EXPERTS' ANSWERS TO

Common Questions About Future-Proof Connectivity

The “future-proof” plant floor is prepared for whatever tomorrow has in store—whether that’s new assets, new software, expansion, or other anticipated and unanticipated advancements.

Future-proofing your plant floor—and equipping players across the enterprise for what that entails—is no small feat, and one you shouldn’t have to tackle alone.

What should your future-proof plant floor look like—and what does it take to get there?

Continue reading for valuable expert insights on four common future-proofing questions.

Question #1:

WHAT IS OPC UA?

OPC Tunneling with OPC Unified Architecture (OPC UA)

For most businesses, data consolidation, sharing, and visibility across the enterprise is a top priority. This is not necessarily a new IIoT (Industrial Internet of Things) initiative. OPC Classic (OPC DA) enabled many organizations to achieve these objectives. However, there have been several obstacles caused by limitations in the Microsoft Component Object Model (COM) and Distributed Component Object Model (DCOM). Despite being widely adopted, these two options are limited in the usability and security options required by today's industrial automation and distributed operation environments.

The Latest and Most Capable OPC Specification

Although there are a number of proprietary solutions that can be used for industrial communications and data access from industrial environments, all of them come with inherent challenges because they do not represent a widely adopted industry standard. Fortunately, OPC Unified Architecture (OPC UA), the latest generation of OPC, has become the "go to" standard for these types of projects.

Released in 2008, it is certainly not a new standard, and it has been tested and used in countless applications where it is now considered a "hardened" standard. It is accepted and supported by the majority of industrial vendors and service providers, and provides a reliable cross-platform framework for accessing real-time and historical data and events as well as information modeling. Specific to the challenges mentioned above, OPC UA also enables secure communications for remote connections.

OPC UA was chosen by the closely watched Open Group Open Process Automation Forum (OPAF) in April 2019 as the foundation to their O-PAS™ standard. Many other examples exist where OPC UA has been selected as the standard of choice for various industry forum information models and vendor solutions.

OPC UA incorporates data encryption with RSA standards and authentication based on the x509 Certificate standard. This has been proven to make it firewall friendly, and allows communications within local automation environments, across the enterprise, and through public network segments with high security and performance.

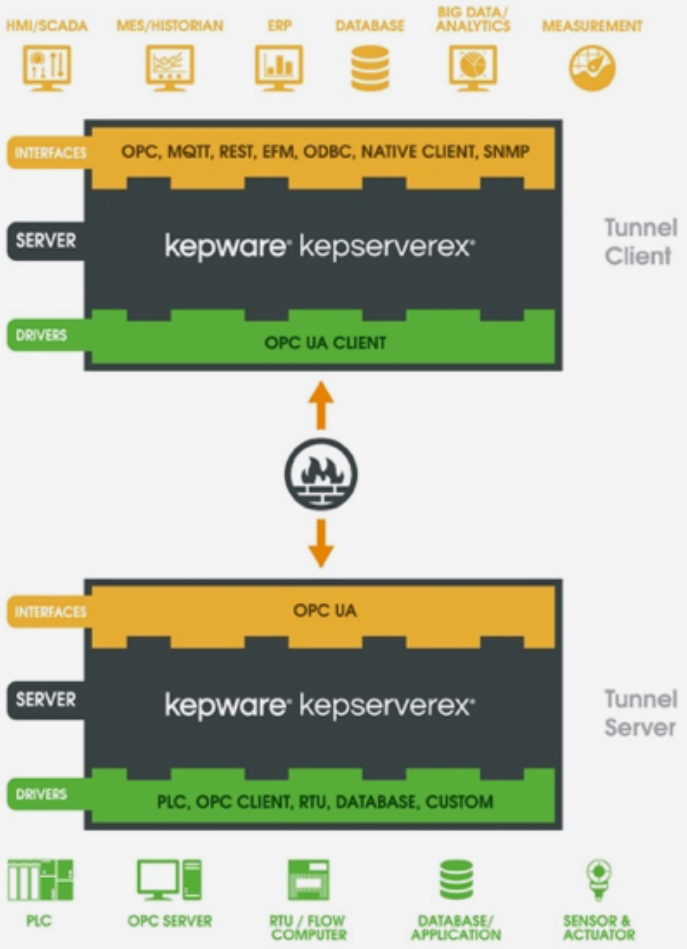
PTC acknowledges OPC UA's advantages, and has leveraged the OPC UA Client Driver and the OPC UA Server interface KEPServerEX® to provide a powerful OPC tunneling solution—see graphic for a high-level architecture of how the tunnel is easily created with this combination.

The OPC UA Client Driver for KEPServerEX provides communications to any OPC UA server, allowing data to be transferred securely and reliably. Because KEPServerEX is both an OPC Classic and an OPC UA server with both OPC DA and OPC UA Client Drivers, it eliminates the reliance on Microsoft COM and DCOM technology. This also enables OPC Classic implementations to utilize the latest OPC UA technology.

Real-World Applications

PTC clients have already benefited from the adoption of this new standard. The Municipal Wastewater Treatment Facility for the City of Orlando, Florida required a firewall-friendly, cross-domain communications technology that interoperated with existing OPC Classic systems. After evaluating a number of options, the city chose KEPServerEX with the OPC DA Client Driver and the OPC UA Client Driver to provide secure, bi-directional data access between multiple municipality SCADA systems.

In another industry where cybersecurity is top of mind, the Kepware OPC UA Tunnel solution was selected to be tested by the Oil & Gas Industry Consortium concerned with cybersecurity known as LOGIIC (Linking Oil & Gas Industry to Improve Cybersecurity) as part of their Real-Time Data Transfer (RTDT) Project. The LOGIIC consortium consists of the U.S. Department of Homeland Security and large Oil & Gas companies such as BP, Chevron, Shell, Total and others.



About the Subject Matter Expert

STEPHEN SPONSELLER

Stephen Sponseller is the Kepware Channel Director, Americas at PTC. He came to PTC via the Kepware acquisition, where he started in 2011 to grow Kepware's Oil & Gas business and now leads a team that focuses on Kepware's multiple Channel programs. Starting his career in 1995, Steve has worked in the manufacturing, computer software, industrial automation, and information technology industries, serving a variety of vertical markets. His first software experience was in 1997 when he worked for PTC the first time (when it was known as Parametric Technology Corporation) as a Quality Assurance Engineer. Steve has a Bachelor's degree in Mechanical Engineering from the University of Pittsburgh and a Master's degree in Engineering from Norwich University.

SOURCES:

https://opcfoundation.org/about/opc-technologies/opc-ua/
https://opcfoundation.org/news/press-releases/the-open-group-open-process-automation-forum-o-pas-standard-of-standards-based-on-opc-ua/
https://www.opengroup.org/forum/open-process-automation-forum
https://publications.opengroup.org/p190
https://www.ptc.com/en/products/iiot/thingworx-platform/thingworx-kepware-server
https://www.kepware.com/en-us/products/kepserverex/drivers/opc-ua-client/
https://www.kepware.com/en-us/industries/case-studies/city-orlando-utilizes-opc-tunneling/
https://www.kepware.com/en-us/about/press-releases/logiic-initiative-oil-gas-cybersecurity/
https://www.automationfederation.org/Logiic/logiic
https://www.automationfederation.org/Logiic/LogiicProjects

Question #2:

HOW CAN WE IMPLEMENT A REDUNDANT CONNECTIVITY SOLUTION?

Building Highly-Available Automated Systems with Redundancy

Redundancy is something that every company strives for in their automated process, but is one of the hardest functionalities to implement successfully. Companies across the globe are working with solutions comprised of disparate devices, HMI/SCADA systems, historians, and MES systems—each of which has varying support for integrating a redundant solution.

By leveraging Kepware's portfolio of products, redundancy is possible even for customers with unique environments. One of the tools we provide is Media Level Redundancy, an advanced option for KEPServerEX that is supported in Master drivers and drivers that do not require third-party interface cards or library files. Accessed in KEPServerEX through the driver's Device **Properties** | **Redundancy** tab, Media Level Redundancy (MLR) was enhanced in the June 2015 release of KEPServerEX version 5.18.

Media Level Redundancy

Media Level Redundancy is used to maintain reliable communications with critical components in an automated environment. It accomplishes this by one of two methods: Communication Path Redundancy (which provides multiple network paths to communicate to a critical device) or Device Pair Redundancy (in which identical devices are configured as a redundant unit). KEPServerEX version 5.18 introduced a new operating mode called "Switch on Trigger" that gave the advanced option to determine connection availability by monitoring a tag's value, quality, or rate of change. These new trigger types provide additional flexibility to design redundant communications and solutions for any automated environment. For example, if redundant devices are intelligently sharing control of a machine, MLR could monitor this status to determine the device with which KEPServerEX should be communicating. Additionally, MLR could monitor a heartbeat item (where supported by devices) to determine if the heartbeat is still active.

Redundancy may also be necessary when utilizing a tunneling solution, and MLR enables connections to redundant OPC servers with the OPC UA Client driver tunneling solution for KEPServerEX. The "Switch on Trigger" feature allows failover to be driven not only by the

tunnel connection but also by the status of the devices communicating with the OPC servers—thus forcing the tunnel connection to swap to the secondary OPC server to communicate with devices. This provides the ability to monitor the "downstream" network connection to devices and allows the system to find alternate paths of communication from additional failure conditions.

Although "Switch on Trigger" uses a single tag to evaluate the trigger condition, it can be extended to monitor multiple tags with Advanced Tags for KEPServerEX. For example, a Derived Tag can be created to compute multiple tags' quality values and provide a "TRUE" condition when some or all of the tags' quality value is "BAD". The Derived Tag is then used as the Trigger value, causing MLR to take action when the Derived Tag computes to a "TRUE" condition. Applying this idea to the tunneling solution discussed earlier, you could create a Derived Tag that monitors multiple devices' states and aggregates these conditions into a single Derived Tag. The tunnel connection could move to the secondary OPC server when two or more devices cease communicating with the primary OPC server, with the Derived Tag providing the resultant condition to MLR.

What's Next?

Redundancy solutions are not one size fits all. Equipment and network designs are unique for every application, and solutions need tools that can be flexible within a variety of environments. Extending Media Level Redundancy with the "Switch on Trigger" functionality further adds capabilities to our product portfolio to help our customers build highly-available automated systems.

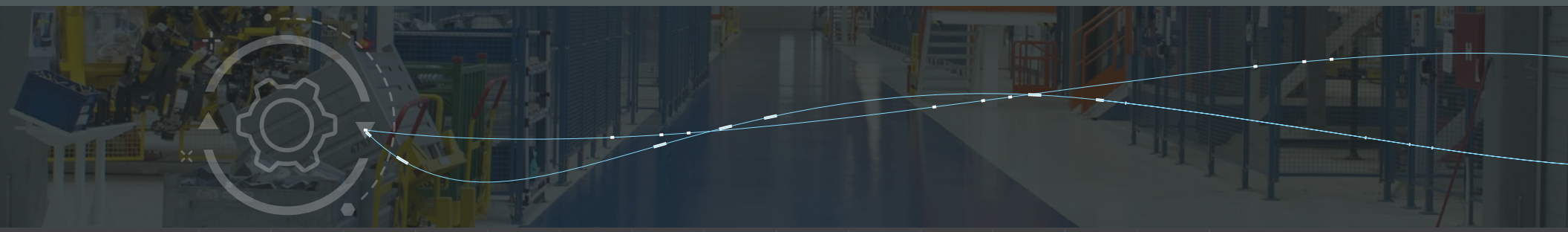
About the Subject Matter Expert

RAY LABBE

Ray Labbe is a Principal Applications Engineer PTC with a focus on Kepware industrial connectivity. Ray joined Kepware Technologies in 2014 and came to PTC with its acquisition of Kepware in 2016. He has previous work experience in the shipbuilding industry integrating complex networked control systems for various systems. Ray combines technical expertise developed over 15 years in networked control system integration with an unbridled enthusiasm for engineering to provide customers answers and solutions.

SOURCES:

https://www.ptc.com/en/products/iiot/thingworx-platform/thingworx-kepware-server
https://www.kepware.com/en-us/products/kepserverex/drivers/opc-ua-client/
https://www.kepware.com/en-us/products/kepserverex/advanced-plug-ins/advanced-tags/



Question #3:

WHICH TAG LINKING PRODUCT IS RIGHT FOR MY APPLICATION?

Product Showdown: LinkMaster vs. Advanced Tags

Beyond the basic needs for an OPC server, many companies have to move data between applications, devices, and systems. Kepware has a few different ways of accomplishing this, including two products that focus on solving that problem directly: LinkMaster (LM) and Advanced Tags (AT). Neither LinkMaster nor Advanced Tags have a tag limit, and both are equally reliable and work extremely well with any KEPServerEX driver. Deciding which one is right for your application can be tricky, however.

LinkMaster

LinkMaster is a standalone product that acts as a bridge between OPC DA servers, OPC DA-enabled applications, or legacy DDE products. LM's strengths come from its ability to link tags both through different OPC DA servers and within the same OPC DA server. Its functionality is limited within those links, however. For example, it can only link data on a data change or a static interval. While LM may be great for simple, bulk data transfers or when moving data between multiple OPC DA servers, it is less functional for more complex situations.

EXAMPLE

A customer monitoring a steel plant needed to link a Temperature Tag from PLC A in a furnace to PLC B. PLC A was communicating through an existing Kepware Server, while PLC B was using a proprietary OPC DA Server (not Kepware). Given that the data exchange was through two different servers and required a simple data transfer, LinkMaster appeared to be the better option.

Advanced Tags

The Advanced Tags Plug-In includes functionality to link data tags, set a trigger based on logical states, and calculate new values from raw measures. As a plug-in, AT can be centralized on the communications server as well as dispersed across multiple locations. It has the ability to "massage" data by executing basic math, logic, or analysis at the tag level, thus bringing data closer to the source. It runs on an instance of the Kepware Server and can link between any data source that we can connect to, using any one of our drivers. This includes devices, databases, any OPC Data Source (not just OPC DA like LinkMaster), and more.

EXAMPLE

One of our Applications Engineers spoke with a customer who produced drilling equipment and needed to find the minimum and maximum size of each part and populate that value into a database for Quality Assurance purposes. Because of the need for data manipulation, AT was clearly the appropriate solution. If the customer also needed to find the average from two different PLCs connected through two different OPC Sources, however, it would be more difficult and would require the functionality of AT and the flexibility of LM. Luckily, users can achieve this by using Kepware's OPC Client Drivers in conjunction with AT.

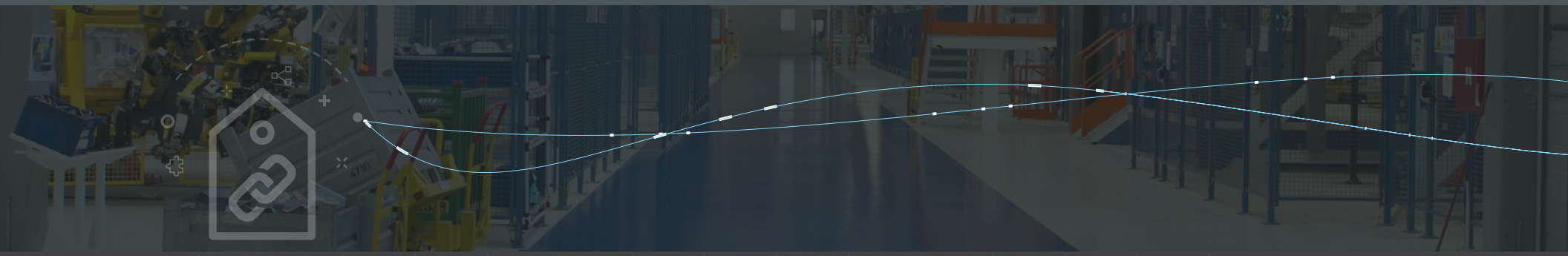
About the Subject Matter Expert

TUCKER EMERSON

For the past 7 years, Tucker has helped customers across every industry—including manufacturing, Power & Utilities, and Oil & Gas—architect their industrial communications to get the most out of their data.

SOURCES:

https://www.kepware.com/en-us/products/linkmaster/
https://www.kepware.com/en-us/products/kepserverex/advanced-plug-ins/advanced-tags/



Question #4:

WHAT IS THE OPTIMAL ARCHITECTURE FOR KEPServerEX WITHIN A PLANT?

Let Operations Drive Server Architecture

Many people ask, "What is the optimal architecture for KEPServerEX within a plant; how many servers and where?" As with most questions of this nature, the short answer is that it depends, but there is some guidance we can provide.

KEPServerEX is designed to scale up for large implementations while retaining a small footprint for small implementations. PTC has some customers with more than 1 million tags in the server, and other customers with only 10 tags in the server. We have customers with dozens of installations per location and other customers with a single installation.

When defining the best practice architecture, administrators should look at the layout of the physical plant, the requirements of the client software the data collection goals, the current or planned network architecture, and the security needs of the business.

Plant Floor Layout

As with any software, there will be times when you have to restart the server or stop all operations to implement certain changes like installing new versions of the software, adding additional licenses to the server, or performing server hardware or operating system updates. The effects of this can be minimized, but ultimately periodic downtime should be expected. Many factories or operations have multiple logical sections within the factory. The material flow within each section is continuous and the machinery is tightly integrated; however, the material flow between sections is not continuous and the machinery is not tightly integrated. In a small discrete manufacturing plant, there may be sections for machining, assembly, painting, inspection, and packaging. With such a layout, it would also make sense to have five server installs—one for each section or zone. In other cases, a single work cell may require its own server. This would be if the cell primarily operates autonomously, if the equipment changes frequently (which would require many changes to the server), or if the hardware and software for the server are updated frequently.

Client Requirements and Data Collection Goals

Another approach is to evaluate the necessity of information to client software. There are many different types of software clients that connect KEPServerEX for plant floor information, from IoT platforms like ThingWorx, or HMI and SCADA to MES and ERP to custom analytics, web, or mobile applications. Some clients are mission-critical, and if they lose their connection to the plant floor, the floor must come to a stop (because they are controlling the floor with a SCADA or MES program, for example, or because they are historizing information from the floor for regulatory purposes). In either case, they may require a dedicated server or even a redundant pair. Other clients may be used for monitoring operations, production or quality analysis, or mobile access. These are important systems, but the factory does not come to a halt if they are interrupted for a short period of time. A typical implementation is to have multiple non-critical clients on a single server: this minimizes both the load on the PLC (by not having many servers opening connections) and the system administration (by reducing the servers).

Network Architecture and Security

The final consideration is to evaluate the network architecture and cybersecurity requirements. In many enterprises, the Operations applications are separated from the business and other IT applications by a firewall or a demilitarized zone, or DMZ. In this case, putting a server in the DMZ and using a secure tunnel to one or multiple servers on the Operations' side provides multiple levels of cybersecurity. The DMZ server can be shut down if it is violated, and the operational servers can restrict the information and level of access available to the DMZ server.

Conclusion

There is not a one-size-fits-all approach to server architecture for a factory or automation operation—there are only guidelines that can be recommended and key information that should be evaluated. In the end, letting the operations of the plant drive the quantity and organization of KEPServerEX—cybersecurity requirements, network layouts, and the relationship of production systems to each other and their higher-level control and data acquisition systems—is much better than relying on cost or software scalability limitations.

BEST PRACTICE CONSIDERATIONS

Plant Floor:
- Natural process separations
- Areas being changed or upgraded frequently

Client Requirements:
- Critical applications vs. secondary applications

Network Architecture and Security:
- Firewall access
- Cybersecurity
- Network segmentation

About the Subject Matter Expert

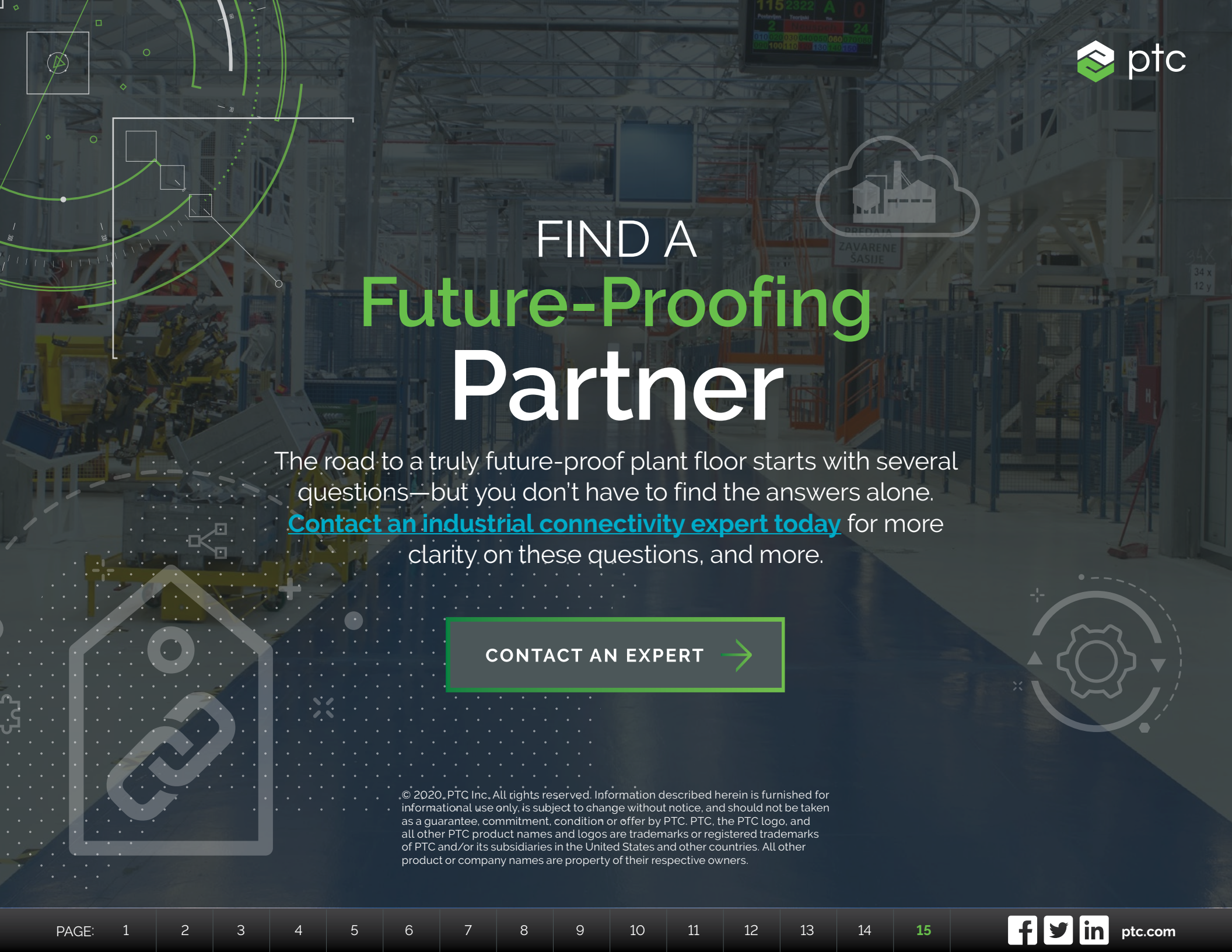
SAM ELSNER

Sam Elsner leads and manages PTC's Kepware Sales Applications Engineering team. Sam joined Kepware in 2011 and brings a unique combination of business and technical expertise developed over a decade of professional experiences in non-profits and the private sector. His professional business expertise is derived from many years of enterprise account management, and his professional technical expertise is derived from many years of systems integration for industrial automation and enterprise IT systems. His passion for technology is said to be contagious.

Sam's Sales Applications Engineering team supports PTC's business development teams, global partner network, and extensive global customer base.

SOURCE:

https://www.ptc.com/en/products/iiot/thingworx-platform/thingworx-kepware-server



FIND A Future-Proofing Partner

The road to a truly future-proof plant floor starts with several questions—but you don't have to find the answers alone. **Contact an industrial connectivity expert today** for more clarity on these questions, and more.

CONTACT AN EXPERT

© 2020, PTC Inc. All rights reserved. Information described herein is furnished for informational use only, is subject to change without notice, and should not be taken as a guarantee, commitment, condition or offer by PTC. PTC, the PTC logo, and all other PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States and other countries. All other product or company names are property of their respective owners.