the journal
from Rockwell Automation rNetwork™
JULY 2024

OEMs DRIVE CYBERSECURITY IN SMART VEHICLES

WHY OT CYBERSECURITY IS A VITAL BUSINESS STRATEGY

CASE STUDY: PACKAGING ROBOTICS WITH OPEN MECHANICS

STAY ON TRACK

AS NEW TECHNOLOGIES CONVERGE WITH OT, MANUFACTURERS SEEK A CLEAR PATH TOWARD A DIGITAL FUTURE.

16

Stay on Track

As new technologies converge with OT, manufacturers seek a clear path toward a digital future.

MICHAEL ANNINO / SHUTTERSTOCK AI

INDEX

22

26

30

FEATURES

DEPARTMENTS

ADDITIONAL RESOURCES

WEBINAR

Industrial Gateways Bridge the Communication Gap

In this on-demand webinar from Spectrum Controls, learn about industrial communication protocols and how gateways facilitate automation in mixed-protocol environments.

https://tinyurl.com/tj612scweb

EBOOK

CPG Automation eHandbook

Dive into real-world examples of consumer-packaged goods firms using digital transformation to achieve peak performance. Get examples from packaging OEMs, food & beverage makers and more.

https://tinyurl.com/tj524cg

WEBINAR

Mitigating Harmonic Disturbances for Better Electrical System Performance

Learn how harmonic disturbances impact electrical systems and equipment downtime, and get best practices for mitigating these effects.

https://tinyurl.com/hp618w

the journal from Rockwell Automation and our PartnerNetwork™

JULY 2024, VOLUME 31, NO. 3

JOURNL-BR093A-EN-P

ENDEAVOR BUSINESS MEDIA

Endeavor Business Media, LLC

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

EDITORIAL & SALES TEAM

EXECUTIVE EDITOR
Theresa Houck
thouck@endeavorb2b.com

MANAGING EDITOR
Amanda Joshi
ajoshi@endeavorb2b.com

ART DIRECTOR
Michael Annino
mannino@endeavorb2b.com

PRODUCTION MANAGER
Rita Fitzgerald
rfitzgerald@endeavorb2b.com

ADVERTISING SERVICES MANAGER
Jennifer George
jgeorge@endeavorb2b.com

ADVERTISING SALES MANAGER
Brian Marz
bmarz@endeavorb2b.com

CORPORATE TEAM

CEO
Chris Ferrell

PRESIDENT
June Griffin

COO
Patrick Rains

CHIEF ADM/LEGAL OFCR
Tracy Kane

CHIEF DIGITAL OFFICER
Jacquie Niemiec

VP/PUBLISHER
Keith Larson

AI Helps Manage Data Overload

In this era of information overload, we often find that data and new technologies bring us more valuable insight than ever before — but the path to implementing them to get that data can be as overwhelming as the influx of information itself. So, it's important to get the train out of the station, so to speak, and move forward with an implementation strategy to get those technologies delivering tangible results.

In fact, many manufacturers recognize that getting value from their data is worth the challenge. According to the latest Rockwell Automation Annual State of Smart Manufacturing Report (rok.auto/sosm), 95% of manufacturers are using or evaluating smart technologies. This is the key to the ever-changing consumer demands, ongoing workforce shortages and supply chain disruptions. Industrial firms need every advantage they can get to increase efficiency and profits.

But you already know this. So how do we go from information overload to getting the right information at the right time to help deliver the right results? Advanced technologies like AI and machine learning are making huge strides. Our cover story, starting on page 16, illustrates what's needed to stay the course on your digital journey and get past the initial implementation stage.

In this issue, you'll also learn how the automotive industry has been adopting digital technologies to improve the flow of information and create a faster, more resilient operation. And with the increase in smart connections — both on the plant floor and in the vehicles themselves — comes the risk of cyber threats. Fortunately, OEMs are helping automakers keep those connections secure and drivers safe.

We hope these insightful stories help you overcome the information overload and drive your digital journey forward. Until next time ....

Theresa Houck

EXECUTIVE EDITOR

Manufacturing is now the #1 target for hackers. In our "Automation Chat" podcast, "What's Really Happening with Industrial Cybersecurity & What You Can Learn," Theresa Houck chats with Fortinet's Richard Springer about a study on unprecedented cybersecurity risks. Learn key takeaways, cybersecurity trends, the role of IT/OT collaboration, and more. Listen on your podcast app or on the web at https://tinyurl.com/3szd37et, or watch their conversation on YouTube at https://youtu.be/esFAKPAbCSY.

How We Help the Automotive Industry

Jodi Marr

GLOBAL LEAD - TECHNOLOGY PARTNER PROGRAM MANAGER

ROCKWELL AUTOMATION

Have you ever gotten into your car on a hot day, ready to head home from work or pick up the kids from school, and reminisced about your very first car — the one that didn't have air conditioning? Well, thankfully, vehicles and the technology used to manufacture them have evolved leaps and bounds over the past several decades since you drove that first vehicle.

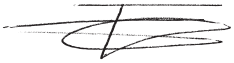
Disruptive technology-driven trends such as electrification, connectivity and autonomous driving are shaping the future of the automotive industry. Tried and trusted, as well as emerging technologies are required to respond to these trends.

The ongoing pursuit to respond to automotive market demands, coupled with supply chain disruptions, consumer demand, geopolitical tensions and rising commodity costs has introduced a suite of complex challenges — and quite honestly, one that Rockwell Automation and its PartnerNetwork™ are ready to face.

The combined power of Rockwell Automation and the PartnerNetwork offers the benefits of industry expertise and a holistic approach, a comprehensive suite of solutions to address unique industry needs, and solutions enabling connectivity, data analytics and predictive maintenance to drive efficiency and increase productivity.

Through collaboration, Rockwell Automation and companies in our PartnerNetwork aim to empower businesses, increase operational resiliency and efficiency, and foster innovation across various sectors around the world.

Learn more about our PartnerNetwork by visiting our Partner Locator (https://rok.auto/technology-locator). ●




Smart starts here
82% of companies using smart manufacturing have experienced increased efficiency.
Allen-Bradley smart devices deliver real-time operational information, allowing you to make informed decisions and prevent unplanned downtime.
To get started on your smart journey, contact your local Rockwell Automation representative.
RockwellAutomation.com
Allen-Bradley
by ROCKWELL AUTOMATION

News Noteworthy

Rockwell Automation, NVIDIA Expand AI in Mobile Robots

Collaboration will involve integrating AI into OTTO Motors autonomous mobile robots to accelerate their development.

Earlier this year, Rockwell announced its ongoing work with NVIDIA to increase the scale and scope of AI in manufacturing. The collaboration is now expanding to involve robotics, supporting the use of AI in autonomous mobile robots (AMRs) to improve performance and efficiency.

The continued collaboration will involve integrating the NVIDIA Isaac robotics platform into OTTO Motors AMRs from Rockwell Automation and production automation applications.

NVIDIA Isaac is an AI robot development platform consisting of NVIDIA-accelerated libraries, application frameworks and AI models that accelerate the development of AI robots such as AMRs, arms and manipulators, and humanoids.

Rockwell Automation also continues its work to integrate NVIDIA Omniverse Cloud application programming interfaces (APIs) with its Emulate3D™ software, bringing users data interoperability, live collaboration and photo-realistic graphics rendering for designing, building, and operating industrial-scale digital twins of production systems.

According to the recently released "State of Smart Manufacturing Report" (www.rok.auto/sosm), AI ranks as the top feature manufacturers believe will drive the biggest

business outcomes. In fact, 83% of manufacturers expect to use generative AI in their operations in 2024.

As part of this collaboration, the Rockwell Automation PartnerNetwork™ now includes NVIDIA, giving Rockwell customers more applications to help make their operations more resilient, agile and sustainable.

eBook Highlights CPG Automation Best Practices

The Journal's 2024 "CPG Automation" eHandbook is designed to help consumer packaged goods firms use digital technology to achieve peak performance. This comprehensive resource is packed with real-world examples of how leading CPG companies are using digital transformation to achieve:

- **Enhanced safety & cybersecurity through smart equipment design.**
- **Modernized operations for improved efficiency.**
- **Increased system visibility and filling accuracy.**
- **Streamlined OT asset management for maximized uptime.**
- **Increased production and quality with digital process automation.**

This educational resource is published by *The Journal From Rockwell Automation and Our PartnerNetwork*™ magazine.

Download the eHandbook at https://tinyurl.com/tj524cg.

2023 Sustainability Report Unveiled

Rockwell Automation has released its 2023 Sustainability Report. It details the company's sustainability progress and outcomes and how it is partnering across the manufacturing industry and communities globally to create sustainable impact and change. Download it at https://rok.auto/sustainability.

In addition to showcasing how the company supports its customers' sustainability efforts, the report highlights the organization's ESG initiatives, sustainability programs and efforts to foster a culture that empowers employees to operate safely, sustainably and responsibly.

It also discusses the company's work toward its goal to be carbon neutral by 2030. It includes information about the company's Scope 3 emissions baseline.

New ESG initiatives highlighted include the company's UN Global Compact, partnership with the Science Based Targets Initiative and a Product Design for Sustainability team.

The report also underscores how the company is helping create a skilled, engaged workforce, and the importance of partnering across government, educational institutions and industry to develop needed workforce skills.

Microsoft Expands Partnership

Rockwell Automation and its Strategic Alliance Partner Microsoft Corp. have extended their long-standing relationship to accelerate industrial automation design and development through generative AI. The companies are combining technologies to empower the workforce and accelerate time-to-market for customers building industrial automation systems.

The first outcome of this collaboration will add Microsoft's Azure OpenAI Service into FactoryTalk® Design Studio™ to speed time-to-market for customers building industrial automation systems.

Adding Azure OpenAI Service into FactoryTalk Design Studio helps engineers generate code using natural language prompts, automating routine tasks and improving design efficiency. It will also help engineers accelerate development and mentor newcomers more efficiently and effectively.

In addition, it will assist in finding relevant help from vast collections of information to further educate developers. This integrated technology could be used to solve other challenges, including quality management and improvement, failure mode analysis, and training workers to execute manufacturing processes through chat-based collaboration with experienced human workers and Azure Open AI Service-based chatbots.

PARTNERNETWORK BRIEF

Southwire Names New EVP. Southwire has named Veronica Braker as its new executive vice president of Operational Excellence. She will strengthen the firm's commitment to continuous improvement. Braker's career includes leading teams focused on operations, EHS, reliability and maintenance and capital expenditure. She is a Lean Six Sigma certified Master Black Belt. She most recently served as SVP of Global Operations at Archer Daniels Midland Company. She also has held leadership roles at Clorox, General Electric, BASF Corporation, Flint Hills Resources and Milliken & Company.

Firms Named Top Ethical Companies

Ethisphere, a global leader in defining and advancing the standards of ethical business practices, has recognized Rockwell Automation, Inc. and companies in its PartnerNetwork™ program as some of 2024's World's Most Ethical Companies.

This is the 16th time Rockwell Automation has been included on the list honoring companies that demonstrate leadership and commitment to business integrity through best-in-class ethics, compliance and governance practices. Only 14 companies have achieved this honor 16 or more times.

Technology Partners nVent, Hubbell Inc. and Southwire, and Strategic Alliance Partner Accenture were also included in this year's list.

The firms were among 136 honorees recognized in 2024. The ranking spans 20 countries and 44 industries. View the full list of 2024 honorees at https://worldsmostethicalcompanies.com/honorees.

Dragos Reveals Cybersecurity Report

Technology Partner Dragos Inc. has released its 6th annual "Dragos OT Cybersecurity Year in Review" covering cyberthreats facing industrial organizations.

The report named the emergence of three new threat groups, including VOLTZITE linked to Volt Typhoon, and found that ransomware continued to be the most reported cyberthreat among industrial organizations, with a nearly 50% increase in reported incidents.

2023 also saw the first time a hacktivist group achieved Stage 2 of the ICS cyber kill chain. Download the full report at www.dragos.com/year-in-review.

PARTNERNETWORK BRIEF

E Tech Group Names VP, Life Sciences & Process Industries. Gold Certified Rockwell Automation System Integrator Partner E Tech Group has named Trent Meyers, P.E. as VP of Life Sciences Central and Process Industries. He brings more than 30 years of experience in engineering and manufacturing operations, including numerous leadership positions. In this role, he will oversee the engineering, project management and project delivery groups while supporting sales and marketing efforts. Prior to joining E Tech, Meyers served as VP of project delivery and general manager at Jedson Engineering. He holds a B.S. in Mechanical Engineering and is a registered Professional Engineer.

SVP, Software & Control Named

Matheus Bulho has been promoted to senior vice president, Software & Control, reporting to Rockwell Automation CEO Blake Moret. Bulho will lead the operating segment that includes control and visualization software and hardware, information software, and network and security infrastructure. He succeeds Brian Shepherd.

Recently, Bulho served as VP and general manager for the Production Automation business unit in the Software & Control segment. He has more than 20 years of experience at Rockwell Automation with prior roles in business management, and technical and sales positions across multiple businesses and regions.

He began his career with the company in the technical support group in Brazil. He progressed to field services engineering, sales engineering, and various business unit functions.

Bulho holds an MBA from the University of Chicago Booth School of Business and a bachelor's degree in electrical engineering from UNESP Brazil.

Plex Named Merit Awards Gold Winner

Plex, by Rockwell Automation, has earned a 2023 Merit Award, receiving the gold for "Automation" under the Software and Apps category. The Merit Awards is an independent awards program for global industries and the markets they serve.

Submissions represent the best in current and next-generation innovations and technologies, and judges award gold, silver and bronze distinctions for each category. For the full list of winners, visit www.merit-awards.com/winners-technology-2023.

PARTNERNETWORK BRIEF

AMCI Now in ProposalWorks. Technology Partner AMCI's PLC module Selection Assistance is a new feature on ProposalWorks™ with 30 different module configurations. Users can find AMCI modules in the Technology Partners section or use the search bar to find a module (**https://configurator.rockwellautomation.com/browse**). The Rockwell Automation ProposalWorks™ software tool simplifies creation of project proposals for automated solutions. It offers preconfigured templates to quickly generate proposals tailored to the project's needs.

Southwire, READY Robotics Team Up

Technology Partners Southwire Co. and READY Robotics are partnering to deploy automation at five of the company's facilities. Participating in the automation pilot are Southwire's customer service center in Villa Rica, Georgia; its Bremen, Indiana campus; and plants in Carrollton, Georgia; Hawesville, Kentucky; and Florence, Alabama.

READY Robotics will deploy industrial robotics, mobile robotics such as automated guided vehicles or autonomous mobile robots, and IIoT across Southwire's corporation using ForgeOS, Ready Robotics' industrial operating system for robotics and automation.

READY Robotics Achieves ISO 27001

Rockwell Automation Technology Partner READY Robotics has received ISO 27001 (ISO/IEC 27001:2022) certification, a globally recognized standard outlining the best practices for an information security management system.

This certification signifies that the firm has implemented a systematic and rigorous approach to managing sensitive company and customer information. Achieving this certification involved a detailed assessment of the company's information security practices, including risk management processes, staff training, physical and technical safeguards and legal compliance.

DRAGOS

Dave Kang

ADVISORY SOLUTIONS ARCHITECT

ROCKWELL AUTOMATION

Kamil Karmali

SENIOR GLOBAL COMMERCIAL MANAGER, CYBERSECURITY SERVICES

Understanding the OT Threat Landscape Helps Manufacturers Improve Cybersecurity

The level of sophistication and frequency of cyberattacks on manufacturers keep increasing, making readiness and incident response capabilities imperative. To explore the latest trends and what they mean for manufacturers, I spoke with two experts on the topic: Kamil Karmali, Senior Global Commercial Manager, Cybersecurity Services at Rockwell Automation and Dave Kang, Advisory Solutions Architect at Rockwell Automation Technology Partner Dragos.

Theresa: Why is the industrial control system (ICS)/OT community especially vulnerable to cybersecurity threats?

Kamil: I think insufficient workforce skills and awareness of security hygiene prioritization are the core challenges. In manufacturing, the top most critical goal has been to keep the production environment up and running. Suddenly, workers who were focused primarily on quality, efficiency and profitability are now the first line of defense against nation-state actors and skilled attackers — without having the proper skills to identify risk and design, implement, and execute a holistic cybersecurity strategy.

Another weakness is when the manufacturing install base is old and in need of modernization, so there are increasing unknown vulnerabilities, making driving cyber investment a challenge due to competing priorities.

Dave: There is a historical aspect as well. In the late 1990s through the early 2000s, as IT networks evolved and threats grew, cybersecurity began to mature. But we in OT are just seeing that now because traditionally, OT has trailed 15 to 20 years behind IT technologies.

Theresa: How did the OT threat landscape change in 2023?

Dave: The growing number and scope of vulnerabilities is impossible to ignore. For example, according to our recently released report, "OT Cybersecurity: The 2023 Year In Review" (https://tinyurl.com/5n6uxdnw), there was a near 50% increase in ransomware attacks against industrial environments last year, with 70% of all attacks targeting manufacturing entities.

It's why cyber is becoming a board-level objective, especially for companies driven by regulatory compliance, and why vulnerability and risk management are moving very quickly to the top — especially in industries with large, disparate install bases such as oil & gas, mining and chemicals.

Theresa: What do you consider to be the greatest vulnerabilities today?

Kamil: To me, critical infrastructure continues to have the greatest threat vulnerability. Attackers are positioned on that industry segment because of its potential for human loss-of-life casualties or disruption; it's the simplest and quickest way to create harm or malice.

Another aspect is what I call "scaling of size." A large manufacturer may have sites around the world at different stages of cyber maturity or

In 2023, there was a near 50% increase in ransomware attacks against industrial environments, with 70% of all attacks targeting manufacturing entities.

security hygiene, using decades-old automation assets that weren't built for security. This is a vulnerability, especially considering how many companies still struggle with the basics around patch management.

Dave: Inertia is another one, the idea being, "We've gone this far without anything going wrong, so why don't we just continue to press forward and take that risk?"

Also, the disparate nature of manufacturing environments and all the growth — by acquisition, organically or just expansion — increases the attack surface and companies aren't prepared to defend against that.

Theresa: Why is having a unified, risk-based response important? What does that look like?

Kamil: A risk-based approach is knowing your vulnerabilities, how to manage them, and how to right-size your investment. What's most important is to never build a strategy purely based on technology.

Rather, what's beautiful about standards like NIST or other governing cyber frameworks is that they allow you to think both proactively and reactively — identify, detect, protect, respond, recover, and governance.

Naturally, every manufacturer is in a different state of their cyber maturity journey, and many are reactively trying to figure out where to start. Companies like Dragos and Rockwell Automation try to put them on a proactive journey, using a framework to help tackle one step at a time.

Theresa: What types of cybersecurity controls are most critical to securing OT?

Dave: First and foremost, based on my experience, you need an incident response plan, and not just "restore from backups." Things like tabletop exercises can really bring to light how ahead or behind any organization might be in terms of responding to an incident.

The response plan will be your stopgap or buffer while you put other controls in place, such as a risk-based OT vulnerability management program for timely awareness of key vulnerabilities and how best to mitigate them.

You'll also want to validate controls from a segmentation basis, examine firewall rules, ensure that your architecture is defensible and deploy some method to monitor traffic for threats.

Kamil: We also see companies moving towards a true security operations center (SOC) provider, or augmenting to a hybrid SOC model, when their operators lack the right skill sets or when IT doesn't know what alerts mean in OT.

Theresa: What key takeaways do you want our readers to remember?

Dave: Don't buy into the fear, uncertainty and doubt. The fact of the matter is this: Defense of your industrial network is possible, and the greatest risk is just doing nothing. Start with the foundational components, which are the most important, rather than striving for perfection. And consider this: if you can stop any one of the stages in a cyberattack kill chain, you have effectively nullified the attack.

Kamil: I would add that you are not alone in this. There are experts who can help you, so if you don't have the right workforce skill set, look to outside partners to help build the cyber journey with you. ●

DRAGOS Rockwell Automation Technology Partner Dragos provides ICS/OT cybersecurity solutions for hundreds of industrial organizations. In addition to technology and service offerings, the firm offers threat intelligence to provide organizations with in-depth visibility of threats targeting industrial environments globally and the defensive recommendations to combat them. Learn more at www.dragos.com.


STAY
ON
TRACK

MICHAEL ANNINO / SHUTTERSTOCK AI

ARTICLE BY

Andrew Hastert

DIRECTOR, DIGITAL PORTFOLIO STRATEGY,
ROCKWELL AUTOMATION

AS NEW TECHNOLOGIES CONVERGE WITH OT, MANUFACTURERS SEEK A CLEAR PATH TOWARD A DIGITAL FUTURE.

According to the latest Rockwell Automation Annual State of Smart Manufacturing Report (rok.auto/sosm), the global labor shortage and skills gap continues to be a top concern. It's becoming increasingly challenging to attract, manage and retain skilled workers. But there is hope.

New and emerging technologies are filling skills gaps and amplifying effort, rather than replacing workers. This makes it possible for manufacturers to do more with less.

Increasing automation and introducing artificial intelligence (AI) and machine learning (ML) technologies are top strategies manufacturers are planning to optimize processes. But many people remain skeptical of the transformative promises of this technology and its ability to overcome workforce gaps.

Past implementation attempts may have resulted in endless pilot projects, where companies strive and fail to achieve the benefits of digital transformation, the Industrial Internet of Things (IIoT) or "big data casual AI." In fact, this experience is so common, it's coined its own buzzword — **pilot purgatory**.

Maybe you've personally suffered from pilot purgatory as you've been lured into the inflated expectations of the innovation of the moment, only to find the initial investment didn't yield intended returns and required more investment at the end.

Riding the Wave

If you've attempted your own venture into applying technology in manufacturing and achieved mixed results, you're not alone. A survey from McKinsey (https://tinyurl.com/ef89hfbw) found more than 80% of companies were stuck in pilot mode for more than a year.

But adoption of new technologies over the last four years has been growing. According to the latest Rockwell Automation Annual State of Smart Manufacturing Report, 95% of manufacturing companies are using or evaluating smart manufacturing technology. There are good reasons for this growth, including:

- Continued inflation.
- Shortage of skilled workers mixed with a new generation of workers.
- The need to prove sustainability outcomes.
- The need to balance across many complex priorities.

Another reason we can't overlook is the surprising boom of new generative AI (GenAI) capabilities along with the raw accessibility for even the smallest of companies. Raw adoption numbers speak for themselves. While it took Uber 70 months to achieve 100 million users, and Instagam only 30 months, ChatGPT set a new bar of just 2 months (see **chart**).

This adoption includes industrial plants, with more than 80% of manufacturers anticipating evaluating GenAI in their operations in 2024 and expecting their technology investments to increase 30% year on year. While the threat of pilot purgatory looms, company leaders clearly worry more about threats to the status quo amidst this time of rapid change.

Foreseeing the Future

Predictive maintenance is one use case for AI/ML with transformative possibilities, but many manufacturers are finding it difficult to achieve, taking a Big Data approach to a problem that requires context from the process and effort to engineer unique algorithms. And companies can't afford to waste any more time in pilot purgatory or ignore the promise of predictive maintenance.

According to Reuters, manufacturing equipment in the United States is on average the oldest it's been in over half a century. Maintenance of this equipment remains a critical indicator of downtime and, in turn, productivity. Yet, maintenance resources are dwindling.

Studies have shown that regular scheduled maintenance could be shutting down your operations more often and longer than planned. Because variable-frequency drives (VFDs) often run the most critical processes in your operations, it's imperative they offer some type of predictive maintenance that monitors the health of the drive along with connected assets.

Detecting failures in time to schedule preventive maintenance and buy replacement parts saves countless hours and dollars. And given today's supply chain and cost constraints, maximizing uptime has gone from a priority to a survival tactic.

Staying Ahead of the Curve

For example. by using intelligent VFDs already on your plant floor, along with predefined ML models from vendors with expertise in mechanical systems, you can now achieve predictive maintenance insights about your equipment without wiring new sensors, investing in cloud storage or hiring data scientists. Most manufacturers have no idea how smart their VFD can be, missing one of the most data-rich sources for their production.

There are other ways to get ahead, including the following:

PRODUCT FOCUS: FACTORYTALK ANALYTICS GUARDIANAI

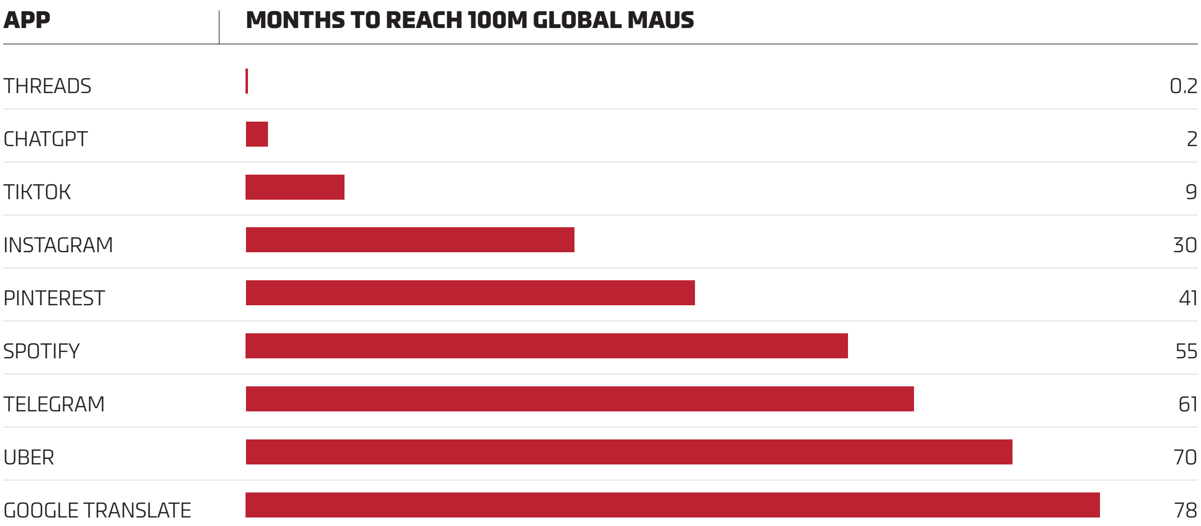
Optimize maintenance activities and reduce unplanned downtime with advanced notice of upcoming asset failures provided by FactoryTalk® Analytics™ GuardianAI™ from Rockwell Automation. Instead of wiring new sensors, this application uses electrical signal data from PowerFlex® 755, 755T-series and 6000T drives for condition-based monitoring.

Rockwell Automation has identified the most common failure modes for pumps, fans and blowers. These common failure modes are canned and built into the application, eliminating the need for data scientists or waiting to characterize real downtime events.

The application is installed in your plant and trained while you're running production so you're testing against known conditions. Learn more at rok.auto/ft-analytics-guardianai.

HOW LONG IT TOOK TOP APPS TO HIT 100M MONTHLY USERS

Threads is estimated to have hit 100M users on July 10, just days after its launch.
Here's how long it took other top apps to reach that:



It took Uber 70 months to achieve 100 million users, and Instagram only 30 months, ChatGPT set a new bar of just 2 months. More than 80% of manufacturers anticipate using GenAI in 2024 and expect their technology investments to increase 30% year on year.

SOURCE: USB/YAHOO FINANCE.

- **With a diverse team, identify the greatest opportunities for business outcomes in your operations.**
- **Develop your business case, success criteria and roadmap for scale.**
- **Recognize success in your immediate and extended teams.**
- **Share learnings, expand functionality, widen integrations and scale value across your operations.**

Manufacturers' biggest competitive weakness in the United States is a shrinking skilled workforce, and the top way leading companies are addressing the skills gap is by increasing automation and AI/ML. This technology presents a transformative opportunity to overcome these challenges and help improve productivity. It's now possible to:

- **Shorten the time to design, commission and operate new systems and equipment.**
- **Focus limited maintenance resources on assets most likely to fail and equip teams with insights into the most probably cause of failure.**
- **Perform root cause analyses in real-time (after eliminating outliers) without having to delve into heavy data engineering effort.**
- **Save engineers time by helping them generate code using natural language prompts, automating routine tasks, and improving design efficiency.**
- **Take otherwise hidden data and find insights to improve on quality, energy consumption and productivity.**
- **Empower the next generation of talent to triage and fix plantwide issues with natural language interfaces.**

Don't wait in fear of pilot purgatory. Lead your team to a place where you're regularly delivering innovative outcomes using game-changing technologies. Tomorrow's industry leaders — and today's preferred employers — aren't slowing down.

APARIAN INC.

Graham Proctor

PRESIDENT

The Role of IO Scanners Supporting Migration to a Modern DCS

For insights about using IO scanners as part of migrating from legacy systems to a modern distributed control system (DCS) using ControlLogix®, *The Journal From Rockwell Automation and Our PartnerNetwork*'s Executive Editor Theresa Houck talked with Graham Proctor, Owner and President of Aparian Inc., a Rockwell Automation Technology Partner.

Theresa: What are the pros and cons of performing a DCS migration to a modern control system?

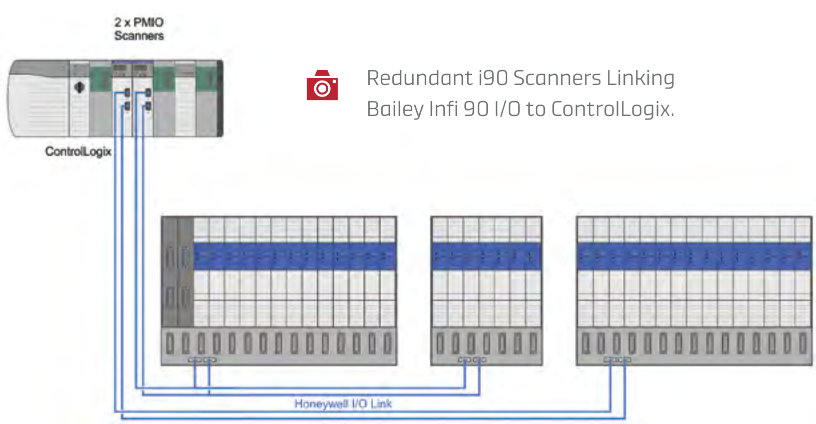
Graham: The pros include improved supportability and maintainability, reduce operational costs, increase operational safety and security, increased productivity and efficiency with faster process control, improved system connectivity and integration, and accessibility to that very important data that the system generates.

On the other hand, there's the capital investment, the disruption to operations caused by the replacement process and operator retraining. The biggest risk lies with the unknowns about how long the project is going to take.

In process plants, the investment in instrumentation is usually much higher than the investment in the actual control system. Strategies for connecting the existing instrumentation to a new control system are being investigated. These include I/O scanners that use the existing IO cards, wiring and instrumentation, or cable interfaces that connect the existing cables to a new IO card.

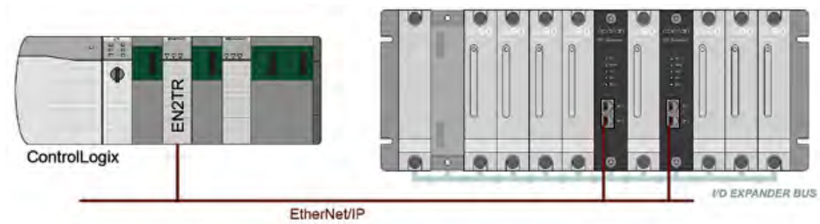
Theresa: What are the benefits of using I/O scanners in DCS Migrations?

Graham: The biggest benefit is a low-risk phased migration path that supports a **go back** option, which enables the control to be returned to the DCS without wiring changes. A phased migration also lets users progress at a speed their budgets and other resources allow. It also supports operational continuity by allowing time for training operators and maintenance personnel and for rewriting



Redundant i90 Scanners Linking Bailey Infi 90 I/O to ControlLogix.

Redundant PMIO Scanners Linking Honeywell TDC 3000 I/O to ControlLogix.



procedures, and reduces the stress on personnel.

A secondary benefit is wiring between instrumentation and I/O cards and the I/O cards themselves are kept in place. That means lower initial costs, and more importantly, lower risk due to human error in the rewiring phase. Downtime for a **rip-and-replace** approach can have significant cost implications.

Another benefit can be observing the live I/O values while the existing DCS control is still running. Documentation of the original DCSs are sometimes lost to history and these systems operate as black boxes. Getting to peek inside is immensely valuable. Access to live data also provides the ability to conduct incremental testing to be sure each phase is validated before continuing.

Theresa: Walk me through the steps of a phased migration using I/O scanners.

Graham: In Stage 1, the first step is adding an I/O scanner to the existing DCS. This can be done in minutes. The I/O scanner is connected to a modern Allen-Bradley® ControlLogix controller and operated in Shadow mode, where control is left with the DCS controller, and I/O values are read-only. This data can be fed to a MES systems for analysis and historization. This might be all a customer needs for now.

Going further, the data can be analyzed and used to develop control strategies for the new control system. HMI screens can be developed, operator training started and procedures written.

Then in Stage 2, control can be moved over to the new system. This can be done by rack, by area or all at once. The DCS controller cards are removed from the rack and the I/O scanners are switched over to Run mode. This is the most critical phase, because the new system still might not function as expected. But if more time is needed to fix unforeseen problems, the system can be quickly and easily switched back to Shadow mode and the DCS controllers reinstalled.

In subsequent stages, the continuing migration would include replacing IO cards and instrument wiring. However, the timing for these events is up to the customer and may be done over a period of months or years, as required.

Theresa: Which DCSs are supported?

Graham: Aparian has three solutions that support these Shadow/Run modes for Rockwell Automation products. These include:

TABLE 1

DCS	Catalog	Name	Mount
Honeywell TDC 3000 PMIO	1756-A-PMIO	PMIO Scanner	In Rack
ABB Bailey Infi 90	A-i90S	i90 Scanner	In Bailey Rack
Emerson Delta V M-Series	A-DVS	DV Scanner	Din Rail Mount

Aparian also has solutions for the Hitachi and GEMLan-D's DecNet and HDLC STARNET networks. However, these don't support shadow mode directly.

Theresa: What about support for redundancy?

Graham: The PMIO supports media redundancy with A and B IO Link cables, while the Delta V and i90 scanners support device level ring (DLR). The IO scanners also support module redundancy that can be used in a redundant ControlLogix architecture. ●

APARIAN INC. Technology Partner Aparian Inc. develops, distributes and supports automation and control solutions that complement, integrate and operate with Rockwell Automation products and solutions. This includes communication and fieldbus gateways, standalone as well as ControlLogix and CompactLogix™ module development, and multiple products for migrating legacy DCS IO to Logix. Learn more at https://tinyurl.com/4a278pva.

How OEMs Drive Cybersecurity in Smart Vehicles

As the automotive industry speeds toward the dream of software-defined vehicles, IT systems are becoming more embedded in the driving experience — opening new attack routes for hackers.

Financial services firm and researcher Evalueserve claims connected cars could exchange up to 4 terabytes of data per day, or the equivalent of around 8 million digital photos. The need to secure this massive data flux is creating an entirely new branch of cybersecurity devoted to the automotive sector.

It's a branch concerned not only with securing data while a connected car is in use, but also across the automotive life cycle, from manufacturing to aftersales.

Automotive industry cybersecurity is evolving rapidly, because OEMs have not traditionally faced IT security threats in the manufacturing or use of their products. Nor has the industry been a major target for hackers, beyond the malware threats faced by all enterprise operations.

The arrival of software-defined vehicles means the auto industry now needs to get ahead of data encryption, IT platform security and the use of AI and other tools for the enhanced identification of vulnerabilities.

Yet, as things stand, "Vehicle-to-everything and vehicle-to-grid communication security development is reactive, as most technology is still pilot phase and requires strong hardware and software integration," said an executive interviewed by Evalueserve.

Factory Cybersecurity

OEM manufacturing does boast several cybersecurity strengths. For example, the industry is already encrypting communications within internal components and

LISTEN TO THE PODCAST

What's Really Happening with Industrial Cybersecurity & What You Can Learn

Manufacturing is now the #1 target for hackers. In this episode of our "Automation Chat" podcast from *The Journal From Rockwell Automation and Our PartnerNetwork* magazine, "What's Really Happening with Industrial Cybersecurity & What You Can Learn," Executive Editor Theresa Houck chats with Fortinet's Richard Springer about a study on unprecedented cybersecurity risks. Learn key takeaways, cybersecurity trends, the role of IT/OT collaboration, and more.

Listen on your podcast app or on the web at **https://tinyurl.com/3szd37et**, or watch their conversation on YouTube at **https://youtu.be/esFAKPAbCSY**.

★★★★

Named Best Podcast 2 Consecutive Years!
2022 & 2023 Apex Awards of Publication Excellence.

uses an architecture design based on isolated zones that minimizes the risk of malware transmission in vehicles.

Similarly, devices that the car might connect to, including cellphones, already use secure technologies such as elliptic curve cryptography. And manufacturers rely on secure cloud providers for data storage and over-the-air software updates.

However, as vehicles add more data entry points, concern is growing about the vulnerability of an expanding attack surface. The industry collaborations required for software-defined vehicle development, often involving small or start-up companies, could also create openings for hackers.

Software-defined vehicles will interact with a growing number of IT systems, any one of which could be compromised by a determined threat actor. It's uncertain whether the legacy systems currently being integrated into connected cars have all the security they might need.

The need to shore up industry defenses is being addressed by an array of cybersecurity providers, operational technology (OT) security specialists and Tier 1 suppliers. These providers are helping introduce cybersecurity best practices such as standardization, code signing, penetration testing, controlled access and monitoring, tamper-evident hardware seals and secure software development life cycles.

In response to security concerns, some OEMs are using virtual security operation centers to aggregate, correlate, analyze and report on vehicle threat data to mitigate risks and manage vulnerabilities.

These centers are usually run by OEMs, for data privacy purposes, but developed by third parties.

Across all fronts, OEMs are seeking to beef up their cybersecurity capabilities, usually in partnership with specialist firms. Only about 5% of current cybersecurity initiatives are developed in house, although this could rise to 20% in the next 10 years as automakers gain experience.

Secure Strategies

Emerging automotive cybersecurity strategies focus on providing several layers of security. One major OEM has built its own vehicle operating system and uses secure wireless local area networks (LANs) to safeguard vehicle-to-infrastructure communication.

The company has also invested in a risk analysis and penetration testing start-up and collaborates with third-party experts on areas such as the provision of a virtual security operation center, training institutions for cybersecurity skills and industry associations for guidance on best practices.

Another global manufacturer has created a dedicated cybersecurity unit and launched a bug bounty program to track down vulnerabilities. It has also invested $4 million to improve its architecture, design principles and threat-analysis risk assessments.

Auto industry players work alongside a range of IT security bodies, including the Automotive Information Sharing and Analysis Center, the U.S. National Highway Transportation Safety Agency (NHTSA), Alliance for Automotive Innovation and the National Institute of Standards and Technology (NIST).

They can also leverage the knowledge and technologies developed for traditional cybersecurity, such as using microservices architectures, to minimize potential attack surfaces and strengthen defenses with secure boot processes and hardware-based security modules.

Some companies are even exploring post-quantum cryptography technologies, in anticipation of traditional bit-based encryption being rendered obsolete by quantum computing.

Evolving Regulations

Standards and industry bodies offer the automotive sector a range of best-practice frameworks, from the International Organization for Standardization's ISO/SAE 21434:2021 road vehicles — cybersecurity engineering standard to Europe's UN Regulation No 156 provisions for software updates.

The ISO/SAE 21434 framework is important because it sets requirements for automotive cybersecurity processes and a common language for communicating and managing risks. One part of the framework concerns the structure, processes and governance for automotive cybersecurity management systems. Another offers guidelines on how to make sure vehicle architecture designs, risk assessment procedures and cybersecurity controls are executed correctly. These cover factory and in-vehicle cybersecurity.

A third concern is how to secure charging infrastructure. Most of this depends on the adoption of best practices such as security by design and blockchain-based data exchanges.

Organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the International Electrotechnical Commission (IEC) are developing cybersecurity standards for emerging vehicle-to-grid and smart-grid implementations.

One challenge is that regulations and best practices vary widely from one region to another. For example, automotive OEMs in Europe all need to comply with laws such as UN Regulation 165, while U.S. OEMs rely much heavier on industrial development more than regulatory limitations.

For more on how the auto industry is driving the evolution of smart cars, download the white paper from Rockwell Automation at rok.auto/EVTrends. ●


could AI help you achieve sustainability goals?
EASTERN MUNICIPAL WATER DISTRICT
IS USING AI-ENABLED CONTROL TO SAVE
2,330 KWH OF ELECTRICITY EVERY DAY
See their story
Rockwell Automation

"Digital data flows to realize step-function improvements."

If we do not grow and change, we will not succeed. Over the past decade, the automotive industry has been at the bleeding edge of developing digital thread capabilities; in a technological arms race to create the leanest, most resilient business possible.

In this race, success means expansion into new markets and a profitable outlook. Failure means being relegated to a case study in future business courses.

ARTICLE BY

Michael Glessner

DIRECTOR, KALYPSO: A ROCKWELL AUTOMATION BUSINESS

Aleksandar Boskovic

PRINCIPAL, KALYPSO: A ROCKWELL AUTOMATION BUSINESS

Close Digital Gaps in the Automotive Industry

Connecting smart technologies into a digital thread provides an uninterrupted flow of information and helps create a faster, more resilient business.

Challenges Facing the Automotive Industry

The global automotive industry is facing increasing challenges, including:

- Recent labor agreements that place a premium on people within manufacturing.
- Generational change leading to sea soned personnel aging out of the workforce to be replaced by less experienced, but more technology savvy workers.
- Governments and regulatory bodies increasing the quantity and complexity of safety, quality and environmental regulatory requirements.
- The pace of innovation needed to keep up, increasing substantially from what was a stable industry.
- The shift towards electric vehicles and hybrids from internal combustion engines.

On top of this, we're seeing significant turmoil globally in the automotive supply chain:

- Management focus on more comprehensive automation of activities that are traditionally difficult to automate.
- Unprecedented supply chain disruptions slowly dissipating.
- Demand uncertainty, driven by economical and political factors as well changes to ownership models and a rise in the sharing economy.

In the automotive industry, while there is great need for digital transformation, there is also great opportunity — because in most cases, foundational technologies and data already are in place. While companies often use these technologies independently of each other, there's value to be gained by connecting them as digital threads within their business. This flow and reuse of data, including analytics, is unlocking value for adopters.

Closing the Gaps

It's hard to define what digital is until you understand how we got to where we are today. Digital technologies, such as computer-aided design (CAD), enterprise resource planning (ERP) and programmable logic controllers (PLCs), have existed for decades in the automotive industry and have contributed to improved operational and financial performance.

As what's possible continues to advance and the candidates for digitization grow, connecting these individual point solutions has become just as important. Users of digital enterprises are realizing the value from the flow of data across such solutions.

The industrial digital thread comprises several interconnected threads, each forming a seamless flow of data that weaves together business processes, systems, products and equipment across the value chain.

This increased connectivity stretches from ideation to product development, through manufacturing, supply chain and service, and closes the loop by integrating feedback from later design stages, operations and customers with products in the field.

Each stage can reuse data from earlier stages, improving operations and efficiencies — so that the virtual improves the physical.

Our model focuses on the importance of closing digital gaps for a complete, uninterrupted flow of information from product design, through to manufacturing and distribution. Linking compatible product lifecycle management (PLM), enterprise resource planning (ERP) and manufacturing execution systems (MESs) into one single thread of information allows for compounding gains on investment, with each successive investment making each capability more powerful. Businesses can be more cost-effective and operate with lower costs, but the true differentiator here is speed.

It's important to be aware of current trends, but it's just as important to be prepared for the unexpected. Electrification has been a paradigm shift, and both drivetrain and battery development have accelerated. This has not only changed the product consumers expect, but also the flexibility manufacturers demand from their process and equipment.

Add to this global supply chain uncertainties and the value of strong change management and the ability to design, develop and order replacement parts rapidly becomes clear.

A complete digital thread can support accelerated rates of change to product and process to get a step ahead of competitors while also supporting operations to decrease error rates or wastage.

Ready for the Unexpected

Enabling the digital thread can make automotive manufacturers and suppliers more agile than their competitors. Unexpected global events that were once great risks to a business' outlook can become their greatest opportunity. The speed at which planning, design and execution decisions can be made increases exponentially, making change your greatest friend and giving you a head start over competitors.

Organizations need a partner that has the tools and know-how to identify and implement a digital thread strategy that goes beyond a patchwork of improvements and uses complementary solutions to produce a coherent, complete digital thread across the whole value chain.

It's important to close digital gaps and build a complete thread. The challenge is identifying how to balance immediate benefits with a long-term approach to closing digital gaps that leaves your business in a position to lead the pack five years from now. ●

READ THE ARTICLE

How to Get the Most Out of Your Predictive Maintenance Data

For many manufacturers and producers. maintenance is still predominantly a reactive endeavor. As simple predictive solutions become more commonplace, however, leading enterprises are looking beyond predictive capabilities to prescriptive insights to advise maintenance functions on what assets and tasks to prioritize.

In this article by Kalypso: A Rockwell Automation business, learn how assessing the criticality and feasibility of predictive maintenance use cases can help you to further prioritize assets and tasks that create the most value.

Find out how they're using advanced analytics and predictive maintenance. Predictive maintenance (PdM) uses statistical, machine learning (ML) and artificial intelligence (AI) techniques to predict asset health issues before they arise.

Visit **https://tinyurl.com/yspfw56h** to read the article.

KALYPSO A Rockwell Automation business, helps companies bring digital solutions to product problems. Whether it's weaving a digital thread from product ideation all the way through manufacturing and service, or advancing operations from automation to autonomy, Kalypso specializes in improving what's being made and how it's made. Kalypso serves the largest names in the discrete, hybrid and process industries, around the world.

Why OT Cybersecurity is a Vital Business Strategy

Recognizing OT system vulnerabilities, focusing on outcomes and using robust cybersecurity measures can help manufacturers protect operations.

ARTICLE BY

Dave Kang

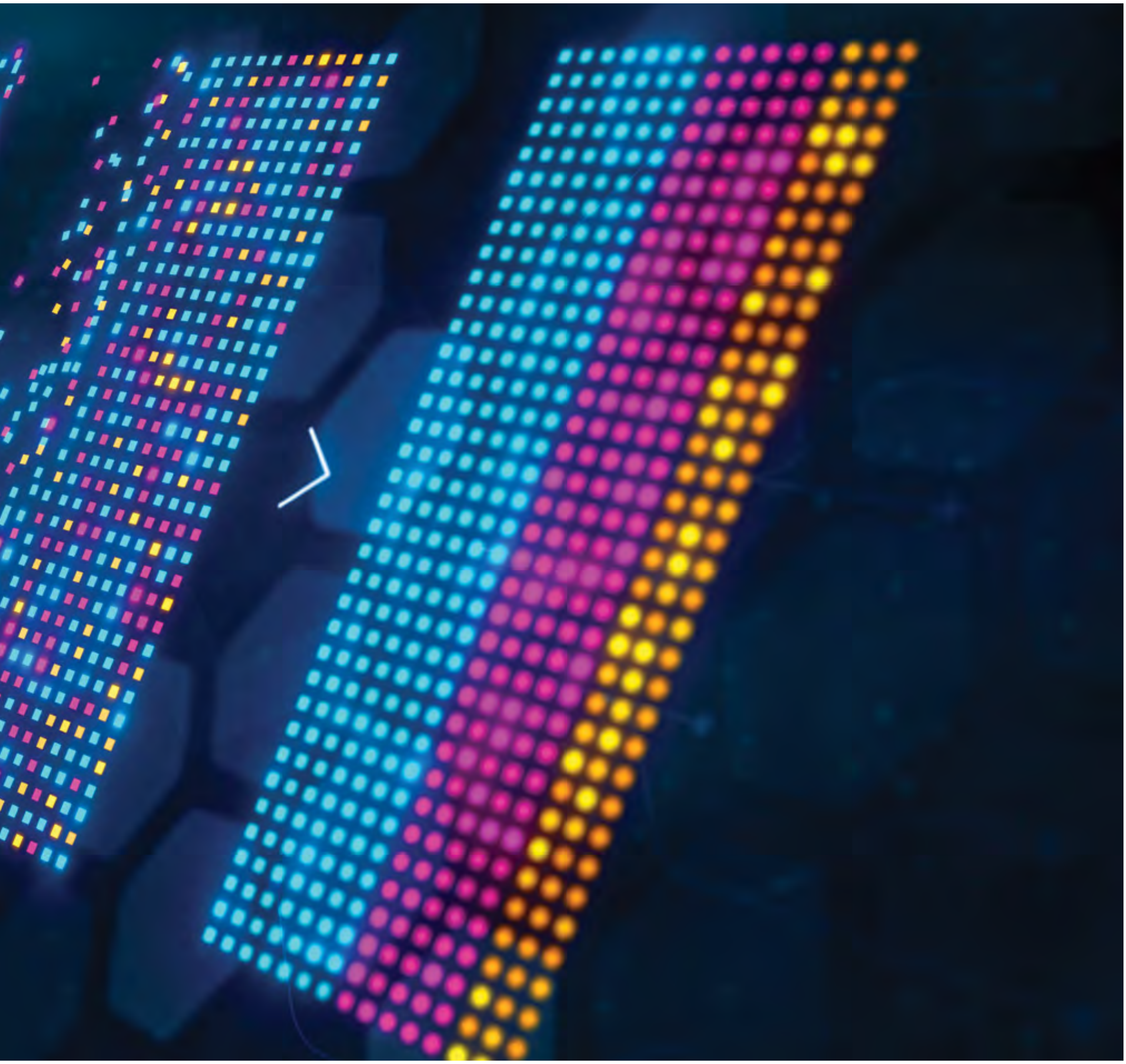
ADVISORY SOLUTIONS ARCHITECT, DRAGOS

Kamil Karmali

SENIOR GLOBAL COMMERCIAL MANAGER, CYBERSECURITY SERVICES, ROCKWELL AUTOMATION

Recognizing the unique requirements of operational technology (OT) environments is the first step in securing them. These systems demand a specialized, OT-specific approach to cybersecurity. This approach must:

- Understand the systems.
- Analyze and log the commands for threat behaviors or to spot misconfigurations.
- Consider the need for minimal disruption.
- Prioritize workforce and equipment safety.



Understanding Operational Risks in Manufacturing

Cybercriminals are constantly devising new methods to exploit vulnerabilities in OT systems. These adversaries range from money-motivated ransomware gangs to sophisticated criminal organizations and state-sponsored actors, all with the capability to disrupt manufacturing operations on a massive scale.

The truly alarming aspect lies in the potential for advanced tools, developed by sophisticated nation states, to fall into the hands of less sophisticated adversaries. These adversaries, driven by financial motives, are willing to target any type of organization.

The operational risks also extend to the supply chain, where a single vulnerability can have cascading effects across multiple manufacturers. Key software components can be a part of hundreds of different systems, affecting hundreds of thousands of devices, like PIPEDREAM, the seventh known industrial control systems (ICS)-specific malware developed by the CHERNOVITE threat group.

The interconnectivity of suppliers, vendors and partners means that securing the manufacturing process is no longer just about protecting your own operations, but ensuring the integrity of the entire value chain.

According to the recently released Dragos "OT Cybersecurity

According to the recently released Dragos OT Cybersecurity Year in Review, ransomware attacks escalated by nearly 50% in 2023, with the manufacturing sector being the primary target.

Year in Review" (https://tinyurl.com/2s3sm7ny), ransomware attacks escalated by nearly 50% in 2023, with the manufacturing sector being the primary target. High-profile ransomware attacks on major companies like Dole, Boeing and Clorox resulted in the shutdown of facilities and substantial financial losses.

Lockbit ransomware alone accounted for 25% of all industrial ransomware attacks, with ALPHV and BlackBasta each contributing 9% of the total.

A pivotal insight from the report: *about 70% of OT-related cyber incidents originated from the IT environment*, indicating the need for robust network segmentation and separate domains for IT and OT systems.

Need for a Cultural Shift

The crux of the challenge lies not just in the technology, but in the mindsets of teams operating and managing OT systems. For decades, the primary focus of manufacturing has been on efficiency and productivity, with cybersecurity often taking a backseat. This must change. Industry must foster a culture where cybersecurity is as fundamental as safety and quality.

Embracing OT cybersecurity requires a cultural shift within the organization, where everyone from the shop floor to the boardroom understands the significance of cybersecurity and their role in upholding it. This shift entails a move away from reactive measures toward a proactive approach that can also be used to increase operational equipment efficiency (OEE) and resilience.

A robust OT cybersecurity program encompasses the entire manufacturing process, with a focus on protecting the most vital assets. Although comprehensive frameworks like NIST and ISA/IEC 62443 exist to guide the development of a thorough plan, their complexity can sometimes hinder prompt action. Drago's recommendation is to start with the implementation of the SANS 5 Critical Controls for ICS, which include:

1. **OT-Specific Incident Response Plan.**
2. **Defensible Architecture.**
3. **ICS Network Visibility and Monitoring.**
4. **Secure Remote Access.**
5. **Risk-Based Vulnerability Management.**

Begin by putting these controls into practice, ensuring they're fully operational and can efficiently handle key scenarios.

As your program evolves, establish a risk management framework. This will allow you to fine-tune your investments and enhance risk mitigation efforts.

How Cyber Controls Affect Efficiency

Implementing the right cyber controls can lead to substantial improvements in operational efficiency and uptime. In production environments, the question of "What happened and why?" is frequently posed. While some answers may be straightforward, identifying the root cause of problems often proves challenging.

Controls that enable the identification of new devices, monitor third-party remote access, and log OT system commands offer a valuable data set. This data can be analyzed to understand events leading up to and following issues, enhancing OT network visibility and monitoring.

Preventing Production Shutdowns and Managing Risks. The question arises: Can we prevent a shutdown of production, or if necessary, how can we execute an orderly shutdown? Implementing risk-based vulnerability management offers alternatives to IT-driven device patches that could halt production lines. In the event of an incident, a robust OT-specific incident response plan, which considers critical processes and safety systems, is essential.

Safeguarding Critical Processes and Assets. Protecting critical processes and assets from Internet of Things (IoT) devices, transient network traffic or third-party remote access is paramount. This involves creating defensible architectures that segment equipment types and networks. Such strategies lead to more resilient operating environments and minimize disruptions.

Maintaining Vigilance in Manufacturing Environments. Staying vigilant and continuously searching for potential problems within manufacturing settings is essential for maintaining operational integrity and safety. This proactive approach helps in early detection and resolution of issues.

Cultivating cyber hygiene and awareness not only strengthens security but also enhances the overall efficiency and reliability of manufacturing operations.

READ THE INDUSTRY PERSPECTIVE

Q&A: Understanding the OT Threat Landscape Helps Manufacturers Improve Cybersecurity

The sophistication and frequency of cyberattacks on manufacturers keep increasing, making readiness and incident-response capabilities vital.

To help you understand the OT threat landscape and how to improve cybersecurity, *The Journal From Rockwell Automation and Our PartnerNetwork*'s Executive Editor Theresa Houck spoke with two experts on the subject: Kamil Karmali at Rockwell Automation and Dave Kang at Dragos.

Read the interview. **https://tinyurl.com/tj724drg**

Role of Leadership in Driving Outcomes

Leadership plays a pivotal role in driving change and instilling a culture that takes cybersecurity seriously. It's imperative for leaders to lead by example, demonstrating the importance of cybersecurity through clear communication, investing in effective tools and training and advocating for continuous improvement. These elements are crucial in fostering a culture that prioritizes OT cybersecurity.

Creating an OT cybersecurity plan is a strategic process that involves multiple stakeholders and detailed planning. The plan should clearly outline the goals, responsibilities, and procedures that will guide the organization's cybersecurity efforts. A few best practices include:

- **Set clear objectives.** What are the most critical assets that need protection? What are the potential threats? What compliance requirements must be met? Answering these questions will help to establish a framework for the cybersecurity strategy.
- **Build in flexibility so you can adapt quickly.** As manufacturing operations evolve and new threats emerge, the plan must be flexible enough to accommodate these changes and allow for adjustments that fortify security measures over time. Adopting an outcome-focused mindset rather than a tactic-centric approach ensures that the organization remains resilient against emerging threats, with a clear focus on achieving desired security outcomes.
- **Engage all stakeholders.** By incorporating diverse perspectives and expertise, you can enrich the cybersecurity plan and foster a culture of shared responsibility and vigilance.

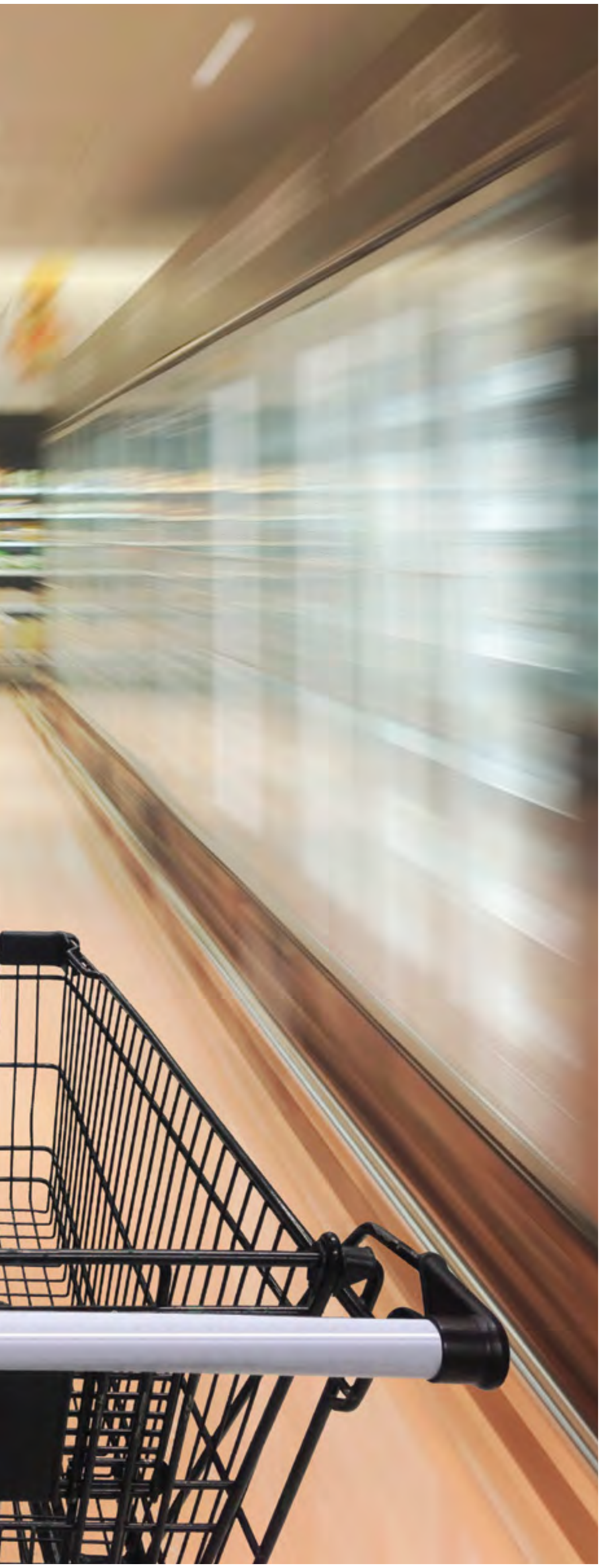
Next Steps

OT cybersecurity is a business imperative, not just IT. It addresses vulnerabilities, fosters a security culture, deploys strong controls, safeguards operations, enables innovation, and creates a competitive edge. Focus on outcomes, leverage advanced monitoring and partner with OT security experts to confront future threats.

DRAGOS Rockwell Automation Technology Partner Dragos provides ICS/OT cybersecurity solutions for thousands of industrial organizations. In addition to technology and service offerings, Dragos offers threat intelligence to provide organizations with in-depth visibility of threats targeting industrial environments globally and the defensive recommendations to combat them. Learn more at www.dragos.com.

Case Study: Packaging Robotics with Open Mechanics

See how unified control for its robotics helped a consumer packaged goods firm achieve an autonomous system capable of performing complex tasks.



ARTICLE BY

autonox Robotics

To become more competitive, industrial firms often begin by integrating automation and corresponding solutions into their existing production. Robots have proven highly efficient in this regard. However, due to the closed platforms used by robot manufacturers, different systems must collaborate within production environments, leading to interface problems by increasing the number of control systems in use. This complicates operations and can result in data loss.

Open mechanics eliminate interfaces and additional controls. With these solutions using unified control, the operator receives a highly integrated and autonomous system capable of performing complex tasks.

Many production areas need to address employee shortages, increase efficiency and maximize flexibility. The following case describes these challenges in packaging for consumer packaged goods, a process that often creates bottlenecks slowing down production throughput.

Consumer Packaged Goods Sorting

In this use case, the machine is used for sorting different goods onto several conveyors with a cycle time of about 1 second per cycle. Requirements include efficiency, speed and precision. Consumers demand high-quality products at acceptable prices, putting pressure on manufacturers to streamline their production and eliminate causes of quality or downtime issues.

An additional requirement is handling consumer goods on moving conveyors, using multi-parallel kinematics with different technical specifications based on varying requirements.

First, it's necessary to have direct contact with the products by sorting them for the first packaging machine. Based on cleaning requirements, kinematics with wipe-down (HND) and wash-down (HHD) options are available.

In this case, two wash-down autonox DELTA kinematics — HHD DELTA RL4-1200-3 kg — are positioning them on an additional conveyor feeding the packaging machine (see **Figure 1**). The mechanics are made of materials approved for the food industry. Coatings of any kind are generally avoided. They can be cleaned with the usual methods of the food industry. Food-grade, also FDA-compliant lubricants are used.

In the design of the mechanics, the external use of hexagon socket screws, springs, tight radii and gaps is avoided as much as possible. The upper arm gearboxes, joint and telescope bearings are (double) sealed.

After the products are packaged, they're case packed into cardboard boxes using a standard autonox DELTA kinematic — DELTA RL4-T1-1200-3 kg (see **Figure 2**). The additional T-shaft offers the possibility of mechanical tool actuation with additional torque available on the tool holder used to open and close a gripper.

Figure 1. In this case study, the machine is used for sorting different goods onto several conveyors. Two wash-down autonox DELTA kinematics are positioning them on an additional conveyor feeding the packaging machine. In the design of the mechanics, the external use of hexagon socket screws, springs, tight radii and gaps is avoided as much as possible. The upper arm gearboxes, joint and telescope bearings are (double) sealed.

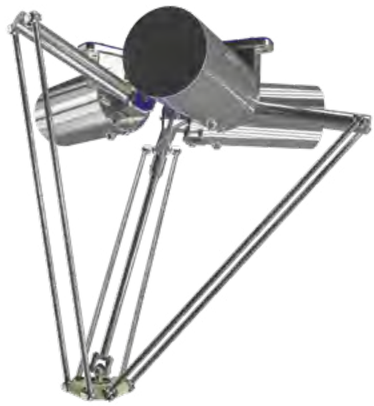


Figure 2. After the products are packaged, they're case packed into cardboard boxes using a standard autonox DELTA kinematic, DELTA RL4-T1-1200-3 kg. The additional T-shaft offers the possibility of mechanical tool actuation with additional torque available on the tool holder used to open and close a gripper.

Design Software and Servo Motors

The system uses unified robot control to eliminate the need for independent robot controllers and a dedicated programming platform, and instead uses a Logix controller and the Rockwell Automation Studio 5000® automation system design software for complete system control. Further value was added by using Allen-Bradley® Kinetix® servo motors and servo drives to maximize the performance and energy efficiency of the robot mechanics.

This optimized control architecture simplified system control, enabled new efficiencies in the design process and accelerated time-to-value for the project.

Robots were programmed using robot libraries embedded in the Studio 5000 environment, and the solution was validated within Rockwell Automation Emulate3D™ software to virtually commission the system in a digital environment before committing to the physical build stage of the project.

Multiple robot kinematics and two different packaging stages (primary and secondary packaging) are controlled using one drive family (for conveyor, robots and process devices) and one control system PLC as one machine. This makes the robots organic to the machine design in every way.

PRODUCT FOCUS

autonox Lean Line Mechanics

In addition to the autonox DELTA classic line from autonox Robotics, autonox Lean Line mechanics models are soon available for up to 6-kg payload. For direct integration into the machine structure, this design is also available without a head plate. The direct connection of the gearbox support to the machine frame reduces the overall height. HND Design is possible.

Lean Line mechanics require additional maintenance compared to autonox standard DELTA mechanical designs and do not have the same high range of performance options available, but they do offer a good price point with a reliable design for cost-sensitive applications.

A new feature for our Lean Line is the use of the telescopic shaft for Tool Actuation "T Shaft." The telescopic shaft can also be used to actuate the end effector (e.g. opening/closing a product gripper). There are internal threads for mounting the end effector on the tool holder. This is useful because no media (hoses, cables, etc.) need to be routed to the end effector. The actuator, which is usually heavy, is located above the robot (on the head plate).

Learn more at **https://tinyurl.com/mvx6c5rh**.

The advantages include having the same drive families throughout the machine — conveyor, robot, etc. The OEM can focus on the solution without worrying about learning and supporting different control systems for the robot and the machine.

This results in one production data system in the control system on one network, providing the customer with these benefits:

- **Better synchronization of robots and surrounding devices, such as independent cart technology, because they're all motion axis under one controller.**
- **One operating environment and programming system for complete system control, including integrated safety.**
- **Maintenance service time and stock are reduced due to using the same parts (motors and drives) for all moving parts, including the robots.**

AUTONOX ROBOTICS Autonox Robotics, based in Willstätt, Baden-Wuerttemberg, Germany with offices in Suwanee, Georgia, United States, is a Technology Partner in the Rockwell Automation PartnerNetwork™ program. The company specializes in developing and producing control-independent robot mechanics, that can be connected to any automation platform. Its customers are mechanical engineering companies and robot integrators interested in an end-to-end control platform. Its product line consists of more than 300 different mechanics.

HARDY PROCESS SOLUTIONS

New Weigh Controllers with Dual-Core Processor

The HI6800 and HI6850 combine direct process control with fast, accurate and stable weight data essential to manufacturing operations. Preprogrammed application packs simplify setup and commissioning or use customized controller programming. Optional configurations include digital and analog I/O, DC relays, mapping and up to 4 channels of scale inputs per instrument. The latest dual-core processors support advanced weighing applications.

www.hardysolutions.com/hi6850

POSITAL - FRABA

Meet POSITAL's IXARC Encoders with IO-Link Connectivity

POSITAL's IXARC family of encoders are available with IO-Link communication interfaces. This low-cost, easy-to-implement communication system can simplify your control system network while retaining full functionality, including absolute outputs and programmability. With thousands of mechanical configurations available, you can select devices that are exactly right for your system.

https://tinyurl.com/2w7vkxup

ADVANCED MICRO CONTROLS INC.

NXAE2 Mini-Nexus Resolver Interface

The NXAE2 Mini-Nexus from AMCI is a flexible plug and play resolver interface designed to seamlessly integrate with the Rockwell Automation CompactLogix® 5380 controller and 5069 platform. Learn more at www.amci.com/plc-automation-products/e2-mini-nexus-resolver-interface/

https://tinyurl.com/539ckr65

Hygienic Stainless Steel GFCI

Technology Partner **Littelfuse Inc.** offers the hygienic stainless steel Shock Block SB5000 designed to reduce unnecessary tripping and potential shock by following an inverse trip time and using DFT filtering. This model features a hygienic stainless steel enclosure with a NEMA 4X and IP69K for food preparation environments.

The unit is available in 32 and 60 A models for GFCI, special-purpose ground-fault circuit interrupter, or equipment ground-fault protective device applications. It meets the USDA Sanitation & Food Code for metallic enclosures on the plant floor.

It features AIS 304 stainless steel, a 10° sloped top, FDA-compliant blue silicone gasket, and accessories for off-wall or flush mounting.

Industrial Computers and Monitors

The **ASEM™ 6300 industrial PCs** from Rockwell Automation are available in box and panel form and are designed for greater customization. The devices work with FactoryTalk™ Optix software for seamless deployment to HMI solutions.

The units are based on the seventh-generation Core i3, i5 and i7 Intel Kaby Lake H and Intel Celeron Skylake processors to handle complex industrial applications. Touch screen technologies enhance ease of use. Various display sizes and standard or low-profile bezel units feature resolutions up to full high definition.

The industrial PCs are one of the solutions in the new FactoryTalk Optix portfolio that allows users to choose their own technology mix of both Rockwell Automation and third-party controllers.

PRODUCT SPOTLIGHT

MEDIUM VOLTAGE VARIABLE-FREQUENCY DRIVE

The **PowerFlex® 6000T medium-voltage VFD** from Rockwell Automation now supports permanent magnet (PM) motor applications for energy efficiency and sustainability goals. The VFD handles high-speed applications up to 120 Hz output frequency, from 11 kV up to 680A.

Expanded predictive maintenance capabilities using TotalFORCE® technology communicate real-time component health data to help reduce downtime. It provides predictive maintenance alerts for fans, transformers, airflow, motor and machine bearings, and lubrication. The drive also displays runtime alerts for critical components.

The secondary precharge support is now housed within the existing footprint, reducing costs and floor space. The drive offers more configuration options, including ENETR for EtherNet/IP™, plus 13TCOMMP1 for PROFIBUS®, encoder cards and I/O modules. Integrated CIP Security™ helps protect against cyber threats.

The VFD is engineered for new and retrofit variable torque, constant torque and high-speed motor applications.

Expanded On-Machine Portfolio

Rockwell Automation has expanded its **On-Machine™ solutions** that permit decentralized control architectures where components are field-mounted rather than kept in large electrical enclosures.

This approach offers more simplified, modular machines that can have lower total costs, reduced footprint and less time to operation. With components easily accessible, factory personnel can proactively identify and address problems and increase system uptime.

The expanded range of On-Machine solutions include ArmorKinetix distributed servo drives, ArmorBlock 5000® I/O blocks, Armor™ PowerFlex® drives, and ASEM™ 6300PA On-Machine industrial pcs.

Production Scheduling Software

Rockwell Automation introduces **Finite Scheduler,** an update to its software portfolio to help customers modernize production scheduling with reliable and responsive finite capacity capabilities. Using data from the manufacturing process, Finite Scheduler was built to improve scheduling accuracy, increase throughput and drive on-time delivery.

The system goes beyond MRP systems and considers additional factors that influence manufacturers' production operations. It is designed to keep up with frequent changes and provide more accurate data than manual compilations.

PRODUCT SPOTLIGHT

PLC-TO-EDGE CONNECTOR

Technology Partner **Softing** introduces edgeConnector for the integration of Allen-Bradley® PLCs, providing convenient access to data from ControlLogix® and CompactLogix® controllers.

The data from the controllers is made available on edge devices or virtual environments via OPC UA and MQTT. This facilitates flexible integration into on-premises or cloud environments without modifying the existing PLC configuration.

It is easy to configure locally via an integrated web interface. Alternatively, remote global mass configurations are possible via REST API.

The connector operates on standard hardware and can be managed centrally. The integrated MQTT publisher/subscriber functionality allows the flexible setup of IIoT solutions. Security standards include SSL/TLS, X.509 certificates, authentication and data encryption. This gives users a secure way to integrate data from production into IIoT solutions.

Threat Detection Services

Rockwell Automation and Technology Partner **Dragos** have collaborated on a Threat Detection Service offering that features the Dragos platform. It provides a comprehensive cybersecurity service for companies looking to secure their OT environments and mitigate risk.

The platform provides on-premises and cloud options, continuous updates, asset visibility and prioritized vulnerability management. Combining industrial cybersecurity services with a scalable, customizable platform from Dragos is designed to help enterprises of any size detect threats before a significant compromise occurs.

Brush Strips for Cable Management

The Brush Entry System (BES) brush strips from Technology Partner **icotek** are a practical solution for organizing network cables in 10-in. and 19-in. switch cabinets from various manufacturers. Integrated spring locks provide tool-less assembly and disassembly. To install or remove the brush strips, simply release the spring locks on both sides.

The brush strips allow cables to be routed easily and obscure the view of the cables inside the switch cabinet for a more organized appearance. They also protect against the ingress of dust and dirt while facilitating air circulation.

They are made of powder-coated steel with polyamide brushes and are suitable for a temperature range from -30°C to 80°C.

PRODUCT SPOTLIGHT

CENTRALIZED MOTOR CONTROL SOLUTIONS

The **FLEXLINE™ 3500 low voltage motor control center** (MCC) from Rockwell Automation is designed to unlock production data and increase uptime and productivity. By integrating with smart motor control devices, the MCC delivers real-time operation and diagnostic data for critical equipment.

The modular MCC design is customizable to meet low-voltage motor control applications and factory footprints. The technology is engineered for a range of industries from food and beverage to oil and gas. When integrated with smart VFDs, the MCC helps reduce power consumption.

The MCC is engineered to integrate motor control and power distribution into one centralized package, meeting IEC 61439-1&2 standards for global customers.

The smart devices within the MCC help reduce unplanned downtime with alarms and advanced diagnostic information, reduce maintenance and energy costs, increase production throughput, improve plant and personnel safety, and reduce engineering and commissioning costs.

PRODUCT SPOTLIGHT

GENAI PRESCRIPTIVE WORK ORDERS

Rockwell Automation introduces **Fiix Prescriptive Maintenance GenAI prescriptive work orders** for its Asset Risk Predictor (ARP) software, creating a predictive and prescriptive maintenance solution to help eliminate unplanned downtime. It is designed to transform ARP's failure predictions into detailed, actionable work orders for maintenance teams.

Work orders are generated using asset data, completed work orders and trusted maintenance sources. Teams then can review and edit work orders, and instantly push them to any CMMS or EAM tool. All data is kept private and protected by the highest security standards.

Fiix Prescriptive Maintenance can be used independently from the Fiix CMMS or integrated with any third-party CMMS or EAM.

ADVERTISER INDEX