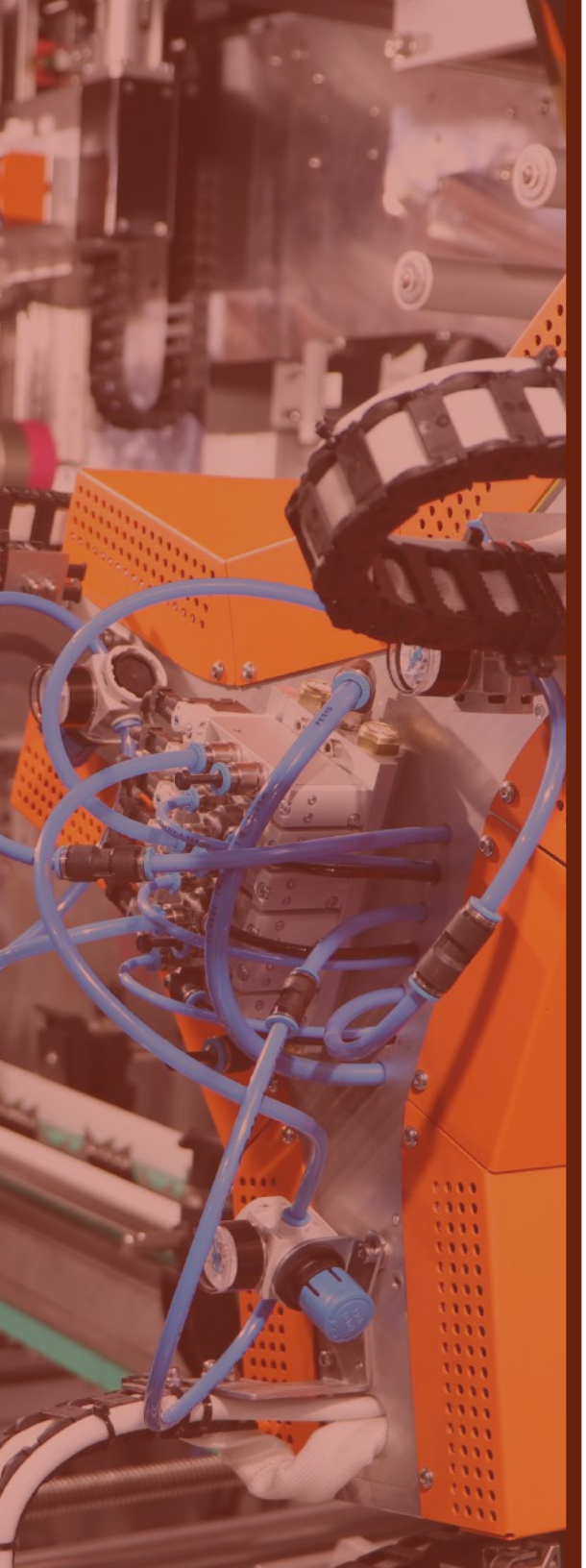
Industrial Networking

SUMMER EDITION

CONTROL ENGINEERING eBOOK | HMS



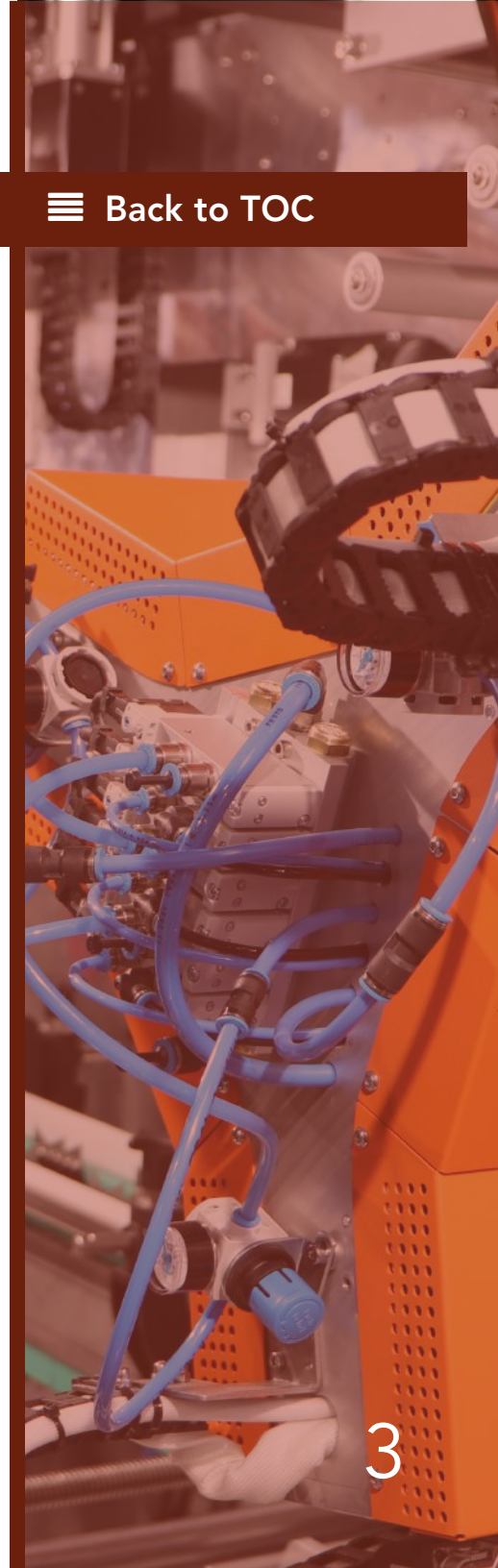
Contents

New PICMG InterEdge standard helps open, modular process control systems

A new process automation hardware standard, PICMG InterEdge, defines a vendor-neutral, open standard for edge computing and I/O module hardware. InterEdge began as part of the O-PAS (Open Process Automation) Standard from The Open Group's Open Process Automation Forum (OPAF). See related 4-part open process automation series from Control Engineering.

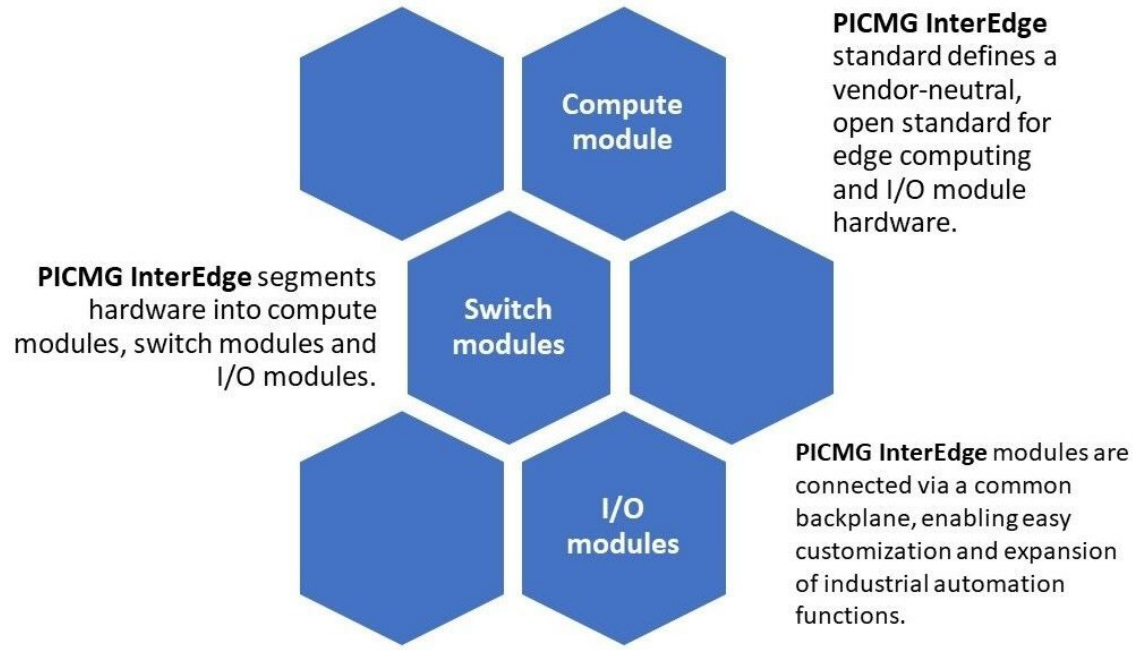
PICMG, the consortium for open hardware specifications announced the release of InterEdge, a modular architecture for process control systems (PCS). The InterEdge specification, said to be compatible with IEC 61499 and IEC 61131, "promises to revolutionize the industry with an interoperable, multi-vendor alternative to proprietary Industrial PCs (IPCs), programmable logic controllers (PLCs) and distributed control systems (DCSs)," the organization said in a Feb. 26 announcement, as explained to Control Engineering at the ARC Industry Forum in a open process automation discussion.

InterEdge defines a vendor-neutral, open standard for edge computing and I/O module hardware, PICMG said. It segments hardware into compute modules, switch modules and I/O modules. All of these modules are connected via a common backplane, enabling easy customization and expansion of industrial automation functions. InterEdge 0 R1 supports single- and multi-channel I/O implementations, and a forthcoming specification will be optimized for single-channel I/O.



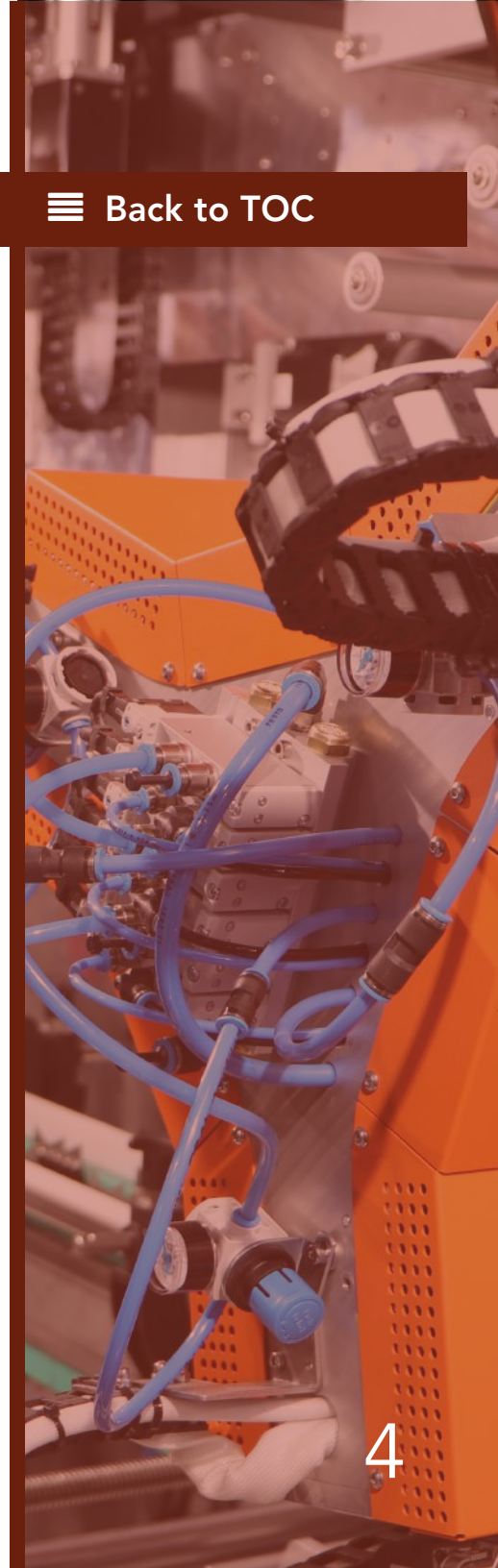
Back to TOC

Back to TOC



"Business needs evolve at an ever-increasing rate," said Francisco Garcia, Americas regional instrument lead at ExxonMobil Technology and Engineering Co. and member of the InterEdge technical working group. "InterEdge delivers an interchangeable base hardware standard for industrial manufacturers looking to adapt to changing business needs. As a result, providers can deploy and scale dedicated physical assets and focus on value-added software and services."

Figure 1: PICMG InterEdge defines a vendor-neutral, open standard for edge computing and I/O module hardware, segmenting hardware into compute modules, switch modules and I/O modules. All of these modules are connected via a common backplane, enabling easy customization and expansion of industrial automation functions. InterEdge 0 R1 supports single- and multi-channel I/O implementations; a forthcoming specification will be optimized for single-channel I/O. Courtesy: Control Engineering using information from PICMG



Back to TOC

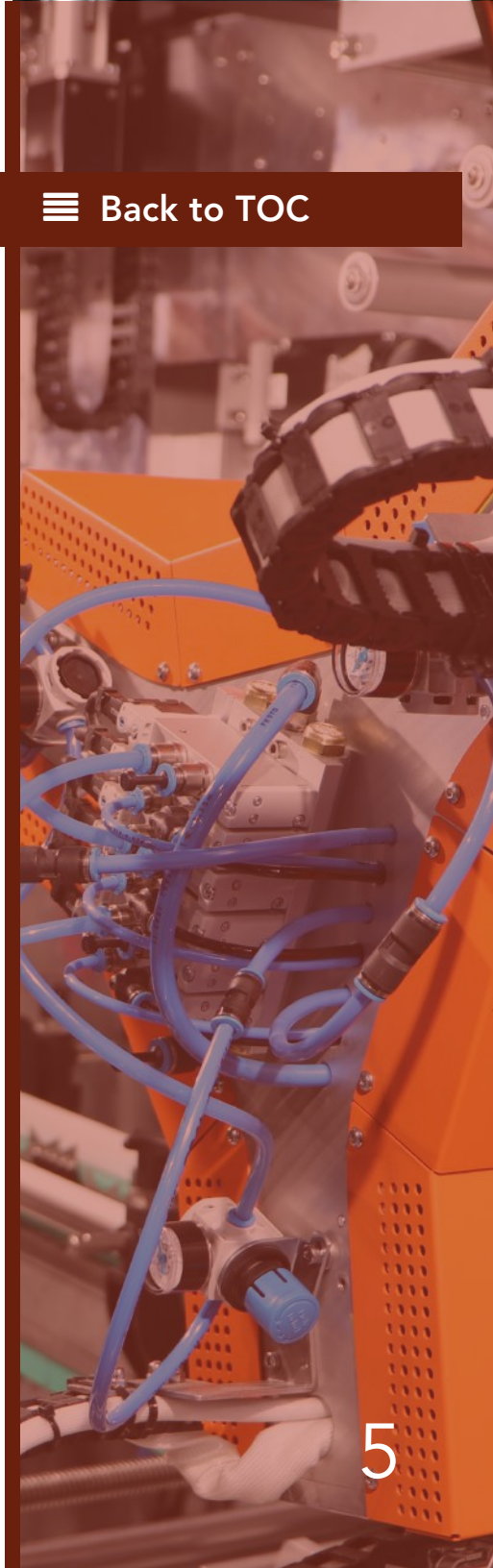
Shared standard for the process industry; upgrades without hardware lock-in

PICMG said with the modular approach of InterEdge, it can flexibly incorporate the functions of disparate automation systems into one platform. This common platform can be deployed across automation, chemical refining, oil and gas, pharmaceuticals, metals and mining, pulp and paper, food and beverage and other process industries.

By replacing proprietary edge devices, InterEdge eliminates vendor lock-in, the organization said, simplifying integration and maintenance and enables online upgrades, for significant cost savings when using open process automation (up to 52% in initial hardware and software costs, according to system integrators involved).

In the past, edge components remained in place for decades with static functional capabilities due to the difficulties of upgrades, PICMG explained. In contrast, the hot-swappable interoperability of InterEdge allows industrial organizations to quickly adapt to changing market demands and technological advancements, PICMG said. Now manufacturers more easily can improve competitiveness through emerging trends in artificial intelligence (AI), industrial internet of things (IIoT) and Industry 4.0 initiatives.

Matt Burns, global director of technical marketing at Samtec and chair of the InterEdge Technical Working Group, said, "InterEdge allows industrial manufacturers to transition from proprietary hardware to an open architecture where they can choose fit-for-purpose components, replace obsolete hardware, add computational resource and upgrade hardware security in a running plant at virtually zero switching costs."



Back to TOC

"InterEdge does for industrial control systems what the Open Compute Project did for data centers," Burns added.

Widespread industry leader support via Open Process Automation Forum (OPAF)

InterEdge originated as part of the O-PAS (Open Process Automation) Standard from The Open Group Open Process Automation Forum (OPAF), a consortium of more than 110 leaders in process automation including system suppliers, engineering firms, governmental bodies, research institutions and end customers. PICMG InterEdge standard joins other PICMG multi-vendor hardware standards including CompactPCI and Com Express and PCI-ISA, among those familiar to automation. PICMG and OPAF have committed to working together to push for the same widespread adoption of InterEdge.

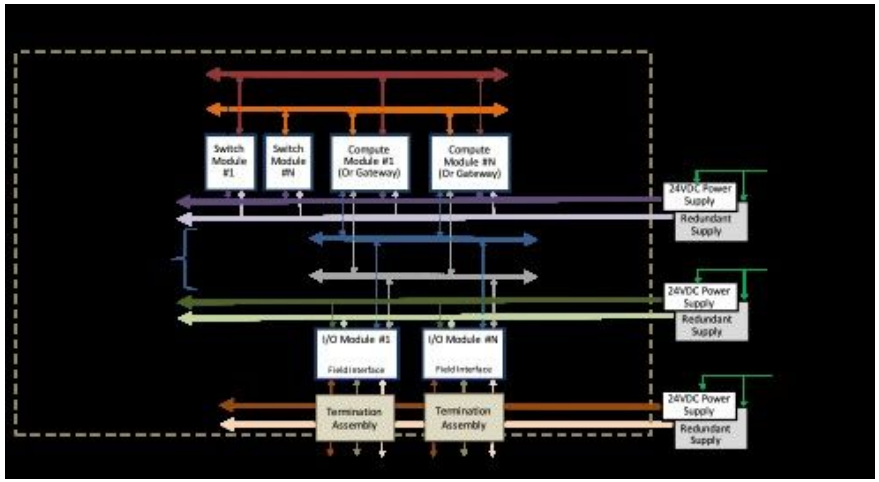


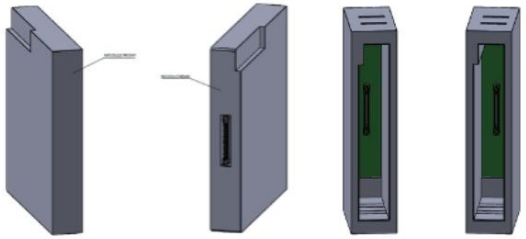
Figure 2: Dimensions (shown) and interfaces are included in the PICMG InterEdge standard, as explained here: https://www.picmg.org/openstandards/interedge/. Courtesy: PICMG

Jessica Isquith, president of PICMG, said, "PICMG felt it was critical to release this because it lays the groundwork for subsequent iterations of the InterEdge specification that will address the broadest range of industry use cases possible. We are eager to support the continued progress of InterEdge and its ability to revolutionize industrial edge environments."

Back to TOC

Physical and Mechanical Characteristics of InterEdge

InterEdge specifies Module dimensions, physical interfaces, and mounting details to ensure compatibility and performance. Compute and Switch Modules must be 35 mm wide, 215 mm tall, and between 120-200 mm deep. Single-Channel I/O Modules are 14 mm wide, 90 mm tall, and between 55-70 mm deep. Multi-Chanel I/O Modules will be included in a future revision of the specification.



All Modules are mounted within cradles. For Compute and Switch Modules these cradles must be at least 55 mm wide, 250 mm tall, and between 108 mm deep. Single-Channel I/O Modules are a minimum of 20 mm wide, 105 mm tall, and 38 mm deep.

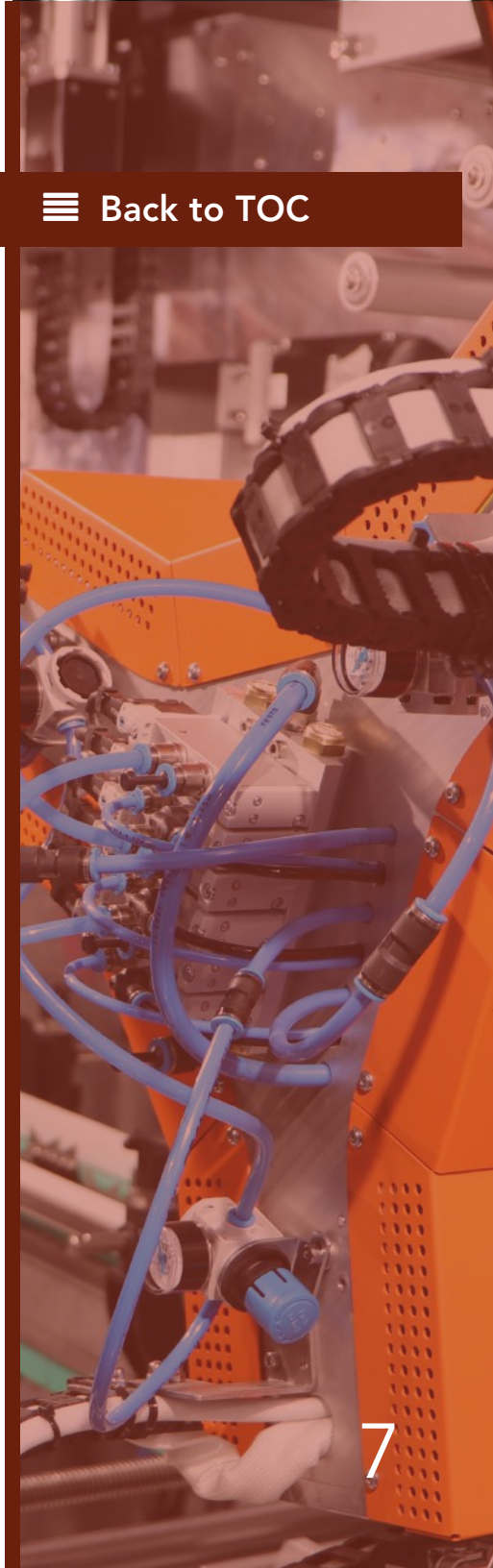


Figure 3: PICMG InterEdge standard architecture helps open process automation, according to PICMG and Open Process Automation Forum. InterEdge 0 R1 supports single- and multi-channel I/O implementations and a forthcoming specification will be optimized for single-channel I/O. Learn more about PICMG InterEdge at https://www.picmg.org/openstandards/interedge/ Courtesy: PICMG

As of the Feb. 29, the price to license the InterEdge specification was $750 on the PICMG website.

How to join the PICMG InterEdge working group, more about PICMG standards

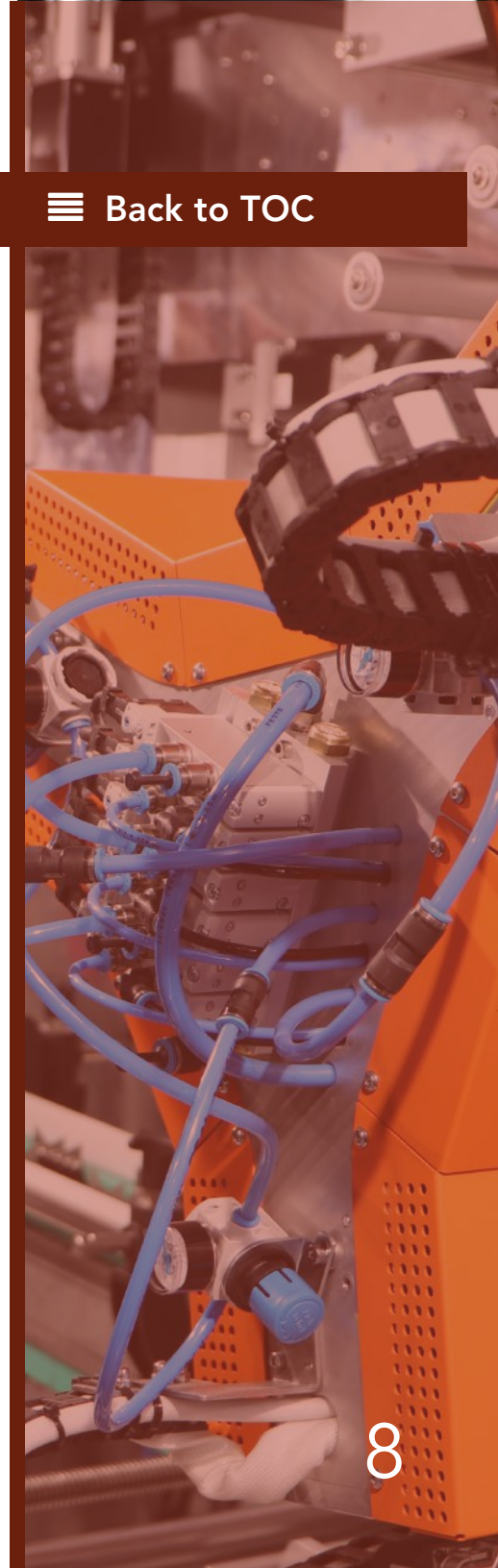
Those interested in specification development efforts can join the PICMG InterEdge working group by emailing info@picmg.org. Founded in 1994, PICMG based in Wakefield, Massachusetts, is a not-for-profit 501(c) consortium of companies and organi-

Back to TOC

zations that collaboratively develop open standards for high performance industrial, Industrial IoT, military and aerospace, telecommunications, test and measurement, medical and general-purpose embedded computing applications. More than 140 member companies specialize in a wide range of technical disciplines, PICMG said, including mechanical and thermal design, single board computer design, high-speed signaling design and analysis, networking expertise, backplane, and packaging design, power management, high availability software and comprehensive system management.

Mark T. Hoske

Mark Hoske *has been Control Engineering editor/content manager since 1994 and in a leadership role since 1999, covering all major areas: control systems, networking and information systems, control equipment and energy, and system integration, everything that comprises or facilitates the control loop. He has been writing about technology since 1987, writing professionally since 1982, and has a Bachelor of Science in Journalism degree from UW-Madison.*



Anybus® BY HMS NETWORKS Communicator

Easy, Secure Protocol Conversion

Back to TOC

Anybus Communicator User Interface: The world's most user-friendly web UI for industrial gateways

In this video we introduce the Anybus Communicator's web user interface. Not just easy to use, it is the world's most user-friendly industrial gateway platform.

New products for next-generation, open automation infrastructure controller

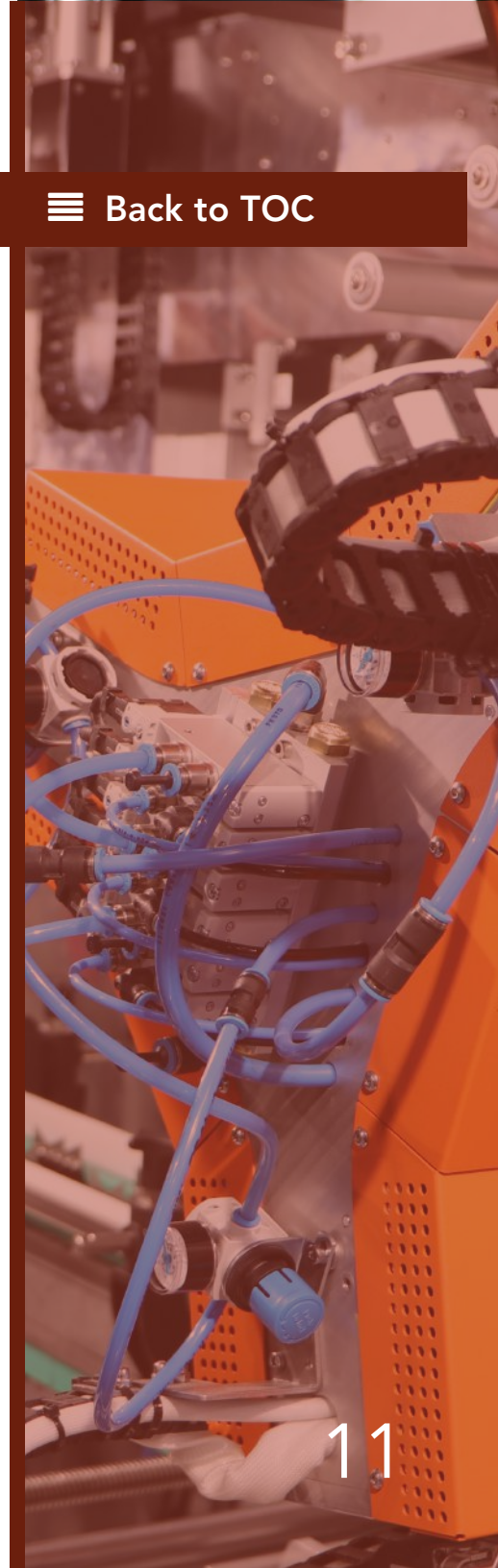
Schneider Electric delivers next-generation, open automation infrastructure, distributed control node (DCN) with independent software-defined controller, in collaboration with Intel and Red Hat, as announced at the 2024 ARC Industry Forum.

Schneider Electric, in collaboration with Intel and Red Hat, announced the release of a Distributed Control Node (DCN) software framework Feb. 6, after a Feb. 5 preview to media and analysts at the 2024 ARC Leadership Forum in Orlando. See additional insights from the preview below. Schneider Electric, with U.S. headquarters in Boston, provides digital transformation, energy management and automation software and hardware.

An extension of Schneider Electric's EcoStruxure Automation Expert software, the new framework enables industrial companies to move to a software-defined, plug-and-produce automation architecture, aiming to enhance operations, ensure quality, reduce complexity and optimize costs.

Next generation of industrial control

Aligned with the goals of the Open Process Automation Forum (OPAF), an organization dedicated to driving interoperability and portability, the three collaborators created a modern, network-based architecture intended to enable the next generation of industrial control.



Back to TOC

Back to TOC

"This project is the culmination of two years of co-innovation to create efficient, future-proof distributed control systems," said Nathalie Marcotte, senior vice president of process automation at Schneider Electric. "The DCN framework is key to fostering an open automation approach, enabling industrial businesses to grow and innovate for the future. Its interoperability and portability help our customers enjoy the freedom of shaping technology around their business needs – and not the other way around."

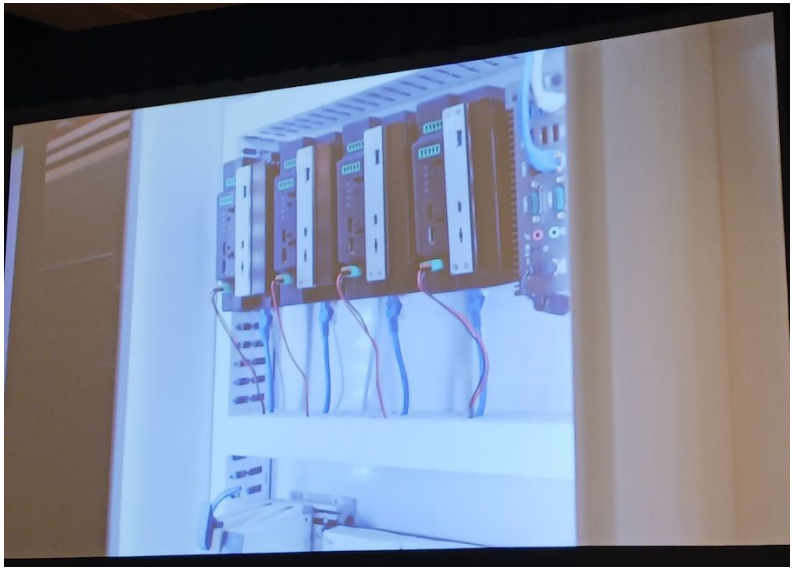
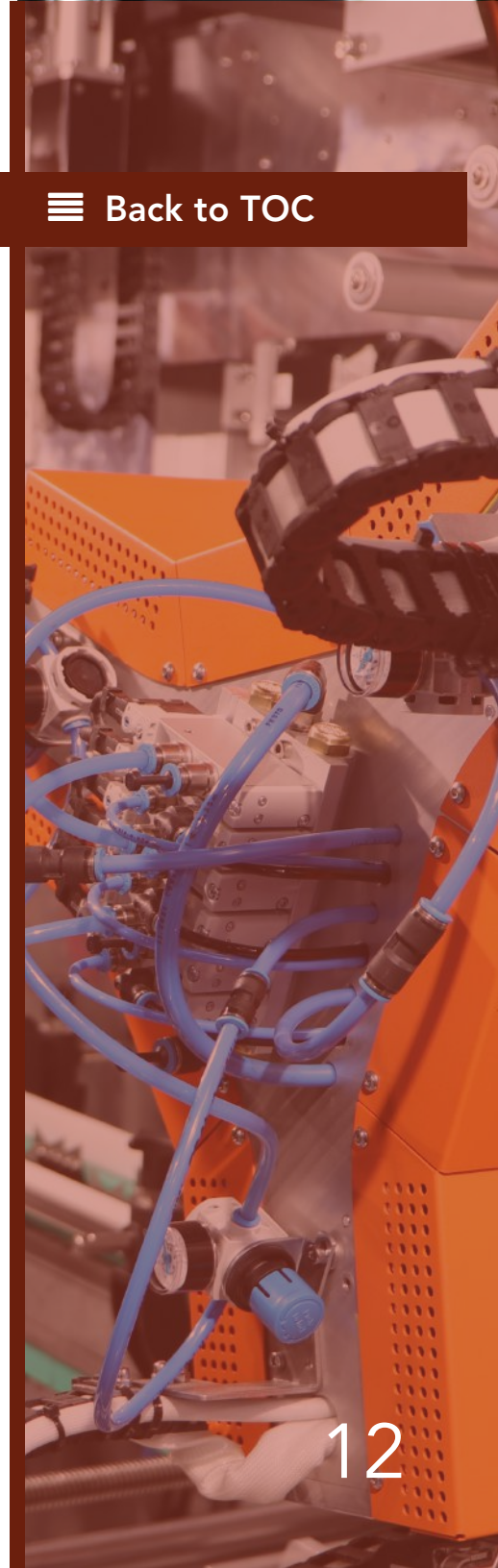


Figure 1: An advanced computer platform (ACP), which supervises the control workload by providing the content control and automation capabilities needed to deploy workloads securely and programmatically, along with virtualization and monitoring functionalities, was part of the Schneider Electric open interoperable automation discussion during the 2024 ARC Industry Leadership Forum by ARC Advisory Group. Courtesy: Mark T. Hoske, Control Engineering

Red Hat, in collaboration with Intel, recently announced a new industrial edge platform that helps provide a modern approach to building and operating industrial controls. Since implementing this platform, Schneider Electric has deployed Red Hat Device Edge in the new DCN software, in addition to Red Hat Ansible Automation Platform and Red Hat OpenShift at the compute layer for DCN deployments, combined with a control infrastructure from Schneider Electric and reference architecture from Intel.



Back to TOC

The framework has two main components: an advanced computer platform (ACP), which supervises the control workload by providing the content control and automation capabilities needed to deploy workloads securely and programmatically, along with virtualization and monitoring functionalities (Figure 1); and the DCN, which are low-power, industrial systems using Intel Atom x6400E series processors, dedicated to running controls and designed for workloads of mixed-criticality (Figure 2).

Figure 2: Schneider Electric, in collaboration with Intel and Red Hat, announced the release of a Distributed Control Node (DCN) software framework Feb. 6, after a Feb. 5 preview to media and analysts at the 2024 ARC Leadership Forum in Orlando by ARC Advisory Group. Courtesy: Mark T. Hoske, Control Engineering

Christine Boles, vice president of Intel's network and edge group and general manager for federal and industrial solutions, said, "Open and interconnected commercial solutions will help usher in the transition from fixed function proprietary devices to flexible and dynamic software-based infrastructures. Intel has a long history of driving open system approaches across its ecosystem. This collaboration with Schneider Electric and Red Hat to develop a software-defined control system showcasing next-generation distributed control nodes built on general purpose compute and operating

Back to TOC

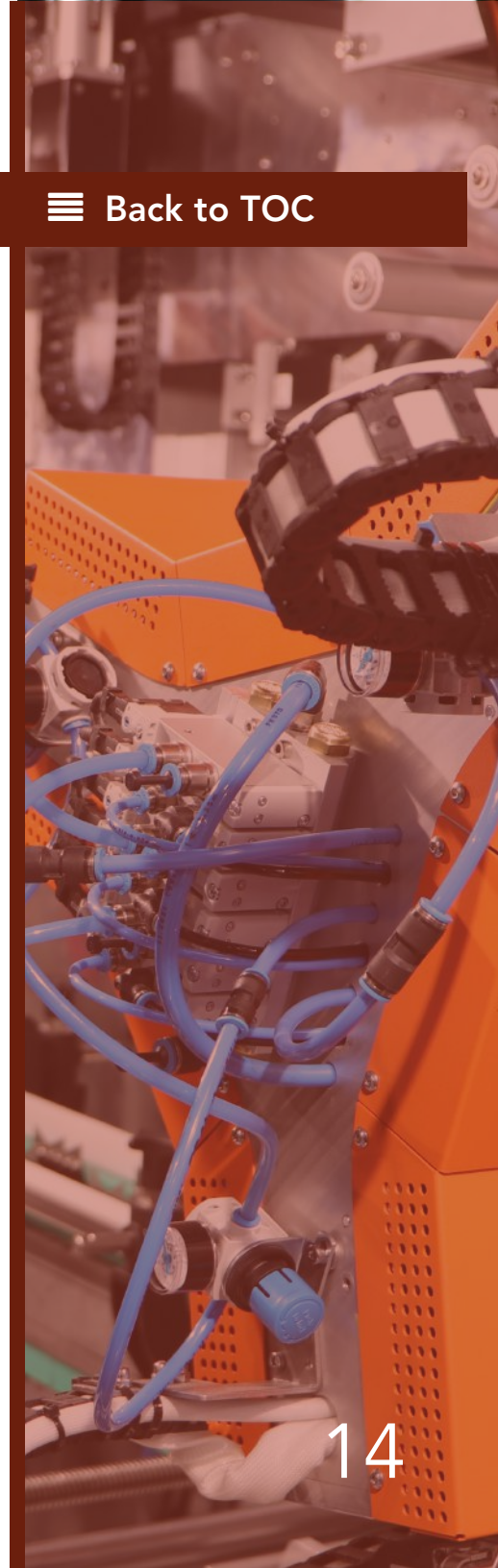
systems brings about this transition to the industrial sector."

Figure 3: Andre Babineau, Schneider Electric, PA strategy director, previewed the new distributed control node at a Feb. 5 news conference during the 2024 ARC Industry Leadership Forum by ARC Advisory Group. Courtesy: Mark T. Hoske, Control Engineering

Francis Chow, vice president and general manager of in-vehicle operating system and edge at Red Hat, said, "Red Hat is committed to helping manufacturers implement autonomous operations on the shop floor. By working closely with our partners, like Schneider Electric and Intel, we can help build scalable, software-defined factories and operations capable of advanced automation and interoperability," using "a consistent platform approach. We're excited about this collaboration, and this is only the beginning. By taking these steps now, we can help set the industrial sector up to explore all the possibilities AI, edge computing and more have to offer."

The architecture was demonstrated at the 2024 ARC Industry Leadership Forum in Orlando, Florida, Feb. 5-8.

Schneider Electric said it drives digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.



Back to TOC

Technology overview: Schneider Electric's Distributed Control Node (DCN) software framework

At the 2024 ARC Industry Leadership Forum, Schneider Electric, Intel and Red Hat discussed the DCN software framework from Schneider Electric.

Figure 4: Panel discussed open and inclusive technologies for industrial automation at the 2024 ARC Industry Leadership Forum by ARC Advisory Group. Michael Martinez, Schneider Electric EcoStruxure Foxboro, DCS leader (left) also served as moderator. Christine Boles is vice president of network and edge group, Intel; Kelly Switt is senior director, global head of intelligence edge, Red Hat; Jason Norris is Phoenix Contact group leader global market development; and Ravi Jagasia is Stahl global business development. Courtesy: Mark T. Hoske, Control Engineering

Michael Martinez, Schneider Electric EcoStruxure Foxboro, DCS leader, said the open and inclusive DCN framework intends to help end users challenged to be more agile and deal workforce issues, including shortages of qualified labor and retiring talent, a combination that challenges organizations with legacy control systems to keep up with market demands. Martinez characterized OPAF efforts as "beyond open to interchangeable. How can we create a technology environment to adapt at the speed of innovation?" he asked a panel (Figure 4).

- Boles, Intel, mentioned above
- Kelly Switt, senior director, global head of intelligence edge, Red Hat

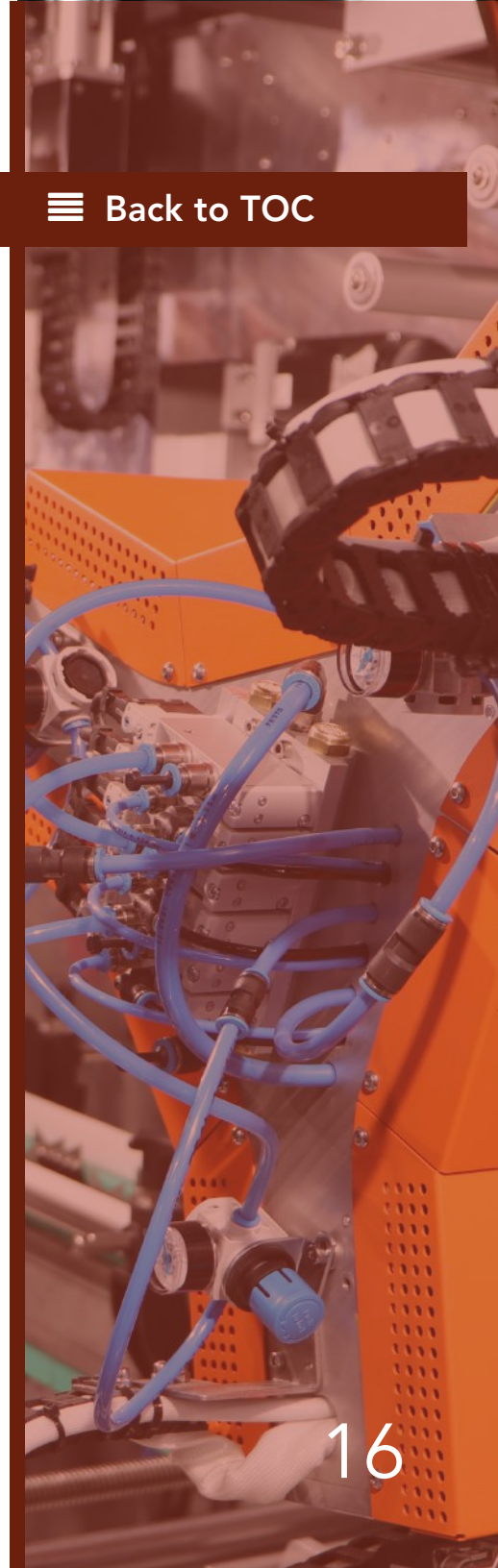
Back to TOC

- Jason Norris, Phoenix Contact group leader global market development
- Ravi Jagasia, Stahl global business development.

How is Intel making automation products suitable for industrial use?

Boles said Intel has served many industries in the industrial sector with products and technologies, but challenges are too great for companies to solve alone. Bringing capabilities from different industries for a new approach, to defining specifications and standards, evolving to a more open approach. It happens only when multiple companies work on open platform and put innovation on top, building on OPAF reference designs of a few years ago. Now companies are building on reference designs, to produce distributed control nodes in a new system to "revolutionize how automation systems work. It's very excited to see how industry is progressing."

Switt said Red Hat has been revolutionizing the IT industry for 30 years with open-source code and the Linux operating system, allowing the IT industry to produce needed products using a rich open-source platform. Intel contributes as much or more code than we do, Switt said. Cloud computing advanced to the telecommunication industries 10 to 12 years ago, with network virtualization functions; 4G and 5G systems became open and interoperable. The same transformation is taking place here, driven by market needs, including next-gen talent who appreciates training on new technologies. Switt said Red Hat is known in the government sector for strong use of cybersecurity standards and open access to data, to improve operations and extract software value with hardware and system resiliency. With easier access to data, companies can think differently about how to run operations. We intend to collaborate and democra-



Back to TOC

tize data use so companies can better innovate and run their businesses.

Martinez said select partners have been doing this a long time for IT. For OT, it needs to be proven and made robust in a software-defined future. The concept has been well proven in other areas. When you go to a trusted website, users don't worry about website security. That's what we're trying to accomplish. Users need to feel comfortable moving to next-generation architectures. "Automation industry vendors have trained customers how to buy our products. Now technologies can start to solve problems without users having to adapt their processes to the product."

Figure 5: Schneider Electric demonstrates an application use case at the ARC Industry Forum for open and interoperable automation. Among topics covered were software-defined controllers and rugged controller hardware (an edge controller) that can operate software separate from the supplying vendor, as has been the model in IT applications, but fewer OT or automation applications. Courtesy: Mark T. Hoske, Control Engineering

Boles noted that the telecommunications could not have progresses 4G to 5G without this shift to open-source architectures. In the telecommunications industry this open-source architecture is foundational. Manufacturers and utilities can take advantage

Back to TOC

of what's already been done in other industries.

Switt noted that it is a different way of thinking. Manufacturers ask for a spec sheet, but that's not available with open-source software.

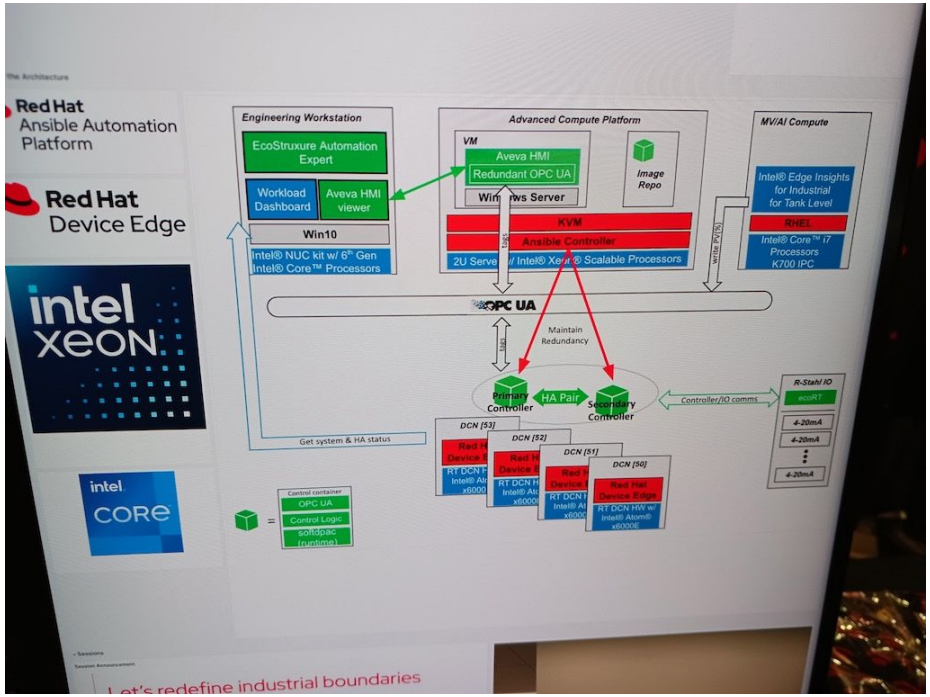
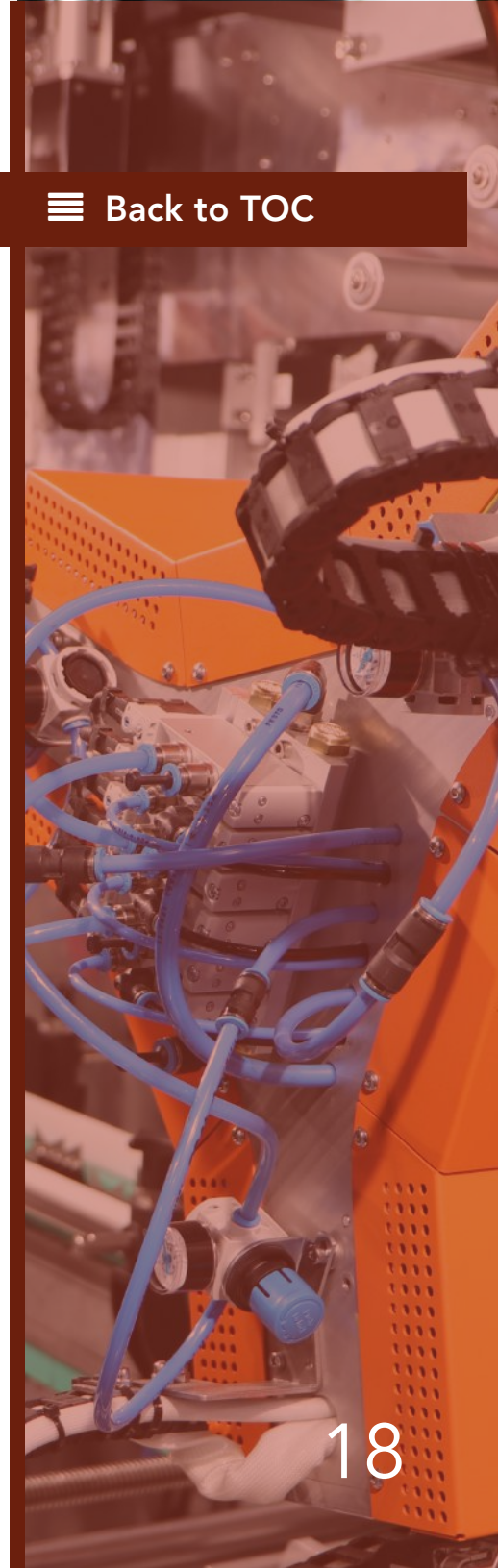


Figure 6: An open interoperable multi-vendor automation architecture was part of numerous discussions during the 2024 ARC Industry Leadership Forum by ARC Advisory Group. Courtesy: Mark T. Hoske, Control Engineering

Martinez said industrial automation is moving away from proprietary systems. OPAF standards have redefined "open" so everything can talk to everything else, share information. Workforce demands an end to proprietary languages of past, where engineers to be network specialists and cybersecurity experts. This multi-vendor inclusive solution provides a more resilient automation platform (Figure 5), Martinez explained, with easier connections through the supply chain. Customer can expand, update or add automation and keep the facility running (Figure 6). Working with other automation technology vendors, it's easier to incorporate technologies from other vendors without reconfiguring systems or the input/output (I/O) system infrastructure. Vendors' products should work together in a software-based architecture with software-based configuration. Learn more.



Back to TOC

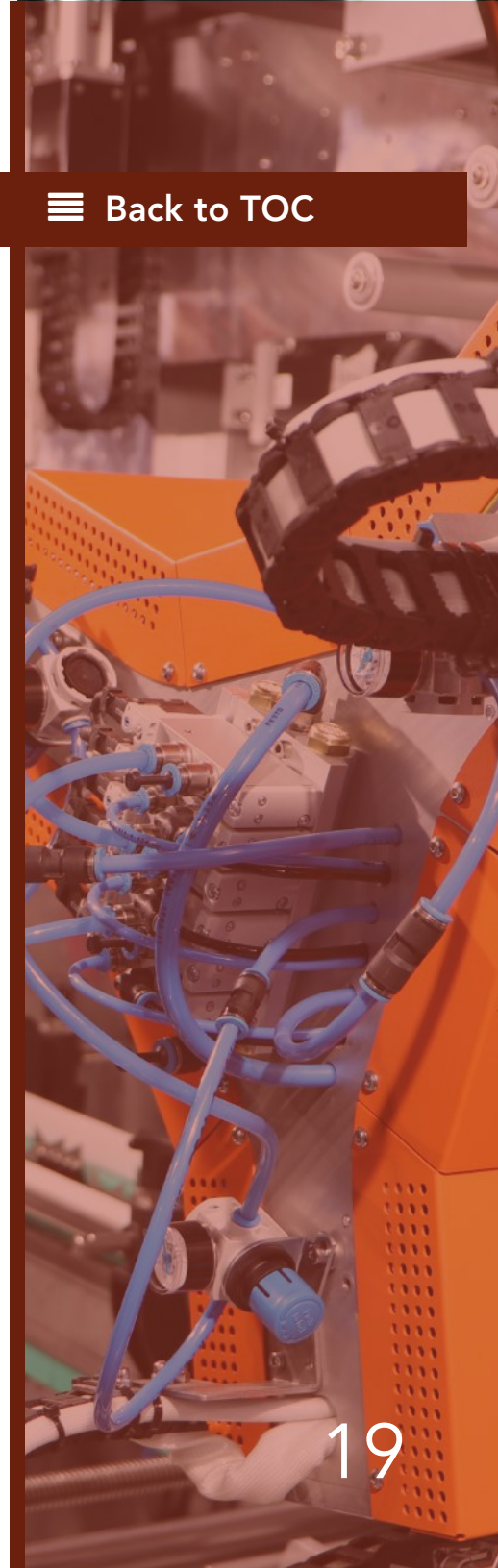
Norris noted that while OPAF and universalautomation.org both have open visions, they are not the same thing. "I'm a hardware guy, and connectivity is a physical thing." He said when a sensor comes into a network, it needs standard interfaces to connect and communicate. Automation vendors traditionally offer specific software. In some cases, in requests for proposals (RFPs), customers are looking for a more open concept, an open second channel to talk to proprietary systems. He sees interest in OPAF and gets more questions from customers with field trials.

Martinez said OPAF would create language to help users request open-source architecture in specifications. Perhaps 15% or less know-how to put open-source request in specifications.

Jagasia said Stahl serves hazardous area markets and appreciates that sensor data can be transfers and enhanced with internet or cloud connections and applications. Open-source data efforts have been lost in the past. Plug-and-play architecture is needed, he suggested.

Martinez said open architecture automation can add scalability and create an industrial automation platform programmable logic controller (PLC), with process control and high-speed machine control capabilities in one platform. The open vision allows multiple vendors of hardware and one software application running on any hardware. Customers can build applications for processes and integrate them into larger applications.

Norris said Phoenix Contact and Schneider Electric share a common sales channel in the U.S. market. Phoenix Contact has done lab and integration tests with open architectures, and while customers have interest, they have not deployed as of early February.



Back to TOC

Martinez the platform allows creation of independent applications that don't require lots of system integration, so customers or system integrators can develop without worrying which hardware it will deploy on. He asked, "What are you doing to add value?"

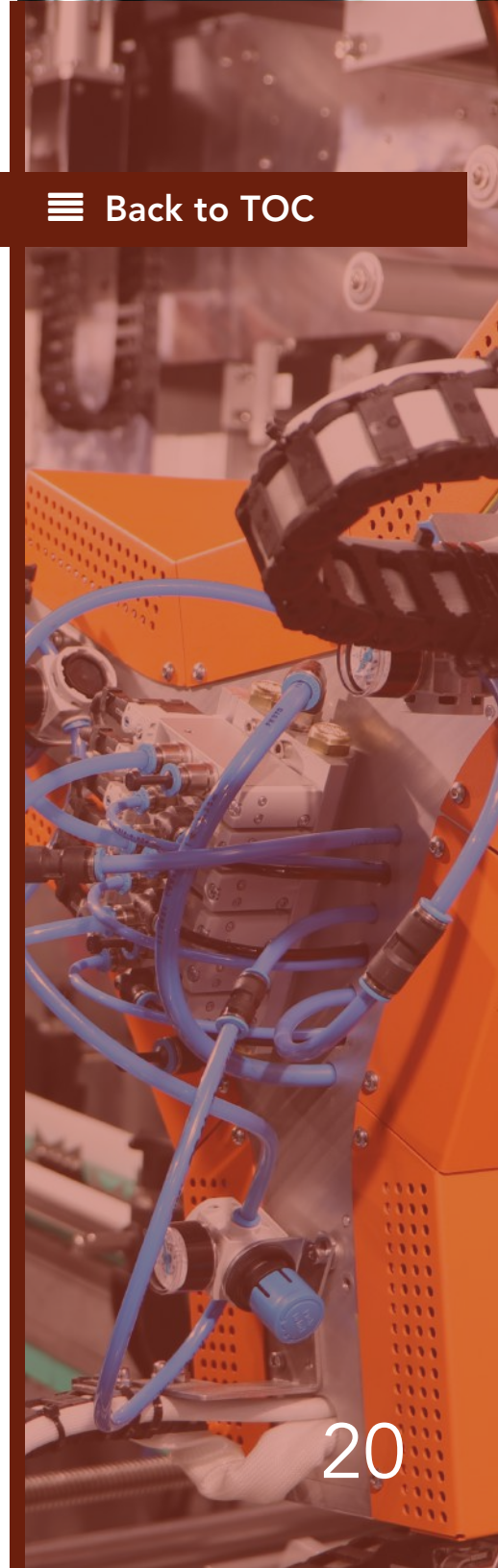
Boles said the software-defined approach used in other industries, deploys workload where needed and now is building momentum in the industrial space. The utility industry grid cannot handle changes in supply and demand. Intel is working with a range of industries to bring IT capability to the edge of operations. Challenges for reliability and resiliency are similar.

Automotive industry over-the-air software updates

Switt gave an example of the automotive revolution. Many startups in automotive disrupted how cars are made. Now trusted brands are changing how they make vehicles. Linux is going into cars. With a need for physical safety, functional safety was added to Linux. To supplement components in the physical car, a software-defined vehicle can receive over-the-air updates. Red Hat is working with large system integrators to do virtual testing in the cloud about how deploy updates in cars while at a gas station. Industries can learn from each other. Automotive industry, for instance, is asking for a Linux equivalent to safety integrity level (SIL) 3.

"We need to open our minds to what others are doing to learn and share," Switt said. Perhaps this will end the practice of updating a plant's controllers with USB sticks, she added.

Martinez agreed that over-the-air updates would be useful. Use of a distributed control node for automation applications provide ability to move platform to another.



Back to TOC

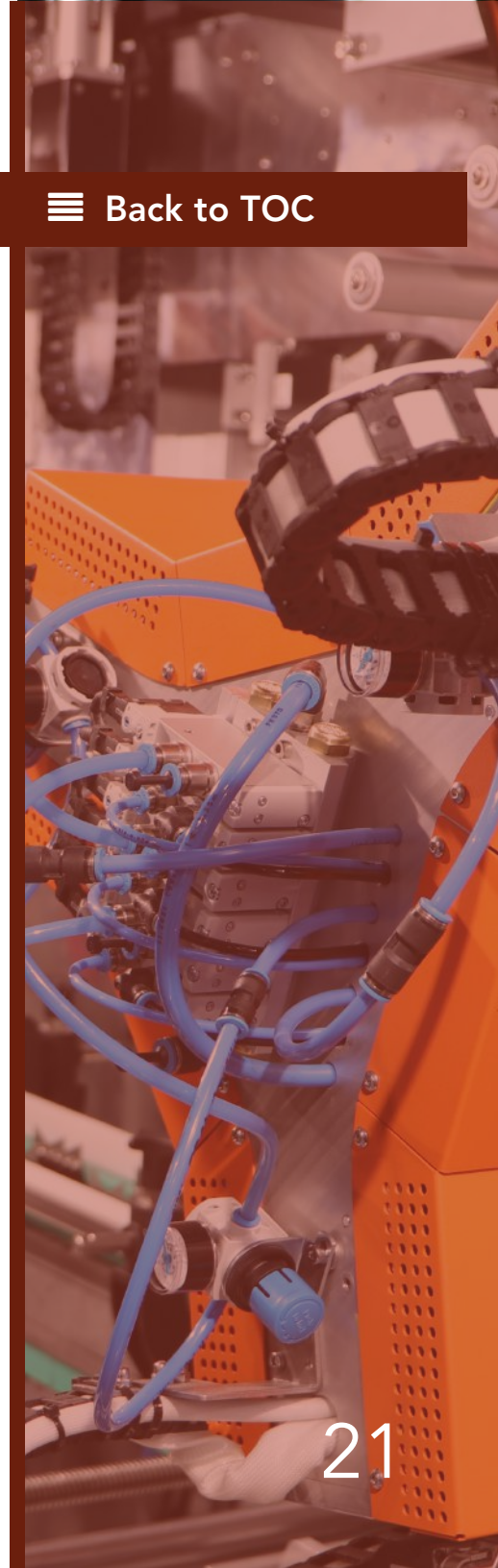
Software-based controllers allow users to redeploy workload to other areas for added capacity or redundancy as needed. Martinez said this more sustainable infrastructure takes less space and uses less hardware.

News conference preview of Schneider Electric DCN software framework

At a Feb. 5 news conference at the 2024 ARC Industry Forum, Schneider Electric, Intel and Red Hat explained more about the platform. Tom Eck, U.S. media relations manager, Schneider Electric, introduced Andre Babineau, Schneider Electric, PA strategy director, new distributed control node, and Heather Cykoski, SVP industrial and process automation NAM operations, SE. Cykoski said the introduction is designed to drive efficiencies and processes as we move into Industry 5.0 and realize advantages of a software-defined architecture.

Babineau, PA strategy director, commenting on the new distributed control node, said Schneider Electric's collaboration with Intel started two years ago. Based on the OPAF reference design, the DCN's IT technology integration leverages Intel hardware and software with lowest total cost of ownership. Babineau said it brings resilience to a control system by leveraging standard technologies. When a failure occurs at night, it's easy to bring it back to the desired state. Also, software updates bring the highest level of cybersecurity without shutdown.

Boles said working with OPAF created an open-platform approach. Reference design uses an Intel Atom x6400E se processor. The optimized OT software stack is helped with Red Hat, providing industrial edge software functions on rugged hardware.

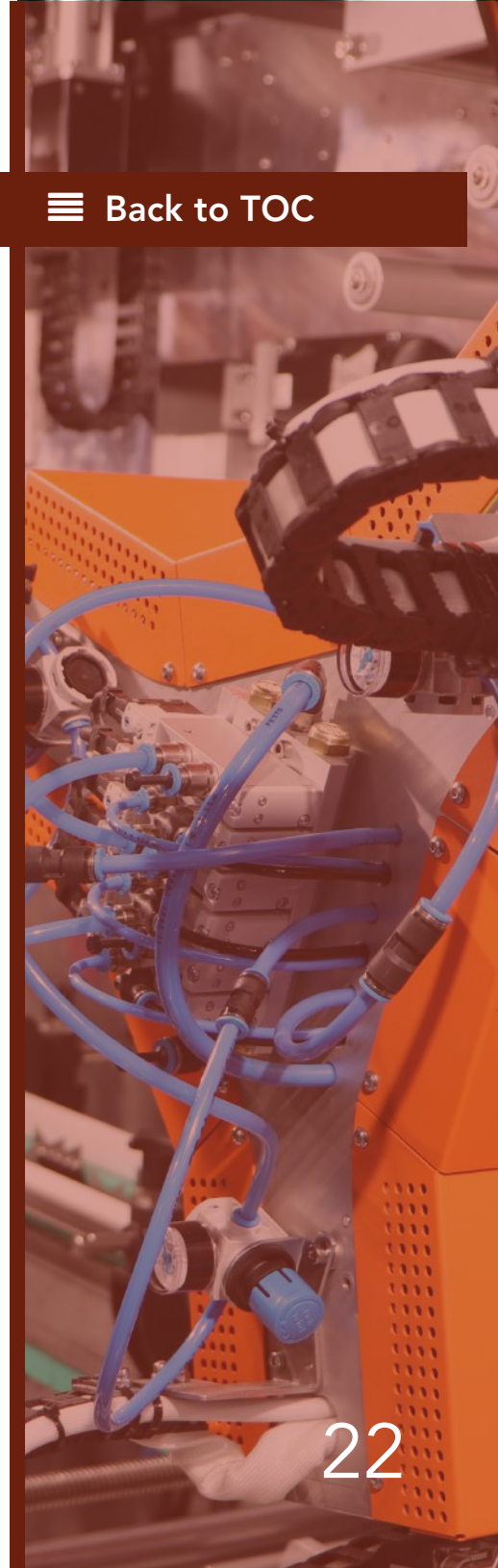


Back to TOC

Babineau said the approach uses IT-OT integration, decouples hardware and software, creates agnostic software architecture, is scalable and future proof and is AI ready. Also, he said, a DCN is better than a PLC because it can load the software you want. A PLC's firmware is burned in.

Mark T. Hoske

Mark Hoske *has been Control Engineering editor/content manager since 1994 and in a leadership role since 1999, covering all major areas: control systems, networking and information systems, control equipment and energy, and system integration, everything that comprises or facilitates the control loop. He has been writing about technology since 1987, writing professionally since 1982, and has a Bachelor of Science in Journalism degree from UW-Madison.*



Defending industrial automation against cyberattacks

With reports of cyberattacks on the industrial sector becoming all too familiar, Thomas Vasen, Anybus Business Development Manager Network Security at HMS Networks, outlines five strategies companies can adopt to fortify their defenses and avoid becoming the latest victim.

Rise of cybersecurity attacks

Cybersecurity is rapidly becoming a significant concern in industrial automation. The World Economic Forum highlighted in 2023 that manufacturing is the sector most targeted to cyberattacks. Furthermore, Orange Cyberdefense reports that the manufacturing sector had Common Vulnerability Scoring System (CVSS) severity scores 33% higher than the global average. The increasing number of attacks on Industrial Control Systems (ICS) is particularly worrying. Gartner predicts a bleak future: by 2025, cyberattacks are expected to harm or endanger humans.

The time for action is now. Here are five strategies companies can adopt to effectively mitigate the risk of cyberattacks.

1. Understand that OT is not just another version of IT

The first step is to adopt the correct mindset. In the 1990s, **Netheads vs Bellheads** debated the future of telecommu-

Back to TOC

nications. While Bellheads advocated for traditional methods, Netheads argued that voice should be treated like any other data and transmitted over IP. Three decades later, Netheads' vision has prevailed, with voice being transmitted over the Internet like any other type of data. Users have even come to accept deterioration in call quality due to the increase in latency and frequently dropped packets. Today every phone call feels like an intercontinental one.

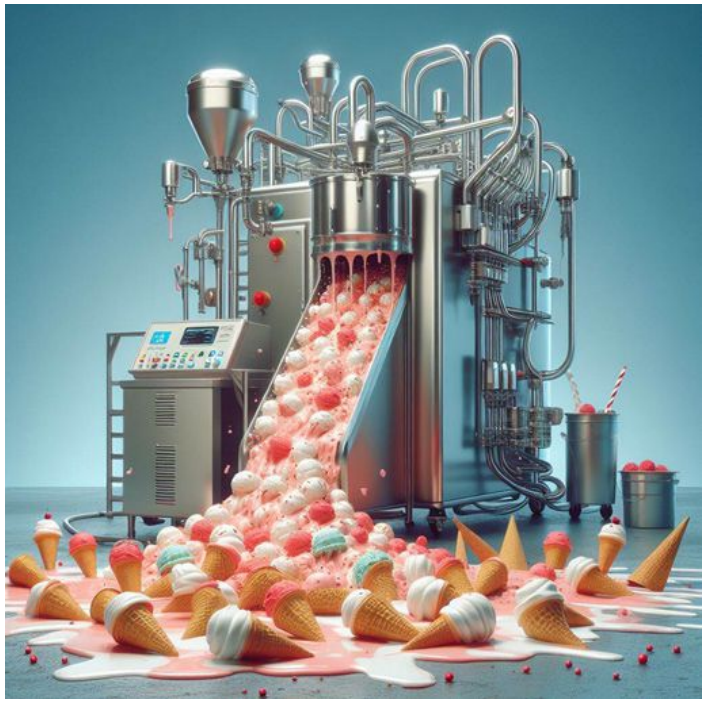


Figure 1: In OT, network downtime would lead to production processes grinding to a halt, resulting in financial losses, and wasted ingredients or materials.

However, the situation with Operational Technology (OT) is fundamentally different. Unlike Information Technology (IT), OT cannot tolerate compromised quality and increased latency, as even minor disruptions can have catastrophic consequences. Treating OT as merely another version of IT is a serious mistake, as OT operates under distinct principles and requirements. While IT prioritizes data integrity and confidentiality, OT demands deterministic data and uptime assurance.

This distinction is especially critical in industries like manufacturing, where even minor disruptions can lead to significant financial losses, material wastage, and operational downtime. In IT, occasional network downtime or data loss may be manageable inconveniences. However, in OT, a similar disruption can have far more severe consequences. Imagine if an ice cream machine were to malfunction due to a network outage or

Back to TOC

data inconsistency. Not only would the production process grind to a halt, but the perishable ingredients would spoil, resulting in financial losses and wasted ice cream. And nobody wants that.

So, while it's natural for OT to adopt IT technologies (there are lots of benefits of using Industrial Ethernet over traditional fieldbus networks) it must be acknowledged that out of the box IT does not satisfy OT's requirements. Hence, the rise of industrial communications protocols, and as such, the need for specialized OT security products and solutions.

2. IT and OT must work together

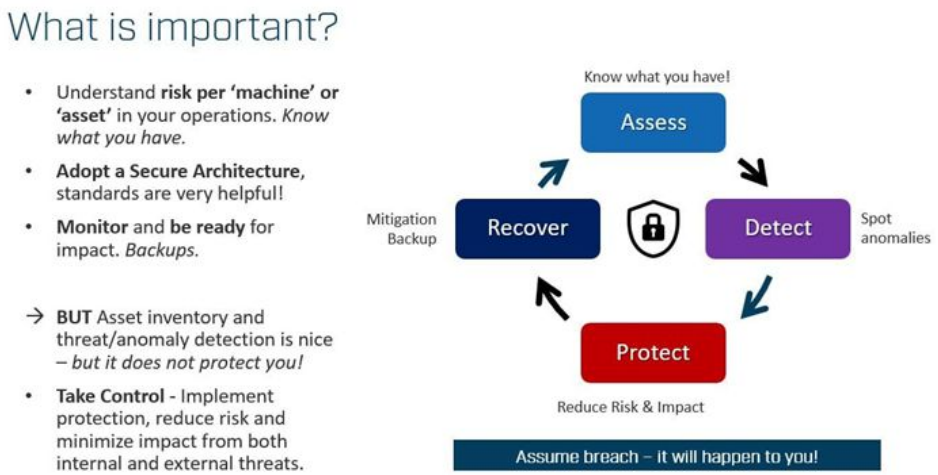
While the Chief Information Security Officers (CISO) is under scrutiny and manages the security budget, often including that for OT, it is the operations manager who bears the responsibility of ensuring uninterrupted production in the factory. This situation creates an inherent conflict due to differing priorities. IT professionals adhere to the CIA framework, prioritizing Confidentiality first, followed by Integrity and then Availability. In contrast, operational personnel prioritize Safety, followed by Availability, Integrity, and lastly, Confidentiality – forming the (S)AIC sequence.

Back to TOC

This dichotomy results in conflict and friction, yet the underlying shared objective remains clear: safeguarding business continuity. Recognizing this common goal, CISO (IT) and the Operations Manager (OT) must collaborate to navigate these challenges and harmonize their approaches to secure business continuity.

3. Develop a comprehensive OT security plan

Securing OT environments requires a proactive and customized approach to the unique challenges of industrial operations. Companies must conduct a thorough identification and assessment of their assets, understanding the risks associated with each machine. Rapid detection of anomalies is important, but more crucial is the implementation of robust protective measures to safeguard these assets. Having a comprehensive recovery plan in place and implementing measures to minimize impact is also important and is commonly recommended by experts such as those from ISA/IEC 62334.



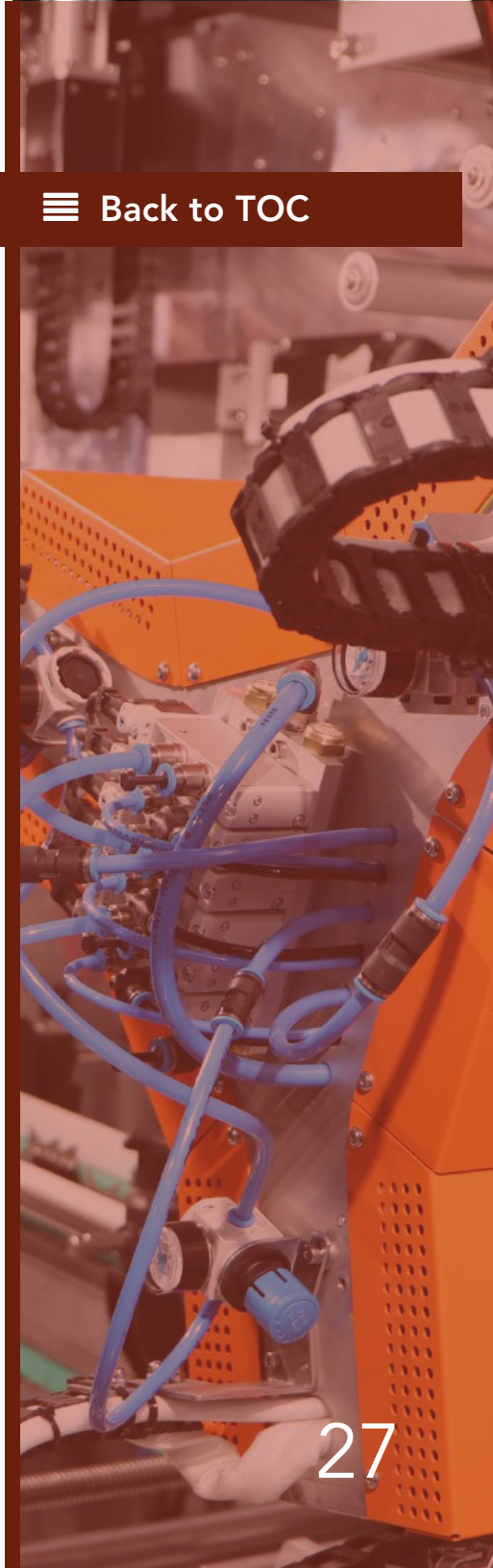
Currently, many companies focus on asset inventory and threat detection. While these are important, they are not sufficient to protect OT environments. Companies must also implement measures to protect their assets.

Back to TOC

4. Protect yourself with Network Segmentation

Network segmentation is an excellent way to secure OT environments. By dividing networks into zones and separating with conduits providing access controls, companies can bolster security and prevent unauthorized access. The benefits of network segmentation include:

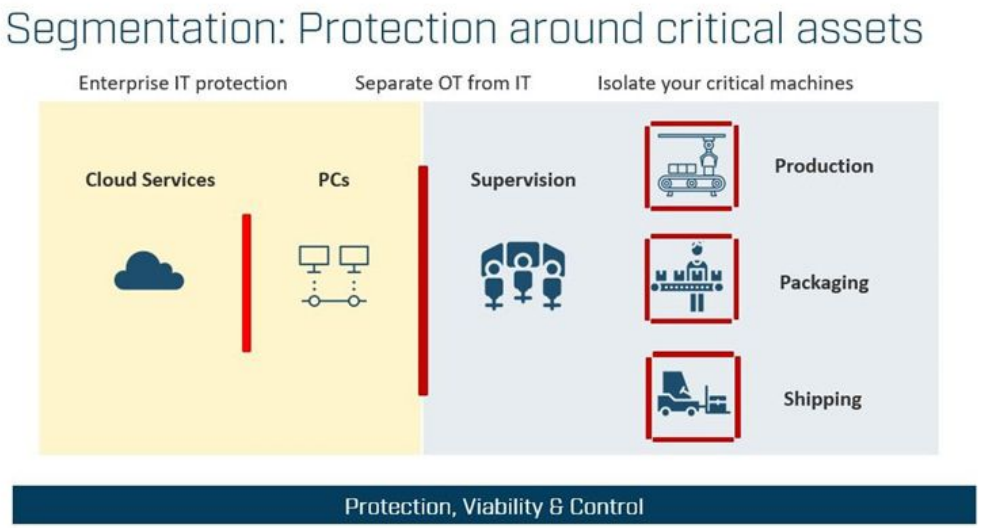
- **Protection from outside traffic -** Separation from IT!
- **Inspection of inside traffic –** Downtime is often caused by internal threats, intentional, or unintentional.
- **Guarding remote access traffic –** Allowing remote maintenance can be critical for your uptime, but it can also be a backdoor for threats to enter your network. Take granular control of the traffic flow.
- **Isolation of visiting workers –** Know what's plugged into your network and control what it can access.
- **Secure uninterrupted industrial communication between machines –** implement secure fast-paths for communications between machines only.
- **Continuous data extraction for analytics –** Monitor both the security and the efficiency of your processes in real time



Back to TOC

- **Early warning on deviations and abnormal behavior –** Stay a step ahead on issues that risk downtime – both caused by faults and cyber threats.

Segmentation differs inherently from IT's perimeter protection approach. In IT network protection, measures are implemented to prevent outside threats from infiltrating the network, while also enabling users to freely browse the internet and utilize a wide range of cloud services. However, for OT segmentation, the focus is on exerting control in both directions to compensate for the lack in access control in OT that exists in IT. OT segmentation uses a deny-by-default approach where every flow in each direction is controlled, as threats can originate from multiple directions.



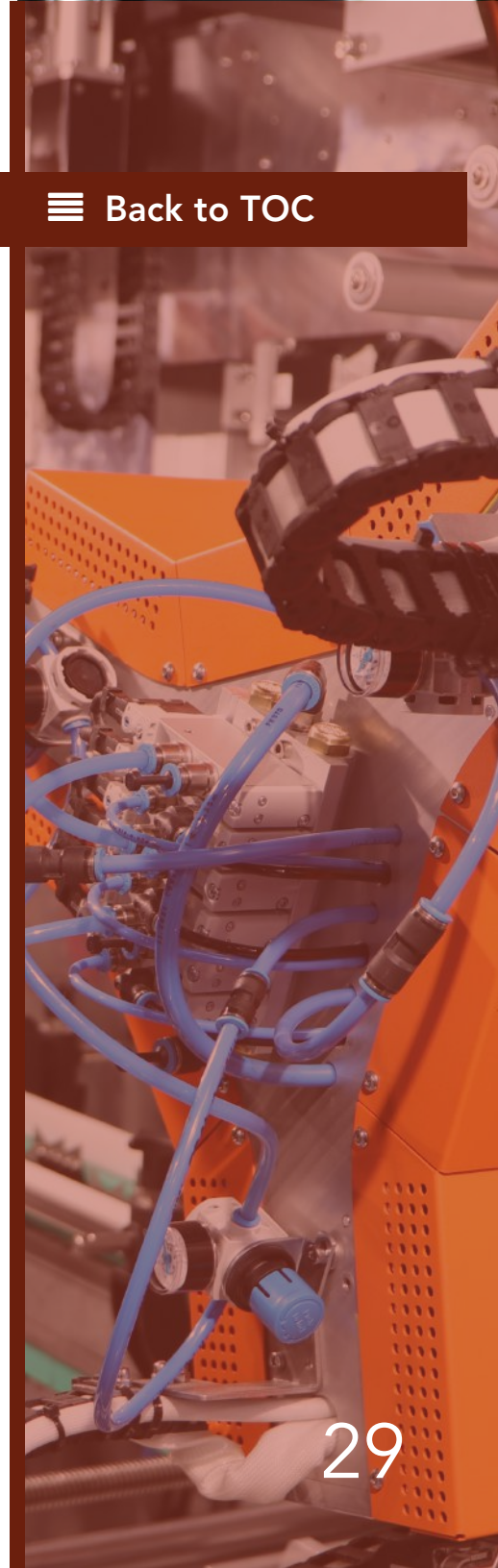
5. Team up with an OT expert

So no, OT is not just another form of IT. Implementing cybersecurity measures in industrial automation is undeniably complex and demanding work. It requires meticulous attention to detail and a deep understanding of the unique challenges presented by OT environments. Partnering with an OT expert like HMS Networks is not just a good

Back to TOC

idea; it's a smart investment. By leveraging their extensive experience and specialized knowledge, companies can save time and, more importantly, ensure that their cybersecurity strategy is effective. With HMS Networks' products and support, companies can navigate the complexities of OT cybersecurity with confidence and peace of mind.

Lastly, partnering with experts like HMS Networks can provide invaluable support in navigating the complexities of cybersecurity in industrial automation. Leveraging their expertise and specialized secure solutions, companies can bolster their defenses with confidence and peace of mind. In essence, by adopting these strategies and taking proactive measures, organizations can fortify their defenses against cyberattacks and safeguard their industrial processes from potential disruptions and financial losses.



Industrial networking 101: Everything you need to know

Industrial networking is vital to today's manufacturing landscape. From different types of networks to key components and best practices, this guide will help you navigate the intricacies of industrial Ethernet networking.

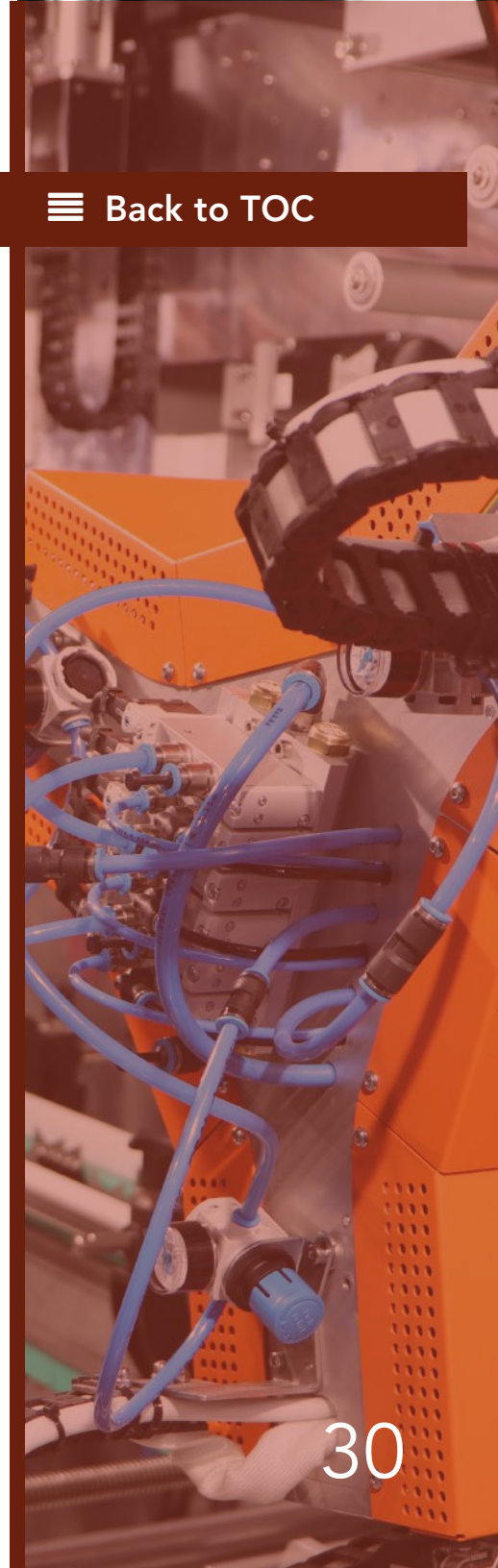
What is industrial networking?

Industrial networking refers to the interconnected infrastructure of devices and systems used for seamless data communication and control in industrial environments. It enables efficient automation, monitoring and optimization of industrial processes, alongside the sensitivity of protocols that are required to maintain consistent communication amongst devices without interruption. The majority of this communication is millisecond dependent, and some is even microsecond dependent.

Importance of industrial networking

Modern Industrial Ethernet networks are essential for driving efficiency and productivity within manufacturing facilities. It allows for real-time monitoring and control of equipment, enables predictive maintenance and facilitates data-driven decision-making. Having a reliable and stable industrial network is vital to any organization; it is the backbone or foundation to all operations, whether that entails implementing a thin client solution, engaging in data collection, operating an industrial software solution or even expanding an existing facility.

For example, one would not want to build a house without a solid and reliable foundation. The additional weight of the floors above would lead the home to before it was even completed.



Back to TOC

Back to TOC

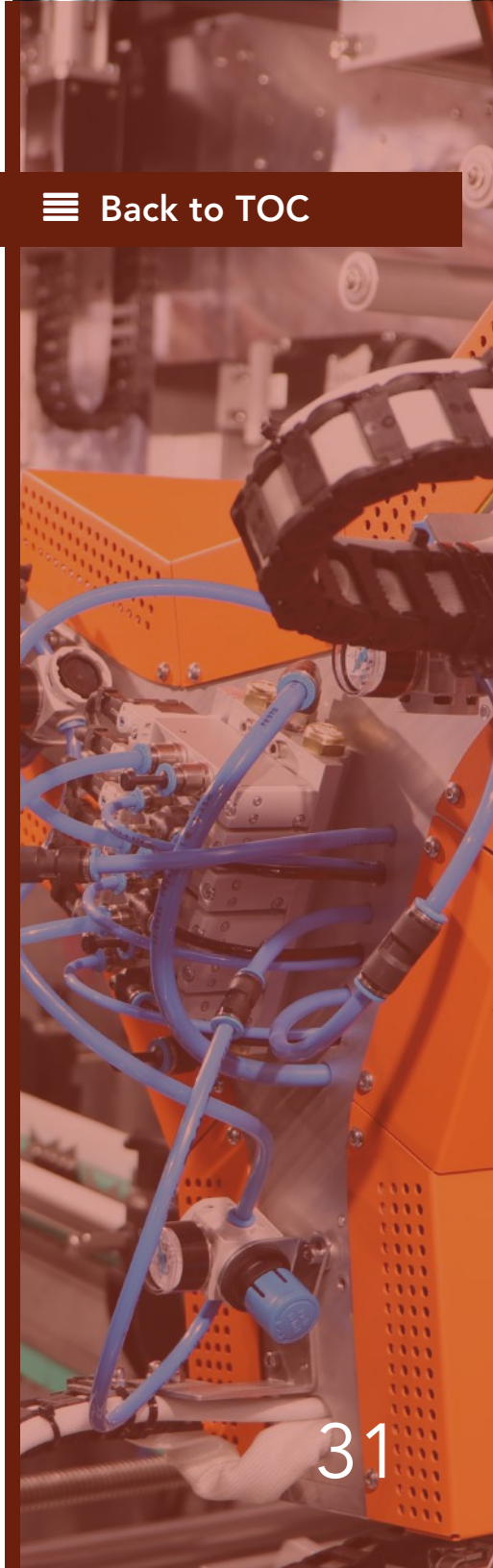
Industrial control system networking

Industrial control system (ICS) networking refers to the Ethernet network infrastructure and protocols used specifically for connecting and supporting industrial control systems on the plant floor. These control systems are responsible for controlling and monitoring various processes and equipment in manufacturing plants.

The goal of ICS plant floor networking is to provide reliable and secure communication infrastructure that ensures smooth and efficient operation of industrial processes. It involves the use of specialized networking technologies and protocols designed to meet the unique requirements of industrial environments, such as high reliability, determinism and real-time communication.

Some common technologies and protocols used in ICS plant floor networking include:

- Ethernet/IP
- PROFINET
- Modbus TCP/IP
- DeviceNet
- CIP (Common Industrial Protocol)
- PTP (Precision Time Protocol).



Back to TOC

By implementing robust and secure plant floor networking technologies, industrial organizations can optimize their operations, improve productivity and ensure the safety and reliability of their manufacturing processes.

Types of industrial networks

Ethernet/IP: Utilizes standard Ethernet technology for high-speed communication and seamless integration with devices.

PROFINET: A powerful, open Industrial Ethernet standard providing real-time communication and flexibility.

Modbus TCP/IP: A widely used protocol for connecting industrial devices over Ethernet.

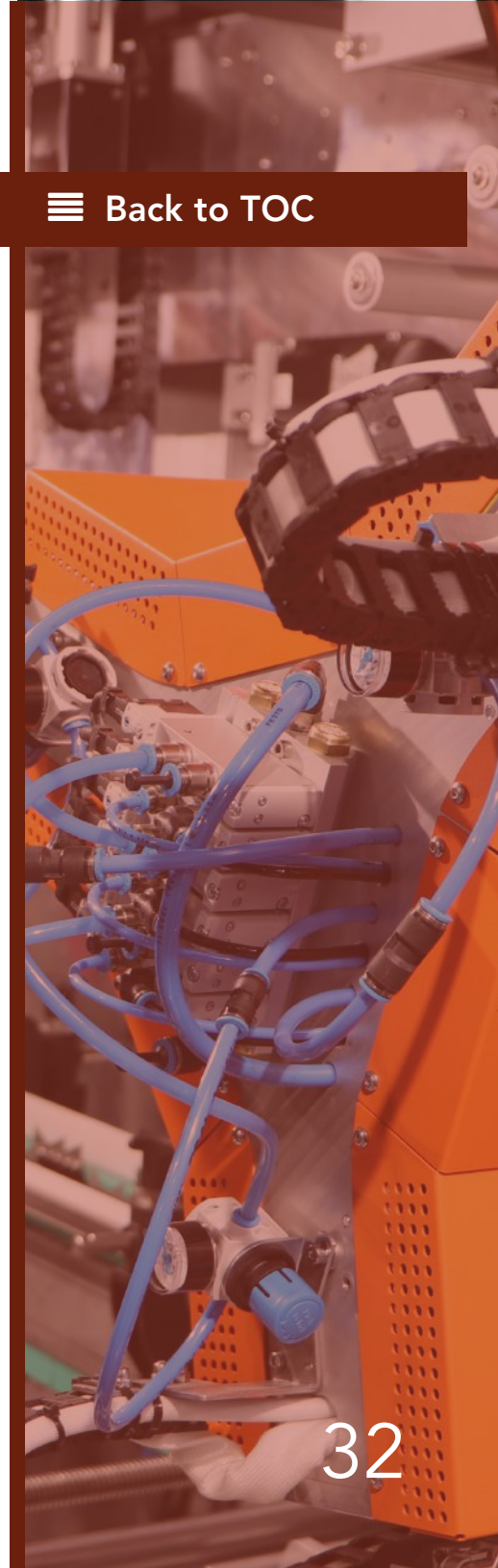
DeviceNet: An industrial network protocol designed for connecting simple devices and sensors in a network.

Components of industrial networks

PLCs (programmable logic controllers): Powerful industrial computers that control and automate various processes in manufacturing.

HMI (human machine interface): Graphical interfaces that allow operators to monitor and interact with industrial machinery and systems.

SCADA (supervisory control and data acquisition): Control systems that gather and analyze real-time data from industrial processes for monitoring and control.



Back to TOC

Industrial ethernet switches: Specialized switches for industrial environments that provide reliable and efficient network connectivity.

Industrial Ethernet cabling: Whether it is fiber or copper, the horizontal and structured network cabling, patch panels and patch cables provide that provide the passive network infrastructure for a reliable system.

Benefits of industrial networking

Improved productivity: Streamlined operations and efficient communication result in increased productivity and output.

Reduced downtime: Proactive monitoring and predictive maintenance minimize unplanned downtime.

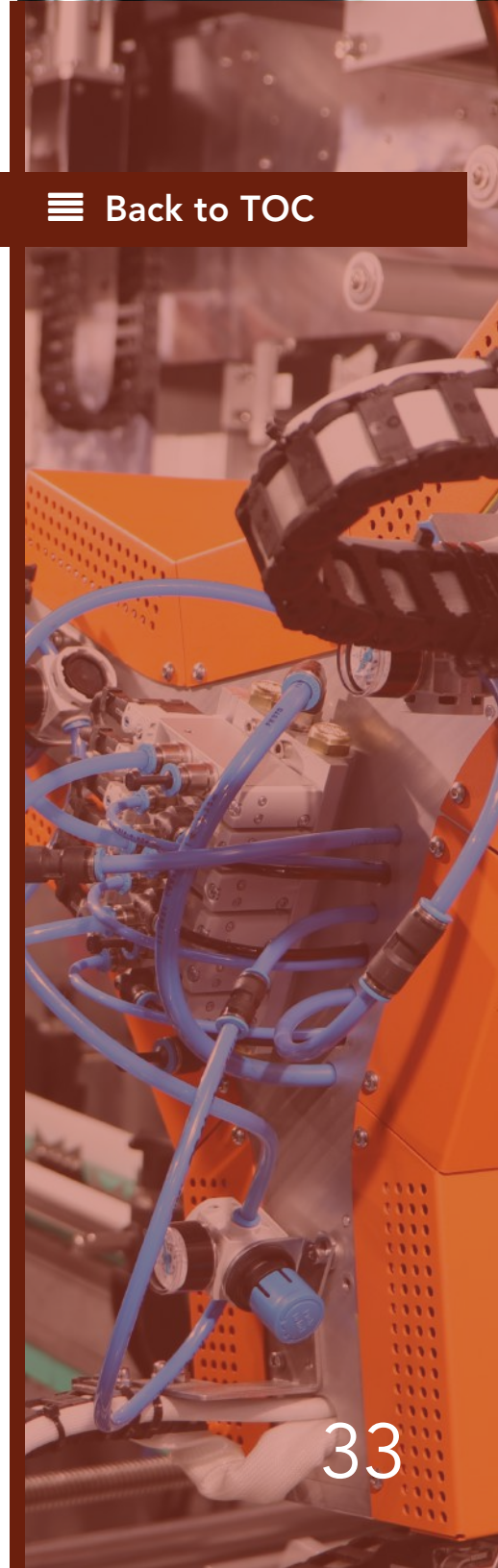
Enhanced communication and data sharing: Real-time data sharing between devices and systems enables better collaboration and informed decision-making.

Best practices for industrial network design

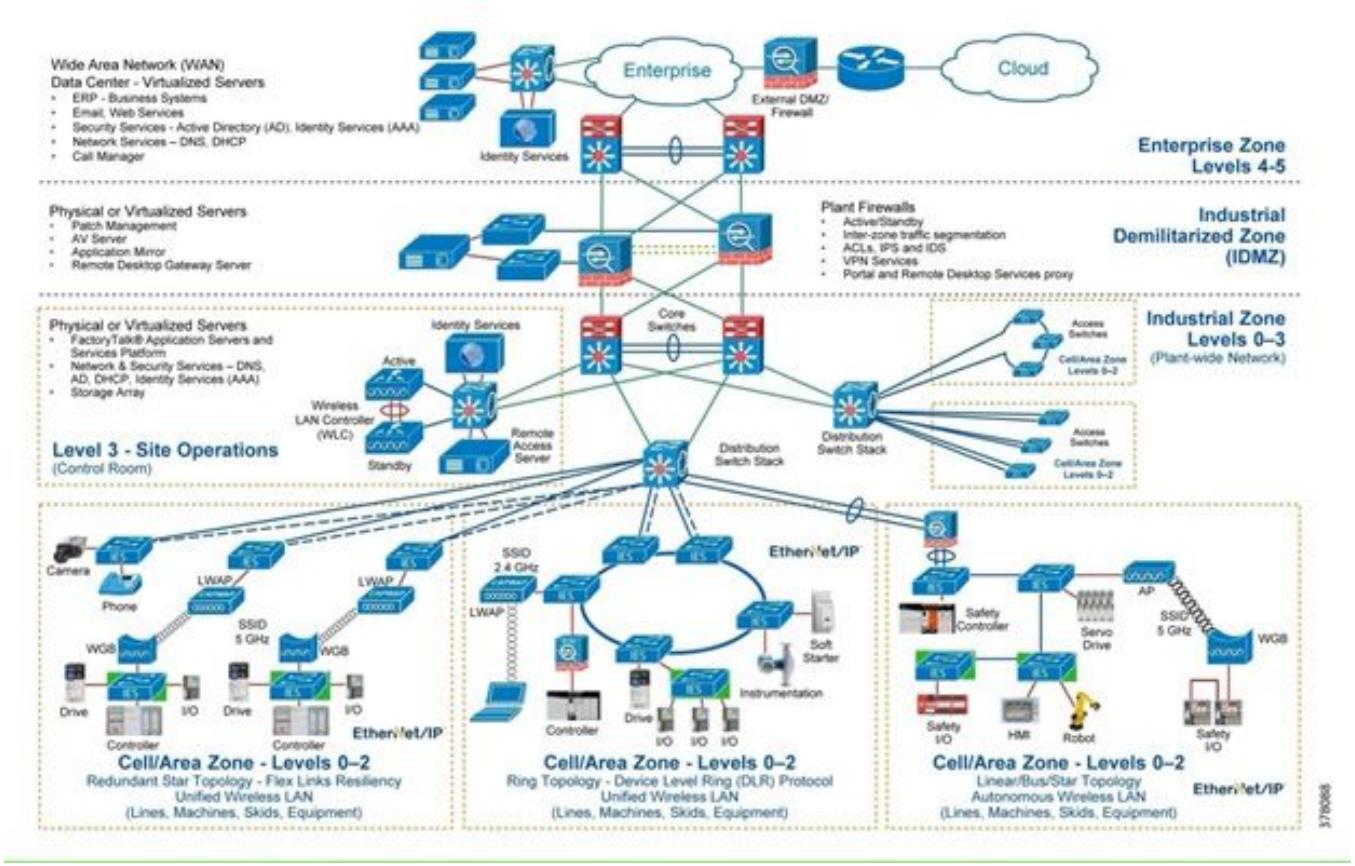
Network segmentation: Dividing the network into logical segments ensures stability, security and proper traffic management.

Redundancy and fault tolerance: Implementing backup systems and redundant paths to minimize the impact of failures.

Security measures: Robust cybersecurity protocols and strategies to protect networks and sensitive industrial data from threats. Use a defense-in-depth approach to align



Back to TOC



Cisco and Rockwell Automation's Converged Plantwide Ethernet (CPwE) model provides a scalable and secure network infrastructure guide for industrial applications.

with industrial security standards such as IEC-62443 (formerly ISA99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

Cisco and Rockwell Automation CPwE model: Converged Plantwide Ethernet (CPwE) includes comprehensive network architectures developed by Cisco and Rockwell Automation. It provides a scalable and secure network infrastructure guide for industrial applications, integrating various automation and control systems. CPwE incor-

Back to TOC

porates the best practices mentioned above, along with additional guidelines specific to Rockwell Automation products and technologies.

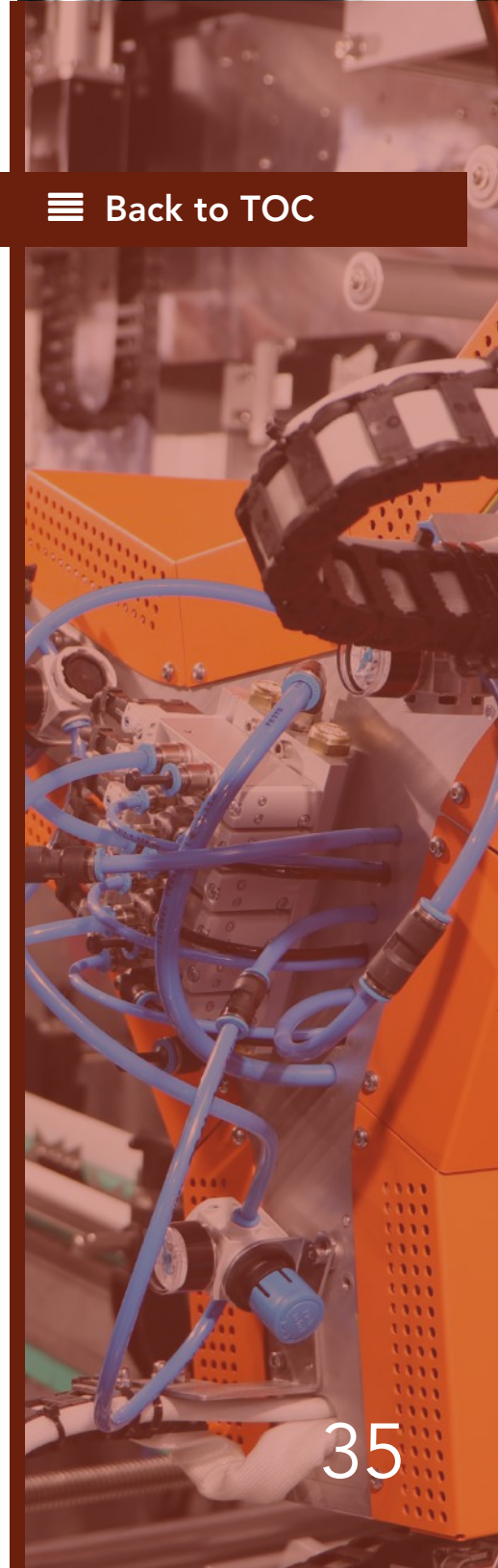
Examples of industrial network implementations

Here are a few examples of industrial networks the challenges and benefits they offer for industrial automation systems. From the oil and gas industry to pharmaceuticals, automotive, and food and beverage, these are real-life design scenarios that have been actualized. From streamlined network infrastructure to improved scalability and security, modern industrial network best practices are revolutionizing the way industries operate.

Automotive manufacturing: Industrial networks are widely used in automotive manufacturing plants to integrate different systems and devices, such as robots, conveyors and quality control systems. It ensures seamless communication and coordination between these components, improving overall efficiency and productivity.

Food and beverage industry: Industrial networks are implemented in food and beverage production facilities to connect various equipment, such as mixing machines, packaging lines and quality inspection systems. This enables real-time monitoring and control, enhancing product quality and safety.

Oil and gas sector: Industrial networks are utilized in oil and gas refineries and production facilities to integrate critical systems, including pumps, valves and safety devices. It enables efficient monitoring, control and optimization of these processes, ensuring safe and reliable operations.



Back to TOC

Design example 1: Industrial ethernet network for the oil and gas industry

The challenge: Oil and gas operations require resilient and highly secure communication networks to ensure smooth production and safety.

The solution: Design a secure, scalable and reliable Ethernet network infrastructure using redundant devices and cabling paths that supports critical communication and control systems.

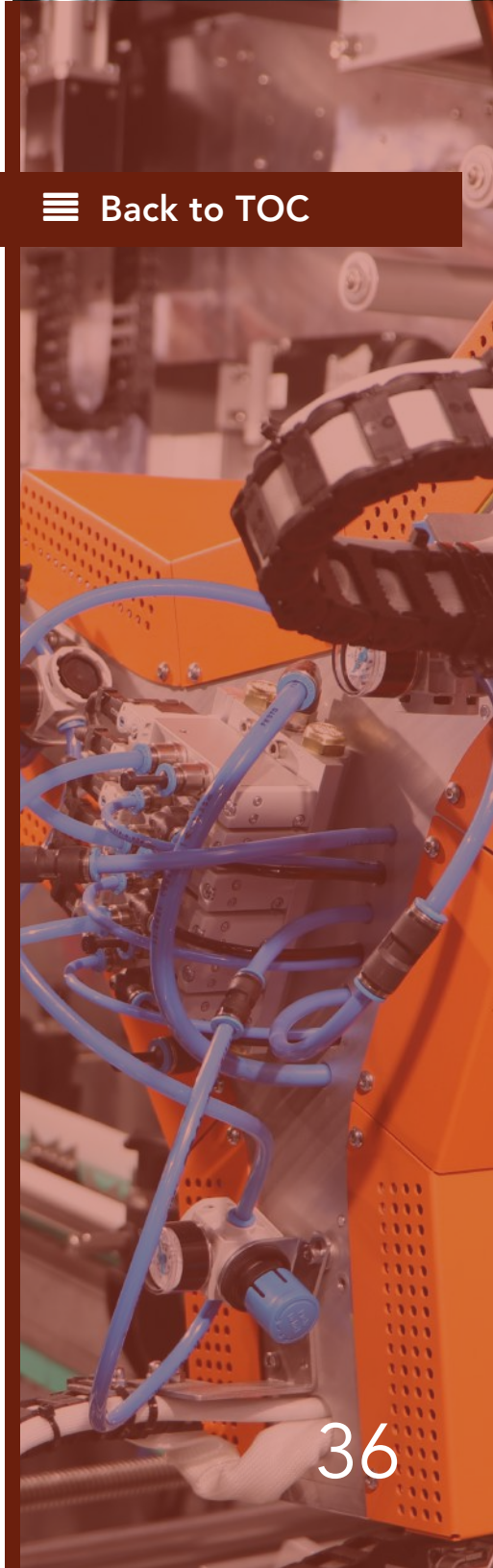
The benefits: Improved operational efficiency, enhanced safety,and reduced downtime contribute to increased profitability for oil and gas companies.

Design example 2: Industrial ethernet network for the pharmaceutical industry

The challenge: Pharmaceutical facilities struggle with network complexity and the need to comply with strict regulatory requirements.

The solution: Design a physically secure network architecture, with sophisticated monitoring capabilities, and verifiable change control to ensure compliance with industry regulations like FDA 21 CFR Part 11.

The benefits: Improved data integrity, simplified network management and enhanced regulatory compliance elevate pharmaceutical companies' operational efficiency.



Back to TOC

Design example 3: Industrial ethernet network for the automotive industry

Efficient production processes: Industrial Ethernet networks enable seamless integration of manufacturing systems, optimizing production efficiency and reducing costs.

Real-time operational insights: Industrial Ethernet networks empower automotive manufacturers to collect data from OEM equipment and production lines with valuable insights for better decision-making.

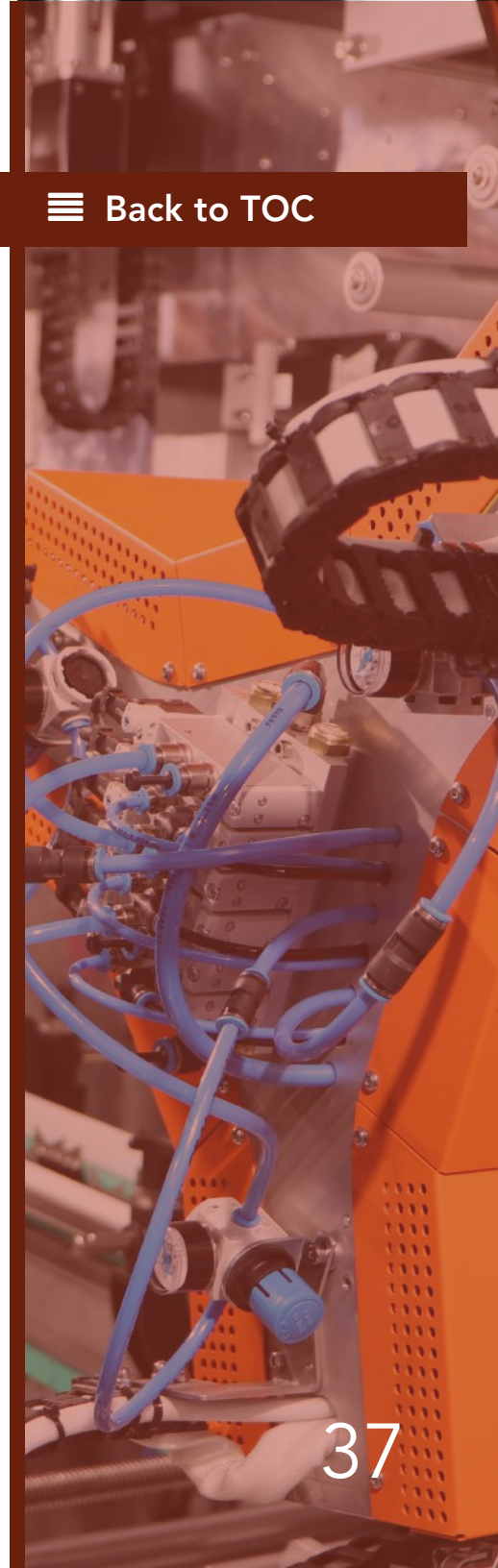
Scalability for future growth: Modern Industrial Ethernet networks accommodate the evolving needs of the automotive industry, allowing for easy integration of new technologies and systems.

Key takeaways from Industrial Ethernet network design examples

Unleash operational efficiency: Industrial Ethernet networks empower businesses to optimize their operations, reduce downtime and enhance productivity.

Enhance network security: Industrial Ethernet networks allow for robust cybersecurity measures to be put in place to protect critical industrial systems from potential threats.

Enable scalability and future-proofing: Industrial Ethernet networks allow for easy integration of new technologies and adaptability to evolving industry demands.



Back to TOC

Differences between enterprise networking and industrial networking

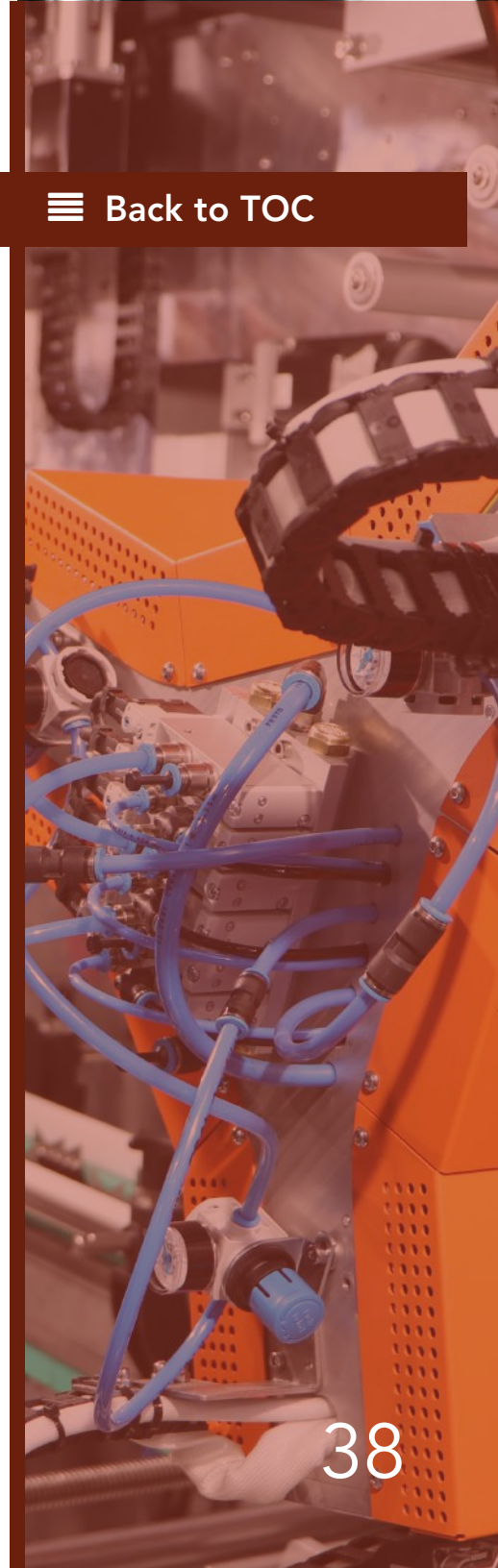
Enterprise Networking refers to the networking infrastructure and systems used by businesses and organizations for their internal communication and data exchange. It typically involves connecting office devices, such as computers, printers and servers to provide access to shared resources and services.

On the other hand, industrial networking focuses on networking solutions specifically designed for industrial environments such as manufacturing plants, oil refineries and power generation facilities. Industrial networks are built to support the unique requirements of industrial automation and control systems, including real-time communication, reliability and cybersecurity.

While both enterprise networking and industrial networking share some common networking principles such as network segmentation and security measures, industrial networking places a greater emphasis on factors like determinism, robustness and compatibility with industrial protocols and standards.

Industrial networks often require specialized networking equipment and technologies that can handle the harsh conditions and stringent demands of industrial applications, such as high temperatures, electrical noise and mission-critical operations.

By adopting best practices for industrial network design, organizations can ensure the availability, integrity and security of their industrial networks, enabling smooth operation of critical industrial processes and systems.



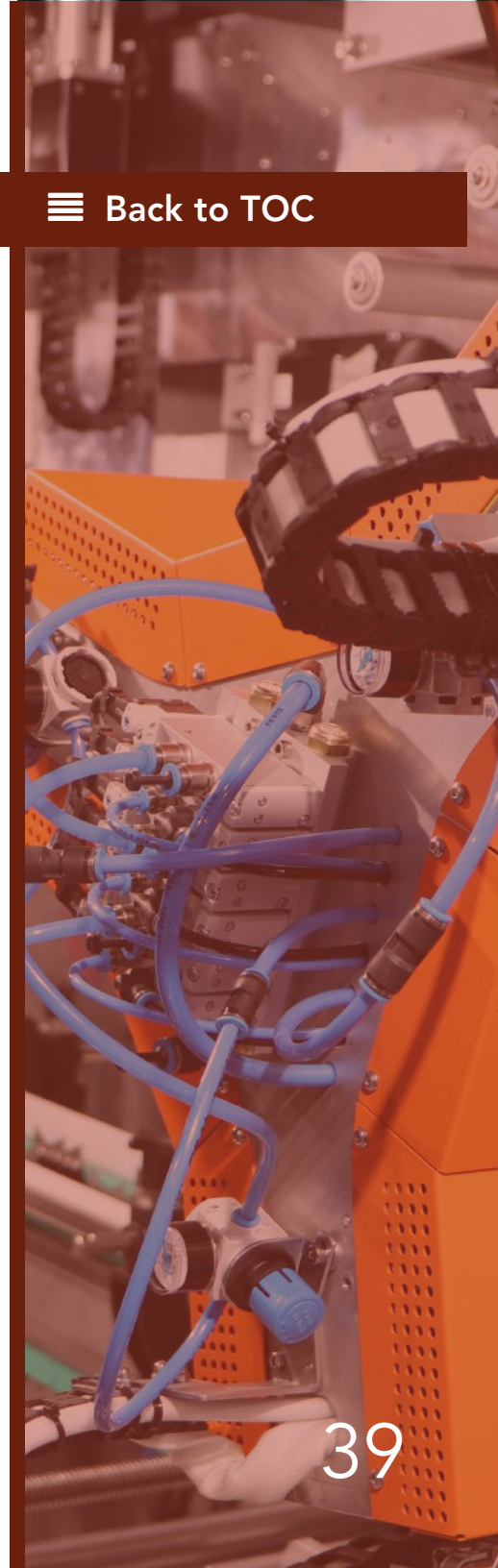
Back to TOC

Conclusion

Industrial networking is the backbone of modern manufacturing, enabling efficient operations, real-time monitoring and data-driven decision-making. By understanding these types, components and best practices, you can harness the power of industrial networking to optimize productivity and drive success in your organization.

Nick Roe

Nick Roe *is a Senior Engineer with Matrix Technologies. Bachelor of Science from Purdue University in Computer Network Engineering. Working majority of the 15 years engineering in the field in the Automotive Industry and with a Rockwell Automation Distributor. Currently holding my CCNA, CCNP from Cisco, Plant wide converged ICS design and Machine level network design from Rockwell Automation, pairing this with the Panduit physical network design. He can be reached at nmroe@matrixti.com.*



How to use TSN to improve machine design performance, precision

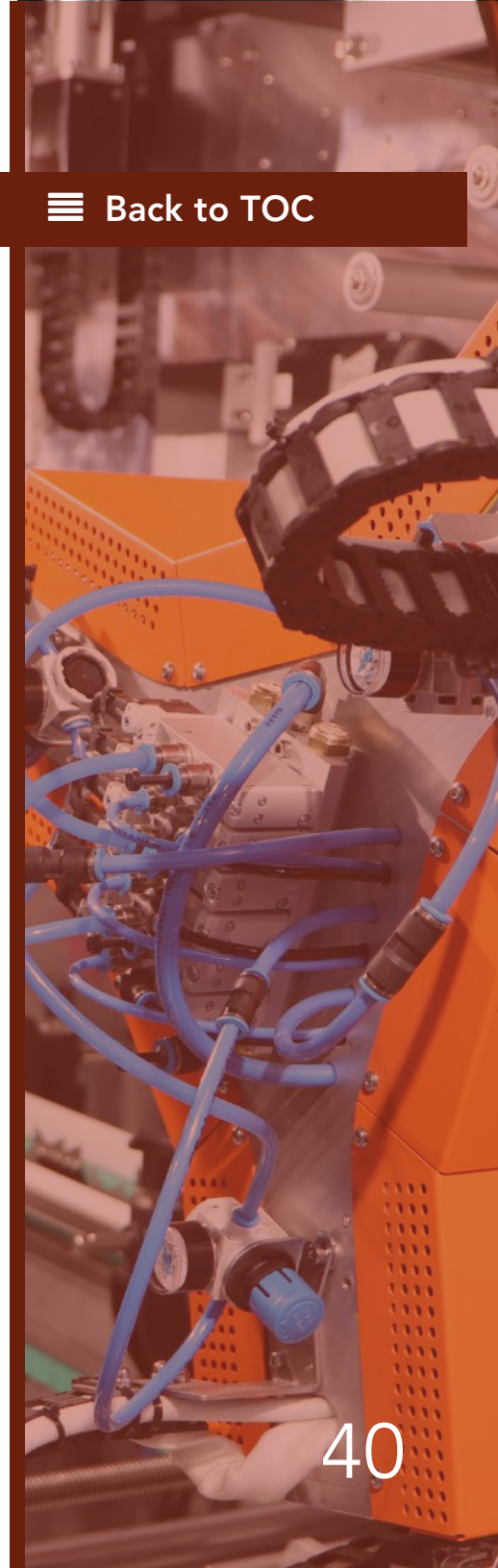
An original equipment manufacturer (OEM) that specializes in pad printing and hot stamping machines used time-sensitive networking (TSN) to improve overall performance, accuracy and precision for its motion control applications.

Printing and stamping are among the most demanding motion control applications, as they use multiple axes that need high levels of synchronization to operate effectively at extraordinary speed with high repeatability. When looking at communications requirements, these motion control functions need to be supported by deterministic, real-time communications across multiple axes.

At the same time, end users are demanding ever-more high-speed, advanced machines, meaning that implementing a network technology that can achieve this is key. Time-sensitive networking (TSN) can address these requirements and offers future benefits. These include the possibility of using a converged network architecture to simplify machine design, reduce costs and decrease time to market. This is enabled by multiple kinds of traffic being combined, rather than using separate networks as in the past.

Poland-based original equipment manufacturer (OEM) Keller was keen to adopt automation devices and industrial communications solutions. When machine designers there wanted to develop a universal, modular machine for direct, multi-color printing on cylindrical goods, such as bottles, they asked an automation vendor for help. The team set out to identify the most suitable options to create the best machine to support future ambitions and customers' needs.

Back to TOC



Back to TOC

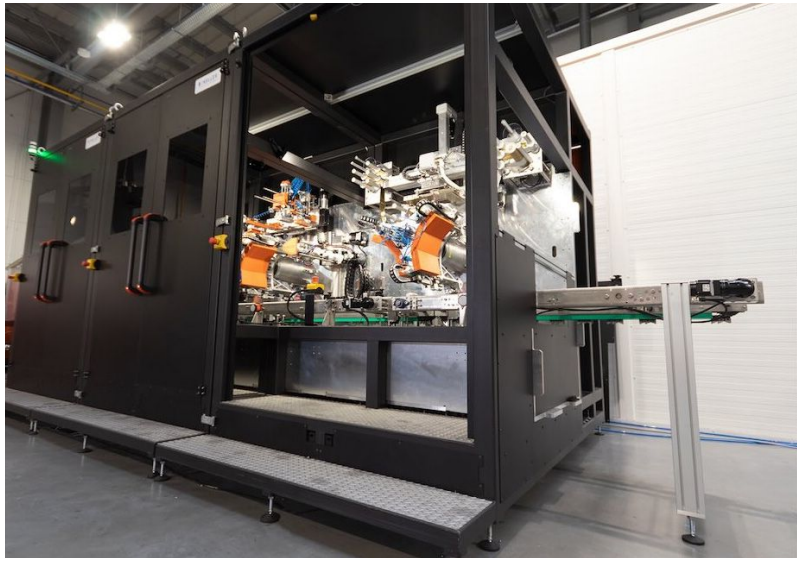


Figure 1: In its drive to serve the market with state-of-the-art printing technologies, Keller was keen to adopt the most promising, innovative automation devices and industrial communications solutions. To develop a universal, modular machine for direct, multi-color printing on cylindrical goods, such as bottles, machine designers asked Mitsubishi Electric for help. Courtesy: CC-Link Partner Association (CLPA)

Automation system uses industrial Ethernet with TSN

The unique setup developed by the companies, which combines screen printing and hot stamping on cylindrical objects, used an industrial automation system that incorporates CC-Link IE TSN network technology. This includes servos controlled by a programmable logic controller (PLC).

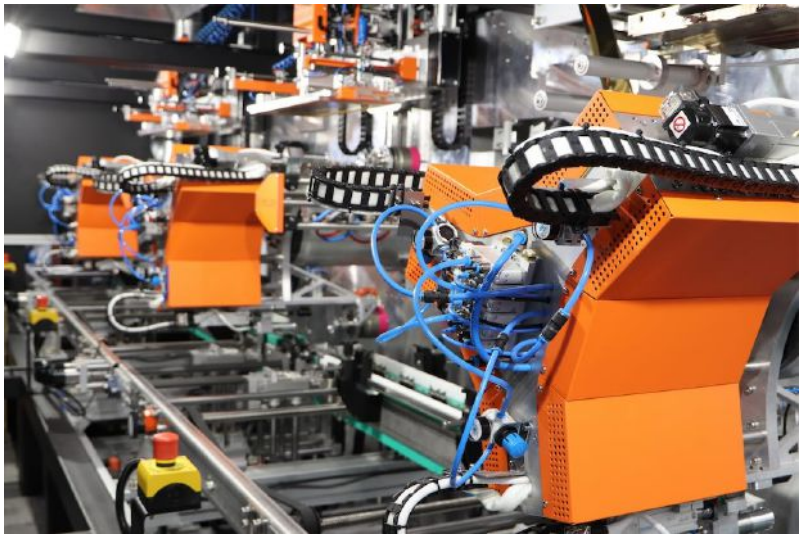
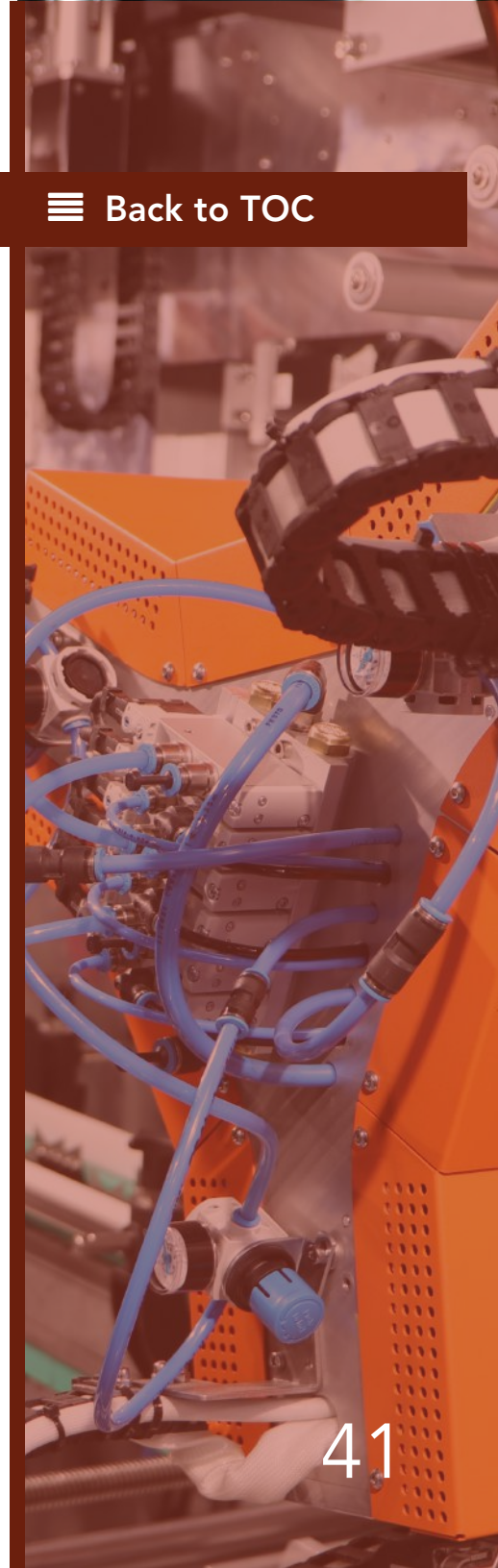


Figure 2: Keller wanted a really advanced and ambitious setup, with 20 axes per color head and a total of 65 servo drives, in addition to 18 auxiliary virtual axes. Courtesy: CC-Link Partner Association (CLPA)

They used a combination of TSN and gigabit bandwidth to offer Keller a system that could provide fully deterministic control of up to 128 axes. It also enabled extreme synchronization



Back to TOC

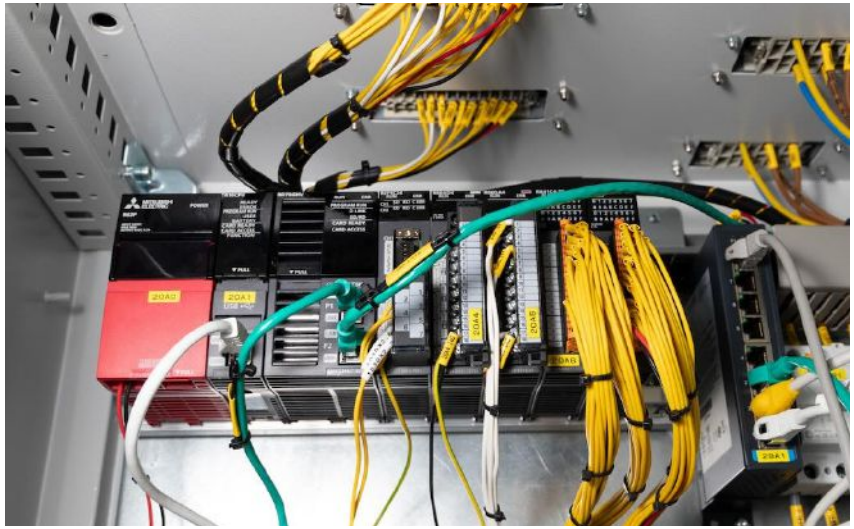


Figure 3: Keller's unique setup, which combines screen printing and hot stamping on cylindrical objects, utilizes an industrial automation system that incorporates CC-Link IE TSN network technology to offer ground-breaking performance. Courtesy: CC-Link Partner Association (CLPA)

accuracy in the order of micro-seconds. This helped ensure the machine can deliver prints of consistently high quality while maintaining a rate of 3,000 units per hour, with a plan to reach 3,600.

Michal Cydzik, product manager for control systems at Mitsubi-shi Electric, said, "What Keller wanted was a really advanced and ambitious setup, with 20 axes per color head and a total of 65 drives, in addition to 18 auxiliary virtual axes. CC-Link IE TSN provided the necessary determinism, capacity and bandwidth required to handle this while deliver-ing the performance Keller needed."

Figure 4: The setup includes Mitsubishi Electric's Melsec MR-J5 servos controlled by an iQ-R series PLC,A which are all compatible with CC-Link IE TSN. Courtesy: CC-Link Partner Association (CLPA)

Back to TOC

Figure 5: CC-Link IE TSN network technology offers Keller a system that could provide deterministic control of up to 128 axes. It also enabled extreme synchronization accuracy in the order of microseconds. This ensures that the machine can deliver prints of consistently high quality while maintaining a rate of 3,000 units per hour, with a plan to reach 3,600. Courtesy: CC-Link Partner Association (CLPA)

Opening the door to future-oriented manufacturing

The resulting machine offers end users a modular, versatile solution that delivers enhanced productivity, cost-effectiveness, flexibility, and high print quality. Moreover, the setup is scalable, as it can incorporate up to eight colors (and their necessary axes) and is reconfigurable. It can be extended to include additional printing modules to deliver a highly integrated system. The result was an industry leading machine enabled by an open industrial Ethernet technology.

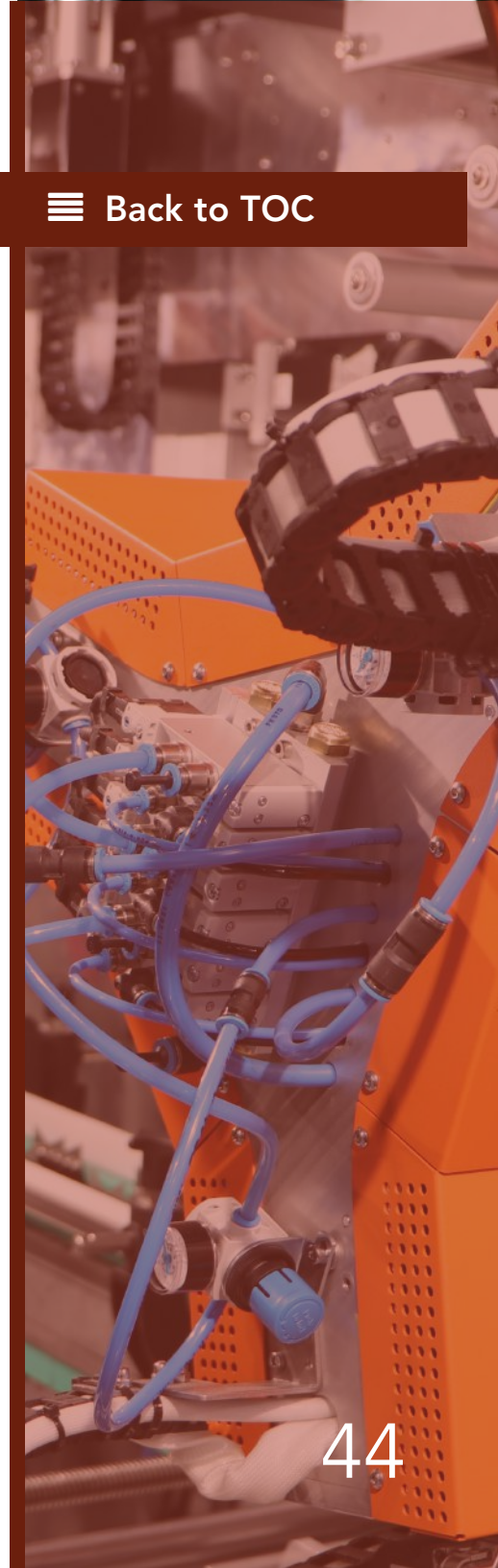
Figure 6: The resulting machine offers end users a modular, versatile solution that delivers enhanced productivity, cost-effectiveness, flexibility and high print quality. Courtesy: CC-Link Partner Association (CLPA)

Back to TOC

Thomas Burke, global strategic advisor for the CLPA Americas, said, "It's really exciting to see how Keller is using CC-Link IE TSN to stay ahead in its field. Keller has tapped into the technology's full range of features to create efficient, high-performance solutions for its customers. What's more, it's looking ahead by planning to add new features like vision systems, all on the same network. This approach not only simplifies the design process but also cuts costs and speeds up time-to-market. Keller's work is a great example of how CC-Link IE TSN is making a real difference in various industries."

Thomas Burke

Thomas Burke *is global strategic adviser for CC-Link Partner Association (CLPA). He is the founder of the OPC Foundation and spent much of his career developing software, hardware and firmware for industrial automation, including at Rockwell Automation. CC-Link Partner Association (CLPA) is a CFE Media and Technology content partner.*



Important technological developments to watch for 6G

Several requirements are needed to be considered when designing a 6G radio to further improve link range as well as enhance data rate as research begins.

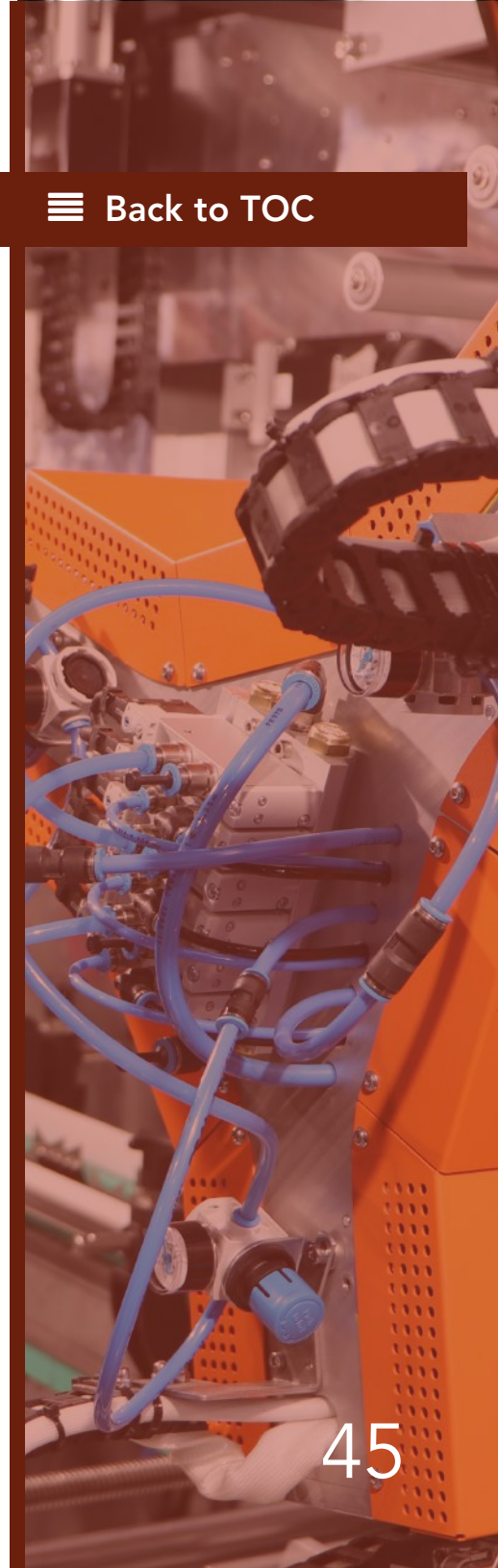
While 5G is still starting out and getting a foothold, 6G research has already begun. That begs the question: What exactly is 6G, though, and what are the emerging areas to watch?

It starts at the most basic level – the frequency band. In 5G, sub-6 GHz (3.5 to 6 GHz) and millimeter wave (mmWave, 24 – 100 GHz) bands are the two new bands among the spectrum covered. In 6G, the frequency ranges under consideration include 7 to 20 GHz frequency band, W-band (above 75 to 110 GHz), D-band (110 to 175 GHz), bands between 275 and 300 GHz, and in THz range (0.3 to 10 THz). The bands between 7 and 20 GHz are considered because of the need for coverage that will enable mobile and "on the go" applications for numerous 6G use cases.

The W and D bands are of interest for both 6G access and Xhaul (e.g. fronthaul, backhaul) networks. A solution that meets the objectives of both services is to be considered. As of September 2022, worldwide spectrum allocations do not go beyond 275 GHz. Nevertheless, frequency bands in the range 275-450 GHz have been identified for the implementation of land mobile and fixed service applications, as well as radio astronomy and Earth exploration-satellite service and space research service in the range 275 to 1,000 GHz.

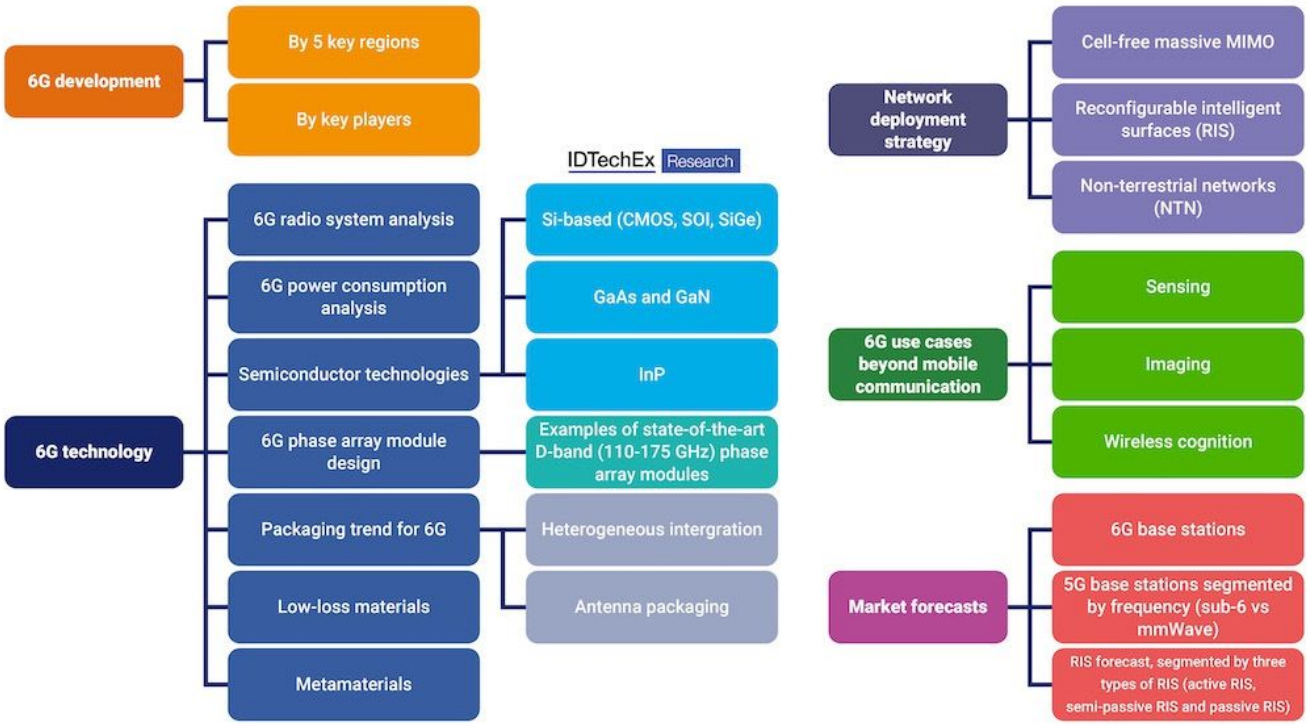
What can 6G do and what are its challenges?

By exploiting the large bandwidth in the THz frequency band, 6G is expected to enable 1 Tbps data rate. However, this rate is very challenging to achieve as a large



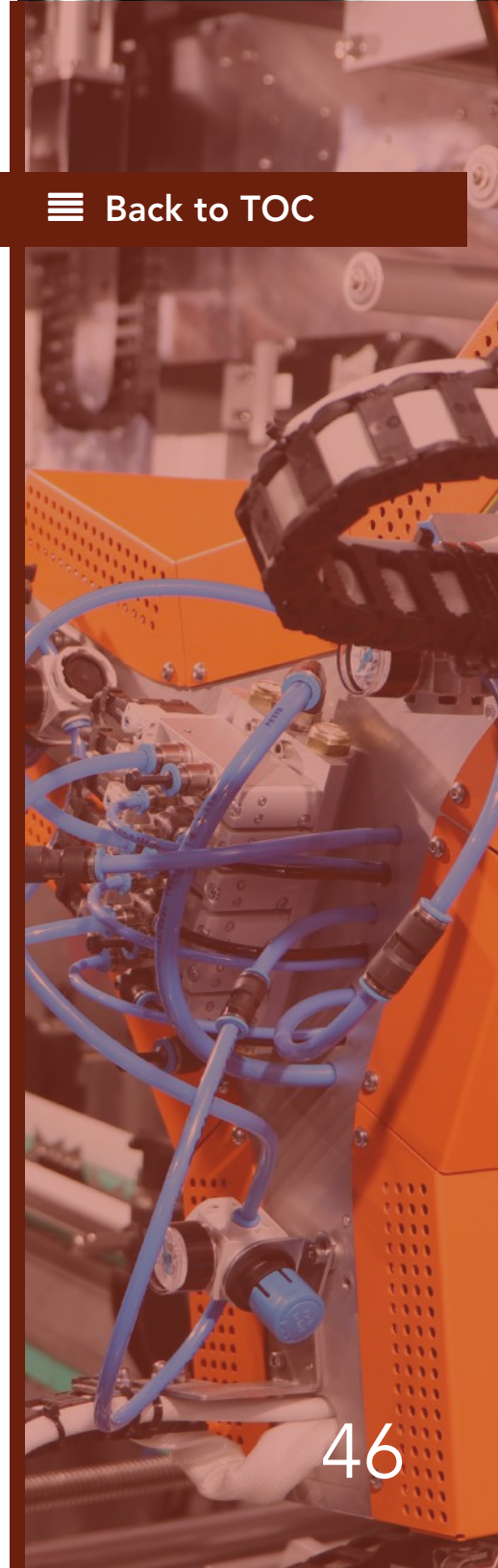
Back to TOC

Back to TOC

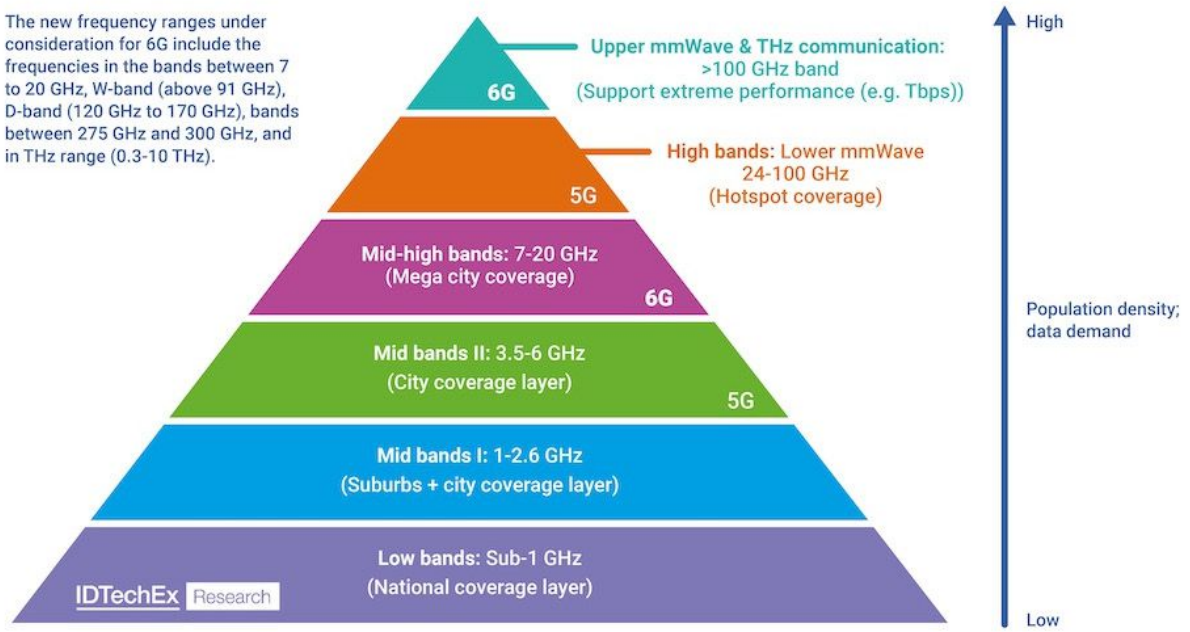


Key areas of coverage in the IDTechEx report "6G Market 2023-2043: Technology, Trends, Forecasts, Players". Courtesy: IDTechEx

continuous bandwidth is required, but in reality, the bandwidths that are available for use are limited and split over different bands. Another aspect is that spectral efficiency makes a direct trade-off with the required signal-to-noise ratio (SNR) for detection. The higher the required SNR, the shorter the respective range becomes due to transmitted power limitations at high frequencies as well as added noise. As an example, Samsung's state-of-the-art D-band phase array transmitter prototype currently demonstrates the furthest travel distance of 120m but only achieves 2.3 Gbps. Other groups show higher data rates, but the over-the-air travel distance is only at centimeter level.

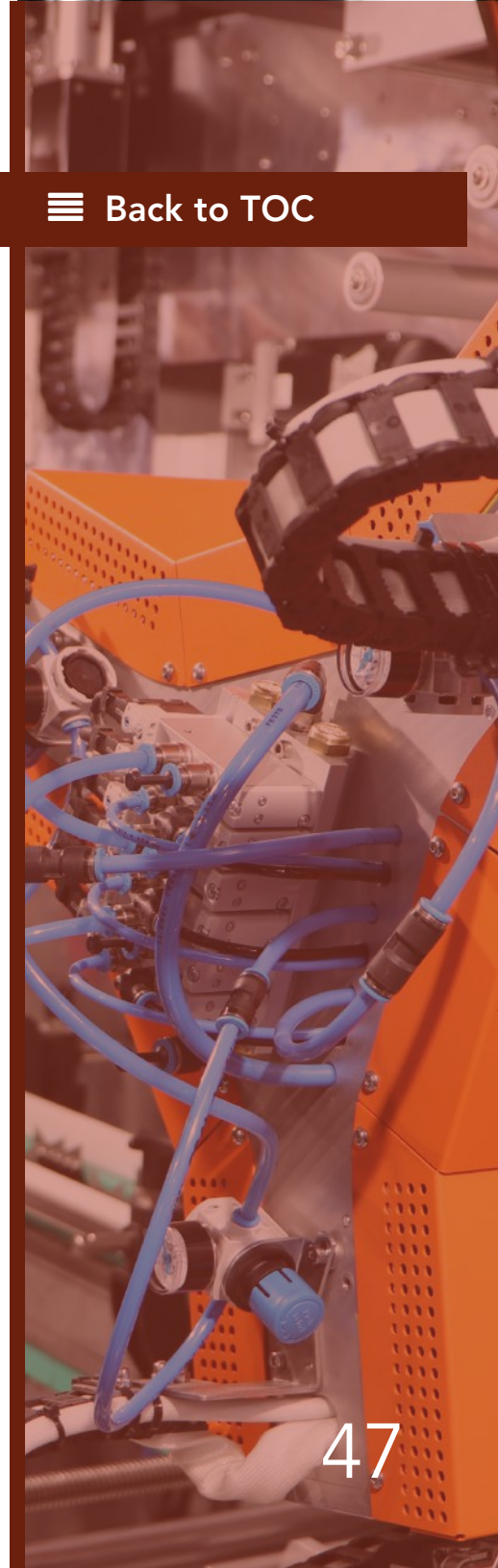


Back to TOC



Overview of 6G spectrum deployment strategy. Note that even though by definition the THz band runs from 300 GHz to 10 THz, telecom professionals have found it simpler to classify beyond-100 GHz applications as THz communications. Courtesy: IDTechEx – "6G Market 2023-2043: Technology, Trends, Forecasts, Players"

To further improve link range as well as enhance data rate, several requirements are needed to be considered when designing a 6G radio. For example, selecting appropriate semiconductors to boost link range is critical, pick low-loss materials with a small dielectric constant and tan loss to prevent substantial transmission loss. To further reduce transmission loss, a new packaging strategy that tightly integrates RF components with antennas is required. However, one must remember that as devices get increasingly compact, power and thermal management become even more critical.



Back to TOC

In addition to device design, network deployment strategy is also a crucial area to research in order to address NLOS and power consumption challenges. Establishing a heterogeneous smart electromagnetic (EM) environment, for example, is being investigated, utilizing a wide range of technologies, such as reconfigurable intelligent surfaces (RIS) or repeaters.

Overview of 6G spectrum deployment strategy. Note that even though by definition the THz band runs from 300 GHz to 10 THz, telecom professionals have found it simpler to classify beyond-100 GHz applications as THz communications. Courtesy: IDTechEx - "6G Market 2023-2043: Technology, Trends, Forecasts, Players"

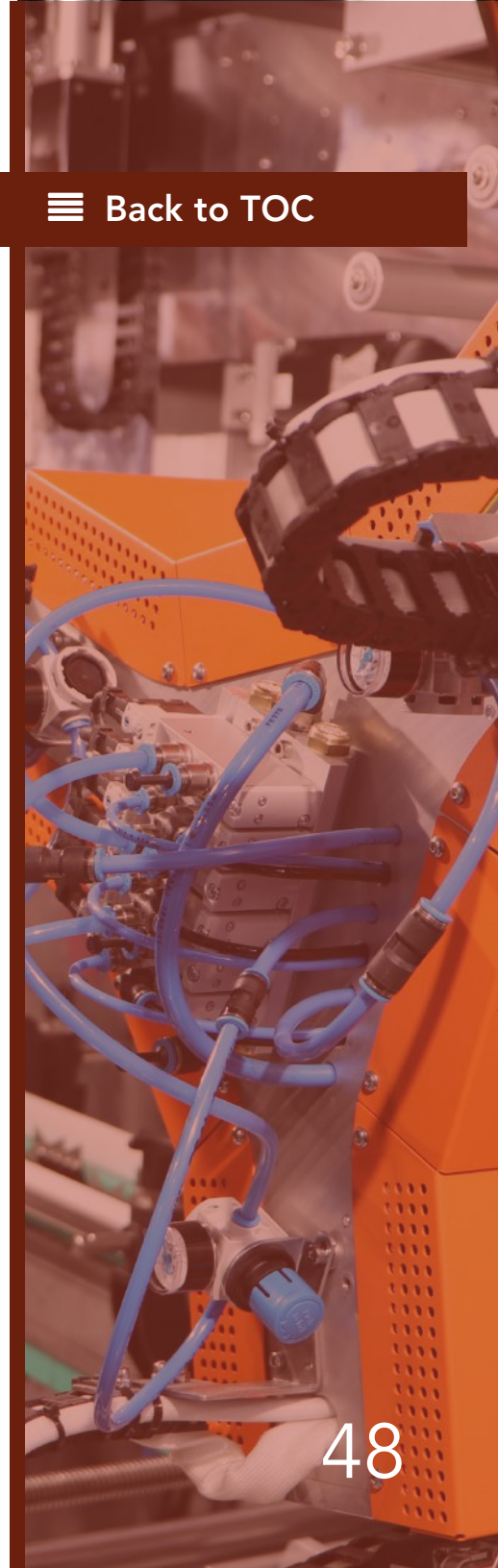
Potential applications for 6G

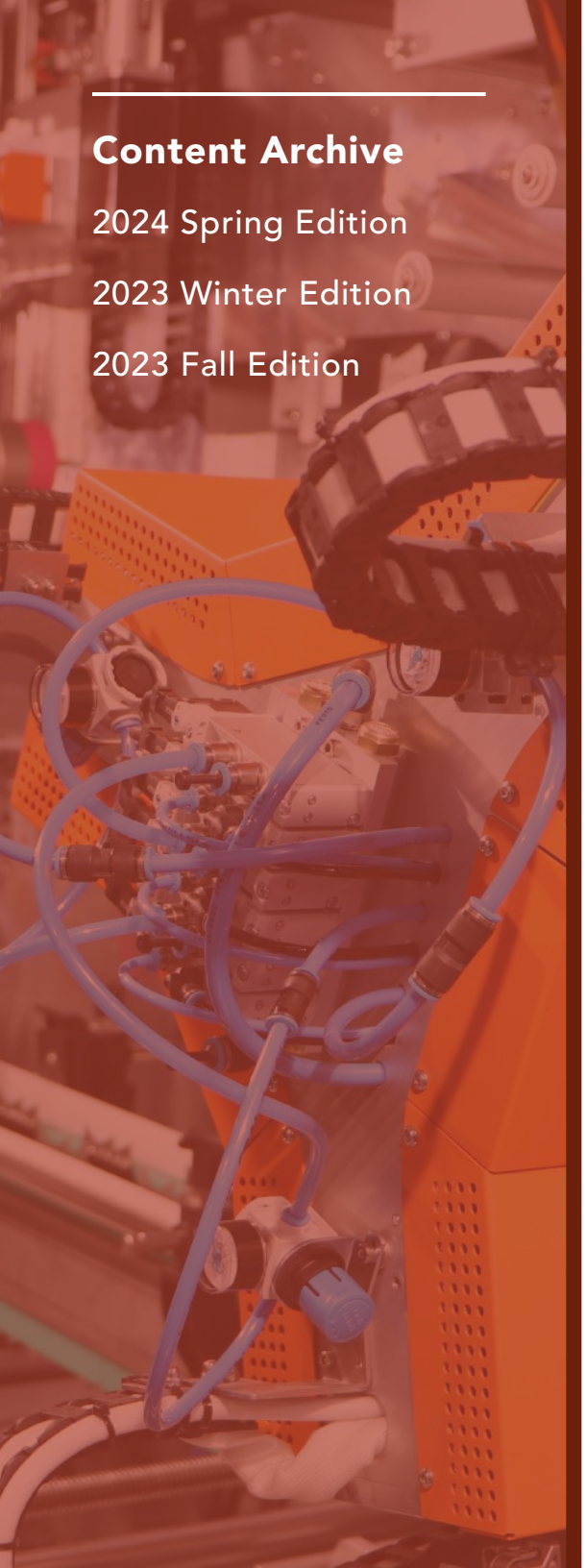
One significant change of 6G to previous communication generations is that it will now include non-terrestrial networks, which is a key development item in 6G that enables conventional 2D network architectures to function in 3D space. Low-altitude platforms (LAPs), high-altitude platforms (HAPs), unmanned aerial vehicles (UAVs) and satellites are examples of non-terrestrial networks (NTNs). China sent the world's first 6G satellite in November 2020. This year, Huawei tested the NTN 6G networks using low earth orbit (LEO) satellites. More and more activities in this area show that NTN networks will for sure be a key development trend.

Despite communications, 6G is also expected to tap into the world of sensing, imaging, wireless cognition, and precise positioning. Apple patented its THz sensor technology for gas sensing and imaging in iDevice. Huawei also tested several integrated sensing and communication (ISAC) prototypes. Many more studies and trials are underway to fully leverage the potential of 6G THz frequency bands.

Yu-Han Chang

Dr. Yu-Han Chang, *senior technology analyst at IDTechEx.*





Content Archive

2024 Spring Edition

2023 Winter Edition

2023 Fall Edition

Industrial Networking

Thank you for visiting the Industrial Networking eBook!

If you have any questions or feedback about the contents in this eBook, please contact CFE Media at *customerservice@cfemedia.com*

We would love to hear from you!