



the
Journal
from Rockwell Automation and our PartnerNetwork™

NOVEMBER 2021

How Vulnerable is Your System?

Learn how to identify and mitigate your DCS's cyberthreat vulnerabilities and improve your automation security posture.



5 WAYS THE IIOT CAN BOLSTER OIL & GAS CYBERSECURITY

PROTECT AGAINST CYBERTHREATS AT THE DEVICE LEVEL

DAIRY PLANT TRANSFORMS FROM MANUAL TO FULLY AUTOMATIC



SPECTRUM

C O N T R O L S

Enhancing Your Rockwell Automation Control System for over 35 years!



76 Products Available on 10 Platforms

Multi-Protocol Gateways

5069 CompactLogix I/O

PowerFlex I/O Cards

2080 Micro800 Plug-in I/O

1734 POINT I/O 

2085 Micro800 Expansion I/O

1756 ControlLogix I/O

InView Industrial LED Displays

1762 MicroLogix I/O

1794 FLEX I/O

1769 Compact I/O 

1746 SLC™ 500

spectrum@spectrumcontrols.com
spectrumcontrols.com



SILVER
Technology Partner
 A ROCKWELL AUTOMATION PARTNER

We understand how important it is to find the right expertise for your industry application needs.

KNOWLEDGE + KNOW-HOW

You are assured to get the best-fit products, solutions and services for your specific requirements.



Micropilot FWR30 – The cloud connected radar level sensor



- Transparency – full and secure access to information on asset and inventory status, from anywhere at any time
- Simplicity – from procurement to operations, simplified commissioning, handling and processes
- Flexibility – suitable digital services defined by user needs, scalable from Netilion Value via Netilion Inventory to SupplyCare Hosting
- Reliability – precise measurement with wireless high-end 80Ghz sensor technology

Do you want to learn more?
www.us.endress.com/fwr30



Strategic
Alliance

A ROCKWELL AUTOMATION PARTNER

Endress+Hauser 

People for Process Automation



12

How Vulnerable is Your System?

Get tips on how to identify and mitigate your distributed control system's cyberthreat vulnerabilities and improve your automation security posture.



18



24



33

FEATURES

18 Protect Against Cyberthreats at the Device Level

Strengthen your Defense-in-Depth strategy using IEC standards and the CIP Security protocol that secures communications between PLCs and devices.

21 Enhance Cybersecurity with Network Segmentation

An open and unsegmented network is a gift to cyberattackers. By using network segmentation, you can restrict their access and limit potential damage.

24 5 Ways the IIoT Can Bolster Oil & Gas Cybersecurity

The digital capabilities used on the business side to help compete can also protect your oil and gas operations from cyberthreats.

28 How a Dairy Plant Transformed from Manual to Fully Automated

An automation infrastructure overhaul and new e-records and reporting are optimizing operations and Grade "A" PMO compliance for its milk powder plant.

33 University Cuts Heating System Alarm Response Time

SCADA and alarm monitoring software help protect a campus' new heating system and thus lowering GHG emissions, cutting costs and better using resources.

DEPARTMENTS

- 7 Viewpoint** **37 Partner Showcase** **42 Ad Index**
- 8 News + Noteworthy** **38 Product Focus**

ADDITIONAL RESOURCES

INDUSTRY PERSPECTIVE

Trends Enabling Reliable Warehouse Automation

In this Q&A, Panduit's Mike Berg discusses trends pressuring warehouses and distribution centers, new technologies making them better equipped to handle demand, and what manufacturers can learn from warehouse automation. Read the interview: <https://bit.ly/tjpan2021ip>.

PODCAST

Proper Termination and Grounding of VFD Cables

Steve Wetzel from Southwire Co. shares why cable termination is important, how to achieve proper termination, the best way to terminate a cable's shield and ground wires, and more. Also find out one concept Steve wishes all users understood about VFD cables. <https://bit.ly/tjswpod21>



Enjoy “Automation Chat” from *The Journal*

Join Theresa Houck, Executive Editor of *The Journal* From Rockwell Automation and Our PartnerNetwork magazine, for our “Automation Chat” podcast.

Enjoy short, informative and fun conversations with industrial automation pros about technology, digital transformation, industry trends, workforce challenges and more.

Available on your favorite podcast app, or listen here:

rokthejournal.podbean.com



the Journal

from Rockwell Automation and our PartnerNetwork™

NOVEMBER 2021, VOLUME 28, NO. 6

JOURNL-BR066A-EN-P



1501 E. Woodfield Rd., Suite 400N
Schaumburg, IL. 60173, 630-467-1300

PUTMAN EDITORIAL & SALES TEAM

VICE PRESIDENT & GROUP PUBLISHER

Mike Brenner
mbrenner@putman.net

EXECUTIVE EDITOR

Theresa Houck
thouck@putman.net

MANAGING EDITOR

Amanda Joshi
ajoshi@putman.net

ADVERTISING SALES MANAGER

Michael Connaughton
mconnaughton@putman.net

PRODUCTION MANAGER

Rita Fitzgerald
rfitzgerald@putman.net

ART DIRECTOR

Michael Annino
mannino@putman.net

PUTMAN MEDIA PUBLISHING TEAM

PRESIDENT AND CEO

John M. Cappelletti

VICE PRESIDENT, CONTENT

Keith Larson

CIRCULATION MANAGER

Patricia Donatiu

VICE PRESIDENT, CREATIVE & OPERATIONS

Stephen C. Herner



©The Journal From Rockwell Automation and Our PartnerNetwork™, 2021, Volume 28 Number 6, is published six times a year by PUTMAN MEDIA, INC., 1501 E. Woodfield Rd., Suite 400N, Schaumburg, IL 60173 (Phone 630/467-1300). Address all correspondence to Editorial and Executive Offices, same address. Printed in the United States. ©The Journal From Rockwell Automation and Our PartnerNetwork 2021. All trademarks, company names and product names referred to throughout this publication are used for identification purposes only and are the properties of their respective companies. All rights reserved. The contents of this publication may not be reproduced in whole or part without consent of the copyright owner, including digital reproduction. SUBSCRIPTIONS: Qualified-reader subscriptions are accepted from Operating Management in the industrial automation industry at no charge. To subscribe or unsubscribe, email Carmela Kappel at ckappel@putman.net. Putman Media Inc., which also publishes Chemical Processing, Control, Control Design, Smart Industry, Pharma Manufacturing, Plant Services, and Food Processing, assumes no responsibility for validity of claims in items reported. Putman Media, Inc. is not affiliated with Rockwell Automation, Inc. "The Journal From Rockwell Automation and Our PartnerNetwork" is a trademark of Rockwell Automation, Inc. and its use in the title and masthead of this publication is by license granted by Rockwell Automation, Inc. to Putman Media, Inc. Some photographs and other illustrations printed in this publication may be used with safety equipment removed or altered for illustrative purposes. However, in actual operation, it is recommended that all correct safety procedures and equipment always be utilized.



My Idealism is Mostly a Blessing

I'm an idealist. That creates many advantages for how I perceive people and work and life events. It also can be tough when people don't do what they say they'll do, or when situations are unfair, or when sad things happen. But I believe everything happens for a reason — even if there's no way to comprehend what reason could possibly exist for the behavior of mean people or horrible events that happen.

The idealist in me is proud of how our industry's firms have used creative thinking and innovation to survive during the pandemic. Fist bumps to those of you who pivoted your operations to help people by making masks, respirators and other vital supplies, or who gave to their communities in need. Elbow bumps to those of you who found ways to innovate and continue producing and employing your workers.

And many of the changes you've made have led to permanent improvements that might even be speeding up your digital transformation journey. It's important to keep up with those trends, so I encourage you to download our [2021 Industrial Automation Trends eBook](https://bit.ly/tj21trends), available at <https://bit.ly/tj21trends>. You'll learn about 7 key trends enabling manufacturing performance and supply chain stability.

You also can keep up with what's going on by subscribing to our "Automation Chat" podcast. It's interesting and useful info from people in the thick of things who really know the trends and how they affect you. Listen on your favorite podcast app or on the web at <https://rokthejournal.podbean.com>, or watch our conversations on YouTube at <https://bit.ly/3cey4VH>. They're fun, short, informative chats.

Now, it's appropriate to repeat what I said last year at this time: I sincerely wish you and your loved ones health and happiness in 2022 and beyond. **Until next year...**




Theresa Houck

EXECUTIVE EDITOR



News Noteworthy

New Alliance to Address Air Quality and COVID-19

Rockwell Automation and The Pyure Company will collaborate to provide solutions to improve indoor air quality and combat the pandemic.

Rockwell Automation Inc. and The Pyure Company announced a five-year strategic agreement to work together to provide solutions that improve indoor air quality and fight the spread of COVID-19. Pyure, a global air purifying technology company, designs and manufactures ultraviolet-based commercial air purifiers. Pyure's solutions kill more than 99% of the most common indoor pathogens including the COVID-19 virus, according to the company.

As the pandemic has accelerated the need for companies to become more resilient, agile and sustainable, Pyure will integrate the IIoT- and knowledge-capture solutions from Rockwell Automation. The company's FactoryTalk® InnovationSuite, powered by PTC, will help Pyure collect, aggregate and securely access industrial operations data. As a result, Pyure's customers will be able to access real-time data indicating how Pyure is protecting their environments, while integrating data and control into their building management strategy.

The joint technology assets will allow users to compare indoor and outdoor conditions to choose

the best strategy for their building and industrial processes. Users will also be able to manage their Pyure systems from a single location and integrate their own devices into a common gateway, dashboard and mobile app platform, giving them the ability to remotely troubleshoot and receive system service.

Pyure anticipates that eventually, the trending and optimization data made possible by this partnership will be used in settings where air quality data must be recorded for reporting.



Endress+Hauser Receives Top Sustainability Rating

Rockwell Automation Strategic Alliance Partner Endress+Hauser has achieved 76 out of 100 points in the international EcoVadis sustainability rating, four more than in the previous year. The Group achieved a ranking in the top group for the fifth year in a row in 2021 and is now among the top 1% of the companies compared.

Endress+Hauser achieved further improvements in the areas of environment and sustainable procurement. In terms of ethics, labor and human rights, the company was able to maintain its position in the benchmark comparison. As a result, the company entered the top group in terms of results, and now achieves a platinum medal after the gold standard, the highest performance level of the EcoVadis audit.

The annual audit serves as a key strategic indicator for the sustainability of Endress+Hauser's development. EcoVadis uses 21 criteria from the environmental, social and ethical fields to evaluate companies worldwide for their sustainability. In addition to a sector comparison, organizations receive suggestions for improvement. They can also rate their own suppliers accordingly on an internet platform. To date, about 75,000 companies have been certified by EcoVadis.

Endress+Hauser publishes detailed information on the EcoVadis sustainability audit at www.endress.com/ecovadis.

Rockwell Automation and Comau Collaborate

Rockwell Automation and Turin, Italy-based Comau, a global industrial automation and robot manufacturer, are joining forces to give businesses vital tools to maximize manufacturing efficiencies through unified robot control solutions.

Engineers will be able to program their entire machine in one environment, including Comau robot arms directly controlled through Logix-based controllers from

+ PARTNER NETWORK BRIEF

Hammond Power Solutions Acquires Mesta Electronics, Inc. Ontario-based Hammond Power Solutions Inc. (HPS), a Rockwell Automation Technology Partner, has acquired a 100% equity ownership of Mesta Electronics Inc. Mesta, located in North Huntingdon, Pennsylvania, designs and manufactures standard and custom active filter and induction heating products.



At Endress+Hauser's Gerlingen, Germany campus, a 'wind tree' with tiny turbines generates green energy. For the fifth year in a row, the company improved its ranking in annual sustainability audit.



The combined Rockwell Automation and Comau solutions provide users with analytics and digital twin capabilities to gain deeper insights into machine performance and potential production optimization.

Rockwell Automation. Rockwell Automation Studio 5000® design software is designed to provide relief from the time-consuming task of trying to coordinate traditionally separate machine control and robot systems to work together using two different software tools.

Machine builders, system integrators and others can use digital engineering tools such as Emulate3D digital twin software from Rockwell Automation. It creates digital models of production lines, auto-generates machine control code, and has built-in capabilities for Comau robots. The combined Rockwell and Comau solutions' analytics and digital twin tools help users gain deeper insights into machine performance and potential production optimization.

Operators can view both line and robot control systems on a single interface using the FactoryTalk® software suite from Rockwell Automation. In-plant and remote technicians only need to learn and maintain one architecture to monitor both systems.

FANUC Collaborates with MSSC

Rockwell Automation Strategic Alliance Partner FANUC America and the Manufacturing Skill Standards Council (MSSC) have aligned to co-market the stackability of their respective industry-recognized certifications to help certify more technicians in robotics and automation.

This alliance is designed to address the acute shortage of skilled industrial robotics and automation operators in industrial manufacturing.

+ PARTNER NETWORK BRIEF

HPS Names CFO. Rockwell Automation Technology Partner Hammond Power Solutions (HPS) has appointed Richard Vollerling as chief financial officer and corporate secretary. He replaces Chris Huether, who is retiring after a 35-year career at HPS. Huether will remain with the company until the end of 2021 to ensure a smooth and orderly transition. Most recently, Vollerling was with Teknion Corporation, a Canadian-based manufacturer with more than 3,000 employees, where he held the position of CFO since 2019. Prior to this appointment, he held several progressively senior leadership roles within the organization.



Both organizations offer their certification assessments through NOCTI/Nocti Business Solutions (NBS), which certifies assessments that follow international standards for personnel certification (ISO 17024). NOCTI/NBS have developed and validated the end-of-course assessments for both FANUC and MSSC to certify their technicians. This partnership creates a streamlined approach for schools and industry partners when administering the certifications.



Lakkundi Joins Rockwell Automation

Rockwell Automation, Inc. announced that Veena Lakkundi has joined the company as senior vice president, Corporate Strategy and Development. She will report to Rockwell Automation chairman and CEO Blake Moret.



Lakkundi joins Rockwell Automation following a progression of roles with increasing responsibility at 3M. She was most recently senior vice president and chief strategy officer and interim leader of Technology, Transformation and Services.

She succeeds Elik Fooks, senior vice president, Corporate Development, who announced his retirement earlier this year.

+ PARTNER NETWORK BRIEF

DENSO Celebrates 50 Years. DENSO Products and Services Americas (DPAM), Inc., celebrates the company's 50th anniversary in the United States. The company's history in the United States dates back to March 1, 1971, when the company incorporated as Nippondenso. In 1999, DPAM launched DENSO Robotics, a Rockwell Automation Technology Partner, to market high-performance industrial robots. DENSO's advanced robotic technology is found in electronics, pharmaceuticals, biomedical devices, food processing, aerospace, technology and other products and industries that require precision manufacturing.

Rockwell Automation Acquires Plex Systems

Rockwell Automation, Inc., has acquired Plex Systems, a cloud-native smart manufacturing platform operating at scale. Plex offers a single-instance, multitenant SaaS manufacturing platform, including advanced manufacturing execution systems, quality and supply-chain management capabilities.

Plex has more than 700 customers and manages more than 8 billion transactions per day. Its software capabilities will be further differentiated by Rockwell Automation global market access, complementary industry experience, and ability to turn real-time data into actionable insights. Its platform helps customers to connect, automate, track and analyze their operations and connected supply chains.

Plex will report as part of the Software and Control operating segment of Rockwell Automation, which provides hardware and software offerings for the design, operation and maintenance of production automation and management systems. ●



Universal Industrial Gateway



12 Protocols

- | | |
|---------------------|--------------------|
| 1. EtherNet/IP | 7. DF1-CIP |
| 2. EtherNet/IP-PCCC | 8. PPI |
| 3. Modbus TCP | 9. S7comm (ISOTCP) |
| 4. Modbus RTU | 10. HostLink |
| 5. Modbus ASCII | 11. CCM |
| 6. DF1-PCCC | 12. DirectNET |

- 6 Ports and 12 Protocols all in one Gateway
- 72 Protocol Combinations
- Supports Multiple Protocols Simultaneously
- Browser Based Configuration
- No I/O Tree Changes
- No Ladder Logic to Program

Contact us for your
Free Demo Unit:

spectrumcontrols.com/demo

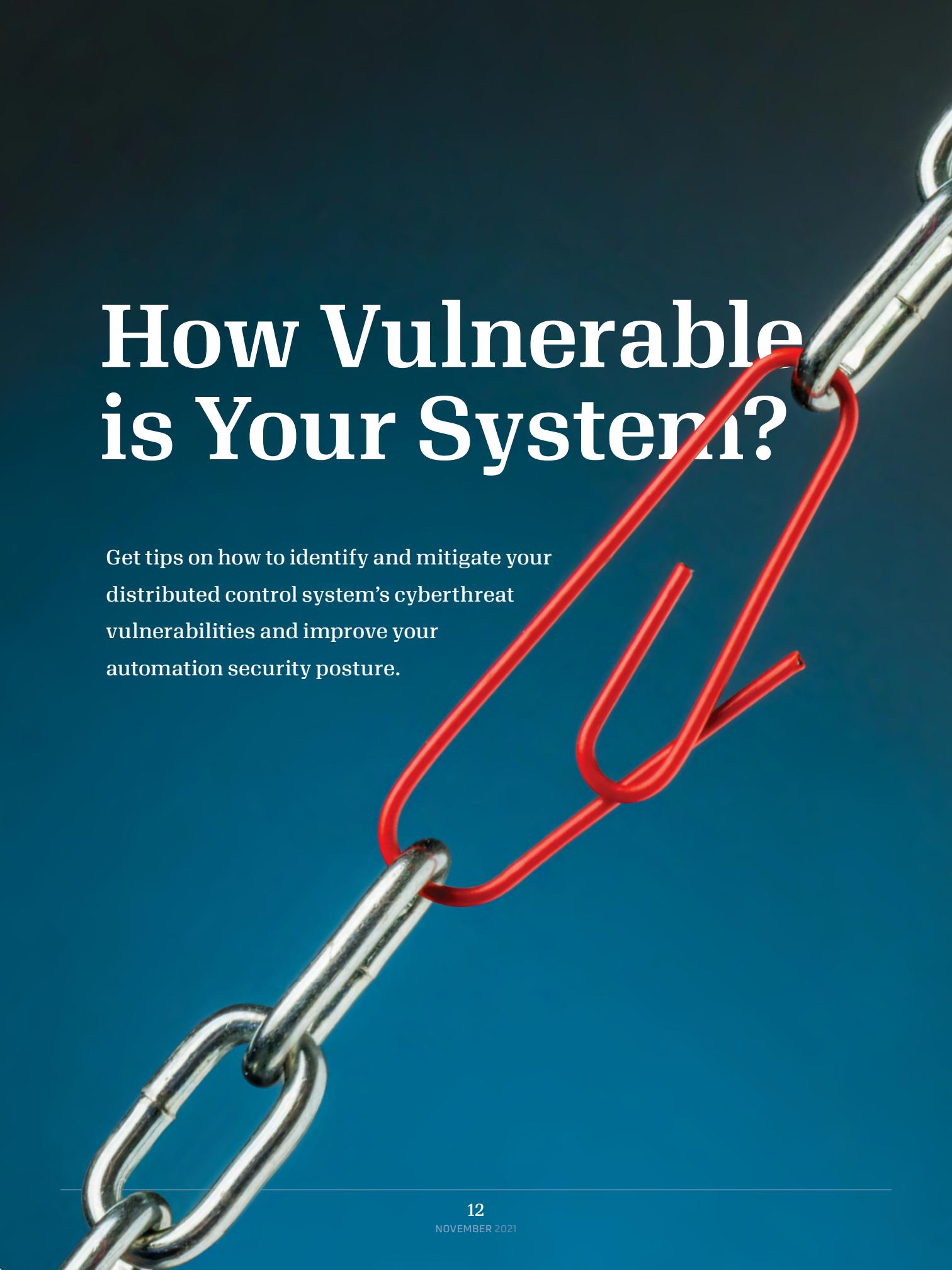
spectrum@spectrumcontrols.com

+1 425-746-9481



SILVER
Technology Partner

A ROCKWELL AUTOMATION PARTNER



How Vulnerable is Your System?

Get tips on how to identify and mitigate your distributed control system's cyberthreat vulnerabilities and improve your automation security posture.

ROCKWELL AUTOMATION

Tim Mirth

PLANTPAX PLATFORM LEADER

Just as most of us, if we're lucky, haven't crossed paths with sophisticated criminals in our everyday lives, most industrial automation users haven't had to face major cyberthreats from bad actors. But many manufacturers and producers don't know how vulnerable their systems are — and unfortunately, the ramifications of an attack go deeper than lost product.

Threats and bad actors are out there — just ask the 18,000 companies affected by the recent SolarWinds hack; or the Colonial Pipeline attacked by ransomware in May 2021 that affected consumers along the U.S. east coast; or the Oldsmar, Florida water treatment plant hacked in February 2021; or the industrial and energy-producing facilities targeted by the infamous Stuxnet malware attack on PLCs in 2009. And there's a myriad of industrial cyberattacks you've never heard about.

Manufacturers and producers are increasingly facing cyberthreats, particularly ransomware, as well as data breaches. In fact, more than half of respondents to a recent survey reported a data breach in the year prior.

As plants become more interconnected and dependent on the Internet, and as digital transformation becomes less of a buzzword and more of a norm, vulnerabilities increase and risks compound. At a plant, an attack could mean lost product, unscheduled downtime, worker safety issues, losses of confidential and/or proprietary information, and sometimes negative consequences on the company's public image.

To truly mitigate risk, every producer needs to be proactive about knowing what risks are out there, understanding their vulnerabilities, and prioritizing mitigation tactics from there. The bottom line? Don't just assume you're safe from cyberattacks. You must be proactive to protect your system. Attackers constantly evolve and so must you.

When it comes to system security, the real goal is to improve your risk posture.

DCS Cybersecurity: Assess Your Risk

When it comes to a distributed control system (DCS), plant managers and engineers know cybersecurity is essential. How can you help verify that your system is secure? And how can you do that if you don't know all the nuances of your system?

People often immediately think to create strong passwords and are aware of the need to implement software updates and patches in our everyday computing environments. But cybersecurity for a process system — which contains any number of products including, but not limited to controllers, networking,

HMIs, advanced analytics, and most importantly people — requires a more comprehensive plan.

That plan should consider not just the IT/data management side of things — computing, software and hardware — but also operational technology (OT) cybersecurity. OT systems, like a DCS, control the physical aspects of the plant and have special requirements beyond typical IT security measures.

A comprehensive plan should align to international standard ANSI/ISA-62443-3-3, which provides security guidance for industrial automation and control systems and defines procedures to implement a secure system. This standard is considered by many industrial cybersecurity experts to be the global standard for now and the future. Because it was written by multivendor/user security experts in industrial automation, it has specifically addressed the idiosyncrasies of our industry.

Based on the ANSI/ISA-62443-3-3 standard, the first step in any cybersecurity plan is to take an accurate inventory of all the devices and interfaces that make up the system and understand any vulnerabilities they have.

A risk assessment led by a trusted third-party partner can make a huge difference, because it's easy to miss things that are right in front of us. This assessment will help producers find vulnerabilities and allow the site to understand what level of risk they can tolerate. Then site managers can make the best choices for threat mitigation in their company.

4 Common Challenges & How to Deal with Them

Once a risk assessment is complete, securing a system can seem daunting, but generally accepted countermeasures exist that will improve your security posture. The ever-increasing connectivity of automated plants provides unprecedented visibility into systems, resulting in advanced analytics



LISTEN TO THE PODCAST

Lessons from the Colonial Pipeline Cyberattack

The ransomware attack that shut down the Colonial Pipeline on May 7, 2021, is considered the most impactful cyberattack against U.S. critical infrastructure. In this “Automation Chat” podcast, Executive Editor Theresa Houck talks with Grant Geyer, Chief Product Officer at Claroty, to examine how the cyberattack happened, its impact, and lessons learned that can help every industrial firm.



Also learn about the asset operator's role as the first line of defense; how converged IT/OT networks are vital for efficiency, but also increase the attack surface available — and what to do about it; the technical and organizational features of a well-thought-out cyber defense; and more.

Listen on your favorite podcast app or on the web at <http://bit.ly/tj21claropod>, or watch on YouTube at <https://youtu.be/rFxa2-wyquw>.



Allen-Bradley

by ROCKWELL AUTOMATION

make sure it's genuine

PURCHASE WITH CONFIDENCE FROM AN AUTHORIZED DISTRIBUTOR

Avoid the dangers of unauthorized resellers and counterfeit products



No Warranty Coverage



No License for Firmware or Software



Safety & Security



Reliability



Regulatory Compliance

The only way to know that you are receiving a new, authentic Rockwell Automation product is to purchase directly from an authorized source. Use our partner locator to find your local authorized distributor: <https://rok.auto/buy>



Learn more at
rok.auto/avoid-unauthorized



**Rockwell
Automation**



The ANSI/ISA-62443-3-3 standard is considered by many industrial cybersecurity experts to be the global standard for now and the future.

and data that can help improve processes, create efficiencies and increase profitability. But that connectivity can leave systems exposed and vulnerable to threats.

Decision-makers exploring DCS-related cybersecurity improvements might face one or more of the following common challenges. Here are 4 typical challenges and tips to consider for overcoming them:

1. Open Systems.

When the Stuxnet computer worm struck and spread easily throughout control systems, it highlighted just how open those systems were. Open protocol networks are a historical hallmark of DCSs and usually are considered a huge benefit. But the additional avenues of risk associated with online, connected control systems might leave producers more vulnerable.

The Zone and Conduit model can help mitigate the threat and keep critical assets segmented from most vulnerable areas. This also prevents open networks from being exposed to easy avenues of attack. The ISA 62443 series of standards supports [zones and conduits](#).

Also, [managed firewalls](#) are an important part of protecting open systems.

2. Legacy Equipment.

Every plant has equipment of varying vintages, and many manufacturers take a piecemeal approach to upgrading their system. That means a new PLC might be on the same network as a computer running Windows XP. These older machines, especially if they haven't been updated in many years, are potential entry points for viruses, worms and hackers.

This is where a risk assessment can expose a vulnerability and develop a strategy to strengthen them. In larger plants, you may not even know there's still an obsolete operating system on your network. Replacement is critical. However, if it's not possible, some protection could be gained with [network segmentation](#) building layers of defense.

3. Evolving Workforce.

Employee turnover internally and at external partners and vendors is another big challenge for producers. Turnover for system integrators, in particular, often is extremely high. The people who have access to your plant and systems are an important piece of the overall cybersecurity puzzle. Breaches can be caused by innocent mistakes and those with nefarious intentions.

Do you know who manages user accounts and system access for your company? Are there any accounts that have remained active and unused for years? Adhering to [international standards](#) and managing your users as part of a cybersecurity strategy can help mitigate risk.

4. Unknown Return on Investment (ROI).

It can be difficult enough to get management buy-in for investments when the ROI



DOWNLOAD THE EBOOK

2021 Industrial Automation Trends & Automation Fair Directory

Edge computing, simplified infrastructure, digitized devices, advanced analytics, AR and AI are just a few of the 7 top trends enabling your manufacturing performance, automation strategy and supply chain stability. Plus, get the 2021 Automation Fair® event preview and exhibitor's list to see technologies on display from industry leaders supporting those trends.

Download this free resource from *The Journal From Rockwell Automation and Our PartnerNetwork™* magazine by visiting <https://bit.ly/tj21trends>.



is clear. With cybersecurity or any risk mitigation initiative, it's less about how much money the company will make and more about what you don't want to lose. Cyberattacks can cause losses of production and uptime, communications, information and, worst-case, safety of workers.

With a proper risk assessment, vulnerabilities, risks and mitigation strategies can be evaluated and allow producers to ask: What risk are we willing to accept? What will it cost to make the changes needed to feel comfortable in our risk posture?

It might not be as expensive as you think to make changes, and the opportunity cost for not protecting is too great to pass up implementing even some simple measures. Determine your risk posture and protect your most vital assets.

Security for Outcomes You Need

Threats can come from every direction, and the more layers of defense we implement, the more likely we'll mitigate true risks and not become a statistic. When it comes to system security, the real goal is to improve your risk posture.

If you're like many producers, you may not realize the true breadth of the threat landscape. You may not know just how vulnerable you are. Fortunately, trusted providers are looking out for their producer customers — helping them to be both proactive and reactive in the face of continuing and evolving cyber threats.

It's important that your industrial automation provider takes security seriously, aligns with the ANSI/ISA-62443-3-3 standard and builds their products and systems in accordance with that

standard. This standard is considered by many industrial cybersecurity experts to be the global standard for now and the future.

Because it was written by multivendor/user security experts in industrial automation it has specifically addressed the idiosyncrasies of our industry. To explore your risk tolerance and security posture, ask your provider about a comprehensive risk analysis, which can help you take a proactive stance beyond your DCS.

You'll need an evolving plan to properly secure your DCS. Select one that keeps these three favorable outcomes in mind and won't trap you from making the progress you need to run your business: enhanced overall security, flexibility and digital transformation. ●



Free Exclusive Content from *The Journal*

You're just 1 click away from getting free online articles from *The Journal*. Just go to rok.auto/thejournal-subscribe. Check "The Journal" box to get your free e-newsletter that brings you the digital edition of *The Journal* every issue – plus additional Web-exclusive how-to articles, case studies and product news from Rockwell Automation and its Encompass™ Product Partners and Solution Providers.

rok.auto/thejournal-subscribe

Sign up today!



ROCKWELL AUTOMATION

Oliver Haya

BUSINESS DEVELOPMENT MANAGER,
ETHERNET/IP TECHNOLOGY
ADOPTION

Protect Against Cyberthreats at the Device Level

Strengthen your Defense-in-Depth strategy using IEC standards and the CIP Security protocol that secures communications between PLCs and devices.

- Industrial operations are increasingly becoming the target of cybersecurity attacks. Organizations are adding new devices with network connectivity as they migrate from traditional fieldbuses and stand-alone operation. Additional connections are being created between the IT and operations technology (OT) space and machine builders increasingly offer analytics if their machine can be connected to the cloud.

International standards for cybersecurity, known as IEC 62443, are being updated and expanded, including requirements for end users, system integrators and device manufacturers. These standards require Defense-in-Depth (DiD) strategies to reduce the risk of attacks that can cause harm through these network connections.



DOWNLOAD THE EBOOK

2021 Industrial Automation Trends & Automation Fair Directory

Edge computing, simplified infrastructure, digitized devices, advanced analytics, AR and AI are just a few of the **7 top trends** enabling your manufacturing performance, automation strategy and supply chain stability. Plus, get the 2021 Automation Fair® event preview and exhibitor's list to see technologies on display from industry leaders supporting those trends.

Download this free resource from *The Journal From Rockwell Automation and Our PartnerNetwork™* magazine by visiting <https://bit.ly/tj21trends>.

As you advance the cybersecurity of your operations, you need more capability at deeper levels of the DiD strategy. Have you performed cybersecurity assessments, minimized your attack surface with cybersecurity essentials and implemented best network segmentation practices? If you're ahead of all these, you're on the right track.

Even with strong security policies and protections, adding security at each layer improves your resilience against cyberattacks. For example, how will you

protect your process if a malicious actor has access behind your firewall? You may be susceptible to various attacks that need additional measures to mitigate.

Why a Firewall Isn't Enough

A malicious actor could create an unauthorized connection to hardware in your system by pretending to be another kind of device. This has been demonstrated recently in industrial automation, with an imposter computer improperly configuring devices and

injecting code based on insecure identification credentials.

Another attack type that's possible without communication integrity is the man-in-the-middle attack, and a variant of that: the replay attack. During these attacks, someone would intercept and modify data between two devices, sometimes after collecting data that can be used to mimic normal operation. This could mask abnormal behavior that can cause equipment damage or endanger human safety.

Cybercriminals also could gain proprietary information by snooping on the network traffic between industrial devices. Data transmitted without

confidentiality could be used for harm. This includes accessing secret recipes going from the manufacturing execution system (MES) to the programmable logic

controllers (PLCs), analytic data that could be used to steal manufacturing best practices, or production volume information that could be used to short stocks.

Defense at the Device Level

To bolster security at the device level and reduce the risk of those attacks, IEC 62443-3-3 and IEC 62443-4-2 include common minimum requirements for device identity, integrity and authenticity of communications, and options for confidentially transmitting data. Four of the requirements in the standard (SR 1.2, SR 3.1, SR 3.13, SR 4.1) are almost impossible to implement at a system level without the right hardware and firmware at the device level.

If you want to use devices from multiple vendors that meet those system requirements, standards and conformance testing are needed.

The [CIP Security™](#) protocol is an open standard from ODVA, which helps solve important communication requirements that device vendors using industrial Ethernet cannot solve themselves. This standard is the only standard designed for securing communications between PLCs and devices.

The CIP Security protocol provides mechanisms for validating device identity, device authentication, data integrity and data confidentiality. All three of the functional requirements and their requirement enhancements can be met using CIP Security and configured using [FactoryTalk® Policy Manager](#) from Rockwell Automation.

Rockwell Automation is releasing CIP Security on more products each year, and other vendors are adopting this standard right now. Some upcoming devices include retrofit opportunities to reduce the risk of cyber incidents with existing equipment, too. So, don't think that you must wait for a greenfield plant to make improvements. Start considering when and how you will add more layers to your Defense in Depth. ●

Anybus®
BY HMS NETWORKS

Wireless Bridge

Anybus® Wireless Bridge enables you to create an industrial wireless connection in an industrial Ethernet network.



FEATURES & BENEFITS

- Suitable for AGV's (Automatic Guided Vehicle)
- Maximum range of 400 meters
- Easy setup via push button or web interface
- Access Point functionality for up to seven clients

For more information about our wireless solutions visit anybus.com



Enhance Cybersecurity with Network Segmentation



An open and unsegmented network is a gift to cyberattackers. By using network segmentation, you can restrict their access and limit potential damage.

● **A**n open and unsegmented network is a gift to cyberattackers.

Once an attacker finds and exploits the most vulnerable point of entry, it could turn into a potential "kid in a candy shop" scenario. They may be able to pivot to more easily access a larger part of the network and potentially anything connected to it — from product designs or recipes, to machine controls, to company finances.

And it's not only external threats that pose a danger on an unsegmented network. Internal threats, whether it's a disgruntled employee or human error like an incorrect system



When implementing network segmentation, consider how it will be applied across your entire organization.

change, also can wreak havoc when there are no network boundaries or access limitations.

This is why network segmentation should be part of every company's industrial security strategy.

Network segmentation separates your network into multiple smaller networks and allows you to establish zones of trust. This can help limit the access of outside security threats and contain any damage they cause.

It also can help give employees and business partners access to only the data, assets or applications that they need.

Levels of Segmentation

Virtual LANs, or VLANs, are most commonly associated with network segmentation. These are broadcast domains that exist within a switched network. They allow you to segment your network logically — such as by function, application or organization — instead of physically.

VLANs can secure devices and data in two ways. First, you can block devices in certain VLANs from communicating with devices in other VLANs. Second, you can use a Layer-3 switch

or router with security and filtering functionality to help to protect the communications of devices that do talk to each other across VLANs.

But while VLANs are an important part of segmentation, they're only one solution. You should also use other segmentation methods across different levels of your network architecture.

One example is the use of an industrial demilitarized zone (IDMZ). It creates a barrier between the enterprise and manufacturing or industrial zones. All traffic between the two zones terminates at this barrier, while still allowing data to be securely shared.

Other segmentation methods to consider using include access control lists (ACLs), firewalls, virtual private networks (VPNs), one-way traffic restrictors, and intrusion protection and detection services (IPS/IDS).

Think Holistically

When implementing network segmentation, consider how it will be applied across your entire organization.

Some companies create purpose-built firewalls at individual facilities. But this can lead to "islands" of security. Different sites will have different firewalls, making it difficult to deploy them in a consistent manner or centrally manage them.

It's also important to think about segmentation within your company's long-term needs.

Purpose-built security solutions are too often rigid — they may meet your needs today but can't flex or evolve with your business to meet tomorrow's operating or security needs. Purpose-built solutions also tend to rely on the expertise of a small number of employees.



DOWNLOAD THE SPECIAL REPORT

How to Keep Up with — and Contribute to — Single Pair Ethernet Standards

Single Pair Ethernet (SPE) creates a plant-wide infrastructure that allows legacy industrial networks to migrate to single Ethernet networks while delivering power, control and information to edge devices. In this new report from Panduit, learn about recent developments in SPE network infrastructure for new applications and higher capabilities, and how easy it is to stay up to date with and take part in improving the ever-evolving standards.

Download this insightful report from Panduit at <https://bit.ly/tjpandspe21>.



Plus, those employees can take vital security or maintenance knowledge with them if they leave.

The solutions you use to implement network segmentation should be flexible enough to grow with your operations. And they should be standardized so the appropriate worker(s) at any site can use and maintain them.

Help is Available

Network segmentation is a well-known IT concept, but it's still taking hold in the industrial world. The industrial companies that are implementing it are discovering the challenges that come with applying it across an entire Connected Enterprise, such as managing segmented data and scaling it to grow with production operations.

If you're unsure of where to begin or what segmentation method to deploy, freely available resources can help.

The Converged Plantwide Ethernet (CPwE) design guides are a good place to start. Guides on topics like [IDMZs](#), [industrial firewalls](#) and [networking considerations](#) can help you deploy segmentation using the latest technologies and industry best practices.

The guides are jointly developed and tested by Rockwell Automation and Cisco®, and build a foundation to other collaborative products and services to help you segment and secure your network. We also offer training, network and security services, and technologies. ●



WEIGH YOUR OPTIONS

With Helm Load Cell Input Modules



- ▶ Two Channel
- ▶ 24-bit Resolution
- ▶ 1 Millisecond Update
- ▶ Direct Connection to Standard Load Cells – no Analog Input or Summing Box Required
- ▶ Weighing, Packaging and Filling
- ▶ Stamping, Forging, and Diecast
- ▶ Thermoforming
- ▶ Pharmaceutical
- ▶ Assembly



HELM Our expertise comes from experience...since 1962

HELM INSTRUMENT COMPANY, INC.

361 West Dussel Drive • Maumee, OH 43537

419-893-4356 • www.helminstrument.com • Sales@helminstrument.com



SILVER
Technology Partner
A ROCKWELL AUTOMATION PARTNER

Micro850®
expansion
module



5 Ways the IIoT Can Bolster Oil & Gas Cybersecurity

The digital capabilities used on the business side to help compete can also protect your oil and gas operations from cyberthreats.

SENSIA

Omar Sikander

GLOBAL ALLIANCE MANAGER



PHOTO BY KEVIN HARRIS ON UNSPLASH



● **C**ybersecurity is no longer a concern only for tech experts in the IT department. It's also top of mind for executives in the board room and operators in the oilfield.

And for good reason. More frequent, sophisticated, high-profile cybersecurity attacks on oil and gas operations have put the industry on edge.

Breaches are disruptive and expensive — costing some companies hundreds of millions of dollars. And incidents like the May 2021 ransomware attack on Colonial Pipeline that impacted gasoline supplies by shutting down pipelines, among others, remind us an attack in the digital world can have dangerous consequences in the real world.

You need comprehensive security as operations become more digital, but it doesn't need to come at the expense of business-improvement goals. In fact, quite the opposite. The same digital capabilities that can help you better compete — like seamless connectivity, production intelligence and remote support — also can help fortify your operations.



With a continuous, real-time inventory of operational equipment, you can stay on top of risks to your production environments.

Security Synergies

As you plan and design your cybersecurity strategy, capitalize on aspects of your connected operations that have shared security and operational benefits. Five key examples include the following.

1. Dynamic Asset Inventory

It's hard to mitigate threats if you don't know what they might target in your operations. So, a comprehensive, real-time understanding of your connected equipment and systems is essential.

Historically, taking inventory of equipment required physically sending someone to production sites. This process is time consuming, especially if you have dispersed and remote operations. It's also limiting, because the data captured only gives you a snapshot in time of your inventory.

The Industrial Internet of Things (IIoT) is changing this. Now, using software or connected services, you can use the same communications path as your control systems to gather asset data.

With a continuous, real-time inventory of operational equipment, you can stay on top of risks to your production environments. For example, you can quickly see if security advisories, firmware updates or new patch releases are relevant to your installed base.

You also can better manage operations. For instance, the data can help track life-cycle risks and inform your modernization strategy.

2. Real-Time Process Visibility

Knowing what equipment you have isn't enough; you also need real-time visibility into how, when and where people are accessing or manipulating it.

A threat-detection service can identify normal behavior across your oil and gas network and monitor your operations 24/7 for deviations from that baseline. Operators can then be alerted of any irregularities or potential threats in real time.

This visibility can help you uncover a threat like an outsider security attack at multiple stages, including:

- **When they first gain a foothold on your network.**
- **When they're moving around the network to do recon on your operations.**
- **When they're making changes to assets (systems, equipment, networks) to carry out an attack.**

The service also can help detect more common human errors and operational issues that, while lacking nefarious intent, can still disrupt operations. For instance, it could reveal an OEM remotely accessed and made changes to a controller in the wrong location.

3. Life Cycle Management Support

According to the 2019 Global Energy Talent Index report, 40% of oil and gas respondents said a skills crisis has already hit the industry. And nearly 30% said the crisis would take hold in the next five years.

To lessen the impact of the skills shortage, more companies are looking to outsource the responsibility of managing their oil and gas production systems. And who better to monitor, maintain and modernize the systems than the companies that supply them?

One major oil and gas producer turned to a diagnostic reliability service from Rockwell Automation to reduce its cybersecurity risks and lower its business costs. As part of the service, the provider continuously scans the process-control network of the oil and gas producer to identify, interrogate and monitor control hardware. It captures key data — such as its part number, series version and firmware version — and tracks status, health and parameter changes.

The service helped the producer comply with a new corporate cybersecurity policy. And it led to

operational improvements, such as more proactive maintenance that helped reduce manpower costs in the field and pump more barrels of oil per day.

4. Disaster Recovery

In the event of a security incident, having a plan and policies in place can help you recover as quickly as possible. This will help minimize the impact of security incidents and maximize uptime.

A response plan can help you contain, eradicate and quickly recover from threats to your operations. It should include the steps workers need to take to get back to a fully operational state.

Policies are just as crucial. For example, they should define a method for backing up critical operational assets. Without backups, you could find yourself the victim of ransomware and having to decide: Should we pay someone to re-engineer our systems or pay the attacker to get them back?

One solution is asset-management software. It can automatically back up application code and configurations for devices like controllers, drives and operator terminals.

5. Good Security Fundamentals

To achieve a fundamental level of security, every oil and gas company should use security best practices — known as security fundamentals, and sometimes hygiene.

Some are simple, like changing the default log-ins used in any new network equipment you purchase. Software with authentication and authorization is another best practice. It allows your IT or security team to define who can access the software, what actions they can take and where they can perform those actions.

Other security fundamentals are more complex. For instance, control and enterprise traffic shouldn't be treated the same on your network. If the network infrastructure that handles both these traffic types goes down, then your entire enterprise is no longer functional. That's why you should use an industrial DMZ to segment control and enterprise traffic.

In addition to securing operations, these best practices can also have operational benefits. Segmentation, for example, allows you to connect remote employees and partners with on-site workers to more quickly troubleshoot and resolve downtime issues.

Know Before You Go

Getting the most from your connected operations and securing them can go hand in hand. But before you do anything, you need a strategy to identify where you can be more competitive and where threats lie. Then, you can see where these two areas share common ground.

If you're unsure of what to do or where to start, reach out to a service provider that can help you plan, deploy and optimize connected oil and gas operations. Also, make use of freely available resources like the Converged Plantwide Ethernet (CPwE) design guides from Rockwell Automation and Cisco®. They can help create more competitive operations using the latest technologies and security best practices. ●



DOWNLOAD THE EBOOK

2021 Oil & Gas eBook Examines Colonial Pipeline Cyberattack

The 2021 Oil & Gas eBook reveals key lessons from the May 2021 Colonial Pipeline ransomware attack. Also see how a pipeline company's digital transformation project increased IT/OT efficiency; how remote surveillance helps optimize artificial lift systems; how to detect water carryover in natural gas; how control loop performance monitoring helps process operations; and how electrical engineering software can improve oil & gas processes. Published by *The Journal From Rockwell Automation and Our PartnerNetwork™* magazine. Download it at <http://bit.ly/tj2021ogeb>.

How a Dairy Plant Transformed from Manual to Fully Automated

An automation infrastructure overhaul and new e-records and reporting are optimizing operations and Grade “A” PMO compliance for its milk powder plant.

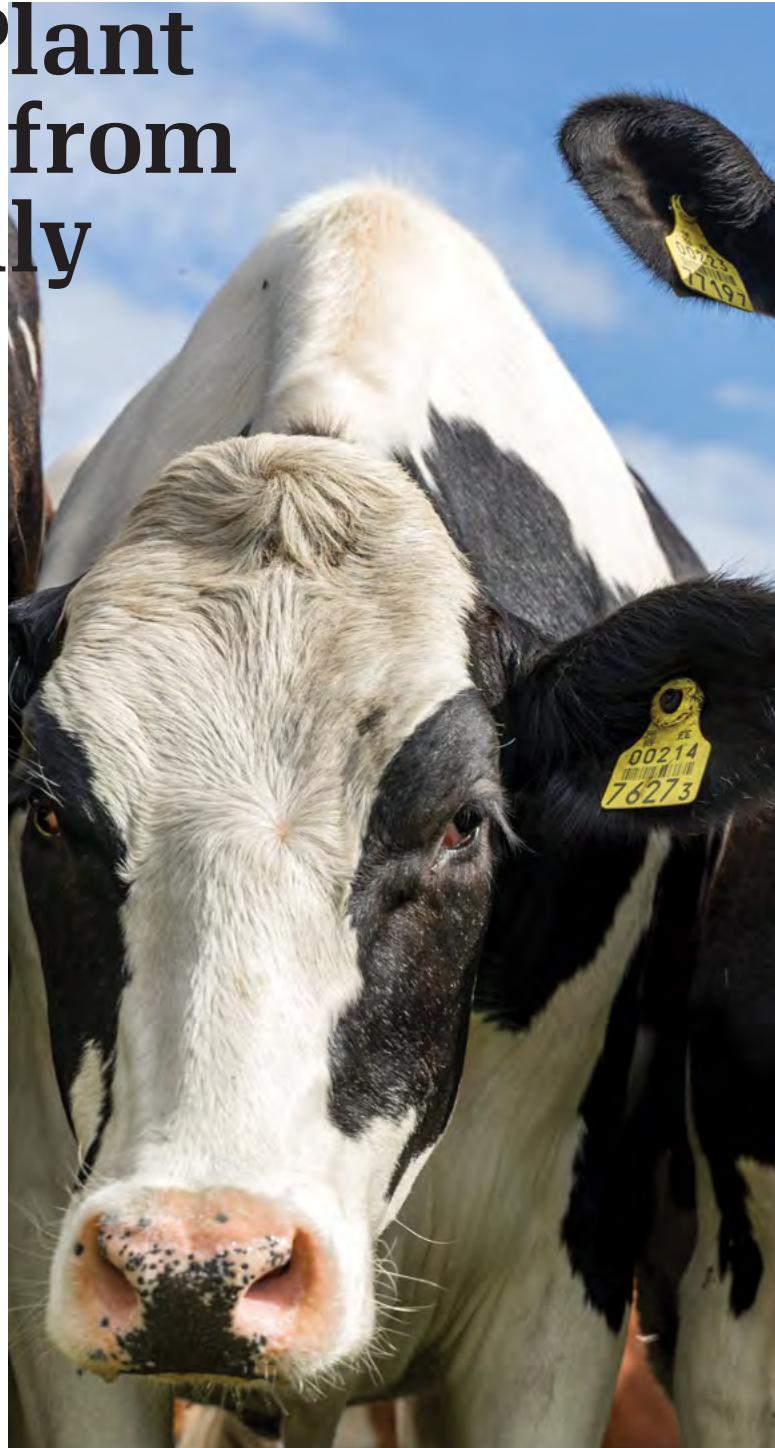
Sheila Kennedy

CONTRIBUTING WRITER

The acquisition of an entirely manual milk powder plant created a unique but welcome challenge for a national dairy producer: how to transform the facility into a fully automated manufacturing operation with improved milk production, advanced water conservation, and modern electronic records and compliance reporting, all while achieving its financial goals.

The outdated plant’s throughput was hampered by challenges with operator traffic flow, product storage capacity and the timely unloading of milk. Its legacy milk handling, processing and cleaning systems were driven by labor-intensive processes, introducing the potential for inconsistencies in product quality, yield, and traceability.

The paper-based records and chart recorders used to track crucial Grade “A” Pasteurized Milk Ordinance (PMO) compliance were vulnerable to loss, damage and human error.







DOWNLOAD THE EBOOK

2021 Food & Beverage eBook Discusses How to Achieve Better Performance



Our 2021 Food & Beverage eBook explains how producers are using smart manufacturing to boost performance and product consistency for food safety, changing consumer tastes and stiffer competition. See how one food processor migrated to a modern DCS and cut the factory's waste by \$500,000 yearly. Discover how electrical engineering software is changing the food industry. And learn about PID controller tuning, edge computing, cross-protocol network communication, mitigating packaging-machine hazards and more.

Published by *The Journal From Rockwell Automation and Our PartnerNetwork™* magazine. Download the free resource at

<http://bit.ly/tj21fbebook>.

To solve these problems, the dairy producer engaged the services of St. Louis, Missouri-based Rockwell Automation Gold System Integrator [Malisko Engineering](#), who helped design, develop, document and implement state-of-the-art process control and automation solutions along with electronic data collection, storage and reporting capabilities. The difference between the before and after state is extraordinary and so are the benefits being realized at the plant.

Performance Optimization Opportunities

The dairy producer targeted manual processes for replacement and articulated high-level guidance on desired process control and reporting requirements. For example, reliance on paper records for PMO compliance had to be eliminated.

"Old clean-in-place (CIP) and product storage records were on old circular chart recorders, which recorded limited data. Anytime there was a quality issue, someone had to dig through these records," observes Dan Jacoby, automation solution consultant at Malisko Engineering.

The vision for the plant encompassed multiple layers of optimization, including:

Increase capacity: Add additional milk receiving and storage capacity to improve operational efficiency and yield across the entire milk processing system.

Embrace automation: Greatly reduce the risk and dependence on operator control by incorporating automation.

Conserve water: Process cow water, which is condensate produced by evaporating skim milk into condensed skim, into legal, usable Pasteurized Equivalent Water (PEW) water for reuse in cleaning and product flushing.

Streamline data management:

Implement a new, computerized data collection, storage, reporting, and records system compliant with PMO Appendix H (Pasteurization Equipment and Procedures and Other Equipment) part V (Criteria for the Evaluation of Electronic Data Collection Storage and Reporting).

Simplify compliance: Develop PMO-compliant solutions for CIP records, such as raw and heat-treated product storage tank temperatures, and for silo storage monitoring.

Expedite troubleshooting: Reduce troubleshooting time by designing operator interfaces that "lead" the operator to the likely source of a problem and providing more thorough and accurate system documentation.

Facilitate remote support: Provide remote access to the control system to enhance support and troubleshooting.

Verify system security: Establish a robust and secure network with the ability to tie into the antiquated legacy network.

Strict cost and timeline limitations added to the complexity of the project. The chosen system integrator had to work within a limited capital budget and



The local state health inspector commented on how impressed he was with the solution.

meet a very aggressive project schedule in the middle of a pandemic. Tight coordination of activities between multiple trades and engineering disciplines was required, and a phased start-up approach was necessary to avoid adversely affecting plant production.

"The plant is a balancing plant, so it takes in all the excess milk in the region," explains Jacoby. "Downtime is hard to schedule and almost impossible during the annual dairy flush season. All in all, this creates short windows for downtime while the milk is diverted to other plants."

Capable Team Delivers Comprehensive Solution

The dairy processor selected Malisko Engineering as its integration partner due to the company's capabilities and knowledge of dairy processing, particularly industrial networking, virtualization, reporting and PMO compliance. Malisko specified several Rockwell Automation solutions for the plant's transformation, including PlantPAx® using FactoryTalk® View SE, FactoryTalk Historian, Asset Framework Event Framing, ThinManager®, Allen-Bradley® ControlLogix®, Flex™ I/O modules, and Stratix® switches.

"Originally they were going to go with Allen-Bradley PanelViews, but we were able to help them realize the benefits of a FactoryTalk View SE distributed system using a PASS-C server configuration," says Jacoby. "That gave them a huge amount of additional capabilities — more HMIs in the facility, the ability to access any process from anywhere, and remote troubleshooting."

The project took place during the COVID-19 pandemic. It kicked off in early 2020; start-up occurred in phases beginning in January 2021, and the biggest phases are already complete, including receiving bays and raw product storage, loadout bays and the PEW system implementation. Start-ups of product silos are in progress, including automating existing silos and starting up new silos.

Besides designing and delivering the advanced automation systems, controls, and data collection and reporting platform based on the dairy processor's high-level functional descriptions, Malisko also documented the system architecture, functionality, operations and requirements; created all configuration and programming according to the client-approved documentation; and helped train the workforce on the new automation tools.



LISTEN TO THE PODCAST

How Automating Production-Line Labeling Can Help Prevent Bottlenecks & Recalls

Printing equipment sometimes isn't considered a resource that generates revenue. But if a printer goes down, no product is going out the door. This is vital in the beverage, dairy and food industries.

In the *The Journal* magazine's Automation Chat podcast, "How Automating Production-Line Labeling Can Help Prevent Bottlenecks & Recalls," Executive Editor Theresa Houck is joined by Adem Kulazovic, Director of Product Management at Domino Amjet, to talk about how coding automation can help improve productivity, reduce errors and avoid unplanned downtime.

Coding automation means automating the manual process of ensuring the correct information is printed on the right products and packages, reducing human error in label selection and management, then integrating that data with existing ERP or SCADA systems. They also chat about the importance of industrial communications standards such as Fieldbus for communication and data sharing; and more.

Listen on your favorite podcast app or on the web at <https://bit.ly/tj20dominopod>, or watch the conversation on YouTube at <https://youtu.be/vIg1yIGbtsM>.

The digitally transformed plant is a quantum leap from its earlier, entirely manual state, and already the benefits are manifold.

Impressive Impacts on Operations

The new solution achieved the stated goals and then some. For instance, after meeting with Malisko's PMO subject matter expert for a complete review and verification testing of the new system for PMO compliance, the local state health inspector commented on how impressed he was with the solution.

"Now, by utilizing FactoryTalk Historian Asset Framework and Event Frames, we are able to capture a full CIP matrix, including start, stop, step, alarms, nonconformances, KPIs [key performance indicators] (temp, flow, conductivity) and more," says Jacoby.

"For the product storage in silos, we are able to create a report from the minute the product enters the silo until it is drained and a CIP is started. That is an essential piece for traceability," he says. Furthermore, the CIP data logging and e-reporting is system agnostic and can be applied to CIP systems of various configurations.

Other significant achievements include:

- **Increasing production uptime and processing capacity.**
- **Providing a greatly improved system for milk receiving and storage.**
- **Reducing shrinkage (product loss) with tighter process controls, visualization and alarming.**
- **Delivering a verifiable electronic reporting suite compliant with PMO.**
- **Reducing CIP cleaning cycle times and chemical usage while confirming effective equipment and process line cleaning.**

- **Accelerating maintenance troubleshooting through "breadcrumbing," intuitive messaging and notifications, and access to comprehensive system documentation.**
- **Expediting decision-making through automated and on-demand reporting on CIP and silo monitoring and statuses.**
- **Mitigating risk by providing a secure network system and secure access via a web portal.**

Optimization is Ongoing

The dairy producer now is focused on further operational improvements and has Malisko Engineering enhancing and expanding the manufacturing automation systems.

"Now we are working on decreasing shrink through the plant," notes Jacoby.

"We have the field instrumentation to monitor the process, and we are historizing many data points (optic sensors, flow, valve positions, etc.) to verify that product has fully been flushed through the system before transitioning to drain," he says.

The digitally transformed plant is a quantum leap from its earlier, entirely manual state and already the benefits are manifold. The decision to acquire and upgrade the plant is delivering immense and increasing value to the dairy producer from both an economic, environmental, compliance, and health and safety perspective.

Additional optimization initiatives will make the return on investment that much stronger. ●

MALISKO ENGINEERING Malisko Engineering, a Rockwell Automation Gold System Integrator and SI Hall of Fame member, is a CSIA certified manufacturing automation integrator with capabilities in plant-floor control, process automation solutions, manufacturing intelligence, power quality and energy management (PQ&EM), industrial IT and validation. The company has designed, developed, and deployed hundreds of Rockwell Automation systems from simple, single-unit PanelView™-based systems to complex, plant-wide PlantPAx® systems.



FROM WIN-911 SOFTWARE

University Cuts Heating System Alarm Response Time

SCADA and alarm monitoring software help protect a campus' new heating system and thus lowering GHG emissions, cutting costs and better using resources.

- In Canada, higher educational institutions generally use 60% of the electricity allocated to the educational sector, which is equivalent to that consumed by a city of 430,000 households. The operation of academic buildings is associated with significant amounts of water, energy and carbon flows. Effective energy management improves the local and national environment by reducing carbon dioxide (CO₂) emissions that result from energy use.

SCADA systems are used to remotely operate and monitor universities' complex heating systems from a central location. By monitoring and controlling remote equipment and resources, SCADA systems provide greater efficiency in terms of faster and more coordinated system control than human operation, as well as lower operational costs and better use of scarce human and financial resources.



The university's team can move onto the floor and visually check the engines and perform maintenance tasks without running up three floors from the boilers to the control room to simply acknowledge an alarm.



Commitment to Sustainability

With 67,000 students and 18,000 faculty and staff, the University of British Columbia (UBC) is British Columbia's oldest and largest university. Its flagship Vancouver campus spans more than 100 acres and comprises more than 160 buildings — including classrooms, research labs, animal care facilities, 12,000 housing beds, an Olympic-size swimming pool, 330-bed hospital, and the world's largest [cyclotron](#).

Until recently, heating these facilities was performed by a 90-year-old steam plant and pipe network that was costly to maintain and frequently broke down. In assessing their carbon footprint, UBC found that 80% of the school's carbon emissions was coming from the natural gas being burned to produce steam for the steam distribution system.

With the commitment of achieving net-zero emissions by 2050 through climate-action initiatives, UBC embarked on an ambitious six-year upgrade. In 2011, leaders created the action plan for a steam-to-hot-water conversion project, which was completed in 2017.

The new \$88-million, 45-MW District Waste Heat Recovery Project installs heat-recovery systems that reduce UBC's reliance on natural gas. The new system redirects the heat recovered to the campus' hot-water district energy system, which supplies the

majority of its buildings with heat and hot water for a cleaner environment.

The system includes a new Campus Energy Center and a Bioenergy Research Demonstration Facility (BRDF), which was also upgraded to produce up to 70% of the campus' thermal energy using clean, locally sourced wood chips and renewable natural gas to power turbines. Prior to installing the new system, more than 8 miles (14 km) of steam pipe was removed. The new system connects more than 160 buildings to a highly efficient hot-water district energy system that includes three 15-MW boilers and burns renewable natural gas to produce thermal energy.

BRDF was built in response to UBC's need to generate sufficient heat and power to meet the campus' growing energy demand through an affordable alternative fuel source that also reduces campus greenhouse gas emissions. The plant converts wood chips into a synthesis gas for heating as well as electricity generation through an internal combustion engine that powers a generator. A first-of-its-kind project in North America, the system processes renewable biomass to generate thermal energy for heating campus buildings.

The new facility is constructed with cross-laminated timber — a sustainable and versatile building material that stores CO₂ instead of emitting it.

The system reduces UBC's reliance on fossil fuels, provides a quarter of campus heating needs, and eliminates 14% of campus greenhouse gas (GHG) emissions. The new heat-recovery systems also are reducing UBC's emissions by more than 1,000 tons of CO₂ annually and will help recover 1 MW thermal, which would otherwise be wasted.

Additionally, the new system is 24% more efficient than the steam plant and pipe network. In 2020, UBC tripled the capacity of its biomass plant, energizing 70% of the Academic District Energy System with clean waste wood, saving an additional \$1 million annually and drastically reducing GHG emissions.

Collaborating for Success

To operate and monitor this new heating system, the UBC engineering team is using the Rockwell Automation [FactoryTalk](#)® SCADA system that reduces complexity, and promotes efficiency and reliability within their operations. Collecting, processing and examining the data in real-time is imperative to keep this system running smoothly.

The automation crew prefers [FactoryTalk](#) to other software because the predictive and augmented maintenance advantages allow them to easily manage and interact with critical data, promoting continuous improvement in the supply chains.

In addition, real-time critical remote alarm-notification software from Rockwell Automation Technology Partner WIN-911 provides "direct connect" integration with [FactoryTalk View SE Alarms & Events](#) and helps UBC mitigate any unplanned downtime. WIN-911 software connects seamlessly and directly to the [FactoryTalk](#) system, sending remote alarm and event notifications to operators' mobile phones.

UBC uses three standalone WIN-911 systems. The first monitors the power source in the Campus Energy Center, and

WATCH THE VIDEO

WIN-911: Industrial Alarm Notification Software Update Makes It Even Easier to Use

In this video, Steven Rivas with WIN-911 explains major updates to its WIN-911 2021 IIoT and industrial alarm notification software, used by 173 of the Fortune 500 companies, that make it even easier to use. It has a direct data connection with a user's Rockwell Automation SCADA system to monitor operations and notify personnel of problem conditions via voice, email, text, and apps on iOS and Android. Watch the video at <https://bit.ly/3CaDspd>.



HPS Centurion P

IMPROVE POWER QUALITY WITH Passive Harmonic Filters

HPS Centurion P passive harmonic filter improves power quality by simultaneously reducing harmonics and improving true power factor.

It is specifically engineered to mitigate harmonic currents created by non-linear loads such as variable frequency drives and other three phase rectifiers.

- 5 to 500 horsepower
- meets IEEE 519 harmonic requirements



The University of British Columbia's new heat-recovery systems redirect the heat recovered to the campus' hot-water district energy system, supplying the majority of its buildings with heat and hot water for a cleaner environment.



the second monitors the hot backup. A third system monitors the various operations of the BRDF power plant. The most important task for the remote alarm notification software is to make sure the three gas-fired water boilers in the CEC are maintained at an optimal level.

The FactoryTalk Alarm and Events connection in WIN-911 uses Subscriptions to bring alarms into WIN-911, which are filtered on four criteria: Names, Class, Severity and Groups. Routes are used to associate Subscriptions with alarm strategies, and configuring Subscriptions and assigning routes for alarm notifications is quick and easy.

"WIN-911 enables our operators to respond faster and more effectively to the ongoing changes and demands of our energy operations," says Huy Pham, industrial controls technical specialist, UBC Energy & Water Services.

Upgraded Notification System

UBC's Energy & Water Services department recently upgraded to WIN-911's new Advanced software platform to leverage the mobile capabilities.

"We have used v.7 Pro with Mobile 911 for years, but chose WIN-911 Advanced to use the new WIN-911 mobile app," Pham explains. "Any alarm that comes through is a critical alarm. We're continually

measuring the system's temperature and pressure. So, when an alarm comes through, the operator can quickly view, acknowledge, and respond [to an alarm] no matter where they are on campus."

WIN-911 Mobile allows the operators to respond faster to ongoing changes and demands without being tied to the control room. The team can move onto the floor and visually check the engines and perform maintenance tasks without running up three floors from the boilers to the control room to simply acknowledge an alarm.

Operators also can drill down into reports from their smartphone, chat with team members to see what options are available and decide how to respond.

From a cost-management perspective, WIN-911 allows the team to maintain the equipment with only one to two staff per shift, making their work much more efficient. ●

WIN-911 SOFTWARE Based in Austin, Texas, with offices in Europe, Mexico and China, WIN-911 is a Rockwell Automation Technology Partner. The company delivers critical machine alarms via smartphone or tablet app, voice (VoIP and analog), text, email and announcer.

PARTNER SHOWCASE

SOFTING INC.

Industrial Networking Communications Modules

Legacy PLCs and networks don't have to stop you from a headend controller upgrade. For example, maybe you have legacy OM1, OM2, OS1, or OS2 fiber connecting your main controller to remote I/O. Our industrial fiber optic networking solutions are specifically built for the purpose of connecting a newer main controller across legacy fiber for phased migrations. Contact sales@softing.us for more information.



<https://bit.ly/Softing>

ADVANCED MICRO CONTROLS INC.

Integrated Stepper & Servo Motors

The easiest way to add motion control to your Allen-Bradley® PLC. AMCI's integrated stepper & servo motors reduce system costs by eliminating the need for separate components, as they're all built-in. Move commands are programmed through Studio 5000®. EDS files and sample programs streamline initial setup and programming. Includes dual-port EtherNet/IP™ networking with DLR, built-in web server, absolute encoder, and safety features. Call 860-516-8771.



<https://bit.ly/3DEHdlb>

SYTECH INC.

XLReporter from SyTech

XLReporter gets the information you need, in the report you want with no programming. Built with Microsoft Open Office standard, it is the first reporting platform in industry to deliver workbook technology to an automated environment. Within minutes, reports are ready to view/email as workbooks, PDF and web pages. It interfaces to FactoryTalk® Linx Gateway, FactoryTalk Historian SE, PanelView™ Plus, OPC and databases. For FactoryTalk View SE, access to the ODBC data logs and File Data Sets is included.



www.SyTech.com

HMS NETWORKS

Unlock New Services with Your Machine Data

The Ewon Flexy 205 is an advanced Internet data gateway from HMS Networks that allows monitoring and data collection for analysis and predictive maintenance. With data logging, alarming, a built-in web interface, scripting and enhanced Internet connectivity, it is a versatile Internet Gateway for your IoT deployment.



www.ewon.biz/products/ewon-flexy/flexy-205

HARDY PROCESS SOLUTIONS

New Hardy Caseweigher for QA with Rockwell Automation PLC

Hardy's all new Caseweigher machine is designed for simplicity using off-the shelf components and a CompactLogix™ PLC control platform with Studio 5000® to use data across The Connected Enterprise. Hardy's 4050CW Checkweight controller samples at 4,800 times per second to provide extremely accurate and fast weight data with a full statistics package.



<https://bit.ly/3znjMXc>



You're just 1 click away from getting free online articles from *The Journal*. Just go to <http://rok.auto/thejournal-subscribe>. Check "The Journal" box to get your free e-newsletter that brings you the digital edition of The Journal every issue – plus additional Web-exclusive how-to articles, case studies and product news from Rockwell Automation and companies in its PartnerNetwork™. Visit

[HTTP://ROK.AUTO/THEJOURNAL-SUBSCRIBE](http://rok.auto/thejournal-subscribe)

SIGN UP TODAY!

Electromagnetic Flowmeter

Rockwell Automation Strategic Alliance Partner **Endress+Hauser's** Promag W 800 flowmeter with battery-powered operation is designed for remote areas where power and wired data transmissions are limited. It provides maintenance-free operation for up to 15 years, and worldwide secure data transfer via cellular radio.

The electromagnetic flowmeter monitors water supply networks, locating leaks and avoiding non-billable water losses. A backlit display makes it quick and easy to read measured values.

The company's SmartBlue app can interact with the flowmeter and provide more comprehensive data retrieval on site. It is also available with various drinking water approvals such as KTW/W270, WRAS BS6920, ACS, or NSF 61. Watch the video to learn more: <https://bit.ly/EHPmG800W>.



FactoryTalk Logix Echo Emulation Software

The **FactoryTalk® Logix Echo controller emulation software** is now available for use with the Allen-Bradley® ControlLogix® 5580 family of controllers from Rockwell Automation.

Using the emulation software, engineers can fully test control code in a virtual environment. With support for up to 17 emulated controllers, the software can emulate a machine, production line or even an entire plant.

Emulated controllers also can be paired with other software for a range of uses. For example, by connecting an emulated controller to a mechanical system model via the Emulate3D digital twin software, users can perform testing and experimentation without large physical equipment.



PRODUCT SPOTLIGHT

IO-LINK SMART SIGNALING SOLUTION

The **Allen-Bradley® 856T control tower stack light system** from Rockwell Automation is designed to meet a range of applications with fewer components. This system's modular design incorporates brighter LED illumination and various sound technologies.

All signals in the system are 24-V AC/DC powered, which means just three power modules can cover the entire system. The latest additions to the line are IO-Link-enabled versions that provide diagnostic information and ease integration into a Connected Enterprise.

IO-link versions of the stack lights allow users to monitor tower light and machine status in real-time, while simplifying remote setup and troubleshooting.

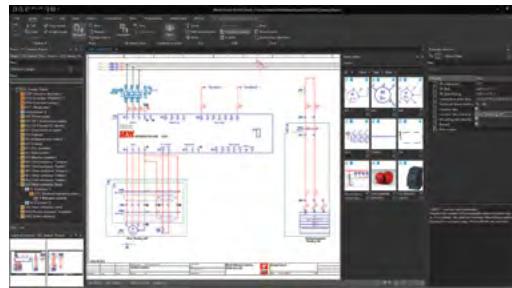


2D and 3D Engineering Module

The EPLAN Platform 2022 from Rockwell Automation Technology Partner **EPLAN Software & Services** has a new user interface that improves overall ease of use. It features optics and functionality based on apps for mobile devices and internationally established desktop applications.

The redesigned user interface includes both 2D and 3D engineering with light and dark display mode options. Variable tabs give users direct access to important and often-used functions.

The multifunctional toolbar with modern ribbon technology adapts to the application, such as when switching from 2D to 3D. It also combines different menus and toolbars into one, making daily work easier.

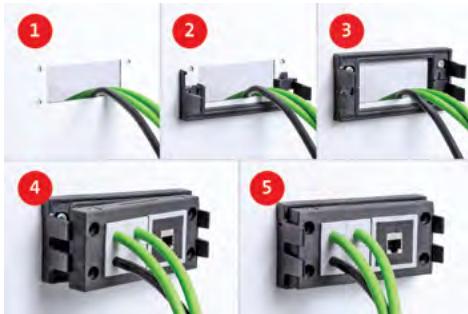


Snap-in Cable Entry Frame

Rockwell Automation Technology Partner **icotek** offers its KEL-SNAP frame as a new splittable version, KEL-SNAP-S. The frames provide a quick and tool-free assembly for several KEL model cable entry frames.

Switch cabinets can be equipped with the frame in advance by the control manufacturer to facilitate subsequent assembly by the machine manufacturer. A seal already is integrated into the frame on both sides.

The splittable snap-in frame also can be retrofitted. If an already installed frame needs modified, a single frame can replace it without the need to disconnect cables already passed through and dismantling the existing KEL.



Intrinsically Safe Industrial Tablet

The intrinsically safe Tab-Ex® 03 D2 tablet from Rockwell Automation Technology Partner **Pepperl+Fuchs'** ECOM instruments brand is the third generation of Samsung industrial device variants for hazardous areas.

Tab-Ex® 03 is based on the Samsung Galaxy Tab Active 3 with high security for data and devices. The Samsung DeX feature allows users to quickly switch to a desktop version. The tablet also offers more RAM and external storage than previous models.

The 8-in. tablet is easy to operate with gloved hands or using the S Penstylus. The device is adaptable to individual requirements and supporting daily work.



Threat Detection Services

Rockwell Automation has added the Cyber Vision solution from Strategic Alliance Partner **Cisco**® to its existing LifecycleIQ™ Services portfolio of cybersecurity threat detection offerings.

As deeper integration between IT, cloud and industrial networks creates security issues that become digitization obstacles, Cyber Vision provides full visibility into industrial control systems. This helps to build secure infrastructures and enforce security policies to support the continuity, resilience and safety of industrial operations.

The addition of Cyber Vision provides a switch-based architecture for operations with existing Cisco solutions, greenfield networks or those updating their Cisco network infrastructure.

PRODUCT SPOTLIGHT

IEC 61850 CONTROLLOGIX MODULE

Rockwell Automation Technology Partner **ProSoft Technology** offers the IEC 61850 module for Allen-Bradley® ControlLogix® systems. The in-rack product integrates seamlessly with a library of electrical protection devices (IEDs) from Rockwell Automation.

IEC 61850-enabled devices support a standardized data structure across these devices, increasing vendor flexibility for end users. Each module supports up to 40 IEDs on a redundant PRP-enabled network, and up to a maximum of 225 I/O connections to the ControlLogix processor.

The module features GOOSE Publisher, which is used to support GOOSE messaging for the product. The software provides a mechanism to interlock relays or load shed using the IEC 61850 communications network.



NEMA-Rated Contactor Options

Rockwell Automation offers new sizes in its line of energy- and space-saving **Allen-Bradley® Bulletin 300 NEMA contactors**. Now available in NEMA sizes 00 to 8, they feature universal electronic coils that reduce inrush apparent power (VA) by up to 68% and sealed VA by more than 75% compared to standard, non-electronic coils. The electronic coils also save engineering time by covering 20 to 500 V AC/DC coil voltages with only four coil options, simplifying selection.



These contactors allow coil input terminals to be moved from the line to load side of the contactors without disassembly, easing wiring and access when building starter assemblies.

Sustainable Light Fixture for Heavy Industries

Rockwell Automation Technology Partner **Dialight** introduces its ultra-efficient, heavy industrial-rated lighting fixture, the Vigilant LED High Bay. This fixture helps companies achieve carbon-neutral operation goals faster while saving money on lighting-related energy costs.

This upgrade expands the total light output range with new 30,000, 35,000 and 40,000 lumen offerings to suit a variety of industrial applications. The fixture is IP66 rated to protect against dust and water ingress, impact-rated to IK10, and offers an operating temperature range of -40°C to +65°C.

The fixture is available with several certifications and verifications to offer greater savings through energy rebate programs, and verify its sustainability.



Remote Alarm Notification Software

Rockwell Automation Technology Partner **WIN-911** has updated its remote alarm notification software. WIN-911 2021 is designed to be more efficient and easier to deploy than previous versions, with reduced installation and configuration time and simplified navigation.

Streamlining capabilities into a simple workspace reduces system resources by up to 50%, providing faster performance and increased productivity. Users can quickly organize alarm notifications based on alarm types, severity or worker roles, and create simple to complex rolling schedules for different staff using calendar-based controls.

The revamped Alarm Sources section allows all SCADA-specific alarm data to be seen in one console for users to filter alarms as precisely or generically as needed. Watch the video to learn more: <https://bit.ly/3CaDspd>.



CIP Security Proxy Device

The **Allen-Bradley® CIP Security™ Proxy** from Rockwell Automation allows users to implement CIP Security on most devices on their network, helping to protect plant operations, including those with older systems.

The unit helps to secure the entire network by working with EtherNet/IP™-compliant devices. It is part of the Defense in Depth strategy, which can help defend against attacks when threat actors can remotely access a network and act maliciously. Users can configure the device through FactoryTalk® Policy Manager software and FactoryTalk system services.

In addition, this device supports motion for Kinetix® drives and offers a web server for viewing diagnostics.



Enhanced FactoryTalk AssetCentre Software

The latest release of **FactoryTalk® AssetCentre software** from Rockwell Automation provides firmware and software life-cycle information for all assets in one place. This saves time because workers no longer need to connect to control cabinets and manually record information for each device.

With the software's enhanced asset inventory functionality, workers can quickly scan a network and see which devices are in a specific life-cycle state. Examples include devices running retired firmware or forecasted to be discontinued in the next six months. This helps identify products in the same life-cycle state so workers can better plan for replacements and upgrades.



Self-Terminating Connectors

The ServiceDrive VFD Cable System from Rockwell Automation Technology Partner **Service Wire Co.** now includes VFD self-terminating connectors for direct wiring (TC-ER), liquid tight, NPT conduit and interlocked armor (jacketed Type MC) installations.

The self-terminating connectors provide a 360° termination method required for critical drive systems to operate properly. When coupled with ServiceDrive shielded VFD cable, the system provides a low impedance path for high frequency current, protecting drives, motors, and surrounding equipment from the effects of EMI and common-mode stray currents.

The system consists of cable, self-terminating connectors and termination kits. Tray and interlocked armor cables include configuration of three NFPA 79-compliant XLPE insulated conductors and three balanced grounds with helically applied 5-mil copper tape shield.



Industrial-Grade Modem

Rockwell Automation Technology Partner **DATA-LINC Group** introduces the HSM240E-SD 2.4GHz industrial-grade modem. This modem's use of smarter and updated technology provides critical connectivity that complements, enhances and extends Rockwell Automation solutions.

The high-speed Ethernet modem is a standard 2.4GHz, license-free wireless Class I Div II, 802.11b/g modem that comes with user-friendly features to increase efficiency and security and reduce the threat of costly downtime.

The modem provides local control and monitoring and can work with Ethernet, serial and digital I/O simultaneously. It supports standard Wi-Fi communication with selectable RF speeds up to 54Mbps in standard mode and 108Mbps in turbo mode for point-to-point and point-to-multi-point communication.

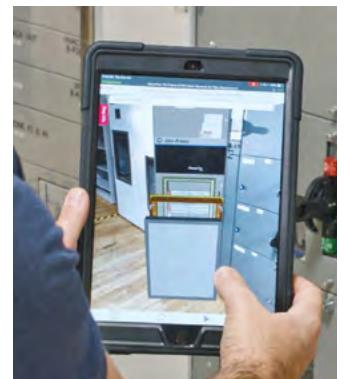


AR Remote Support Tools

Rockwell Automation **LifecycleIQ™ Services** now includes remote support tools that use augmented reality (AR) technology. The Live View Support Tool and Digital Assist Library of Work Instructions allow users to quickly troubleshoot and repair automation equipment to help minimize downtime.

Using live video feed, a Rockwell Automation remote support engineer can view equipment in real time and provide specific, detailed directions for troubleshooting or repairing hardware and software issues.

3D spatial annotations can be made on the screen, so the on-site worker and the remote support engineer can share visual markups to better identify which parts or products need attention.



High-Speed Discrete I/O Modules

Rockwell Automation Technology Partner **Spectrum Controls** offers two new modules, the 5069-IV16F-SC and 5069-OV16F-SC. The modules are compatible with the Compact 5000™ I/O system from Rockwell Automation.

The high-speed discrete input (sourcing) and output (sinking) modules complement the existing discrete I/O for sinking and sourcing from Rockwell Automation, respectively. Included with the fast input module is an input filter that helps improve noise immunity.

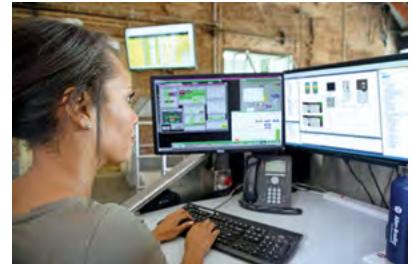
Filtering helps prevent rapid changes of the input data due to contact bounce. The fast output module provides features like no-load detection, short-circuit protection and field power loss detection.



Enhanced FactoryTalk Linx Software

The latest release of **FactoryTalk® Linx software** from Rockwell Automation helps ease system recovery, increases upload and download speeds, and more efficiently brings new devices online. These enhancements free up time for plant engineers to focus on other priorities.

The update adds new security measures, including communications integrity/confidentiality, credential authentication, audit tracking, and configuration backup and restore. These extra layers of security can help reduce unplanned downtime due to security concerns and issues.



The release also adds backup and restore capabilities that allow users to save configuration settings. This helps improve administrator efficiency by eliminating the need to manually reconfigure the entire system during recovery.

ADVERTISER INDEX

Advanced Micro Controls, Inc. (AMCI)	37
Endress+Hauser	3
Hammond Power Solutions	35
Hardy Process Solutions	37
Helm Instrument Co. Inc.	23
HMS Networks	20, 37
Rockwell Automation Authorized Distributor	15
Rockwell Automation Digital Transformation	43
Softing Inc.	37
Southwire Company	44
Spectrum Controls Inc.	2, 11
Sytech Inc.	37



we make

digital transformation possible

The next industrial transformation is here. Are you ready?
We partner with the innovators, problem solvers, builders and makers who believe our world can work better. We strive to expand human possibility by helping you build a Connected Enterprise to enable IoT-fueled digital transformation. We will help you meet today's challenges and prepare for what comes next.

expanding **human possibility**[®]

RockwellAutomation.com

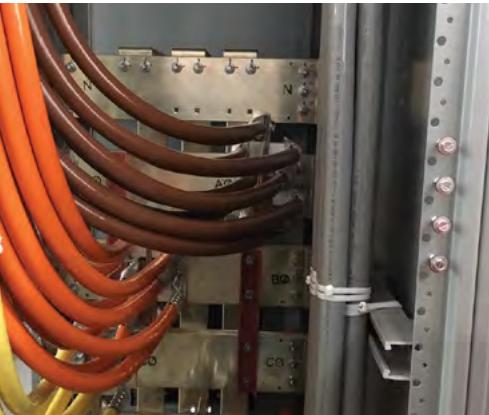


Southwire®



BRONZE
Technology Partner

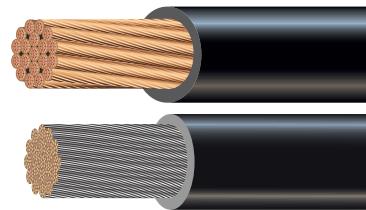
A ROCKWELL AUTOMATION PARTNER



ARE YOU INSTALLING THE BEST CABLE SOLUTION FOR YOUR INDUSTRIAL APPLICATION?

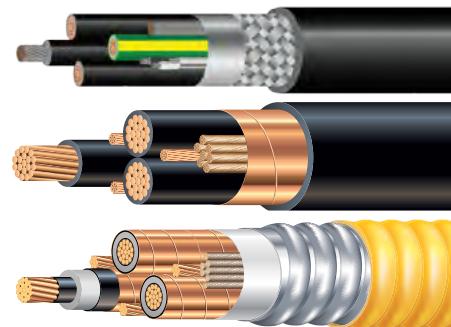
MachineFLEX™ POWER CABLE

Southwire Company, LLC's MachineFLEX™ Power Cable (rated THHN or XHHW) has been designed to help make difficult installations easier. By combining the insulation properties and pulling ease of THHN/XHHW with the flexibility of fine stranded copper, this cable helps to increase efficiency and productivity on the jobsite while improving safety.



VARIABLE FREQUENCY DRIVE (VFD) CABLES

Our NFPA 79 compliant VFD cables help keep your drives and motors running efficiently and help to ensure you're using the safest cable solution for your VFD applications.



To learn more email factoryautomation@southwire.com or visit Southwire.com

Visit us at SOUTHWIRE.COM to learn more

Connect With Us     

©2021 Southwire Company, LLC. All rights reserved.
®Registered Trademark & ™Trademark of Southwire Company, LLC.