK framework

Define the risks for each piece of equipment and identify and prioritize appropriate mitigation techniques. An example is an insecure network architecture with no security policies between the IT/OT zone and no industrial demilitarized zone (IDMZ). After analyzing the network, one attack tree may be a malicious USB connected at the enterprise network. Based on the flat network topology, the USB installs malware with the intent of gaining remote access to an engineering workstation (EWS). Once remote access is gained to the EWS, the adversary can use the manufacturing execution system (MES) software already installed to impair the facility's process or attack the business' ERP system.

Phase 3 – Plan creation

Based on the findings of phases 1 and 2, ICS cybersecurity practitioners can calculate asset risk and identify the cybersecurity gaps that may allow unwanted adversarial activity. Using this information, they can create roadmaps prioritizing these risks while also visually modeling risk mitigation once these risk mitigation activities have been performed.



Realizing efficiencies

Many times, system owners have the opportunity to implement security enhancements in conjunction with other activities requiring planned system downtime. This minimizes the impact on production and of course is preferable to an unplanned shutdown caused by a cyberattack.

By incorporating security enhancements at the same time as system design changes, the security aspects of the system can be validated along with the rest of the system. System owners can also help ensure that any system expansions or improvements are planned and designed with cyberattack prevention in mind via defining minimum security requirements across the enterprise.

Enterprise-level considerations

Most security breaches are the result of intrusions or malicious attacks on the corporate side of the enterprise. In the past, networked manufacturing systems and equipment were separate from the rest of the enterprise and the outside world, and only communicated with each other. But with the advent of smart

manufacturing and IIoT systems such as MES, digital twins, and overall equipment effectiveness implementations, there is greater connectivity between the enterprise network and the manufacturing network. Though this improves efficiency and allows for better planning, it also allows more opportunities for intrusions, malware, and successful phishing attacks, and allows malware to spread to the production floor with potentially catastrophic results. A critical component for managing this connectivity is an industrial demilitarized zone to carefully control traffic between the industrial and enterprise zones.

The rapid adoption of the IIoT also has the potential to allow intrusion, as more and more devices are networked, often with inconsistent implementation without enough security measures. As the IIoT is increasingly adopted, it will increase the vulnerability of the control system network if robust security practices are not rigorously followed. Cloud-based tools and systems also pose new risks that increase the attack surface.

When a system owner performs a risk assessment and mitigation plan using the

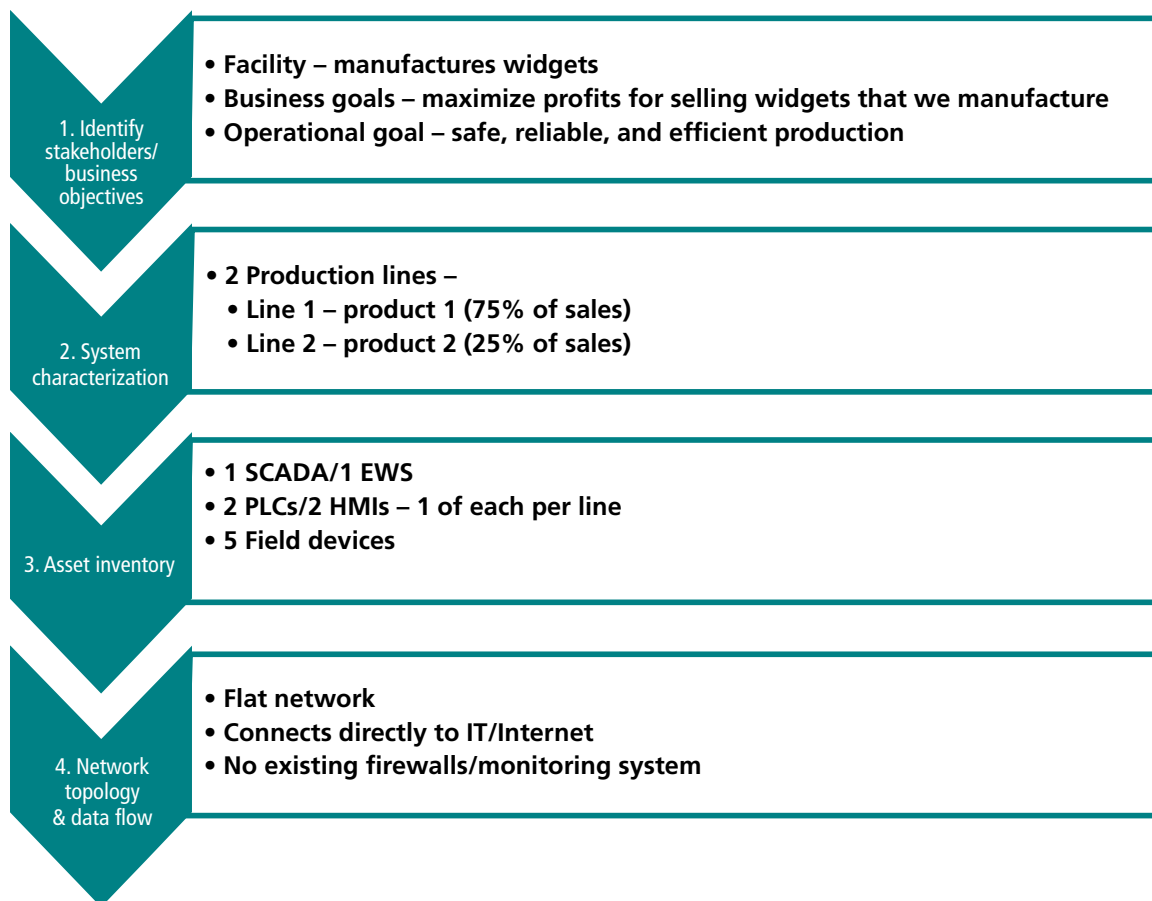
ATT&CK model, system assets should be classified based on criticality, not only from a manufacturing process perspective, but also from the perspective of the potential environmental, safety, and regulatory impacts from a security breach. For smart manufacturing and IIoT system breaches, which affect both the IT and OT environments, the stakes are higher.

The ICS ATT&CK model is not a standard but provides a framework of known activities attempted by cybersecurity adversaries. It defines how adversaries have successfully attacked ICSs, such as smart manufacturing and IIoT systems and provides the mitigation steps to take for each type of known attack. System owners can then line up the mitigations with the standards applicable to each area for an industry-compliant mitigation. Approaches may be guided by closely following ISA-99 and IEC 62433.

What's coming next for defending IIoT systems?

MITRE ATT&CK provides an effective approach to understand risk and prioritize

Figure 2



the security controls to protect smart manufacturing and IIoT systems. Baked into the framework are TTPs that can be applied to IIoT systems, such as initial access through Internet-accessible devices, execution through API, and exploitation of remote services. However, smart manufacturing and IIoT systems still pose unique challenges compared to traditional ICS security.

For this reason, experts and standard bodies are exploring ways to provide guidance for applying cybersecurity standards to these systems. For example, ISA99 recently communicated preliminary plans for adding standards to the IEC 62443 series dedicated to IIoT. In the future, we may see a consensus-driven answer to the question of how to apply cybersecurity standards to these systems.

MITRE is also exploring modifications to its framework to address the IT-OT combination of technologies that comprise smart manufacturing and IIoT systems. For example, articles and discussion are being had regarding a hybrid ATT&CK matrix visualization that combines ATT&CK for ICS and represents the IT portions of ICS attacks in ATT&CK for Enterprise. If a hybrid matrix provides value in tracking attack pathways and effective mitigation measures, it could become a preferred approach for applying ATT&CK to smart manufacturing and IIoT systems. ■

ABOUT THE AUTHOR

Jacob Chapman has a background in automation engineering, project management, account management, industrial networking, and ICS cybersecurity expertise within the food and beverage, pharmaceutical, and energy generation sectors, among others. Chapman currently leads the industrial IT and cybersecurity solutions and services at Grantek, which helps manufacturers develop their facility infrastructures, including their industrial network architectures, local and cloud computing systems, and cybersecurity programs. As Grantek's leader in the space, Chapman maintains involvement and leadership positions in international societies and standard bodies, including as the Cybersecurity Committee chair of the ISA's Smart Manufacturing & IIoT Division, a registered U.S. expert to TC65 of the IEC, and a member of the ISA99 standards development committee.

Security Platform for Micro-segmentation, Remote Access

Airwall Teams, a free, industrial-strength security platform for micro-segmentation and remote access, lets organizations try the standards-based Host Identity Protocol (HIP) to build secure communications channels between devices, regardless of where they are located. This technology ensures secure access across all mobile, corporate, Internet, and cloud networks. Airwall Teams is based on the same network technology as Airwall, an easy-to-manage, enterprise-grade solution that uses HIP and includes a range of scalable hardware gateways and policy management devices. Together they form a private overlay network that sits on top of the existing cybersecurity and network infrastructure.

Tempered Networks

www.tempered.io

Network Security Appliance

The NCA-6520 is a 2U 19-inch rackmount network security appliance with dual third-generation Intel Xeon Scalable processors, high throughputs, built-in crypto acceleration, and NIC module expansion. It has enhanced performance for network security workloads through increased processor cores (up to 40), higher memory bandwidth (1.2 times memory capacity per processor), PCIe-Gen4 support, and fast input/output. Integrated 100 Gbps Intel QuickAssist is a hardware technology that accelerates critical workloads such as data compression and cryptography across server, storage, and network applications.



Lanner Inc.

www.lannerinc.com

ICS Cybersecurity Risk Screening Service

A new service, ICS Cybersecurity Risk Screening, helps industrial organizations gain a high-level understanding of the worst-case risk to operations should their industrial control systems (ICSs) be compromised. Using a consequence-based, initial cybersecurity risk screening methodology, the results expose the potential magnitude of cyberrisk to operations, assist with prioritizing detailed risk assessments, facilitate the grouping of assets into zones and conduits, and help manage budgets and resources appropriately.

aeSolutions

www.aesolutions.com

Proxy Device for Implementation of CIP Security

Industrial companies can now implement CIP Security expansively in their systems with the Allen-Bradley CIP Security Proxy by working with EtherNet/IP-compliant devices. The proxy device allows users with products that are not embedded with CIP Security to define and implement their unique migration roadmap to a CIP Security architecture. It also provides a path forward for products not capable of CIP Security. Configuration can be achieved through FactoryTalk Policy Manager software and FactoryTalk system services. The device also supports motion for Kinetix drives and has a web server for viewing diagnostics.



Rockwell Automation

www.Rockwellautomation.com



Sample of Jobs Available at Jobs.isa.org

See more at Jobs.isa.org, where you can search for available jobs or advertise positions available within your company. ISA Members post resumes at no charge.

Opto-mechanical engineer

Lowell Observatory: As a member of the technology group, the opto-mechanical engineer at the observatory's Navy Precision Optical Interferometer in Flagstaff, Ariz., is responsible for continued development and support of the mechanical infrastructure and optical systems. The position is initially funded for the duration of the upgrade of the interferometer (3–5 years), with the potential to become permanent. The engineer designs, installs, troubleshoots, and validates existing and planned improvements of mechanical infrastructure, opto-mechanical tools, and instrumentation. The position requires the demonstrated ability to design effective mechanical and optical systems with a strong focus on clear and comprehensive technical documentation, root cause analysis, the ability to meet deadlines, and experience in Solid Works and/or inventory . . . see more at Jobs.isa.org.

Water quality control systems technician

Sacramento County: The journey-level class technician in Sacramento, Calif., maintains and repairs pneumatic, chemical, electric, and electronic components; analog and digital networks and systems; analysis equipment; computer control equipment, including computers and computer peripherals; and telemetry equipment used in process instrumentation and control systems. The position requires an AA or AS technology degree and two years of full-time experience in the operation, maintenance, and repair of instrumentation . . . see more at Jobs.isa.org.

Mechanical engineer

Motorola Solutions: The mechanical engineer in Plantation, Fla., will be involved in the design and development of highly sophisticated communication devices for professional and mission-

critical markets in commercial, government, and industrial segments. Responsibilities include preparing concept designs of mechanical components and assemblies that meet product performance, customer requirements and expectations, reliability and robustness requirements, manufacturing processes, and safety guidelines; working with a team of product development engineers to take design concepts through the detailed design process for mechanical components, which include the design of injection molding plastic, die casting, sheet metal stamping, rubber and elastomers, and rigid and flexible printed circuit boards; and interpreting and generating 2D drawings per mechanical drafting standards. A BS or MS in mechanical engineering and a GPA of 3.0 or greater is required . . . see more at Jobs.isa.org.

Machining process engineer

Honeywell: The company's Federal Manufacturing and Technologies business in Kansas City, Mo., manages the U.S. Department of Energy's Kansas City National Security Campus in Missouri and New Mexico, manufacturing components of the nation's defense system. The machining process engineer provides engineering support of highly technical and advanced manufacturing processes and performs project management and design, development, evaluation, and quality control functions. Also, the engineer writes technical reports on results and conclusions drawn from experiments and incorporates findings into formal specifications. The position requires U.S. citizenship, a BS from an ABET-accredited engineering program or a BS in physics from an accredited program, and two or more years of relevant experience . . . see more at Jobs.isa.org.

Senior automation engineer

Bristol Myers Squibb: The engineer in Warren, N.J., will be responsible for the operational readiness of the process automation applications within the cell therapy development operations process scale-up facilities used in the manufacture of cell therapies for GMP and non-GMP activities. Responsibilities include troubleshooting, resolution, and improvement of automation applications, including batch and continuous control and MS operating system and control system interfaces; providing automation expertise for assigned projects led by engineering functions; maintaining lifecycle management of control system and documentation with applicable procedural documents and industry guidance; and leading the use of new technologies on site. Requirements include a BS in engineering, 5–10 years of work experience, and proficiency with Emerson DeltaV, OSI Pi, MS operating system, MS SQL . . . see more at Jobs.isa.org.

Shift supervisor

Hain Celestial Group: This position in Mountville, Pa., will provide leadership and overall direction to an operations team (packaging, line maintenance, materials handling, and processing), including execution of the production schedule; management of planned and unplanned events; performance management; training and administrative tasks. A bachelor's degree is required, and food processing and packaging industry experience is preferred. Experience in the snacking industry is a plus but not required. Additional requirements are regulatory experience with FDA, OSHA, and other agencies; a proven track record in continuous improvement, and strong communication skills (bilingual is a plus) . . . see more at Jobs.isa.org.

InTech advertisers are pleased to provide additional information about their products and services. To obtain further information, please contact the advertiser using the contact information contained in their ads or the Web address shown here.

| Advertiser | Page # | Advertiser | Page # |
|---|--------|---|--------|
| Automation Direct Cover 2 www.automationdirect.com | | ISA Global Cybersecurity Alliance Cover 3 www.isa.org/isagca | |
| Endress + Hauser 3 www.us.endress.com | | MAVERICK Cover 4 www.mavtechglobal.com | |
| Festo 21 www.festo.com | | Moore Industries 6 www.miinet.com | |
| Inductive Automation bellyband www.inductiveautomation.com | | ProComSol, Ltd 33 www.procomsol.com | |
| ISA Books 42 www.isa.org/books | | Tadiran 13 www.tadiranbat.com | |

InTech Advertising

View the Media Planner

<https://tinyurl.com/ISA-InTechMediaKit>

Contact a Representative

Richard T. Simpson

Advertising Sales Representative
Phone: +1 919-414-7395
Email: rsimpson@automation.com

Chris Nelson

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

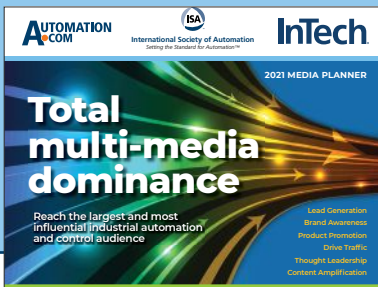
Gina DiFrancesco

Inside Account Manager
Phone: +1 216-509-0592
Email: gina@isa.org

Chris Hayworth

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

Print + Online = Success



Download the ISA
InTech/Automation.com
Media Planner:

<https://tinyurl.com/ISA-InTechMediaKit2021>

Purchase Reprints

An InTech representative can work with you to create a customized reprint package, including hardcopy reprints, PDFs, or mobile-friendly products.

Contact Jill Kaletha at 1 800-428-3340 x149 or jkaletha@mossbergco.com

datafiles

Datafiles list useful literature on products and services available from manufacturers. To receive free copies of this literature, contact each manufacturer directly.

USB HART MODEM

The **HM-USB-ISO** USB HART modem meets industry standards for USB and HART connectivity. The small size, light weight, and durability of the HM-USB-ISO make it ideal for portable use. Operating power is derived from the USB connection. An easily installed Virtual Serial Port driver allows use in any Windows-based application.

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

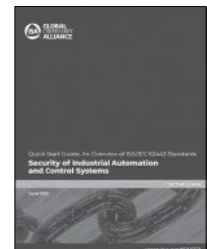
ProComSol, Ltd, Process Communications Solutions
Tel. 216.221.1550; Fax 216.221.1554
sales@procomsol.com; www.procomsol.com
Toll Free 877.221.1551



INDUSTRIAL CYBERSECURITY QUICK START GUIDE

The ISA Global Cybersecurity Alliance's Advocacy and Adoption work group's guide to the ISA/IEC 62443 series of standards includes lists of specific standards documents applicable to various roles within the security environment. The ISA Global Cybersecurity Alliance is a collaborative forum to advance industrial cybersecurity awareness, education, readiness, and knowledge sharing. Membership is open to any organization involved in industrial cybersecurity.

To download a PDF copy of the whitepaper, visit <https://gca.isa.org/isagca-quick-start-guide-62443-standards>. To talk about how your company or organization can join ISA GCA, contact Rick Zabel at rzabel@isa.org.



Electric Vehicle Success Requires Automation Professionals

By Bill Lydon



ABOUT THE AUTHOR

Bill Lydon (blydon@isa.org) is an *InTech* contributing editor with more than 25 years of industry experience. He regularly provides news reports, observations, and insights here and on Automation.com.

The growth of electric vehicles (EVs) will require automation professionals to manage the complexities of increased power generation, distribution, and orchestration of generation resources including solar, wind, and traditional sources. The average person, particularly in developed countries, takes for granted the instant availability of electric power without understanding the engineering and systems needed to generate and deliver reliable power. The average electric vehicle requires 30 kilowatt-hours to travel 100 miles, the same amount of electricity an average American home uses each day to run appliances, computers, lights, and heating and air conditioning. Automation professionals will be critical for designing, building, programing, cyber protecting, and commissioning power distribution and generation automation systems for control, efficiency, and optimization in addition to ongoing oil and gas production.

Global power demand growth

The International Energy Agency (www.iea.org) has projected that by 2030 global electricity demand from electric vehicles (including two/three-wheelers) will reach 550 trillion-watt hours (TWh), about a sixfold rise from 2019 levels. This presents implications and opportunities for power systems. Balancing electrical demand and supply will become an increasing challenge to ensure the smooth integration of variable renewables-based energy generation and the electrification of multiple end-use sectors.

Over the coming decade, managing EV charging patterns will be key to encourage charging at periods of low electricity demand or during high renewables-based electricity generation. Consider the possibility of 250 million electric vehicles on the road by 2030; the share of EV charging in the evening peak demand could rise to 4–10 percent in the main electric vehicle markets (China, E.U., and U.S.).

In addition to lower off-peak electric rates encouraging charging at night, real-time price signals from utilities have been proposed to control a vehicle's charge rate to optimize variable renewable electricity generation. These strategies require automation professionals to conceptualize, design, engineer, and implement systems.

The European Environment Agency report, *Electric vehicles and the energy sector – impacts on Europe's future emissions*, says the share of electricity consumption required by an 80 percent share of electric vehicles in 2050 will vary between 3 percent and 25 percent of total electricity demand across the E.U. 28 member

states (note that the U.K. was still a member at the time of the report). On average, for the E.U. 28, the proportion of total electricity demand required in 2050 will be 9.5 percent, compared with the 1.3 percent assumed in the European Commission's projection. Overall, an additional electrical capacity of 150 GW is estimated to charge electric cars. A U.S. Department of Energy (www.energy.gov) study found that increased electrification across all sectors of the economy could boost national consumption by as much as 38 percent by 2050, in large part because of electric vehicles.

The environmental benefit of electric cars depends on the electricity being generated by renewables. Again, automation is required to orchestrate all sources of generation to ensure power availability and reliability.

Electricity demand fluctuates throughout the day, with a typical profile of higher use during daytime hours then peaking in the early evening. If many people buy electric vehicles and mostly try to charge right when they get home from work, the system could get overloaded or force utilities to deliver more electricity than they are currently capable of producing.

Delicate balance

Optimizing oil and gas will continue to be important, because the transition to all electric vehicles is a long-term effort. Toyota Motor Corporation president Akio Toyoda recently brought this into focus by criticizing what he described as excessive hype over electric vehicles, saying advocates failed to consider the carbon emitted by generating electricity and the costs of an EV transition. He noted that Japan would run out of electricity in the summer if all cars were running on electric power.

The infrastructure needed to support a fleet consisting entirely of EVs would cost Japan ¥14–¥37 trillion (\$135–\$358 billion). "When politicians are out there saying, 'Let's get rid of all cars using gasoline,' do they understand this?" Toyoda said in 2020 at a year-end news conference in his capacity as chairman of the Japan Automobile Manufacturers Association.

Cybersecurity

Automation professionals also have an important role in creating power generation and distribution systems that will be cybersecure. The distributed nature of power systems make them particularly vulnerable to attacks, requiring expert application of ISA/IEC 62443 standards developed by the ISA99 committee and adopted by the International Electrotechnical Commission. ■

Industrial Cybersecurity is a Global Imperative

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

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

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

Founding Members:

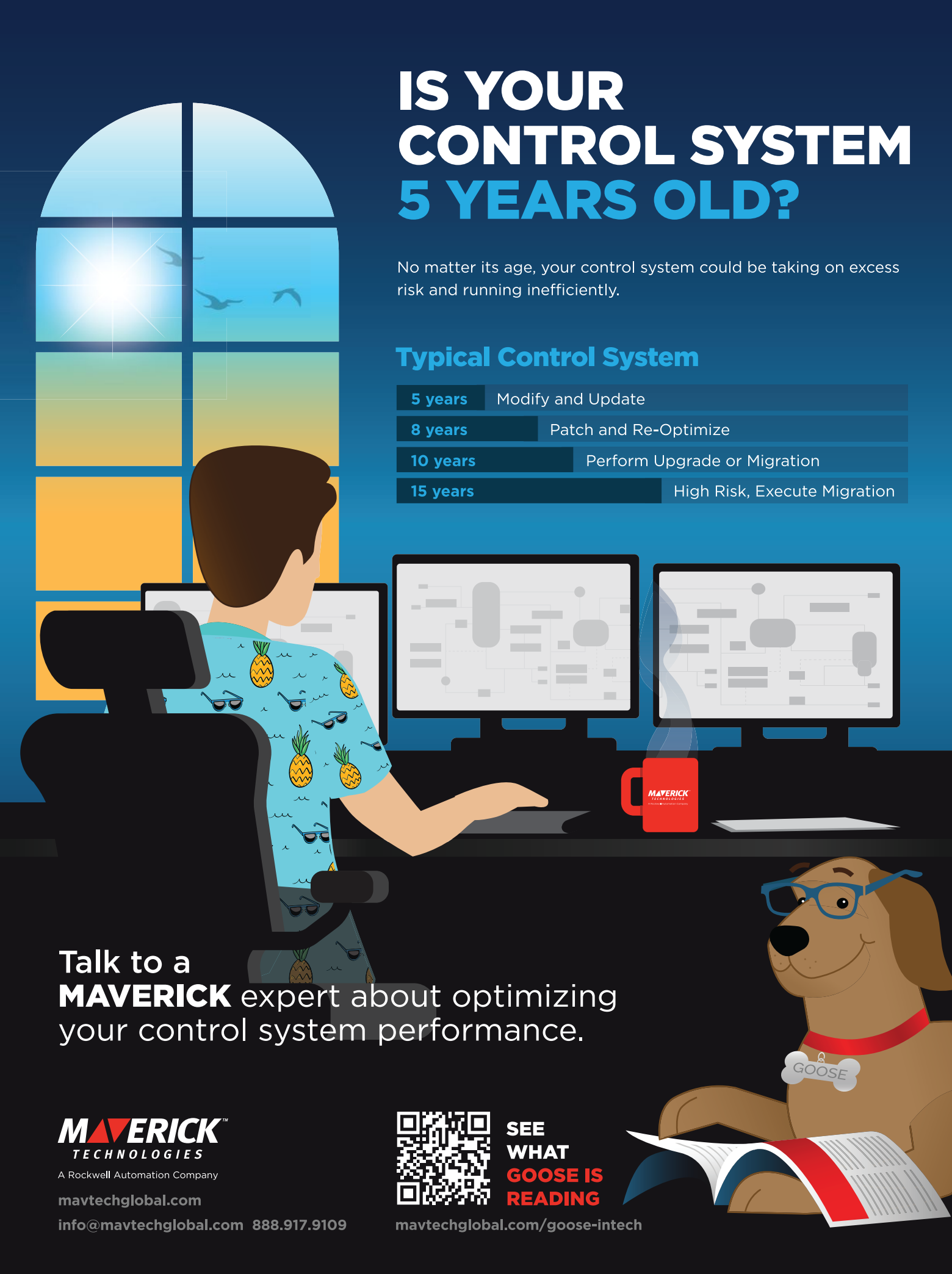


IS YOUR CONTROL SYSTEM 5 YEARS OLD?

No matter its age, your control system could be taking on excess risk and running inefficiently.

Typical Control System

| | |
|----------|------------------------------|
| 5 years | Modify and Update |
| 8 years | Patch and Re-Optimize |
| 10 years | Perform Upgrade or Migration |
| 15 years | High Risk, Execute Migration |



Talk to a **MAVERICK** expert about optimizing your control system performance.

MAVERICK[™]
TECHNOLOGIES

A Rockwell Automation Company

mavtechglobal.com

info@mavtechglobal.com 888.917.9109



SEE
WHAT
**GOOSE IS
READING**

mavtechglobal.com/goose-intech

Ignition! 8.1

by inductive automation

Built For The Plant Floor

Build Mobile-Responsive HTML5 Applications
That Run Natively on Any Screen





! ! 8.1

Try Ignition 8.1 For Free Today at
www.inductiveautomation.com

Built For Everyone



Unlimited Licensing Model

Add unlimited clients, screens, tags, connections & devices.



Cross-Platform Compatibility

Ignition works with any major operating system, even iOS and Android.



Instant Installs and Updates

Install on a server in just 3 minutes, push updates to clients everywhere, instantly.