

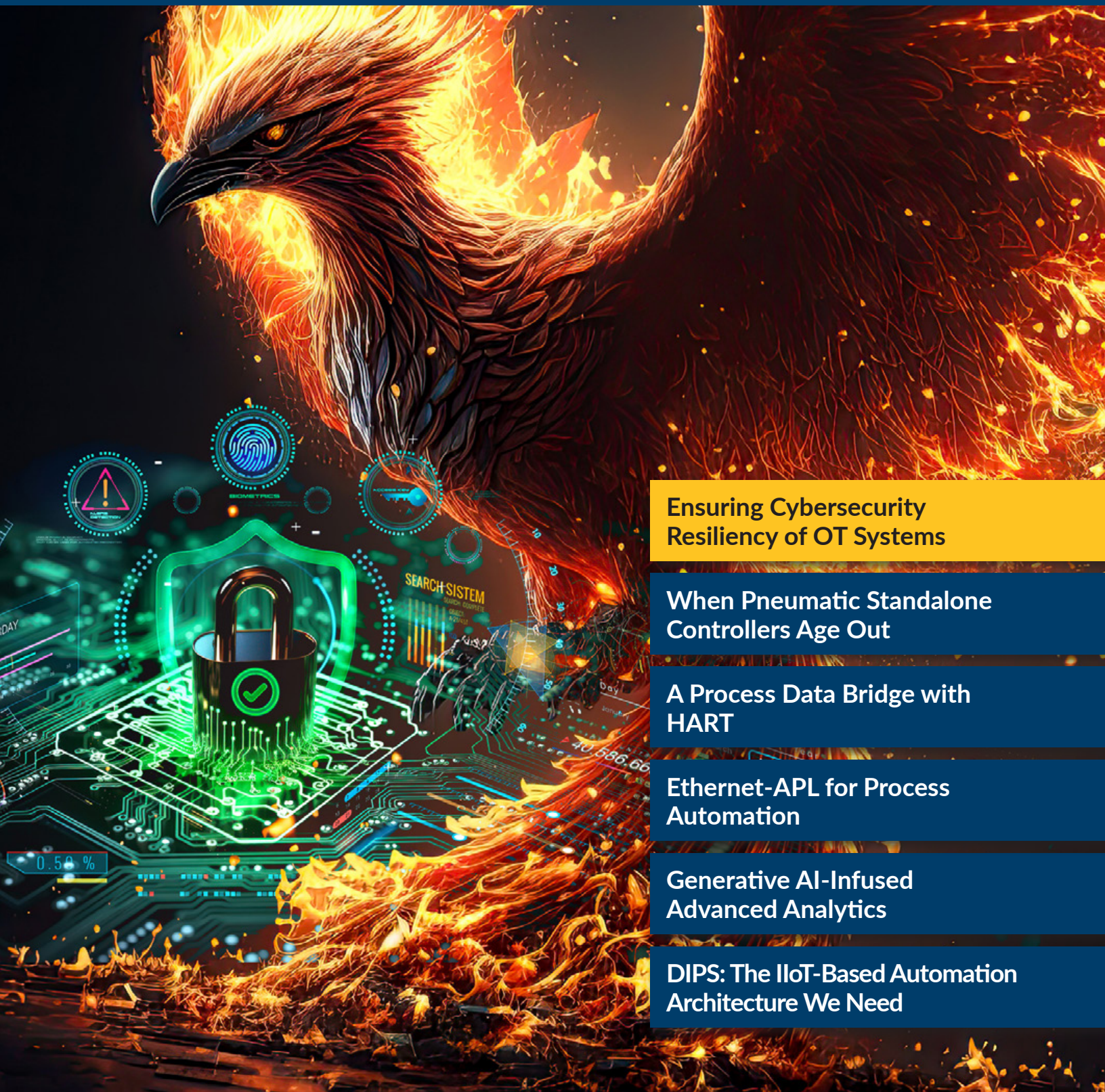
Intech[®]

OFFICIAL PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

APRIL 2024



www.isa.org/intech



**Ensuring Cybersecurity
Resiliency of OT Systems**

**When Pneumatic Standalone
Controllers Age Out**

**A Process Data Bridge with
HART**

**Ethernet-APL for Process
Automation**

**Generative AI-Infused
Advanced Analytics**

**DIPS: The IIoT-Based Automation
Architecture We Need**

WELCOME

Connectivity and OT cybersecurity are the twin themes of this issue of *InTech* digital magazine, the official publication of the International Society of Automation (ISA). Written for engineers, managers, and other automation decision-makers, *InTech* serves ISA members and the wider automation community with practical, in-depth coverage of automation technologies, applications, and strategies that help automation professionals succeed.

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

Don't Miss a Single Issue

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

Rick Zabel, Managing Director

*InTech, Automation.com & Events Sponsorships
International Society of Automation (ISA)*

Advertisers Index

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

 **International Society of Automation**
Setting the Standard for Automation™
Page 11, 46

BECKHOFF
Page 8

Endress+Hauser 
People for Process Automation
Page 6


Page 3


Page 9

MOXA®
Page 4

SEALEVEL®
Page 18


Page 19

VEGA HOME OF VALUES
Page 26

Connect The Dots With Ignition!

The Unlimited Platform for Total System Integration



Go Beyond the Limits

Minimal Size, Maximum Durability

Rugged Durability

- -40 to 75°C operating temperature range available
- High-level EMI/EMC resistance
- Passed a 100% burn-intest

Plug-and-play Simplicity

- Plug-and-play connectivity with QoS and BSP DIP switch functionality

Reliable Network Performance

- Full Gigabit options and Quality of Service (QoS) for optimal performance

Extra-small Footprint

- Plug-and-play connectivity with QoS and BSP DIP switch functionality



Scan or Click
To Learn More



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

GET IN TOUCH

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

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

MOXA®

FEATURES

CYBERSECURITY

12 Ensuring Cybersecurity Resiliency of OT Systems

By Jack Smith

To prevent downtime from cyber attacks, companies need awareness and responsiveness

REMOTE MONITORING

20 When Pneumatic Standalone Controllers Age Out

By Jerry Van Staalduine

With a small solar panel and battery, digital process controllers provide a digital way forward

AUTOMATION BASICS

27 Ethernet-APL for Process Automation

By Thomas Rummel and Christian Bräutigam

With this technology, the digitalization of automation networks is relatively easy to implement

INDUSTRIAL IOT

31 A Process Data Bridge with HART

By Bob Myles

Smart field devices can enable process control, predictive maintenance and more



PROCESS AUTOMATION

36 The Case for DIPS and Distributed, Intelligent Automation

By Deji Chen

How a distributed intelligent production system is made possible by the industrial Internet of Things.

A photograph of two divers underwater in a blue environment. They are both wearing full scuba gear, including tanks and masks. They appear to be interacting, with one diver reaching towards the other's equipment. The lighting is soft, creating a serene and focused atmosphere.

#TeamUpToImprove

Process improvement is like diving.
You need a reliable partner to count on.

Just as athletes rely on their teammates, we know that partnering with our customers brings the same level of support and dependability in the area of manufacturing productivity. Together, we can overcome challenges and achieve a shared goal, optimizing processes with regards to economic efficiency, safety, and environmental protection. Let's improve together.



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

Endress + Hauser 
People for Process Automation

DEPARTMENTS

10 Talk to Me

By Renee Bassett

Connectivity for transformation and resilience

40 Association News

- ISA publishes new book on nonlinear model-based control by R. Russell Rhinehart
- Plan to attend ISA's 2024 Automation Summit & Expo in Charleston, S.C., USA
- A conversation with Deji Chen, ISA Fellow 2024, reveals his extensive work with IIoT standards and systems

44 Executive Corner

By Dustin Johnson

Generative AI-infused advanced analytics fuels digital transformation

47 The Last Word

By Jack Smith

Making Ethernet deterministic has allowed industrial Ethernet to replace fieldbus networks

EDITORIAL & PRODUCTION

CHIEF EDITOR: Renee Bassett, rbassett@isa.org

SENIOR CONTRIBUTING EDITOR: Jack Smith, jsmith@isa.org

EDITOR EMERITUS: Bill Lydon, blydon@isa.org

STANDARDS ADMINISTRATION DIRECTOR:

Charley Robinson, crobinson@isa.org

ART DIRECTOR: Bonnie Walker

DIGITAL DESIGNER: Colleen Casper

DIGITAL PRODUCTION MANAGER:

Melissa Landon, mlandon@isa.org

ISA EXECUTIVE BOARD

ISA PRESIDENT: Prabhu Soundarrajan

ISA PAST PRESIDENT: Marty Bince

ISA PRESIDENT-ELECT & SECRETARY: Scott Reynolds

ISA TREASURER: Ardis Bartle

ISA EXECUTIVE DIRECTOR: Claire Fallon

ADVERTISING & SPONSORSHIP

Rick Zabel, **PUBLISHER**

rzabel@isa.org

Chris Nelson, **ACCOUNT EXECUTIVE**

chris@isa.org

Richard T. Simpson, **ACCOUNT EXECUTIVE**

richard@isa.org

Gina DiFrancesco, **ACCOUNT EXECUTIVE**

gina@isa.org

Cathi Merritt, **ADVERTISING PRODUCT MANAGER**

cmerritt@isa.org

Matt Davis, **DIGITAL MEDIA PROJECT MANAGER**

mdavis@isa.org

2024
Media Planner



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

©2024 International Society of Automation (ISA) ISSN 0192-303X

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

InTech digital magazine is published 4x per year: February, April, June, October. [ISA Members](#) receive *InTech* digital magazine as part of their annual membership and get access to archived issues. Non-members can [subscribe](#) to *InTech* and *InTech* Plus newsletters through ISA's automation news and information subsidiary, Automation.com. *InTech* and the ISA logo are registered trademarks of ISA.

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



International Society of Automation
Setting the Standard for Automation™

What matters most: Your people What protects best: TwinSAFE

PC-based control
One control platform for all machine functions



TwinSAFE
System-integrated with logic in all safety components

www.beckhoff.com/twinsafe

In machine safety, going for “good enough” is never the right choice. Ensuring the safety of your people, equipment and products is simply not optional. TwinSAFE from Beckhoff is the universal safety solution for everything from basic monitoring to complex motion in a fully integrated automation ecosystem. Directly meshing with your PLC, motion control, measurement, IoT and vision technologies, TwinSAFE helps you implement more safety functionality in more places. This comprehensive platform streamlines machine design with programmable safety functionality to safeguard what you value most.



Need a Hand with Protecting Your Process?



Keep Your Process and Plant Safe With **FS Functional Safety Series Instruments** From Moore Industries

Designed and built from the ground up to meet IEC 61508 standards, Moore Industries FS Functional Safety Series instruments help bring the confidence you need to your SIS implementation. Our FS Series now includes the easily programmable, SIL 3 capable SLA Multiloop Safety Logic Solver and Alarm, with voting and powerful built-in math & logic capability.

Keep it Safe by Learning Moore about our FS Series Solutions
Call 800-999-2900 or visit www.miinet.com/fs-automation



Connectivity for Transformation and Resilience

By Renee Bassett, *InTech* Chief Editor



The transformation of industrial businesses is a global phenomenon being pushed by the desire for greater output and efficiency, pulled by technological advances, and challenged by connectivity issues from the mundane (two-wire Ethernet cables) to the potentially catastrophic (OT cyber attacks).

“Industrie 4.0” is one framework helping automation pros transform industrial operations. Launched in Germany and quickly taken up by many companies, Industry 4.0 has become an organizing principle. “Industry 4.0 and related initiatives recognize that efficiently building self-managing production processes requires open software and communications standards that allow sensors, controllers, people, machines, equipment, logistics systems, and products to communicate and cooperate with each other directly,” [said InTech Editor Emeritus Bill Lydon](#) in 2016.

Another framework released by China’s Alliance of Industrial Internet (All) in April 2020—Industrial Internet Architecture 2.0—puts connectivity and communications in the forefront.

Huawei, the Chinese telecommunications giant, [describes](#) the industrial Internet (II) this way: “The industrial Internet is a new infrastructure, application mode, and industrial ecosystem that deeply integrates next-generation information communication technologies with the industrial economy. By fully connecting all elements, including people, machines, materials, and

systems, the industrial Internet builds a brand-new manufacturing and service system covering the entire industry chain and value chain.”

According to Huawei, “With the development of technological and industrial transformation, the Internet has spread from the consumption field to the production field. Industries are also evolving from digitalization to networked and intelligent development, driving the birth of the Industrial Internet.”

In this April 2024 issue of *InTech*, ISA Fellow Deji Chen [describes](#) the functional architecture of the Industrial Internet and its importance. Other authors in this issue dive into physical layer issues addressed by [Ethernet-APL](#) for process automation, smart field devices enabled by the [HART](#) communications protocol, and wireless communications for far-flung process [controllers](#).

The [cover story](#) introduces a related new concept worthy of attention: cybersecurity resiliency. “A core meaning behind cybersecurity is keeping systems up and running and secure against any kind of attack. But when an organization does suffer a hit, the next step in the ladder of protection needs to be resiliency.... OT cybersecurity is evolving into the holistic practice of cyber resilience.”

Look to ISA, *InTech* and Automation.com to bring you more in the months ahead on all these important concepts.





OT CYBERSECURITY SUMMIT

London, UK | 18-19 June 2024



Join us as we explore the forefront of operational technology (OT) security in industries such as energy, manufacturing and building automation.

Our expert speakers and panelists will dive into the leading international standards and conformance systems that are instrumental in safeguarding critical infrastructure and ensuring compliance.

Gain Insights from Experts

Learn from industry leaders, policymakers and cybersecurity practitioners about the latest developments in OT security standards and best practices.

Expand Your Knowledge

Discover how conformance systems are being implemented across industries to improve resilience, reliability and safety.

Network with Peers

Connect with fellow professionals and exchange ideas, challenges and solutions to enhance collaboration and strengthen the industry.

Register Now!

View the full program
and all the event
details at
otcs.isa.org

Special Event

Participate in our immersive OT cyber escape room! Using the latest shared immersive technology, we have created a realistic OT environment in a virtual space.



International Society of Automation
Setting the Standard for Automation™



Ensuring Cyber Resiliency for OT Systems

By Jack Smith

To prevent downtime from cyber attacks, companies need awareness *and* responsiveness.

The Colonial Pipeline hack in May 2021 was the largest publicly disclosed cyberattack against critical infrastructure in the U.S. The attack included multiple assaults against Colonial Pipeline IT systems and, although the operational technology (OT) systems that move oil were not directly compromised, it was a wakeup call for industry and infrastructure. The years since have seen a

much greater understanding of the connection between cybersecurity and business continuity.

Where three years ago “cybersecurity” meant putting out fires and trying to ward off attacks, today companies have realized that attacks are going to happen, and they want to create a plan for cyber resilience—the ability for an entity to continuously deliver

the intended outcome despite adverse cyber events. In this case, the “entity” could likely be your plant and the “intended outcome” is what is produced by your OT efforts.

The adverse event could be intentional, as in a cyberattack, or unintentional as in a failed software update. “Cyberworthiness” is an assessment of the resilience of a system from adverse cyber events. It is applicable to software and hardware elements like stand-alone software, code deployed on an Internet site, browsers, manufacturing equipment, or Industrial Internet of Things (IIoT) devices.


Here’s how to understand how industrial control system (ICS) cybersecurity has evolved, the components of cyberworthiness and cyber resiliency, and how to think about protecting OT systems going forward.

Cybersecurity versus cyber resilience

Cyber resilience is designed to prevent systems and networks from being derailed in the event that security is compromised. The manufacturing line, refinery, or pipeline “stays” operational. Cyber resilience means that cybersecurity efforts are effective without compromising the usability of OT systems.

According to Phil Tonkin, field CTO at Dragos, cybersecurity is concerned with the protection of digital systems, whereas cyber resilience considers the real-world implications of cyber events—extending beyond the digital defense perimeter to encompass the ability of an organization to maintain its core functions and recover swiftly from any form of cyber disruption.

“In the world of OT, infrastructure owners as asset managers are concerned with the integrity and reliability of their assets. An electric company needs to worry about keeping a reliable, efficient, and clean energy supply to its customers. How they achieve that is resilience,” said Tonkin. “It’s not just protecting the system against compromise but managing the risks of downstream effects.”



Cyber resilience is not just protecting the system against compromise but managing the risks of downstream effects.

Greg Hale, editor and founder of ISSSource, said that resiliency is a plan to find ways to keep the plant/network/system up and running despite an ongoing attack. “It is related closely to the business continuity plan. Cybersecurity, on the other hand, is the overall general idea of protecting assets. The government says resilience entails the ability of a system to anticipate, withstand, recover from, and adapt to cyberattacks and natural or accidental disruptions,” he said.

Hale, whose newsletter *The Source* reports on OT safety and security incidents, said in a recent article, “A core meaning behind cybersecurity is keeping systems up and running and secure against any kind of attack. But when an organization does suffer a hit, the next step in the ladder of protection needs to

be resilience—how to stay up and running no matter the type of assault.”

Hale explains the lack of business continuity following the Colonial Pipeline incident. “There was a ransomware attack on the company’s IT department and while OT systems remained up and capable of running, the company shut down completely for about four or five days ‘out of an abundance of caution.’ The real reason was because the company’s billing system was run on the IT side and if that was held for ransom, the company could not bill its customers and therefore could not make any money. So they had to shut everything down. Even though OT was not affected, they had no plan on what they should do to stay running in case of an attack.”

Mansur Abilkasimov, vice president of Cyber and Product Security Strategy and Governance at Schneider Electric, concurs: “Cybersecurity focuses on the implementation of capabilities and controls such as

identification, detection, protection, and so on, whereas resilience relates to the ability to withstand attacks, bring appropriate response, and recover swiftly.” He said the cybersecurity threat landscape is continuously evolving and, as a next step, organizations should validate if their cybersecurity controls can respond to their current environment or threat landscape.

One way to plan for cyber resiliency

As a manufacturer of electrical distribution and control hardware and software products for commercial, industrial and residential markets, Schneider Electric approaches its cybersecurity resiliency planning in a multifaceted way. Abilkasimov said the strategy starts at the top with cybersecurity objectives set by the company’s Global Chief Information Security Officer, or CISO, and the implementation of the strategy is carried out by the executive management team.



Cyber resilience means that cybersecurity efforts are effective without compromising the usability of OT systems.

“A key element of the initiatives are the employees, so the resilience strategy includes robust training and education of all employees,” he said. “The company-wide, risk-informed approach has preventive (breach readiness) and response (breach resilience) measures in place for potential incidents.” It includes:

- **Employee training and awareness:** The company aims to raise employee cybersecurity awareness, provide relevant training, and create a culture to empower employees across IT and OT to act in a secure manner. The training includes an annual baseline awareness course for all employees and role-based trainings for specialized populations including cybersecurity site leaders.
- **Enterprise risk management (ERM) framework:** The company categorizes and translates cybersecurity risks into business and operational scenarios and exposure. This exposure is communicated with the C-suite to drive investments in risk mitigation initiatives. This framework is aligned to National Institute of Standards and Technology (NIST) [Cybersecurity Framework](#) and increases the company’s overall level of cyber resilience.
- **Incident response capabilities:** The company is constantly testing and improving its capacity to respond to operational disruption, damage to customers, compliance issues, and IP theft. Its incident response plans are defined, and stress-tested routinely to ensure preparedness. The Security Operations Center (SOC) operates



Figure 2. One of the classic cases of a lack of cyber resilience is the Colonial Pipeline incident.

- 24/7/365 and is staffed with security analysts leveraging security incident and event management (SIEM) capabilities with OT scenario-based playbooks and responders.
- **Crisis simulation exercises:** Crisis simulations aim at training senior executives through operational roles, enhancing external collaboration and internal coordination, and reviewing internal processes around crisis resolution. The company’s simulation activities follow a comprehensive framework with realistic and risk-based scenarios for the best outcomes and learning. The goal is for simulations go beyond testing and training and focus on examining and improving operational processes while enhancing readiness for future crises through experiential learning. Abilkasimov said the combination of these programs ensures that cybersecurity risk is not an afterthought for the organization, but rather an intentional practice to ensure cybersecurity resilience.

Understand the threats and the vulnerabilities

Another important aspect to resiliency planning is understanding the specific threats to and vulnerabilities of critical systems and assets. “This begins with a thorough assessment to identify the crown jewels—the most critical components of an organization’s operations,” said Tonkins. Based on such an assessment, Dragos advocates implementing controls that are proportionate to the actual threats and vulnerabilities identified.

Tonkins provides an example: A prominent water utility, responsible for managing 20 dams and 2,000 kilometers (1,243 miles) of pipelines, recognized the critical nature of its infrastructure and took steps to adopt a proactive cybersecurity stance to get ahead of potential threats. Audits pinpointed areas that needed improvement, raising leadership’s awareness of the importance of OT cybersecurity.

When seeking a cybersecurity provider, the utility prioritized OT-specific expertise and reputable providers of technology that could provide visibility of ICS assets and communications. The utility adopted the Dragos OT cybersecurity platform to streamline and advanced its cybersecurity programs to ensure the secure delivery of water to more than 5,000 commercial customers and enable critical projects in collaboration with industry, mining, and government agencies, Tonkins said.

The partnership with Dragos resulted in increased efficiency, productivity, and cybersecurity readiness and “the utility is [now]

prepared to counter evolving cyber threats,” said Tonkins. It also plans to expand the footprint of the Dragos Platform in the future by adding sensors at prioritized sites, he added.

Organizations must shift from a futile quest for absolute invulnerability to a more realistic strategy of resiliency, in which they can control the impacts of failures.


Automate—with caution

Sensors and other automation can enhance cybersecurity efforts. Because most cyberthreats, such as ransomware or worm attacks, spread quickly and automated systems can detect and respond to them much faster than humans can. Artificial intelligence can also be useful because it ensures consistency and can perform repetitive tasks with high accuracy. However, it can be easy to rely too heavily on automation to provide cybersecurity, said Zac Amos, features editor at *ReHack* and frequent contributor to the blog put out by the ISA Global Cybersecurity Alliance (ISA GCA).

In the [blog post](#) titled “The Danger of Overreliance on Automation in Cybersecurity,” Amos wrote that “the volume of logs, alerts, and incidents is multiplying exponentially, and automated tools can analyze vast amounts of data without getting overwhelmed. This can

be a double-edged sword, though. Companies should have a healthy balance of tech and human talent when keeping systems safe.”

Amos warns that some of dangers of being overly dependent on automation in cybersecurity include a false sense of security, false positives and/or negatives, lack of context, reduction in human expertise, and reliability concerns. “Believing that automated systems will catch every threat can make organizations complacent. No system is perfect, and new, unforeseen threats are always emerging,” he said.



Crisis simulations aim at training senior executives through operational roles, enhancing external collaboration and internal coordination, and reviewing internal processes around crisis resolution.

“Automated systems can generate false positives, which can desensitize security teams if they happen frequently,” Amos said. “Conversely, false negatives, where a genuine threat goes undetected, can have severe implications.” In addition, “automated systems lack the human intuition and context needed to evaluate the risk and importance of a particular alert. A seasoned security expert can differentiate between a benign activity that looks suspicious and a genuine threat.”

Over-relying on automation reduces the need for human experts, which means an organization might have fewer experts who fully understand the system, Amos added. This can be dangerous if things fail or are compromised. Also, “like any technology, automated systems can fail. Overreliance without redundancy can lead to exposure when these systems experience downtimes,” he said.

Awareness is key

OT cybersecurity is evolving into the holistic practice of cyber resilience—as it must, said Hale. Organizations must “shift from a futile quest for absolute invulnerability to a more realistic strategy of resiliency, in which they can control the impacts of failures.” Resilience means organizations need to identify the most critical assets and determine what they find as an acceptable return to operations.

Compared to three years ago, “organizations are more aware and more tuned into the idea that attacks are going to happen, so they better be protected,” said Hale. “They are learning they must then understand—and have a plan—for what they should be doing and what should happen if an attack makes it in and starts to create issues.” This is also where quality segmentation and micro segmentation come into play, he said.

Industry is maturing in its understanding of cybersecurity, agreed Tonkin. “Gone are the days of lacking broad attention for the topic when it was viewed as a technical issue rather than a strategic one. Today, the subject of managing cyber risks to improve operational integrity and resilience is becoming much

CYBERSECURITY

more aligned with the overall risk management of organizations.”

Tonkin added that this maturation in approach reflects a deeper understanding of the interconnectedness between cybersecurity and business continuity. Organizations are now more proactive in identifying and

protecting critical assets, assessing vulnerabilities, and implementing comprehensive cybersecurity measures that support resilience. This includes not just technological solutions but also organizational and procedural changes to enhance the ability to withstand and recover from cyber incidents.



ABOUT THE AUTHOR

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

The Flexibility You Need Meets The Performance You Demand Finally.



NEW Flexio Fanless Industrial Embedded Computers

- Industrial Processing & Performance with Long-Term Availability
- Solid-State Design Guarantees Extended Operation
- Unmatched I/O Configurability for Automation & Control

Sealevel Systems is the leading designer and manufacturer of rugged industrial computers, Ethernet serial servers, USB serial, PCI Express and PCI bus cards, and software for critical communications. We deliver proven, high-reliability automation, control, monitoring, and test and measurement solutions for industry leaders worldwide.

What's more demanding than your requirements?
Our quality, reliability, and configurability standards.

SEALEVEL[®]
sealevel.com



Reliability, Availability, and Support Beyond the Life of Your Mission

No place to replace a battery.

PROVEN
40
YEAR
OPERATING
LIFE*

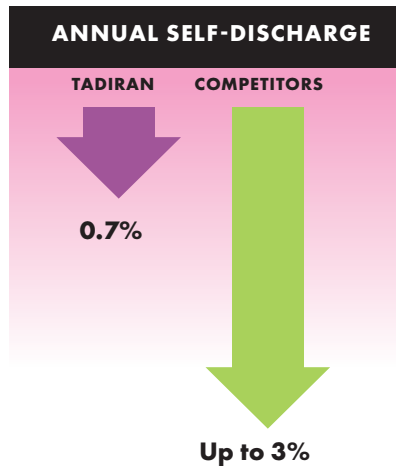
Highly remote locations call for Tadiran batteries.

Battery replacement is costly and often dangerous work. Reduce the risk with Tadiran bobbin-type lithium thionyl chloride (LiSOCl_2) batteries. With an annual self-discharge rate of just 0.7% per year, Tadiran LiSOCl_2 batteries enable low power consuming wireless devices to operate for up to 40 years on a single battery, up to 4 times longer than the competition. Our batteries also feature the highest capacity, highest energy density, and widest temperature range of any lithium cell, plus a glass-to-metal hermetic seal for added ruggedness and reliability in extreme environments.

Take no chances. Take Tadiran batteries that last a lifetime.



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



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

www.tadiranbat.com

When Pneumatic Standalone Controllers Age Out

With a small solar panel and battery, digital process controllers provide a digital way forward.

By Jerry Van Staaldaine

They are out there. Largely ignored and scattered across remote oilfield sites, tank farms, and isolated process units they sit, quietly hissing now and again, and steadfastly doing their job as they have for years. Unfortunately, their days are numbered.

Affectionally known as “wind powered” and incorporating temperature or pressure sensors, standalone pneumatic controllers have been used to locally control level, pressure, flow, and temperature in remote locations for decades, requiring only low-pressure air or line-pressure natural gas for operation. Despite breathtaking leaps in control technology improvements, these controllers are still a simple and acceptable solution for many niche applications.



REMOTE MONITORING

More than 2.3 million of these devices are still in service but many vendors no longer make them, and more are abandoning the market every year. So, finding a direct replacement can be difficult. In addition, pneumatic controllers have a range of inherent limitations—not the least of which is finding personnel skilled with maintaining this technology—that make direct replacement less than ideal. This article discusses alternative process controller designs that address the issues with pneumatic controllers while providing a host of additional benefits.

Quietly doing their job, but for how long?

Pneumatic controllers have been around since the 1940s. Through the years, the pneumatic controller has been minimally upgraded (Figure 1), with some devices incorporating remote setpoints and full PID control algorithms, and a few devices adding some means for remote monitoring. Still, the bulk of applications use a simple local controller keeping a process

on setpoint in a remote area. Through good weather and bad, these devices operate 24/7, adjusting a pneumatic valve as necessary to keep the process on track.

Unfortunately, there are aspects of pneumatic controllers that limit their utility and can create issues. Pneumatic controllers incorporate many moving parts, and over the years those parts eventually wear and fail. Control to setpoint degrades over time and ultimately stops, creating production losses and downtime. Most of these controllers provide no means of remote monitoring or adjustment, so when control degradation or an outright failure does occur, it is not noticed until deviation from setpoint creates problems affecting production.

Even when the existing pneumatic controller is an acceptable solution, fixing the unit or finding a replacement has become increasingly challenging as few technicians can work on pneumatics, and many pneumatic controller vendors have exited the market.



Figure 1: Pneumatic controllers have been in service for decades. While the underlying technology is ancient, the need for local control in remote applications is very much still in strong demand.

Remote control alternatives

Control vendors recognized this developing problem and worked to resolve it. Local controller replacements have become available that satisfy the needs of remote, standalone control—yet take advantage of the latest technology to enable significantly improved control performance, while providing remote access, monitoring, and control.

These replacement digital process controllers do require electrical power, but at less than one watt, this can easily be furnished with a small solar panel and battery. However, the addition of such a nominal amount of power yields dramatic improvements in control capability, and it enables remote monitoring and control. These devices also incorporate several configurable I/O options that allow a single device to address a host of control needs (Figure 2).

The latest process controllers incorporate two analog inputs that can accept 2- or 4-wire inputs. The primary input is used as the primary process variable in a PID loop, and the second can be used to accept a remote hardwired PID setpoint, or it be used to pick up a second process variable for internal monitoring. One of these inputs can be replaced with an integrated pressure sensor with ranges from 0-30 to 0-1,500 PSI, and this value can be used as the process variable in the PID control loop. The PID control loop output is a 4-20 mA signal, or an integrated pneumatic module can provide a 3-15 PSI signal.

The device is rated Class 1 Division 1, and it uses low-bleed Quad O certified components, so it can run on air or natural gas and still meet the latest EPA emission requirements. This allows the controller to be used in a broad range of remote-control applications,

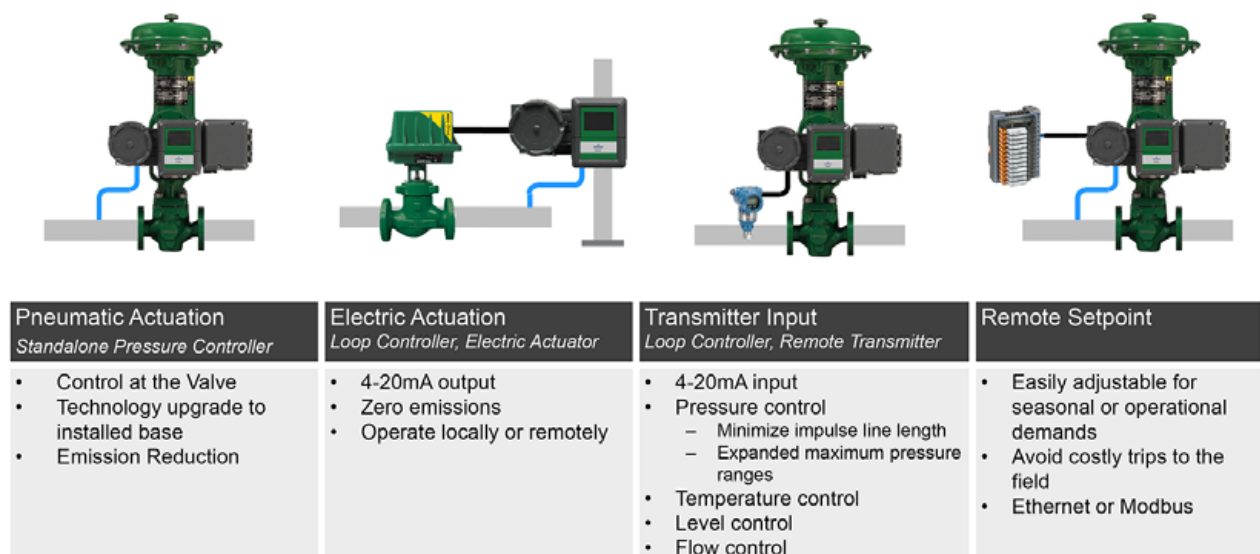


Figure 2: Replacements for pneumatic controllers (Fisher FIELDVUE DPC2K shown) allow a single device to handle a variety of remote control and positioning applications, including PID and remote setpoint control, via electronic or pneumatic signals.

REMOTE MONITORING

including oil and gas industry remote sites and other hazardous locations.

These replacement controllers also include an integral linkless positioner feedback to handle control valve positioning duties. The positioner works on rising stem valves from most control valve vendors, as well as some rotary valve designs. The controller can be mounted on the valve (allowing positioner feedback), or it can be remotely mounted if a positioner is not required. When purchased with the integral pressure sensor and pneumatic output module, this single device can replace a pressure transmitter, controller, and valve positioner.

Taking advantage of technology

These types of hybrid controller replacements also take advantage of the latest technology to address the inherent limitations of pneumatic controllers. The digital PID loop operates on 50 millisecond cycles, making it suitable for very fast and difficult to control process applications.

The list of advanced control options and parameters includes anti-reset windup, dynamic reset limiting, and configurable deadband, enabling this type of controller to provide far superior tracking to setpoint as compared to its pneumatic predecessor. A local digital interface (Figure 3) displays control data, and it allows easy setpoint and configuration modifications at the device.

In many applications, the most important technological advance will be the remote communication capabilities that are now incorporated within the controller. These



Figure 3: A local digital display on a pneumatic controller provides easily visible process data, and a simple six-button interface enables local configuration of advanced controls, alarms, alerts, and communications parameters.

types of devices can typically communicate via Modbus TCP, HART IP, and/or Modbus RTU RS-485. The Ethernet port can handle multiple protocols simultaneously using Modbus TCP or HART IP, and all digital protocols provide remote control and monitoring capability.

This communication capability allows the local controller to independently perform its control tasks, while providing a means to remotely change setpoints, gather analog signals from up to two devices, detect alarms and equipment alerts, and reconfigure the device if necessary. With this capability, the pneumatic controller is no longer an isolated island of automation, but it can instead provide process data to indicate developing problems, empowering plant personnel to react proactively to minimize downtime and production loss.

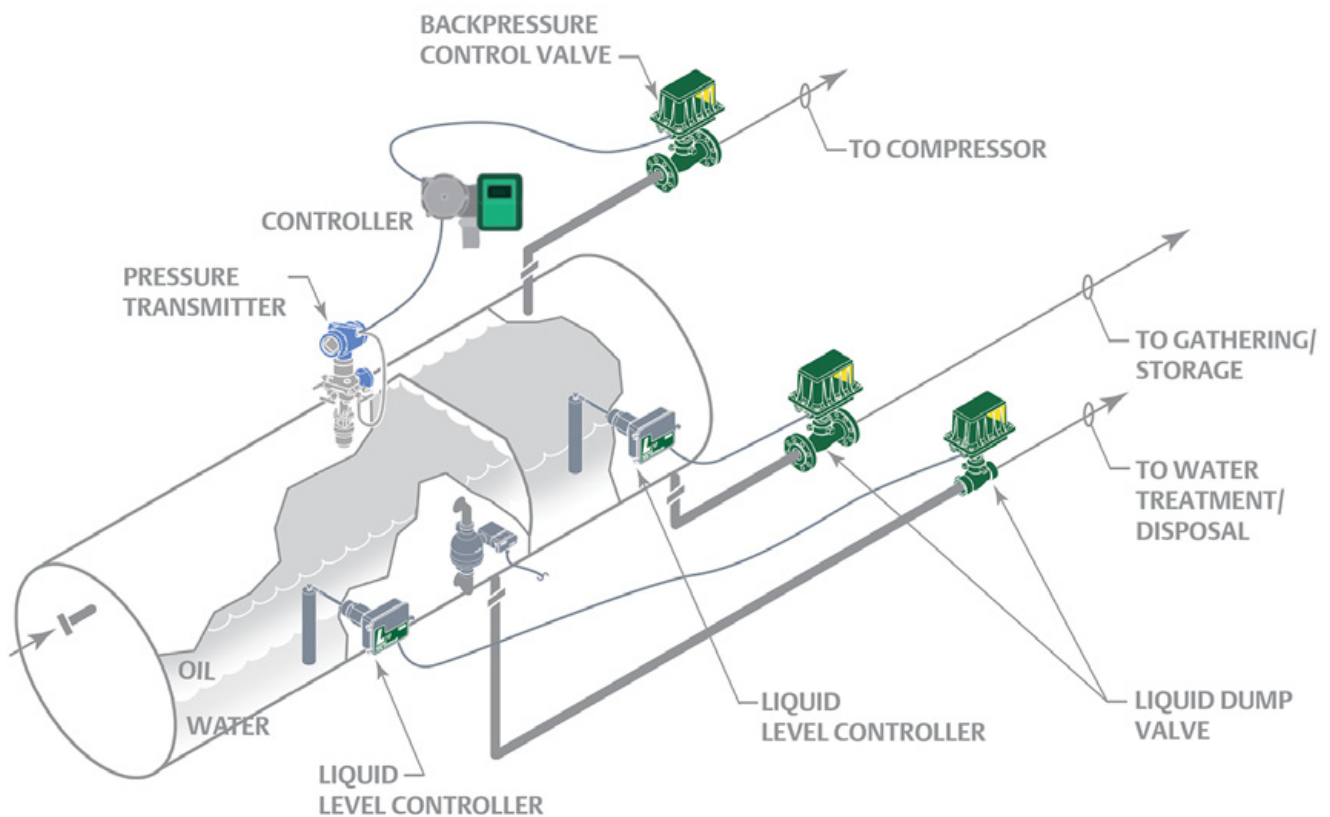


Figure 4: While oil/water and oil level control can be effectively regulated without a PID controller, oil separator backpressure control requires a more advanced solution.

These new controllers have also been designed with ease of use and maintenance in mind. Configuration is simple and straightforward, using intuitive menus at the device, or via a free software application with remote access. Maintenance is greatly reduced due to the lack of moving parts, and when needed it requires little technical knowledge since the pressure sensors and pneumatic output sections are modular and can thus be easily replaced.

Applications for standalone digital process controllers

Standalone digital process controllers are often the preferred solution for a wide variety of single loop control applications. Common use cases include heaters in tank farms,

pressure and temperature controllers for heat trace applications, and fuel gas train pressure controllers. These controllers are also frequently used on equipment skids where local control is required.

Another very common application is a back pressure controller for remote wellhead oil separator applications (Figure 4). While oil/water interface and oil level control can be accomplished by other means, backpressure control on the separator usually demands tighter tracking to setpoint, as can be provided with a PID controller.

These new replacement process controllers are tailor made for this application and are often employed during wellhead

REMOTE MONITORING

electrification projects to limit or eliminate methane emissions. The controllers can also be used in advanced oil recovery projects that require local flow or pressure controls at remote wellhead sites.

Another common application is tank blanketing applications. These advanced pneumatic controllers provide local and independent pressure control, and they also provide a means to remotely monitor tank pressure, and alarm if the blanketing system is not operating correctly. This type of solution is far superior to a blanketing pressure regulator, which tends to droop at high flows and offers no means of pressure feedback.

Conclusion

If your plant has a number of aging pneumatic controllers—or if you encounter an application where remote, independent

control is necessary—consult with your valve automation vendor to investigate new standalone digital process controllers. The control capability of these new solutions is far superior to what has been available to date, and their flexibility allows them to be used in a very wide variety of flow, pressure, temperature, and level control applications.

These pneumatic controller replacements also offer the ability to monitor, control, and even configure these devices remotely, and they provide a wealth of process data previously unavailable from these remote, single-loop control applications. These venerable pneumatic controllers have done their duty for decades, but as they age out, a very capable and superior replacement is now available.

All figures courtesy of Emerson



ABOUT THE AUTHOR

Jerry Van Staaldaine is a 25-year Emerson employee with the Flow Controls business unit in Marshalltown, Iowa, USA. He has been in the automation, measurement and control industry for 35 years, and he is currently responsible for new product development of the [Fisher FIELDVUE DPC2K](#) electro-pneumatic single loop controller.

We bring color into view!

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



256 colors

Individually selectable:

- Measurement in progress
- Sensor switching
- Process malfunction

Compact design



Hygienic adapter system



IO-Link



Adjustment via smartphone



\$518

VEGABAR 39 Clamp 1"

www.vega.com/vegabar

VEGA HOME OF VALUES

Ethernet-APL for Process Automation

**With this technology,
the digitalization of
automation networks
is relatively easy to
implement.**

By Thomas Rummel and Christian Bräutigam

Ethernet-APL (Advanced Physical Layer) is the new standard for the process industry. It is based on the 10BASE-T1L specification as per IEEE 802.3cg and facilitates two-wire Ethernet to the field. The primary advantage of Ethernet-APL is the interoperability and flexibility achieved by the seamless connection of field devices with rapid data

transmission on the information layer, in both small networks at short distances as well as in large networks covering long distances. Importantly for the process industry, Ethernet-APL also supports the intrinsically safe ignition protection type “i” in Ex Zones 0, 1, and 2. With the Ethernet-APL technology, the future digitalization of automation networks is relatively easy to implement, assuming several preconditions concerning network topology are considered as part of the equation.

For end users, Ethernet-APL creates new layout opportunities when building high-performance automation networks. Field devices can be integrated seamlessly into the network—and we’re not talking about a few pieces of equipment but millions of installed devices, such as small sensors, control units, or highly complex analytical instruments. Every year, a similar volume of new devices

is added, with most of these still using 4–20 mA technology, potentially supplemented by digital point-to-point communication over the HART protocol.

Formally adopted in 2021, Ethernet-APL is a new standard for end-to-end Ethernet communication. The standard accounts for the specific requirements of the process industry, like the bridging of large distances with a simple, two-wire conductor that not only handles data communications but also supplies power to the connected field device. Another significant step was taken by increasing transmission rates to 10 Mbps compared to HART and field buses.

APL limits itself to defining a new data exchange standard for Ethernet at the lowest layer, ensuring that it retains compatibility with any Ethernet-based protocols at higher layers. For the first time, this makes transparent communication possible between production and company networks down to field devices, while removing the need for expensive gateways. Automation protocols can be deployed as required, as can web servers, OPC UA, and cloud/edge connectivity.

Network typology variants

Looking at the huge number and diversity of plant types, the various models involved and the range of sizes, a network system should be easy and inexpensive to expand and should offer redundancy while being able to handle the specific requirements of the process industry, including harsh environments or operation in potentially explosive atmospheres. The Ethernet-APL Engineering

[Guideline](#) outlines a number of network topologies for Ethernet-APL networks, although the circumstances for the Ethernet-APL spurs are the same for all topologies. Ethernet-APL devices can be connected to a switch by a Category IV cable (no longer than 200 m) and can communicate at a transmission rate of 10 Mbps. Let's take a closer look at three of these variants.

Variant 1: APL field switches are connected directly to a standard Industrial Ethernet network, with the configuration of the installation environment largely determining the location – i.e., whether these are installed in the control cabinet or out in the field (Figure 1). In this version, the APL switch is connected directly to the control network using normal Ethernet copper cables or fiber-optic cables. The typical transmission rate in this section of the network will be 100 Mbps. This is equivalent to today's Fieldbus

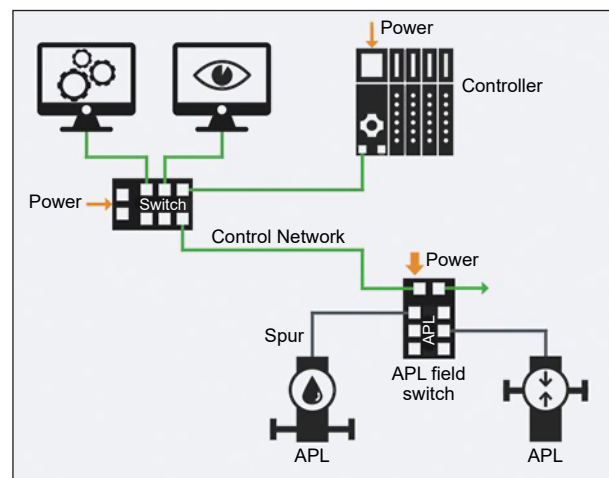


Figure 1. In network Variant 1, APL field switches are connected directly to a standard Industrial Ethernet network, with the configuration of the installation environment largely determining the location – i.e. whether these are installed in the control cabinet or out in the field.

structures and is intended to accommodate the brownfield plants that were installed at a time when the rapid pace of digitalization was not yet foreseeable and process control fell far short of today's requirements—but is now being asked to keep step with 21st-century developments.

Variants 2 and 3: These variants envisage a network structure that is similar to the one in the first variant but are implemented using trunk technology with conventional APL switches (Figure 2). In this scenario, there are two variants that differ in their choice of deploying an APL power switch with an autonomous energy supply or deploying an APL field switch that needs to be powered with an additional energy source.

In terms of installations in ATEX environments, the 2-WISE explosion protection

model (2-Wire Intrinsically Safe Ethernet) should be mentioned at this juncture, which builds on the tried-and-tested FISCO (Fieldbus Intrinsically Safe Concept) model.

Network stability

To ensure that a PROFINET network can be operated to be both stable and fail-safe, it is essential to monitor the load that Ethernet-APL devices are exposed to. Continuous control of load peaks works to prevent sporadic outages affecting individual devices due to overloading. This is achieved by limiting the ingress and egress data traffic at switch ports—as also envisaged by the IEEE (Institute of Electrical and Electronics Engineers)—because where networks transition in the switch from 100 Mbps to 10 Mbps, a higher network load in the 100 Mbps control network is especially critical

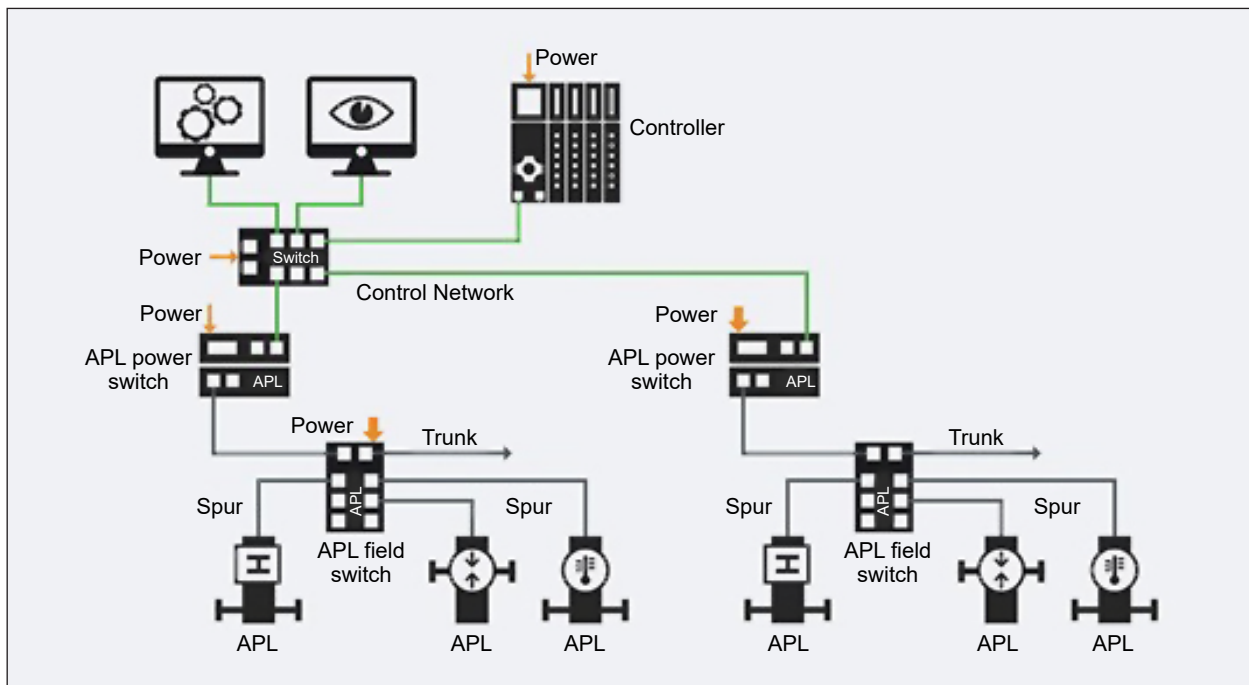


Figure 2. Network Variants 2 and 3 envisage a network structure implemented using trunk technology with conventional APL switches that either have an autonomous energy supply or need to be powered with an additional energy source.

for the Ethernet-APL devices on the 10 Mbps spurs. This 10 Mbps is, after all, only 10% of the data throughput compared with the control network.

APL limits itself to defining a new data exchange standard for Ethernet at the lowest layer, ensuring that it retains compatibility with any Ethernet-based protocols at higher layers.

As already mentioned, the net load is a critical factor that needs to be effectively countered. Accordingly, vendors have developed special Ethernet-APL switches that set the respective net load rate limits to ensure stable network operation without overloading, and which support both copper and fiber-optic connections. These are especially suited to the Variant 1 network topology mentioned above.

One way to implement new Ethernet-APL-compatible devices within a short time-to-market is to use an electronics module

providing all the hardware and software components needed for communications, such as the Softing commModule APL. This SMD hardware module with a pre-installed PROFINET stack offers a configurable application data model as well as command mapping that can be used to migrate existing HART and Modbus devices to Ethernet-APL without code having to be written. Assignments to HART or Modbus commands are made using the corresponding commScripter tool.

Ethernet-APL offers a wealth of flexibility and options for individual network structures and a level of maturity permitting the deployment of corresponding devices in production environments. It has other obvious benefits too as it avoids hardware costs, no dedicated gateway components need to be purchased and no expert-level configuration tasks are required to integrate with the upstream Ethernet infrastructure of the equipment responsible for these gateways. An implementation should nonetheless be planned and structured properly to exploit all the advantages of this new standard—and Ethernet-APL should certainly be considered as a candidate for any future planning work.

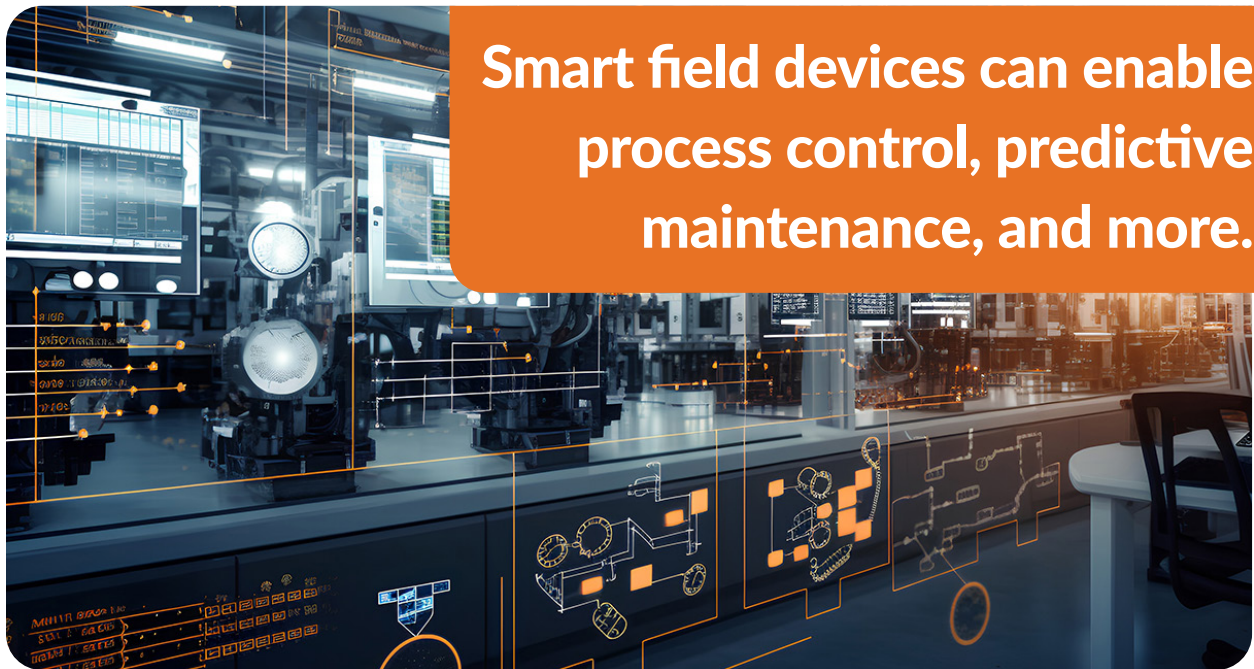
All images courtesy of Softing.

ABOUT THE AUTHORS

Thomas Rummel is managing director and **Christian Bräutigam** is senior product manager with [Softing Industrial Automation GmbH](#), makers of Ethernet APL solutions. A version of this article first appeared in a [Softing blog](#) post.

A Process Data Bridge with HART

By Bob Myles



Smart field devices can enable process control, predictive maintenance, and more.

Moving critical plant floor data into higher level control and information systems—within a manufacturing facility or into the cloud—no longer must be difficult or expensive. The combination of the Industrial Internet of Things (IIoT), industrial Ethernet backbones, and wireless networks means there is a quick and seamless way to share process data with the entire corporate infrastructure. And the devices to build the bridge may already be installed.

HART, a communication protocol that has been around since the early '80s, is the foundation for the more than 40 million HART devices currently installed worldwide. HART

enabled devices superimpose a digital signal upon their 4-20 mA process signal so that it can contain additional process measurements and other variables: instrument status, diagnostic data, alarms, calibration values, alert messages, etc. This data can then be shared from smart HART digital field instruments to mid- and higher-level control, asset management and data information systems without having to upgrade expensive process control interface equipment. This whitepaper excerpt explains how. (See the full paper for more information or visit the [FieldComm Group](https://www.fieldcommgroup.com) website for a more in depth and complete primer on HART.)

Information hierarchies

As the desire to exchange data between industrial and business systems has become more commonplace, the separate information hierarchy levels outlined in the ISA 95 model (Figure 1) have started to coalesce. In prior years, data and information that needed to be exchanged between the lowest plant floor levels 0-2 and the upper Enterprise Resource Planning (ERP) level 4 required expensive Manufacturing Execution Systems (MES) products or custom coding—and often both. The free flow of information has introduced a new set of ubiquitous terms, standards and phrases such as IIoT, smart factory, cloud automation, and Industry 4.0.

While the HART field transmitters are hard at work measuring process parameters and producing a 4-20 mA signal for use by a basic process control system (BPCS), a programmable logic controller (PLC) or some other control system, the rest of the HART data often goes unused. One reason is the prohibitive

cost of installing a plantwide monitoring system to gather HART data. Another is a lack of familiarity with the alternatives.

A simple and cost-effective solution is to use a HART interface device, which makes acquiring HART data a simple proposition (Figure 2). Smart HART field devices like the HES HART to Ethernet gateway built-in security measures, open industry protocols, and ease of programming.

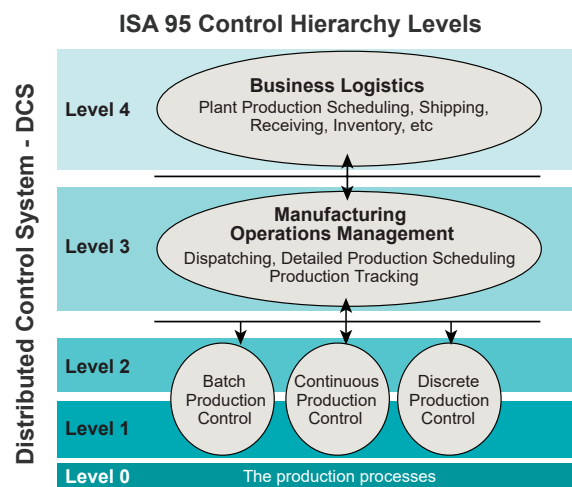


Figure 1. ISA 95 Model showing control and information levels.

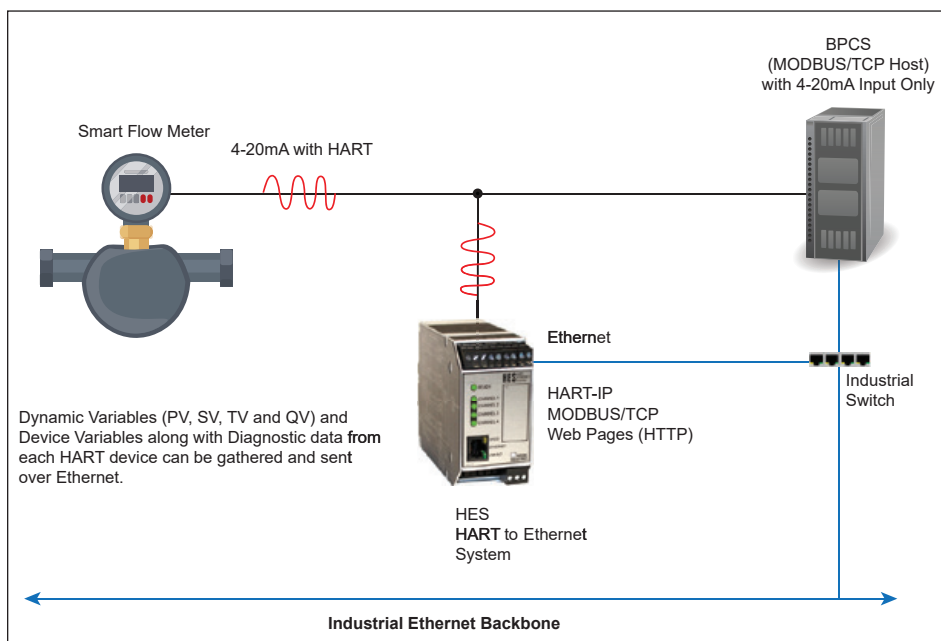


Figure 2. A HART interface device like the HES HART to Ethernet gateway connects to the 4-20 mA process signal and extracts HART process and diagnostic variables and makes them accessible via Ethernet.

Protocol revisions and compliance

It is important to note that HART data uses specifically defined universal and custom commands outlined within the HART specification. The HART specification has also had updates to the protocol, referred to as revisions, which have additional capabilities. Most HART devices operating in the field today use revision 5, 6, or 7.

HART devices can provide a lot of additional data to the primary variable read on the 4-20 mA loop. In addition to diagnostic and status bits and bytes, there are two types of HART variables that you can retrieve from HART devices: dynamic variables and device variables.

All HART variables support IEEE 754 Floating Point values and are retrieved by HART hosts or interface devices (commonly referred to as gateways or multiplexers) from

the field device. Dynamic variables consist of the primary variable (PV), secondary variable (SV), tertiary variable (TV) and quaternary variable (QV). Device variables may also be used in more sophisticated or multi-variable field devices to provide additional process, diagnostic, or status related information. Device variables are only available in HART 6 and 7 revision field devices.

HART interface options

There are many HART interface options: HART enabled 4-20 mA input cards, HART multiplexer (Mux) systems, slide-in PLC gateway cards, custom-coded software interfaces for asset management and MES/ERP systems, and standalone gateways that typically convert the HART data to some other proprietary or open industry format.

Many PLC and BPCS cards installed in legacy systems don't have the capability to

Cybersecurity Considerations

IIoT, cloud storage, big data, and a host of other interconnecting methods and strategies has led to no shortage of production and efficiency increases. Unfortunately, these have not been, nor do they continue to be realized without a cost and threat from cybersecurity issues. For these reasons it is more important than ever that Ethernet-based devices include safeguards within their products to ensure that: network bandwidth is protected, viruses or malware cannot be loaded, unwanted access is not granted, unauthorized reconfiguration of device is not

allowed, and unauthorized writes to memory locations are not accepted by the device.

In addition, physical security of such devices must be restricted to authorized personnel only and process values should be read only—unless the device is required to perform control. Post installation considerations should also be taken to assist onsite protection of site data and property. At a minimum, a two-layer protection scheme should be put in place for any Ethernet enabled device that includes software and physical hardware restricted access.

read the HART data superimposed on the 4-20 mA signal. However, each control system vendor usually has an alternative card or offers an upgrade path for the CPU/controller and input cards to read HART.

HART multiplexers are common. Typically their interface is a custom RS-422, RS-485, or RS-232 serial connection and the multiplexer is custom-configured for a particular vendor's hardware interface, asset management system or control system. Some PLC and BPCS companies offer slide-in chassis-type gateway cards that read the HART data and offer a proprietary backend communication connection to the system. Often, each of these options is quite costly. The most expensive but also most specific HART interface is the one written by

a programmer, which can be customized to exact user and hardware specifications.

Another interface option is a standalone HART gateway. These most often provide the most economical pathway to extracting HART data from field devices. They usually offer one to four channels or ports that allow several HART devices to be multi-dropped for maximum data concentration (Figure 3).

Employing the extracted HART data

Once HART data is extracted from field devices, it is essential that the information is made available in an open and easy-to-interface manner. Now that Ethernet backbones (often further propagated by fiber and wireless modems for

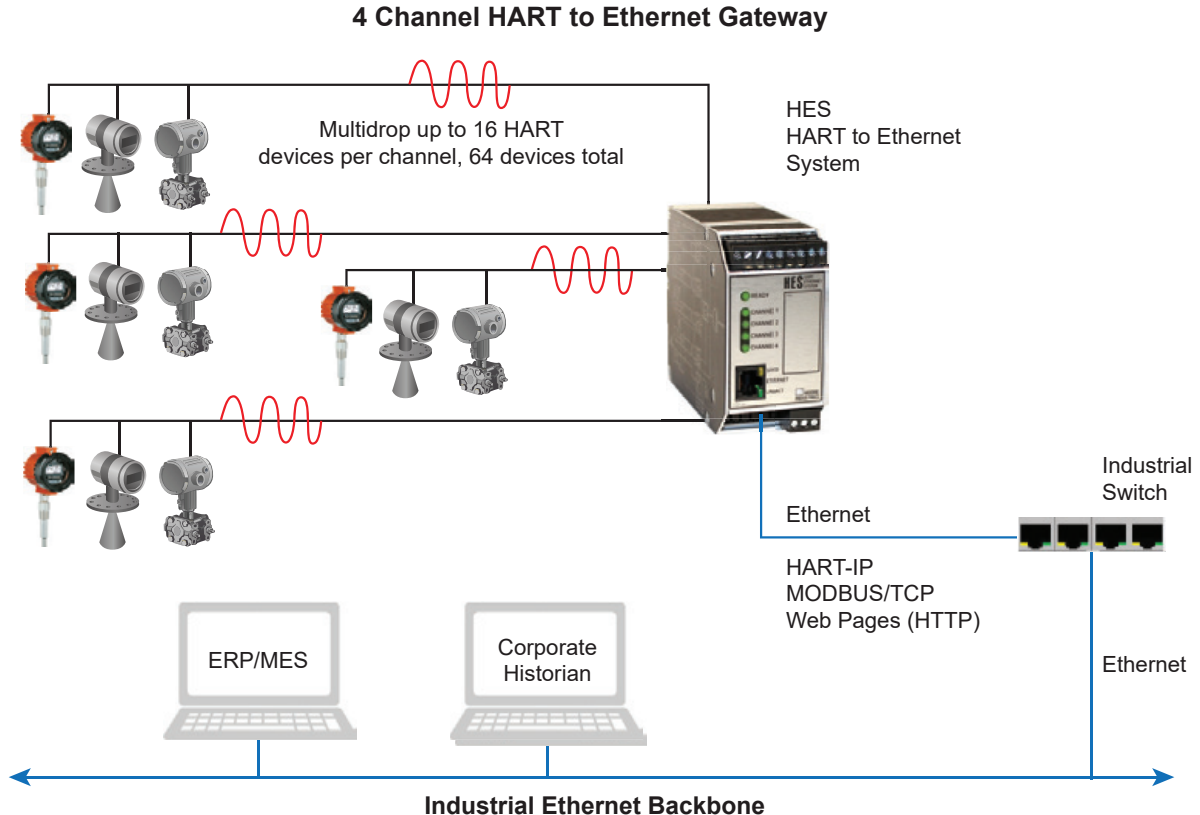


Figure 3. HART to Ethernet gateways offer a quick and economical way of sharing critical HART data with higher level systems.

longer distances) have become the standard for in-plant communication links, any interface device that gathers and holds enormous amounts of data can include an Ethernet port. Likewise, these same devices can support open protocols that run seamlessly over Ethernet networks.

At a minimum, an Ethernet device can offer the viewing of its collected HART process and diagnostic data via web pages supported by any PC, tablet, or mobile device. For users, viewing webpages with an enormous amount of data can be overwhelming. Efforts can be made by device vendors to lay the information out in a table format with easy-to-understand headers and address locations (for other supported protocols) so that additional hosts can be configured more easily.

Employing this HART data for process monitoring, control, predictive maintenance, and process optimization requires that open and vendor neutral industrial protocols be supported. Doing so allows the HART device data to freely flow to most any control, SCADA and monitoring system from any vendor. HART supports Ethernet with HART-IP and HART-IP devices typically allow for any HART field device data to be mapped to a number of device variable locations for reading by a HART-IP host. One of the most installed and supported industrial Ethernet protocols is MODBUS/

TCP, which takes MODBUS data packets and wraps them in a TCP header using IP addressing. This makes implementation by both host computer and field device manufacturers quick and abundant.

Configuration of IIoT devices

For many years, end users have had to deal with custom and proprietary configuration packages from vendors for advanced capability devices. This typically leads to several custom software packages that users must learn, get IT support and permission for, and become familiar with. Most IIoT capable devices are not straight forward field instruments and therefore small handheld configurators are not convenient for setup and configuration. In fact, many HART protocol gateways often require complex database mapping and programming software.

When sourcing or specifying an IIoT device, investigate what the programming interface will be. Several open standards and software packages that vendors have access to prevent the need for custom or expensive programming software utilities. We recommend looking for devices that support FDT/DTM technology for programming, so free software like PACTware can be used.

All figures courtesy of Moore Industries, Inc.



ABOUT THE AUTHOR

Bob Myles is director of engineering for [Moore Industries International](#). He is an *exida*-certified Functional Safety Practitioner (FSP) with nearly 40 years of experience in development of safety-critical systems for commercial aerospace (DO-178C/ DO-254/ ARP4761/ARP4754), military (DO-160), and process monitoring industries (IEC-61508).

The Case for DIPS and Distributed, Intelligent Automation

How a distributed intelligent production system is made possible by the industrial Internet of Things.

By Deji Chen

Editor's note: Deji Chen is a newly named ISA Fellow and the chief editor of the IEC30165 international standard, which describes the industrial Internet of Thing (IIoT) as a real-time system. The multiple standards that he participated in were all about interconnectivity and led the formulation of three Chinese national IoT standards. Chen also participated in the development of OPC standards at the beginning of his career and has been deeply involved in WirelessHART (IEC62591) from creation to market promotion.

The Industrial Internet (II) represents a new stage in the advancement of human society. Its technical architecture is best summarized as a Distributed Intelligent Production System (DIPS), which is a mesh of various II “nodes.” These nodes range from the traditional—various automation systems, devices, or

independent sensors and various enterprise operation systems—to new II nodes such as Industrial Internet of Things (IIoT) platforms, artificial intelligence (AI) platforms, edge computing platforms, and more. DIPS transcends the practical limitations of staying on a single II platform and solves shortcomings caused

by suppliers neglecting the importance of merging their various advanced products into one unified automation architecture.

History

The manufacturing industry is classified into two categories: discrete manufacturing and process manufacturing. These two categories were once unrelated to each other, but now they have become part of the whole in the era of intelligent manufacturing.

In the era of Industry 3.0, the focus was on how to use raw materials to make products; in the era of Industry 4.0, further consideration should be given to auxiliary materials, by-products, and pollution. The representative system of Industry 3.0 is the distributed control system (DCS). What is the representative system of Industry 4.0? Is it an II platform? We believe it should be the Distributed Intelligent Production System.

Besides product manufacturing, DIPS addresses four common categories of concern, as summarized by authoritative international institutions: safety concerns, production efficiency, equipment maintenance, and pollution emissions.

According to the ISA95 standard, the various daily operations of manufacturing enterprises are divided into five layers: The first and second layers, L1 and L2, include various production equipment and control systems involved in automated production. The third layer, L3, is about the production operations, including manufacturing execution systems (MES) and production management. Layer L4 above it includes various business,

management, and decision-making applications. The top L5 layer is about presentation and decision making. A good enterprise not only needs to achieve optimal efficiency for every application in these layers, but also requires coordination and synchronization between applications, as well as interconnectivity of data.

So, in the era of intelligent manufacturing, we need an architecture in which the system can control basic production automation while serving safety concerns, production efficiency, equipment maintenance, and pollution emissions, as well as accomplish all the operations described by ISA95. That architecture is DIPS. Here's why.

DIPS architecture

The industrial systems architecture in the era of intelligent manufacturing should be a distributed one. The core of the DIPS architecture is its nerve center, which manages all the nodes and the entire distributed network. As mentioned, traditional II nodes include familiar automation systems: the DCS system, programmable logic control (PLC) system, safety system, as well as upper layer ISA95 systems including manufacturing execution systems (MES), product lifecycle management (PLM) systems, customer relationship management (CRM) systems, and more. Simple sensors may also be II nodes.

The new market growth point of industrial manufacturing lies outside of automation systems, however. It is difficult to fully integrate safety, environmental protection, energy conservation, process optimization,



and other advanced II services into traditional automation systems. It requires a special class of nodes to perform those duties, which we call II Platform nodes. These nodes complete tasks beyond traditional manufacturing tasks. Here is more on three common II Platform nodes.

Central nerve system. The DIPS nerve center is a special II Platform node. It manages coordination among different nodes and all the operational data. The organization and management of data is already very difficult, and with distributed management, it becomes even more difficult. An important component in the nerve center is the “data sharing configuration.” Any DIPS data can be accessed through the nerve center, and data that is not physically stored in the nerve center is indexed by the “data sharing configuration” module.

AI nodes. We place the data, algorithms, and computing power that represent “intelligence” in a separate AI node. Considering real-time factors, the online operation of DIPS should not be affected by offline AI computation.

Stars. A “star” is a productized general-purpose IIoT platform, so Stars in the DIPS architecture are IIoT Platform nodes. Most of the popular II platforms in China are in fact Stars. A Star can also run in a standalone industrial computer workstation.

Implementation

Standardization and productization are the only ways to achieve DIPS. Standardization enables seamless integration of products from different suppliers.

The IEC30165 standard, published in 2021, describes the IIoT as a real-time system. Multiple II nodes mean that the interconnection between them and the management by their nerve center are very important—and no less important than the II platform itself.

DIPS hardware products include chips, smart devices, communication devices, control devices, and servers. DIPS software products include embedded software in the hardware products and software in the servers. The software in the server is the II platform software.

One example of a successful application of DIPS is a digital transformation project for a leading global phosphorus chemical industry enterprise. Several key modules of the project have been developed. The most important one is the establishment of the DIPS nerve center to support continuous DIPS integration.

The following are two items related to the project’s central nerve system:

1. The “Data Operations Platform” is the project’s DIPS nerve center. It achieves data interconnection and interoperability between production systems and ERP, EAM, OA, SMS platforms, the government emergency management platform, and other systems.
2. There is a preliminary attempt at intelligent production. Chemical enterprises rarely just produce a single product and the by-products of one product are often used to produce other products. We built production scheduling recommendation software and

implemented it on the DIPS nerve center.

DIPS can be implemented in different formats to support different applications:

Enhanced version of the automation system. DIPS, if it contains only one automation system, could be considered as an enhanced version of that automation system. In that case, an II node with advanced service is considered part of the automation system. DIPS with only one DCS node can also be called enhanced DCS. DIPS with one PLC in it becomes an enhanced version of a PLC system. If computer numeric control (CNC) is inside, DIPS becomes an enhanced version of CNC.

Enterprise digital transformation. The overall digital transformation architecture of an enterprise or a conglomerate is a complex DIPS system.

Smart industrial park. It's a standard practice in China nowadays to integrate relevant manufacturing companies inside one industrial park. The internal DIPS systems of various companies in the park are connected to form a park-level DIPS system. There needs to be a DIPS nerve center at the park level.

Smart Industry Supply Chain. The internal DIPS systems of various enterprises on the

industry supply chain, integrated together, form a supply chain DIPS system. There needs to be a DIPS nerve center at the supply chain level.

Smart City. The current smart city practice is still based on the Internet and needs to be improved to be based on IIoT. It can integrate urban infrastructure DIPS, urban building DIPS, urban enterprise DIPS, etc. to form a larger level of smart city DIPS. A new global nerve center is needed.

Summary

DIPS transcends the practical limitations of staying on a single II platform, which is commonly practiced in China. Thus, it redefines the role of the II platform. DIPS surpasses the shortcomings of international suppliers in neglecting system integration to unify into one architecture their various advanced products that only serve segmented requirements.

Whether from the data level or the computing level, II must be of a distributed DIPS format. AI analysis cannot interfere with the real-time operation of DIPS. Finally, standardization/productization is the only way forward.



ABOUT THE AUTHOR

[Deji Chen](#) is an ISA Fellow (2024) and the Chief Scientist at the College of IoT Applications in Wuxi University in Wuxi City, Jiangsu Province, China. He is the founder of ProudSmart, an IIoT company. Chen is involved with multiple standards bodies related to interconnectivity including IEC30165 and IEC62591 (WirelessHART), and the Chinese IoT standards GB/T 38624.1-2020, GB/T 38619-2020, and GB/T 38637.1-2020

ISA Publishes New Book on Nonlinear Model-Based Control



“Nonlinear Model-Based Control: Using First-Principles Models in Process Control” has just been made available by ISA. It is the latest book by R. Russell Rhinehart, ISA Fellow, AIChE Fellow and Control magazine Process Automation Hall of Fame inductee.

First-principles models (engineering models) are used in industry for process design, troubleshooting, training, online analysis, and supervisory optimization. Rhinehart recommends their use for control because they effectively handle nonlinearity, nonstationary behavior, and interacting variables with only one tuning coefficient per controlled variable (CV). Using optimization, the controller can handle constraints and shape the manipulated variables to achieve desired controlled variable trajectories. This book is his collection of practicable methods.

Rhinehart said using first-principles models for control can also enhance the operational staff’s understanding of the process, support auxiliary process management, and keep the mathematics at the engineers’ comfort level. In addition, unifying all models across diverse process management operations ensures continuity and compatibility.

“Most controllers, including model-based controllers, are linear and locally valid. They are tuned or calibrated for one operating region. But when tank levels or flow rates

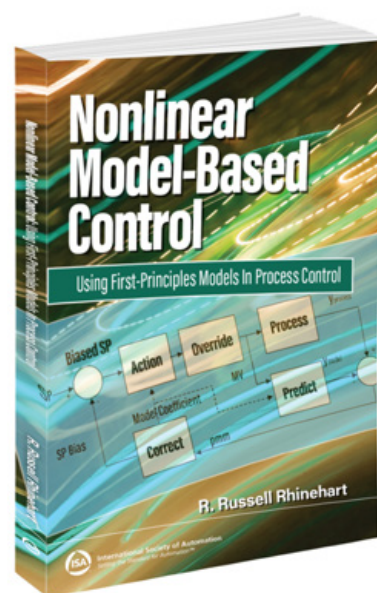
change, the process gain, time-constant, and dead times all change. This requires retuning or recalibration, which can be expensive

and time-consuming. First-principles model-based controllers will work properly throughout the entire operating range. One benefit is that once tuned, they remain tuned until substantial physical changes occur in the process,” Rhinehart said.

First-principles model-based controllers will work properly throughout the entire operating range. One benefit is that once tuned, they remain tuned until substantial physical changes occur in the process

The book explains four control techniques using first-principles models that have been credibly demonstrated for industrial practice: generic model control, process-model-based control, predictive functional control, and horizon predictive control. It illustrates their applications and discusses the pros and cons of each.

Continued on next page



Continued from previous page

To provide a better understanding of first-principles models, the book includes examples of setting up functions for controllers and discusses inherent properties such as ease of tuning, the handling of nonlinearity and interaction, feedforward constraints, and the range of operation.

With experience in both industry (13 years) and academia (31 years), Rhinehart has made it his mission to bridge the gap between industry and academia. Rhinehart is professor emeritus

in the School of Chemical Engineering at Oklahoma State University and was head of the school for 13 years. He received the 2009 ISA Distinguished Service Award and the 2013 Fray International Sustainability Award.

Length: 414 pages. ISBN Print: 978-1-64331-242-2. ISBN ePub: 978-1-64331-243-9. Kindle: 978-1-64331-244-6

Find this and other technical resources for automation and control professionals at <https://isa.org/books>.

—Jack Smith

Plan to Attend ISA's 2024 Automation Summit & Expo

Charleston, South Carolina, USA is the place to be 30 September through 3 October to learn from and network with ISA leaders and automation professionals from around the world.

Industrial, engineering, and business managers and technicians can learn the latest from technical sessions, receive in-depth training, attend Society volunteer meetings, career-skills sessions, and more. Exhibitor booths showcase the latest in OT cybersecurity, instrumentation and automation hardware, software and services.

Attendees get perspective on their day-to-day challenges and insight into solutions from other industries and geographies. [Go online](#) to reserve your room at the Francis Marion Hotel and view more photos from 2023.



A Conversation with Deji Chen, ISA Fellow 2024

Deji Chen, chief scientist at Wuxi University in Wuxi City, Jiangsu Province, China, is one of four individuals recognized in 2024 by the International Society of Automation as an ISA Fellow. The esteemed Fellow member grade is one of ISA's highest honors, recognizing only Senior Members who have made exceptional contributions to the automation profession, in practice or in academia.

Chen has 13 patents ranging from location detection in a wireless network, to a two-mode foundation fieldbus device configurator, to a unified application programming interface for a process control system network. He has written or co-written three books: "Wireless Control Foundation - Continuous and Discrete Control for the Process Industry," "WirelessHART - Real-Time Mesh Network for Industrial Automation," and "Real-Time Data Management in the Distributed Environment," which was his Ph.D. thesis at the University of Texas at Austin, 1999. In addition, Chen has co-authored more than 45 conference papers.

In an exclusive interview with *InTech* magazine, Deji Chen answered questions about his distinguished career.



Deji Chen at a 2022 event in Guangxi Province.

InTech: Can you tell us where you started in industrial automation, and where you are now?

Chen: I joined Emerson in Austin, Texas, as a summer intern in 1995, working on the then secret DeltaV project, the next generation DCS system centered on workstations. At the end of the internship, Mark Nixon hired me. I had been with the Emerson DeltaV team ever since until 2014, except in 2001 when I left for one year to work at Schlumberger. In 2014, I went back to China and joined my alma mater as a faculty member. Now, I am with Wuxi University in Wuxi City, Jiangsu Province, China.

InTech: How and when did you first get involved with ISA?

Chen: I got to know ISA soon after joining Emerson. However, I did not get involved until 2004 when I started publishing at the ISA Expo and in *InTech*. The highlight was receiving the ISA 2007 Excellence in Documentation Award.

The most meaningful work was the translation into Chinese of three ISA award winning books: “Control Loop Foundation,” “Advanced Control Foundation,” and “Wireless Control Foundation.” It was a wonderful experience working with Susan Colwell at the ISA Press.

InTech: Tell us more about your work on Industrial Internet of Things (IIoT), WirelessHART, OPC, IEC30141, and IEC30165.

Chen: WirelessHART is the first international standard on industrial wireless communication in the plant. It was initiated by Emerson. While Mark Nixon and Eric Rotvold were busy co-writing the standard text with Wally Pratt who is from the HART communication Foundation, I led a team of Ph.D. students of Professor Al Mok at the University of Texas at Austin for the literature research and technical verification. The code we wrote was later developed into the testing system for the WirelessHART certification by the HART communication Foundation. The text we wrote was later developed into a definitive book on industrial wireless sensor networks.

OPC was also pioneered by Emerson [among others]. My first job at Emerson was developing this standard with Mark Nixon’s

team. In the meantime, I participated in coding OPC software in the DeltaV system. OPC-UA has become the mainstream standard for IIoT.

After coming back to China, I was invited to work on IEC30141, the IIoT architecture standard. During this period, I initiated and chief-edited the IEC30165 standard (Real-Time IIoT Framework) to emphasize the real-time aspect of an IIoT system.

These standard works, including those of Chinese national standards, are part of my work around IIoT. ProudSmart, the IIoT company I started, has built an IIoT platform product that has been used in many smart manufacturing systems in China.

InTech: Who or what has been most influential to you as far as influencing your career?

Chen: It definitely is Mark Nixon. I started my career working as a summer intern with him. He was my direct boss for most of my time at Emerson, except in the middle he sent me to work on embedded developments to gain more comprehensive knowledge about industry automation, which helped my final Emerson years with him.

InTech: Your three books were published in 1999, 2010, and 2014. Are there perhaps more book titles in your future?

Chen: The book in 1999 was actually my Ph.D. thesis. I have also co-translated seven books into Chinese, including three ISA books mentioned above. Recently, I have written some short essays on IIoT, which I am considering publishing as a book. —Jack Smith

Generative AI-Infused Advanced Analytics Fuels Digital Transformation

By Dustin Johnson

Despite spending billions of dollars on digital transformation, nearly 90 percent of companies are still not achieving their desired results, according to the ARC Advisory Group's December 2022 Survey of Manufacturers. These shortfalls can be attributed to unused or underutilized data, in addition to adopting technologies that are often too complex for subject matter experts to leverage fully.

For these reasons, generative artificial intelligence (GenAI) emerged over the last two years at the perfect time. This transformative technology, a type of artificial intelligence capable of generating new content—such as text, code, and images—in response to user prompts, has the potential to reshape the way industrial organizations analyze data, optimize operations, and make critical decisions. However, the journey from raw data to meaningful insight is still disjointed for many organizations, making it difficult to harness the power of GenAI to uncover more meaningful insights.

As a result, there is a fervent need for software that empowers engineering, operations, and management personnel to achieve faster and more valuable insights from their data, and to act on these insights to achieve measurable business impact. To this end, industrial organizations are achieving success by incorporating GenAI within advanced analytics software, enabling domain experts to harness the software's power while increasing its effectiveness.

GenAI to improve efficiency

GenAI large language models understand human input and efficiently produce text and computer code, while advanced analytics and monitoring software provides clear access to cleansed and contextualized time series and event data. By combining these two technologies, organizations can significantly bolster the power and capabilities of software solutions to recognize patterns, gather insights, make predictions, and recommend actions.

GenAI has the potential to reshape the way industrial organizations analyze data, optimize operations, and make critical decisions.

To achieve the greatest success with this combination, the key ingredients—reliable enterprise data, advanced analytics, and generative AI—must be combined in a workflow with domain experts at the core, not in the background. In fact, the most important technological consideration is how it enables people to adopt new practices and behaviors, in pursuit of specific areas of business value improvement.

Companies can experience immediate business impact by enriching their advanced analytics and process monitoring with GenAI,



empowering employees to enhance their decision making, and improving analytics efficiency across three key areas:

Operational excellence. By providing summaries and detailed explanations in natural language, it is easier for domain experts to understand the full process picture and make data-driven decisions with better accuracy. The result is an ability to analyze massive datasets to identify trends, anomalies, and opportunities, and enable proactive decision-making, leading to immediate operational improvements in production, quality, and yield.

Sustainability. Teams can achieve sustainability timelines with faster results and eliminate stumbling blocks in data and personnel infrastructure. For example, GenAI helps cross-functional teams working with diverse data sets aggregate information for impactful sustainability metrics, reducing the time and effort required for emissions reduction and compliance reporting.

Workforce empowerment. GenAI can be used to power conversational and interactive user interfaces, making it easier for learners to master the crafts within their specific domains. With continuous connectivity to current knowledgebases, GenAI-based training also retains its relevancy, enhancing training sustainment. By providing streamlined access to modern technologies that make domain experts' jobs easier, organizations can attract new talent and retain subject matter expertise by providing a platform that enables motivating impacts.

For a national energy company, infusing GenAI into its existing analytics platform led to measurable and significant time savings. The company's instrumentation and controls team leveraged the Seeq AI Assistant, a GenAI resource embedded across the Seeq industrial analytics platform, to examine a complex relationship between temperature measurements and test well insights. This optimization effort equated to millions of dollars of impact.

Analyzing this complex system requires pre-analysis with special data science techniques, a task that previously required more than four days to complete with support from an outside coding team. With the AI Assistant, however, this step now takes just 15 minutes, providing significantly more time to focus on the process analysis.

Limitations and risks

GenAI promises the potential for significant improvements in the future, but like integrating any new technology, organizations must also acknowledge its limitations and associated risks, including data challenges, a lack of transparency, and data privacy concerns.

To begin with, GenAI results must be validated. The technology is only as good as the data and models it is trained with, and as the saying goes, garbage in equals garbage out.

Organizations must also understand that AI is not a magic bullet for instant solutions. When deployed in the process industries, these models require fine-tuning and customization to meet specific needs. Off-the-shelf solutions may not yield optimal or even reasonable results in many process environments.



Lastly, despite popular discourse, the argument that AI—and GenAI—poses a danger to humanity and can replace human jobs has been overblown in mainstream media. The truth is, GenAI requires human oversight to function effectively. It does not replace the need for domain experts, but instead, it complements their expertise.

By combining GenAI with advanced analytics, industrial organizations can transform their approach to data analysis, process monitoring, and decision making, accelerating time to value and digital transformation success. However, realizing the full potential of GenAI requires careful consideration of its limitations and risks.



ABOUT THE AUTHOR

Dustin Johnson is the chief technology officer at [Seeq](#), responsible for the advanced technology infrastructure, vision, and roadmap of Seeq software solutions. He is a founding partner at Seeq and has played a critical role in growing the Seeq product portfolio to meet the needs of the company's ever-expanding and diverse customer base.

Johnson has more than 20 years of experience in the software industry. Prior to joining Seeq, he served as a chief engineer at aerospace startup Insitu, where he led a diverse and talented group of engineers. Johnson has enjoyed a varied career ranging from space launch support to the development of Wireshark, a popular network analyzer.



International Society of Automation
Setting the Standard for Automation™

Celebrate Automation Professionals Day
with automation essentials!

FLASH SALE

Enjoy 20% off
from 26 April – 29 April

#AutomationProDay

Making Ethernet Deterministic

By Jack Smith

At one of my previous jobs, the company tried to implement a 5BASE-T Ethernet network to collect and aggregate data from automated test systems. Yes, this was over coaxial cable. And no, it was not deterministic. Anything but. The result was multiple network crashes per hour. If only today's robust Ethernet technologies were available at that time.

That was then; this is now

"Over time, industrial Ethernet has replaced fieldbus networks due to its ability to offer a standardized physical layer combined with greater bandwidth," wrote Thomas Burke, strategic global advisor at CC Link Partner Association, in a May 2021 [Automation.com](#) article titled "The Road to Deterministic Ethernet for Industrial Automation." "This allows multiple devices to be connected over one network while ensuring high-speed data transmission. However, standard Ethernet, as defined by IEEE 802.3 specifications, is intrinsically a non-deterministic technology, as it cannot prevent message collisions.

"The different solutions to achieve determinism often consisted of custom, 'proprietary' industrial Ethernet protocols aimed at addressing specific tasks or domains. Thus, their scalability was limited, as each was tailored for a specific application area. Furthermore, while many of them could be considered open, they would not be compatible with each other."

Enter: time sensitive networking

Standard information technology (IT) network equipment can't provide synchronization and/or precision timing. It is not time sensitive. For straight-ahead IT data processing, it is more important to deliver data reliably than to be constrained by time. Therefore, there are no constraints on delay or synchronization precision. Network congestion is handled by throttling and retransmitting dropped packets at the transport layer. However, there is no method of preventing congestion at the link layer. Data can be lost when the buffers are too small or the bandwidth is insufficient, but excessive buffering adds to the delay, which is unacceptable when low deterministic delays are required.

For straight-ahead IT data processing, it is more important to deliver data reliably than to be constrained by time.

The time sensitive network (TSN) standards specified by IEEE 802.1 can be grouped into three key component categories required for a complete real-time communication solution based on switched Ethernet networks with deterministic quality of service (QoS) for point-to-point connections. Each standard specification can be used on its own and is mostly self-sufficient. However, only when used together in a concerted way, TSN as a



communication system can achieve its full potential. The components are:

- **Time synchronization:** All devices that are participating in real-time communication need to have a common understanding of time.
- **Scheduling and traffic shaping:** All devices that are participating in real-time communication adhere to the same rules in processing and forwarding communication packets.
- **Selection of communication paths, path reservations, and fault-tolerance:** All devices that are participating in real-time communication adhere to the same rules in selecting communication paths and in reserving bandwidth and time slots, possibly using more than one simultaneous path to achieve fault tolerance.

Applications that need a deterministic network that behaves in a predictable fashion include control networks that accept inputs from sensors, perform control loop processing, and initiate actions; safety-critical networks that implement packet and link redundancy; and mixed media networks that handle data with varying levels of timing sensitivity and priority.

Burke wrote in a Sept. 2023 *Automation.com* [article](#) titled *Why TSN is Good for Digital Transformation in Manufacturing*: “The most common backbone for IT communications is

Ethernet. The improvement in Ethernet performance is greatly outpacing that of the niche industrial transports based on the needs of a much larger IT market. In 2016, Ethernet specifications were improved to include TSN. This was the missing link to enable Ethernet as the backbone for machine automation, combining IT networks and operational technology (OT) networks, and the combining of control and information communications within a machine. With new products on the market with support for TSN, machine builders can now deliver equipment with a common Ethernet TSN backbone, enabling direct data access with the entire machine, from controller to sensors and actuators.”

Looking ahead

Burke added that industry 4.0 technologies are unleashing a new wave of innovation that is sure to increase performance, improve quality, and reduce costs. With new technology such as Ethernet TSN, we will see machines shift from their original designed for purpose and fixed performance to those that can offer quantified performance, quality and cost metrics, and that will improve over time, based on OEM analytics and feedback.

Fortunately, we’ve come a long way since 5BASE-T.



ABOUT THE AUTHOR

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