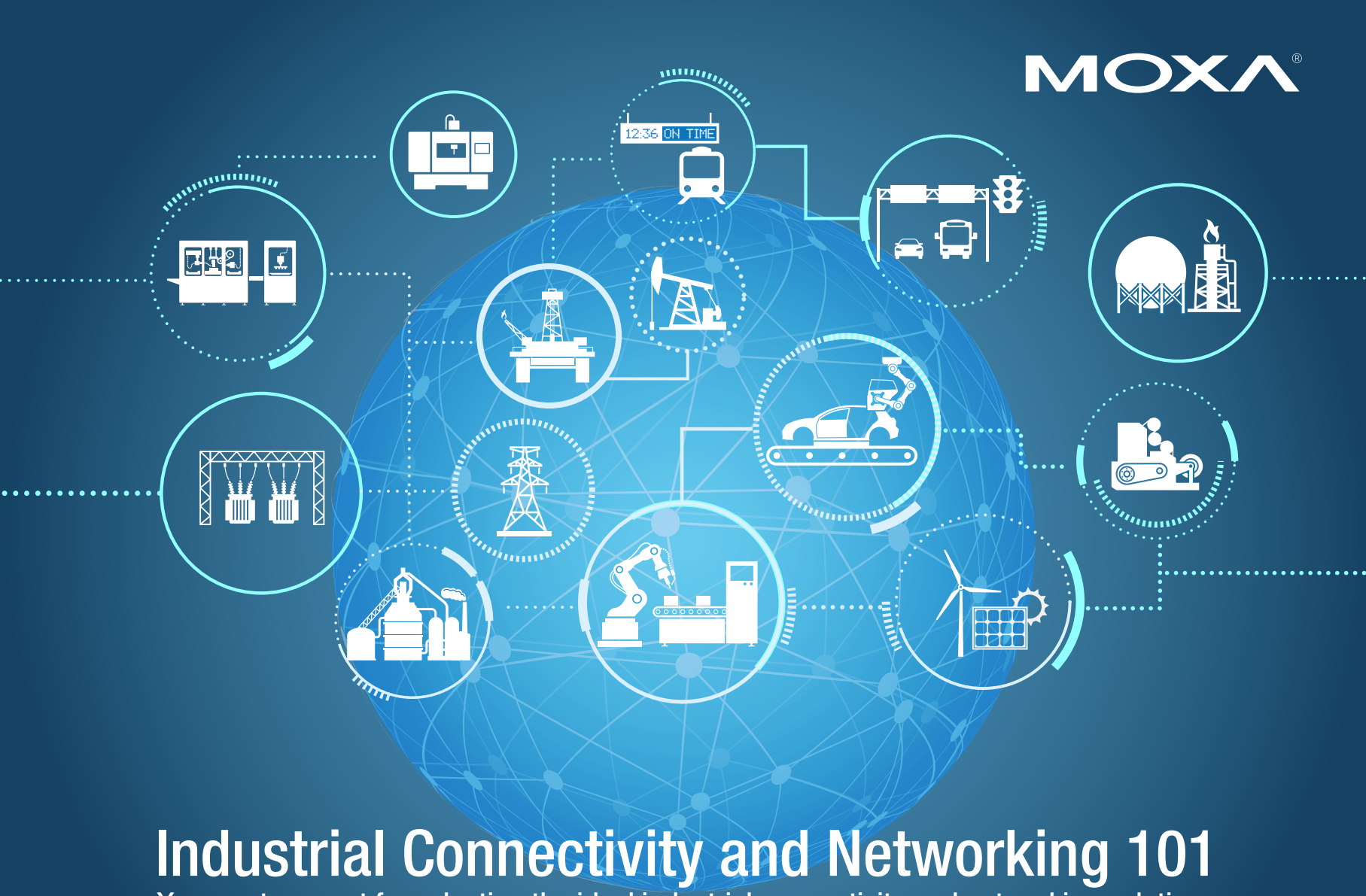



# Industrial Connectivity and Networking 101

Your go-to expert for selecting the ideal industrial connectivity and networking solutions

# Table of Content

## Industrial Connectivity Needs—Now and in the Future


Give New Life to Your Legacy Serial Devices P5

Greater Expectations for Remote I/Os P17

What's Next for IIoT Device Connectivity? P23


## Industrial Networking Needs—Now and in the Future


Gear Up Your Ethernet Switches for Edge Networks P30

Get Unwired to Unleash More Possibilities P40

Your First Line of Network Defense P46

Getting Your Networks Ready for the Future P52


# Foreword

The industrial automation (IA) landscape has transformed substantially since the early days of enabling direct digital control of equipment and devices on the factory floor. Traditionally, the world of operational technology (OT) used to enable industrial connectivity was only concerned with managing physical processes and machinery in manufacturing environments. In contrast, information technology (IT) was only concerned with managing the flow of digital information on office networks.

Although OT and IT initially developed separately from each other, these two disciplines have since converged into a widely accepted "automation pillar" where both OT and IT systems need to connect with industrial field devices. In order to stay competitive in an increasingly connected world, previously unconnected OT assets not only require industrial connectivity, but may also demand IT or cloud capabilities that go beyond on-premises applications in order to effectively draw business intelligence that improves industrial productivity, efficiency, and scalability.

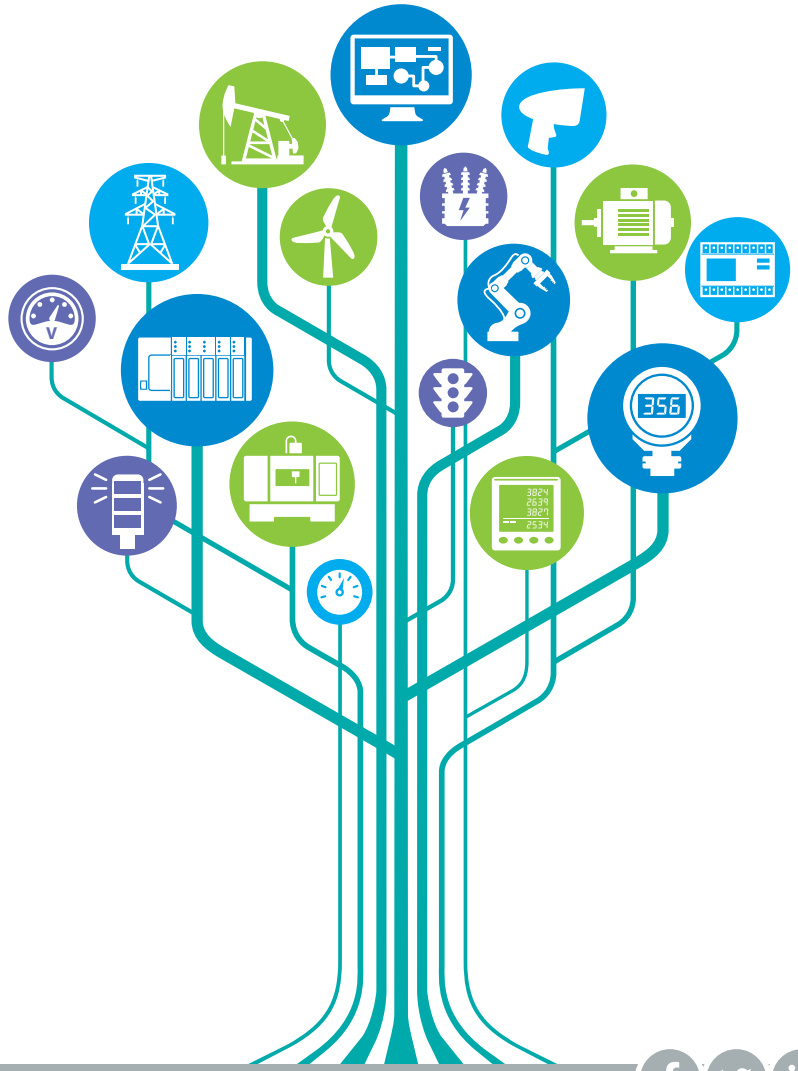
Dubbed the Industrial Internet of Things (IIoT) or Industry 4.0, the current trend towards further convergence between OT and IT networks is already underway and features new forms of industrial connectivity and networking. Unfortunately, the arduous task of choosing the right industrial connectivity and networking solutions in this converged landscape all-to-often befalls an IT engineer who lacks experience with OT protocols and automation systems, or an OT engineer unfamiliar with enterprise IT networking.

With more than thirty years of experience in helping customers overcome industrial connectivity and networking challenges, Moxa has identified several key criteria for selecting the most suitable solutions for industrial automation applications. Whether you are an IA or IT engineer, OT or IT system integrator, plant owner, or system operator, we hope you will find this book helpful in choosing the right industrial connectivity or networking solution for your IIoT project and bridging the gap between OT and IT.

# Industrial Connectivity Needs—Now and in the Future

The first step to enabling IIoT applications is to connect your previously unconnected industrial field devices and assets. Accomplishing this task requires an understanding of what kinds of OT assets you need to connect to and specific connectivity requirements, such as connecting OT assets to a local network or a cloud server. Since OT assets in industrial applications mainly use serial or I/O communication interfaces, understanding how to choose the right serial and I/O connectivity solutions is essential to enable industrial connectivity. Moreover, there are additional considerations you need to keep in mind when connecting OT assets to remote or cloud servers.

In this chapter, you will learn how to choose solutions for serial connectivity, remote I/O connectivity, and IIoT device connectivity.



## Serial Connectivity

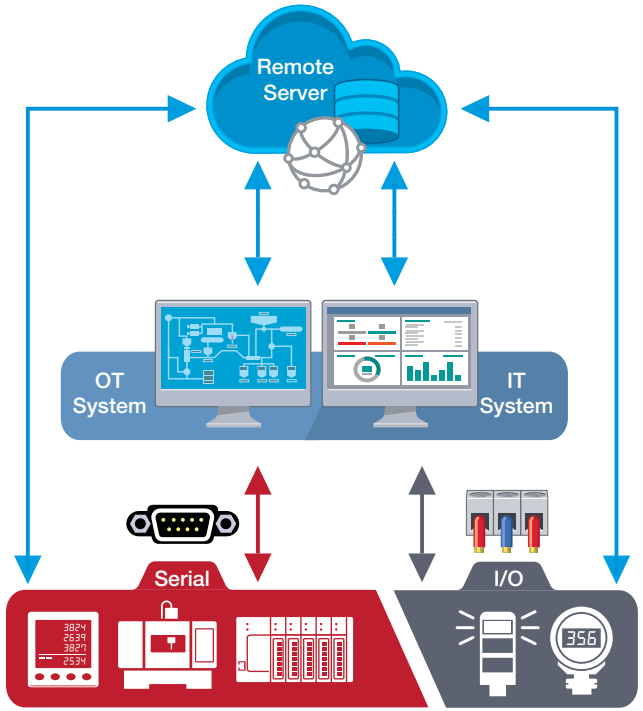
Since the vast majority of legacy machinery, equipment, and field devices still use a variety of standard and proprietary serial communication protocols, you may need a serial device server or protocol gateway in order for a system with a standard Ethernet connection to communicate with legacy serial devices.

## Remote I/O Connectivity

The purpose of remote I/O connectivity is no longer limited to simply collecting and transmitting digital or analog data. In IIoT applications where both OT and IT systems need to acquire data from I/O devices, your remote I/O plays an essential role in making data available to your application systems.

## IIoT Device Connectivity

The connectivity devices you use to connect field devices in IIoT applications may also have additional requirements of their own. For example, connectivity devices may require IT protocols or cloud capabilities to communicate with IT systems or cloud servers. When everything is connected, issues related to managing large numbers of connectivity devices and transmitting data securely also need to be addressed.




OT Assets

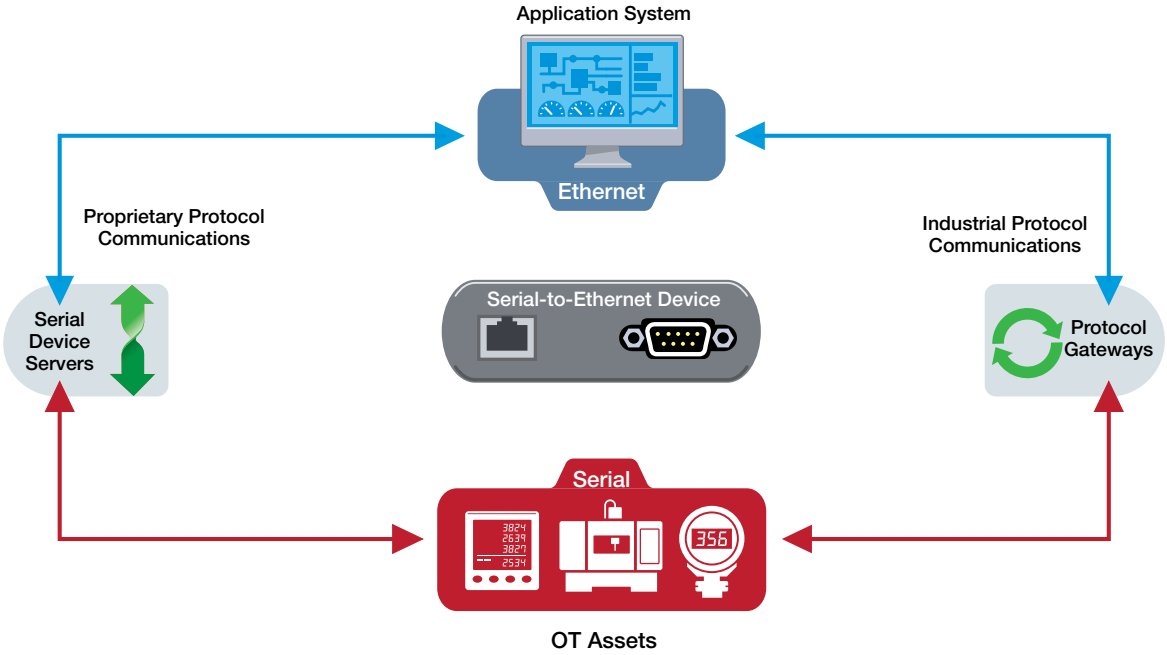
Indeed, enabling device connectivity does not mean you need to get rid of your tried-and-true legacy devices and machinery. A variety of solutions are available for connecting previously unconnected legacy devices to the Internet, as well as collecting and transforming data from different protocols and formats. Let's begin our discussion on the specific requirements for choosing serial connectivity, remote I/O connectivity, and IIoT device connectivity solutions to ensure the success of your IIoT application now and in the foreseeable future.

# Give New Life to Your Legacy Serial Devices

There is no need to say goodbye to all your loyal legacy devices in order to transform your existing industrial automation system into a modern IIoT application. Even though the legacy devices in your industrial edge systems may be older than most mobile phones or laptops in use today, they continue to fulfill a valuable purpose and are oftentimes too costly to replace altogether. However, IIoT applications often take advantage of supervisory control and data acquisition (SCADA) systems that use the Internet Protocol (IP) to communicate over Ethernet networks. Your legacy devices, on the other hand, most likely use serial-based communications with fieldbus protocols, which are very different from IP communications. So how do you connect legacy serial devices with Ethernet-based SCADA systems when they cannot talk to each other?

Replacing all of your legacy serial devices with newer Ethernet-based devices would clearly solve the communication problem. But upgrading all of your equipment would also be costly and disruptive. For example, replacing a serial-based CNC machine is extremely expensive and would take a huge chunk out of the budget of most businesses. Besides, serial devices have their own benefits. For example, RS-485 power meters can perform multidrop communication, which makes wiring easy and efficient. Adding **serial-to-Ethernet solutions** between your serial devices and IP-based systems can help you save costs and effort, and also allow you to enjoy both the simplicity of serial communications and the advantages of Ethernet.

Before we start, you will need to take stock of your serial devices and reacquaint yourself with these old friends. Legacy devices either speak in proprietary protocols or in standard fieldbus protocols, such as Modbus and PROFIBUS, so you need to choose the right serial device server or protocol gateway to enable IP communications.

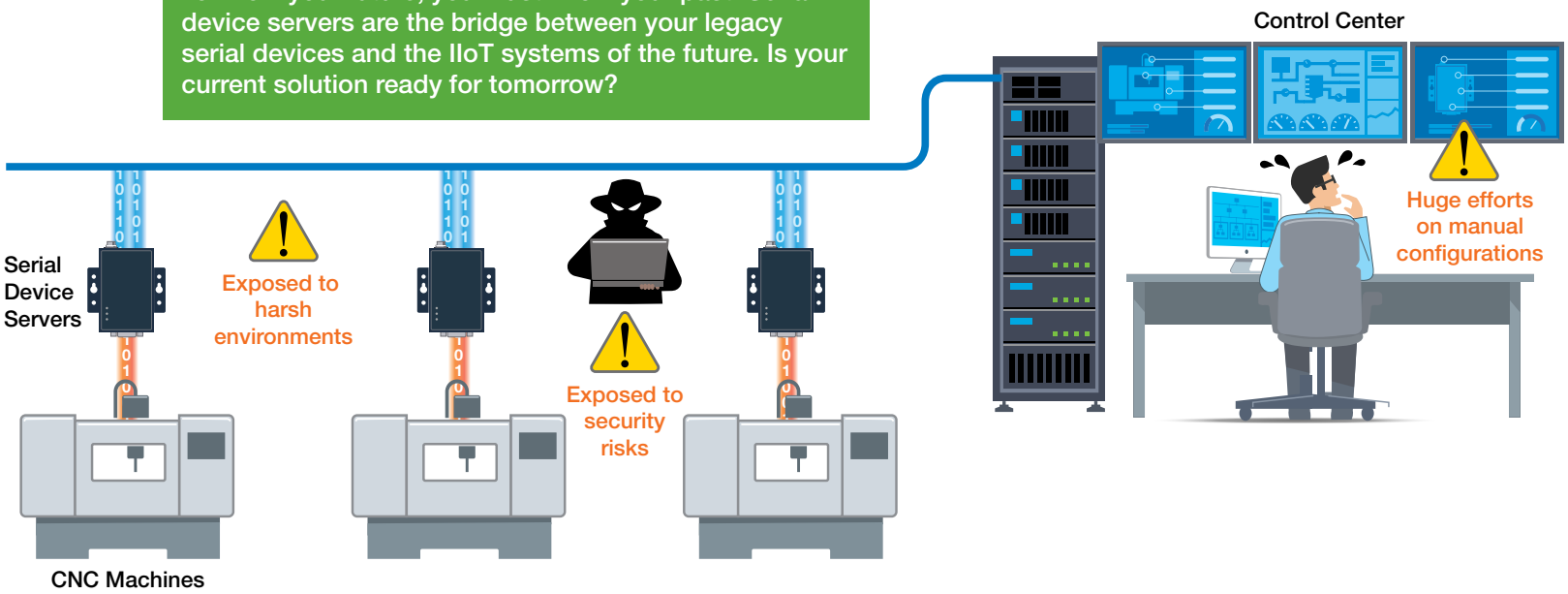


# Key Criteria for Choosing Serial Device Servers

If you need to connect proprietary serial devices over IP networks, serial device servers can provide a simple bridge between your legacy serial devices and modern communication systems. However, without sufficient knowledge of how serial device servers work, you could end up spending unnecessary time and effort. Here are three key criteria you should remember when choosing a serial device server.

## Key Question

To know your future, you must know your past. Serial device servers are the bridge between your legacy serial devices and the IIoT systems of the future. Is your current solution ready for tomorrow?



Key Criteria 1

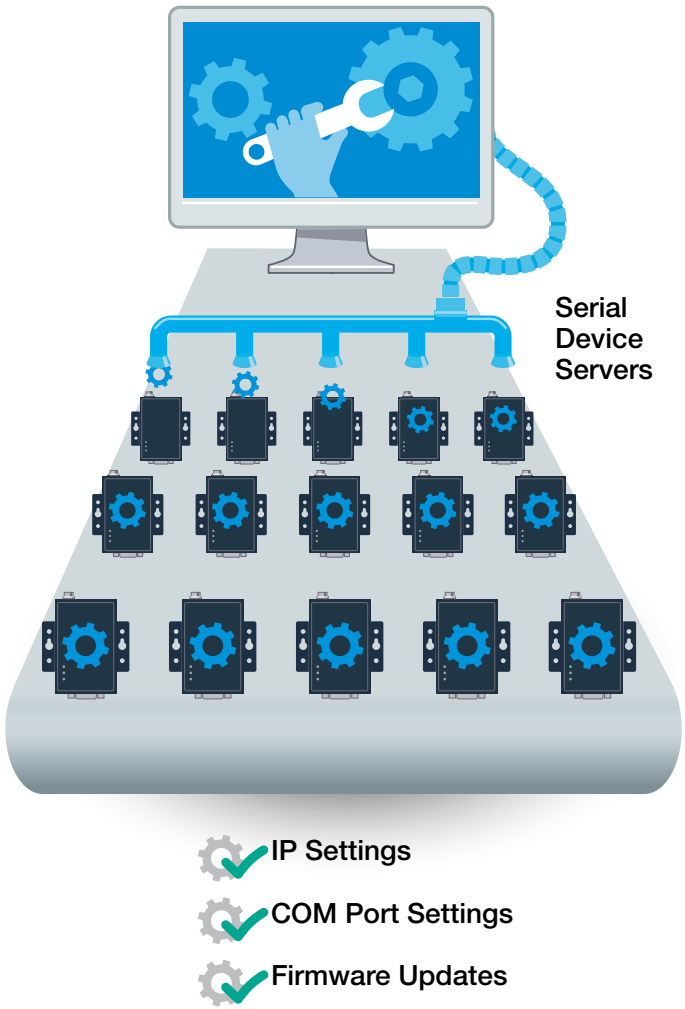
## Make Every Step Count

Compared to completely replacing all your hardworking legacy devices, learning how to use and deploy serial device servers can be a breeze. However, enabling dozens of serial device servers could also take a great deal of time and effort to manually configure countless settings. Whether you are configuring IP addresses for each of your serial device servers, setting up virtual serial (COM) ports, or updating serial and Ethernet parameters, serial device server configurations can be painful if you don't have clear instructions or a smart utility to help walk you through all the steps. The frustration can even extend into the operations phase when you need to manage or maintain dozens of devices.

When choosing a serial device server, check if there is an **easy-to-use web console or utility** to simplify configuration and management. Don't overlook this feature because there will only be more field devices that need to be connected as your network matures. Repeating configuration processes increases the burden of device management and can really wear you down.

### Learn More

Want to learn more serial-to-Ethernet technology? Download our Q&A for answers to frequently asked questions.

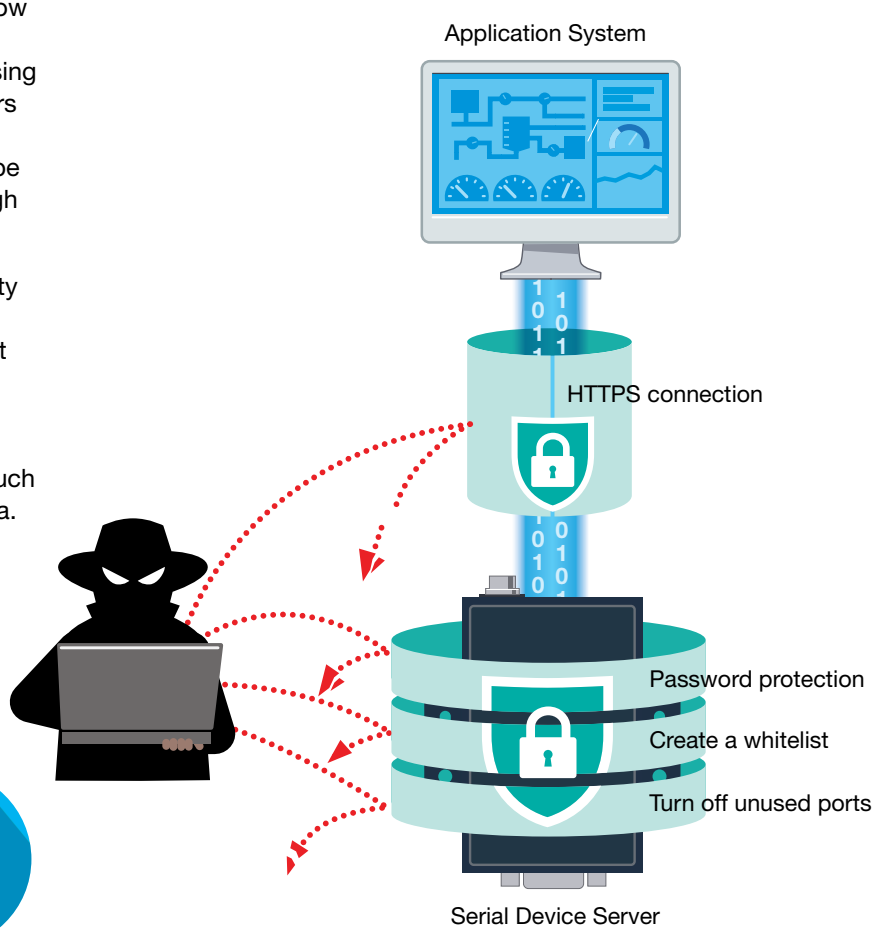


Key Criteria 2

# Protecting Your Networks in a Connected World

In the past, industrial automation only required connecting a limited number of field devices within a small, independent, and private network. In the era of the IIoT, however, industrial applications now require more field devices to be connected over public networks that allow both OT and IT engineers to access field data. Increasing the accessibility of your field devices with the outside world offers innumerable benefits but also exposes your networks to new security risks. Without proper protection, your applications can be extremely vulnerable. People can access your application through countless entry points, including your serial device servers.

Be sure the serial device server you choose has sufficient security functions to keep your data protected. Using **strong login passwords** or **creating a whitelist** are the simplest ways to limit access to your serial device servers to authorized personnel. **Closing unused ports** on serial device servers can also be an efficient way to block unnecessary entrances that could be exploited. During data transmissions, using a secure protocol, such as **HTTPS**, can also minimize unwanted access to your field data.




## Learn More

Want to learn more about how to keep your connectivity secure? Read our device security article now.

Key Criteria 3

## Don’t Forget the First “I” in “IIoT”

Are you still using commercial-grade serial device servers for your industrial applications? Commercial serial device servers may seem adequate if you have been using them for a while or only need to connect a few field devices. But when it comes to IIoT projects that require connecting a large number of field devices and transmitting critical field data on time, you should reconsider. Choosing a serial device server that is capable of enduring harsh environments, such as extreme temperatures or high electromagnetic interference, can minimize the chances of data loss arising from a serial device server shutdown.

Using the above three criteria to evaluate your serial device server options can help you find the right solution for your industrial applications. For example, **Moxa’s NPort serial device servers** are developed with easy-to-use, secure, and reliable features that are ideal for connecting field devices in IIoT applications.


"Look for a serial device server that can keep your IIoT connectivity simple and secure for reliable data transmissions."

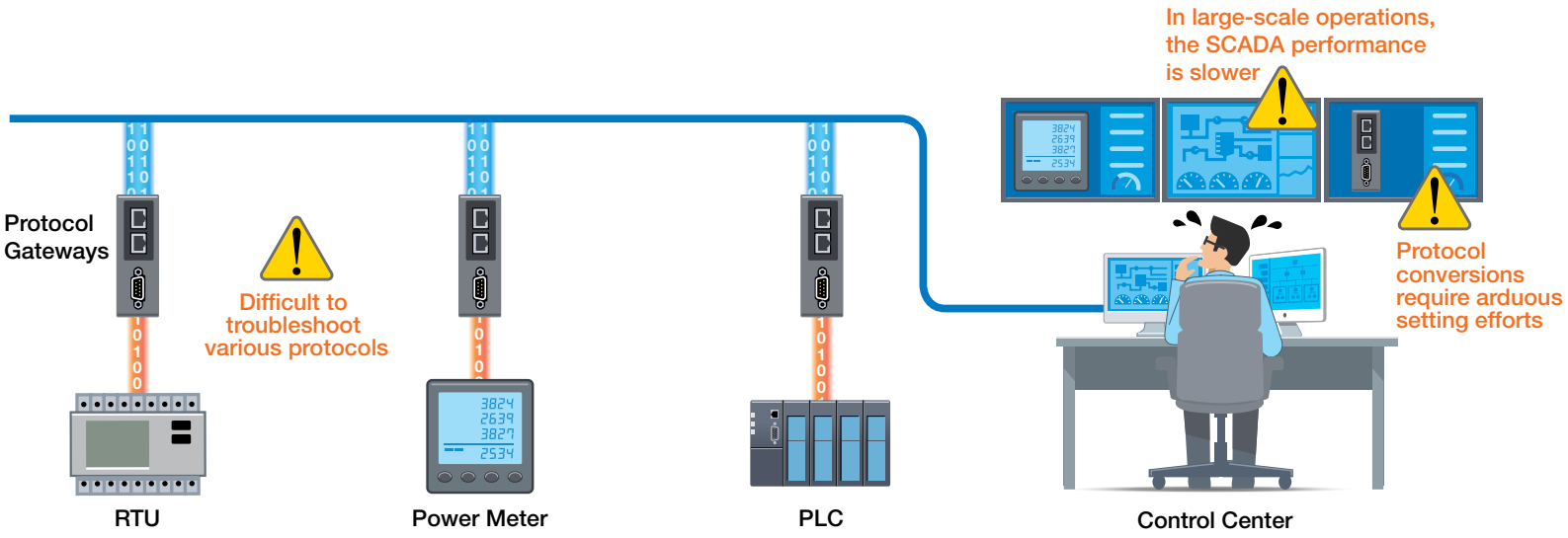
## Key Criteria for Choosing Protocol Gateways

In the past, automation systems were relatively closed off and developed a unique set of highly specialized protocols including Modbus, EtherNet/IP, and PROFINET. These protocols are known as industrial fieldbus protocols and provide unique benefits for different system application purposes. Today, the push towards connected factories has also seen a growing demand for protocol conversion due to two main reasons. First, legacy devices generally use serial-based communication protocols whereas modern SCADA systems, which are becoming increasingly popular in industrial automation, rely on Ethernet communications. To enable smooth data communication between legacy serial devices and SCADA systems, **serial-to-Ethernet protocol conversion** is necessary. Second, a factory may have several independent control systems. To enable system-to-system communication for enhanced operational efficiency and visibility, you need a way to translate data between systems.

Protocol gateways play an important role for smooth data communication in a converged communication system. The following three criteria provide guidelines to help you choose a protocol gateway that offers maximum benefit.

### Key Question

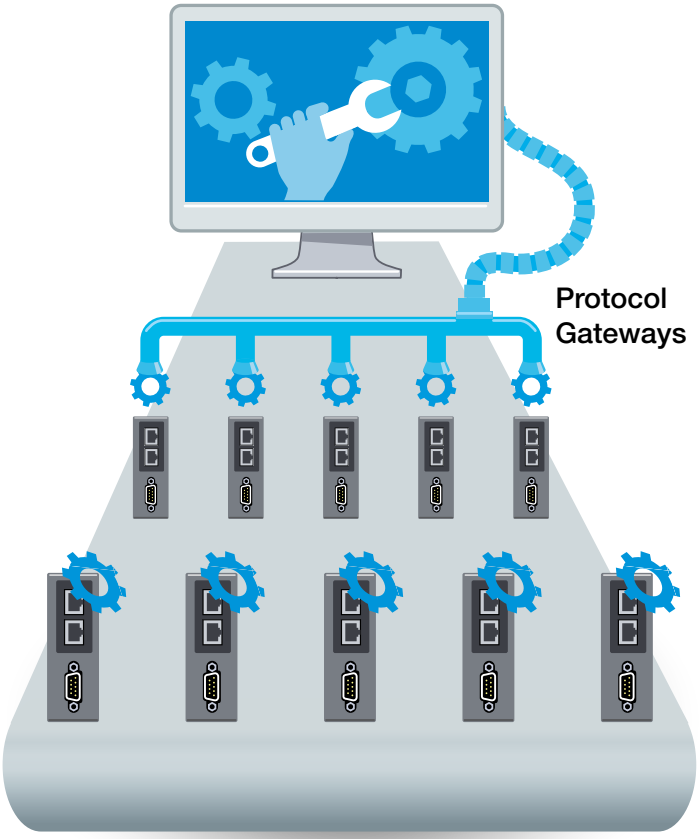
Smooth data communication between legacy devices and modern systems relies on protocol conversion. Wouldn't it be nice to have a protocol gateway to take care of all the complex settings and also keep data communication fast and simple?



Key Criteria 1

## Start Strong With Faster Configuration

If you thought manually configuring IP addresses and COM port settings for serial device servers was painful, just wait until you have to deal with industrial protocol conversion settings. Industrial protocol conversion settings are even more complex and involve many different data formats. Even the most experienced engineer could be overwhelmed. That's why a good protocol gateway does more than just convert different protocols. Besides simplifying byzantine configurations for both northbound and southbound protocols, the protocol gateway also needs to properly map which data from which protocol needs to be converted. A **graphical user interface** that provides these functions on an intuitive and easy-to-use screen can really help speed up the configuration process.




- System Settings
- Network Protocol Settings
- Device Protocol Settings

### Learn More

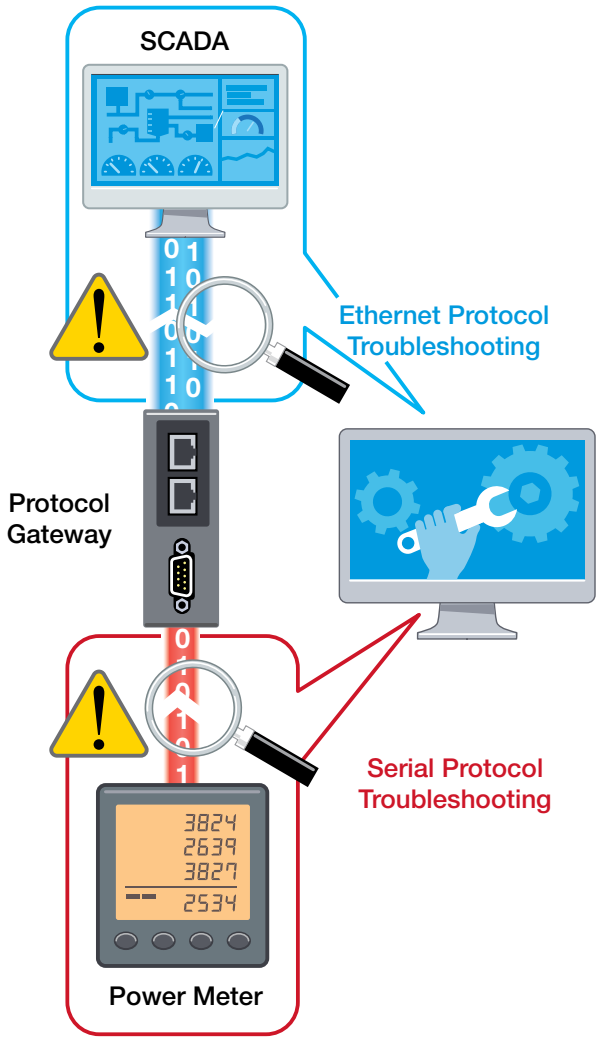
Seeing is believing. Watch our videos and see how easy it is to complete protocol conversions.

Key Criteria 2

## Take the Trouble Out of Troubleshooting

When systems are down, you lose time, productivity, and most importantly, money. Naturally, engineers want to fix problems quickly. But troubleshooting isn't always easy. If multiple devices using different protocols are being connected, pinpointing the cause of a communication problem becomes even harder as you'll need to determine whether the problem originated on the Ethernet end or the serial end. Time and energy are often misspent trying to track down the root cause of a communication failure. Adding to the frustration is the lack of helpful diagnostics tools to pinpoint the root cause quickly.

Troubleshooting protocol conversion issues requires a way to analyze the packets traveling through the gateway. However, troubleshooting tools and capabilities are sometimes limited due to security concerns (for example, third-party utilities might not be allowed by your IT policies) or platform constraints (for instance, you cannot install utility tools directly on a PLC). So, a protocol gateway that has a **handy utility tool** or **built-in troubleshooting features** to quickly identify connection status, timeout frequency, and invalid response counts can really help. Never forget the cost and effort spent on troubleshooting when selecting your gateway solution.




**Learn More**
Download our white paper to learn more about troubleshooting protocol conversion issues.

White Paper

Key Criteria 3

## Data Acquisition Performance Matters

Balancing cost and performance can be a major issue when you require protocol conversion in a large-scale application. When dozens or hundreds of devices require protocol conversion and communication within a single SCADA system, how can you ensure system performance meets your expectations? You could use a one-port protocol gateway for each field device to ensure instant data conversion and transmission, but the cost would be high and maintenance effort could overwhelm your daily operations. Alternatively, high-port density protocol gateways can provide a cost-effective solution with efficient installation and easy management, but performance concerns may arise over data handling. As most protocol communications are based on poll-and-response behaviors, handling large amounts of data polls also creates loading on gateways, which negatively affects the performance and response times of the SCADA system.

Design your network carefully with a combination of one-port and high-port density protocol gateways. When you choose a high-port density protocol gateway, check if its **data polling mechanism** can meet your requirements.

An easy-to-use protocol gateway can tremendously improve your system operation. Check the three key criteria above and choose your solution wisely. For example, consider the **Moxa MGate protocol gateways** that enable efficient protocol conversion and speed up your system operation with smooth data communication.

**Learn More**

Download our white paper to learn how to optimize your SCADA performance.

White Paper

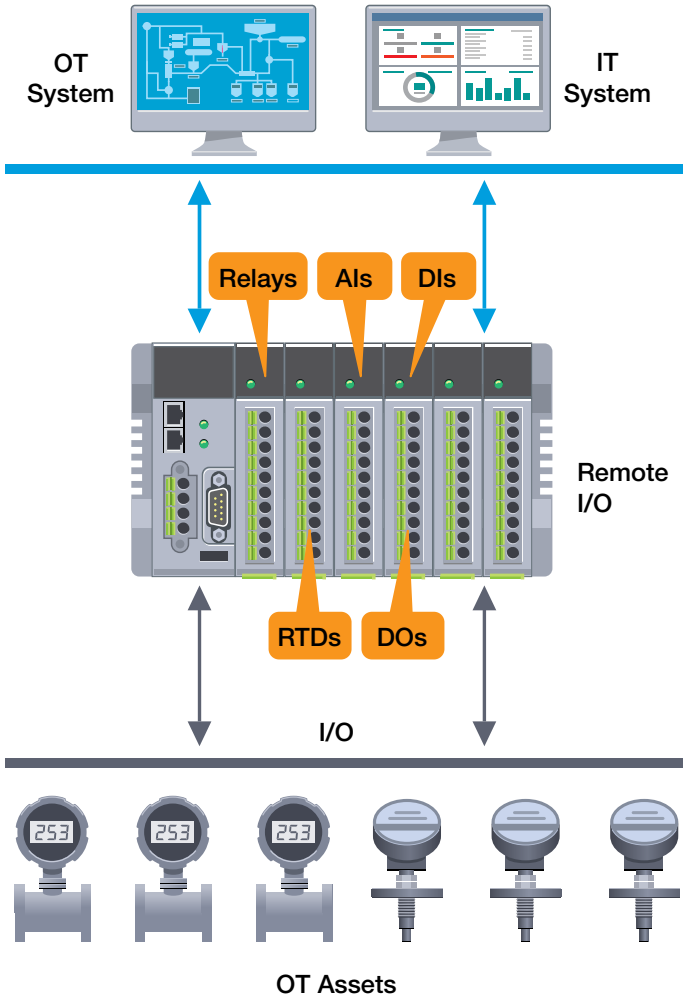

"A protocol gateway should be able to simplify protocol conversions for any-sized applications at any stage in the operation."

# Greater Expectations for Remote I/Os

You cannot draw actionable insights for Industrial Internet of Things (IIoT) applications without data. Remote I/O devices that are used to send and receive input and output signals to and from your sensors, controllers, and other equipment in the field may not resemble the “smart” automated robots immediately associated with the IIoT, but without these humble I/O workhorses, you wouldn’t have any of the remote I/O data you need.

Remote I/O devices are usually deployed at field sites to enable data access and environmental monitoring from a distant control center. I/O data acquisition not only ensures smooth daily operation for your field application, but also provides potential insights that can be used to optimize productivity.

However, the rising complexity of IIoT systems and applications is pushing traditional data acquisition to its limits. Modular remote I/O devices offer clear advantages by allowing you to customize the I/O modules on the remote I/O device itself. In other words, you are free to pick and choose the specific types of I/O modules you want to use, when to use the modules that give you flexible expansion, and how to use the modules based on your choice of communication means. Although modular I/O devices may not be the newest solution on the market today, the flexibility they enable continues to raise our expectations for how to acquire remote data from every node.

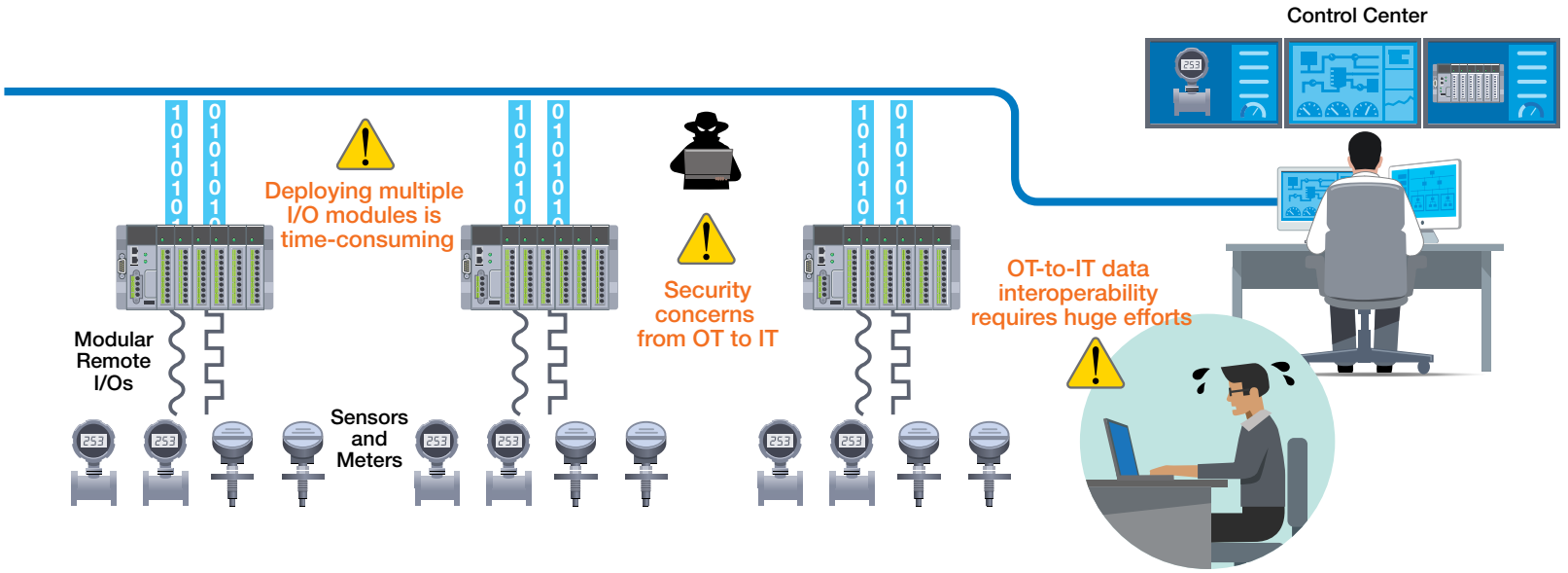


# Key Criteria for Choosing a Modular Remote I/O

It's crucial to choose a modular remote I/O solution that helps you make the best use of your collected data from installation to operation and maintenance. At the same time, you also need to ensure that both your OT and IT systems can use the data you acquire. Last but not least, your remote I/O solution should include or support cybersecurity features to protect the data you painstakingly collected. In this section, we share these key considerations in detail.

## Key Question

To make the best use of I/O data, we need to reimagine the role of remote I/O devices. Can your remote I/O solution handle the changing connectivity requirements in the IIoT era?



Key Criteria 1

# Don't Sacrifice Usability

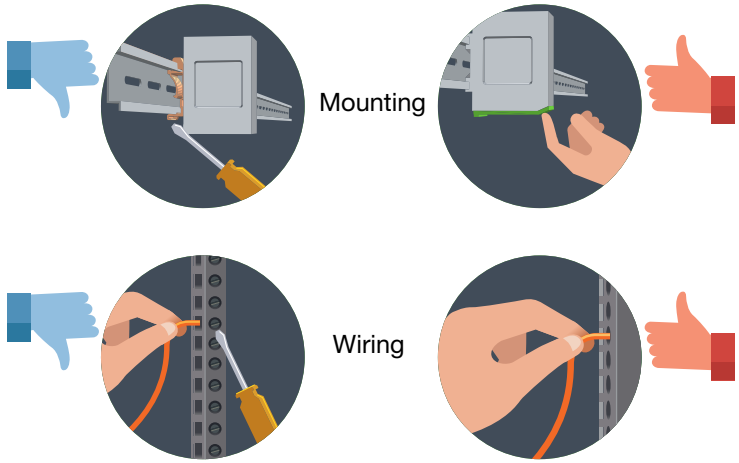
The flexibility afforded by modular remote I/O devices may come with hidden costs and additional effort if you don't pay attention to how the device will be implemented and actually used in your field application. You definitely don't want to sacrifice any usability for the sake of greater flexibility, or you'll end up spending additional effort that cancels out the benefits of modularity in the first place. There are essentially two stages in which usability pitfalls may arise.

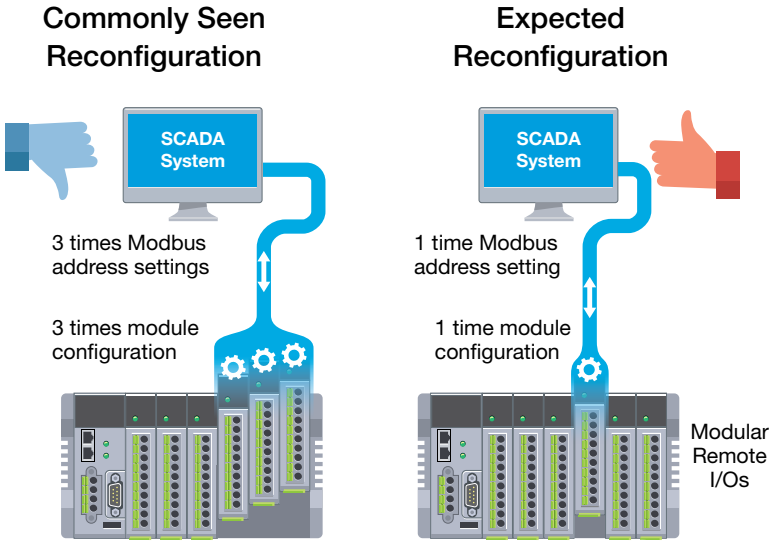
## Initial Installation

Modular I/O solutions are ideal for IIoT applications that have a high volume of different data acquisition needs. So if your application calls for modular I/O devices, then you probably need a large number of I/O modules too. With so many moving parts to keep track of, you don't want to waste time on getting things up and running. User-friendly installation features to look for include **convenient and standardized mounting options**, as well as an **optimized wiring design**.

## Operation and Maintenance

Modular I/O devices are also used to adjust and expand the scale of data acquisition applications. A larger system, however, also requires more time to configure all the additional I/O modules. If a single module is changed within the system, the unchanged module also needs to be reconfigured because of the sequence change. Besides the modules, you also need to ensure that the innumerable SCADA system settings are all up-to-date and comply with every module change. Indeed, a **user-friendly modular I/O solution** can reduce unnecessary effort and should not be overlooked.



Key Criteria 2

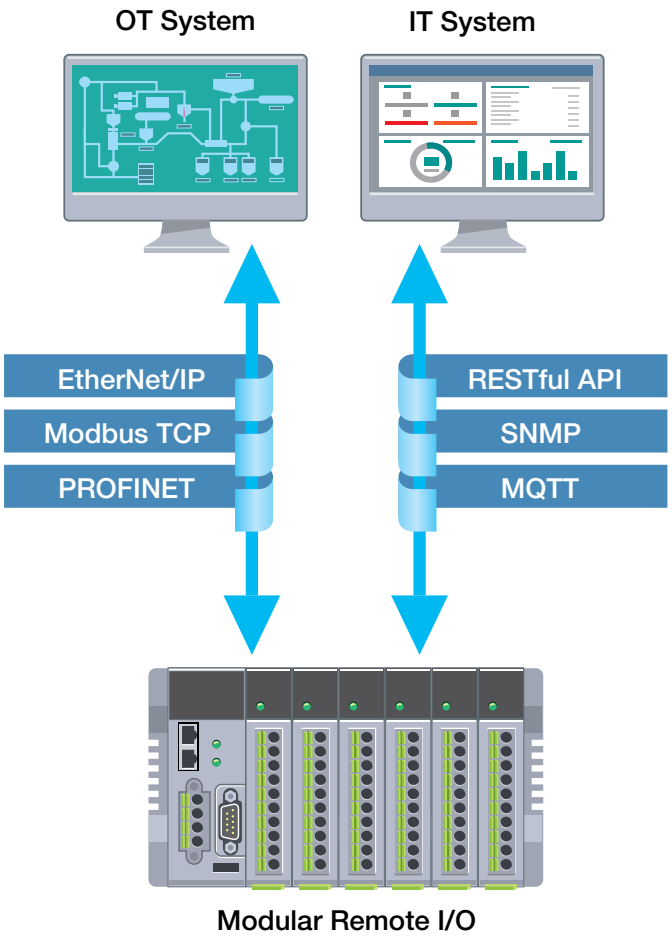
## See the “I/O” in the “I-Io-T”

As mentioned earlier, the convergence of IT and OT systems in today’s IIoT applications has prompted the development of new and enhanced edge devices, including modular I/O solutions. Nonetheless, OT and IT systems still rely on inherently different communication protocols. We don’t need a one-size-fits-all remote I/O solution for both IT and OT, but ensuring all parts of your IIoT application fit and work together is critical. For instance, emerging IT protocols, such as **MQTT**, **SNMPv3**, and **RESTful APIs** can enable OT applications to leverage traditionally IT-based analysis tools or services. Choosing a modular remote I/O that is future-proof with IT/OT readiness is essential in the age of IIoT.

**Learn More**

Download our white paper to learn more about how you can leverage MQTT protocol.

White Paper

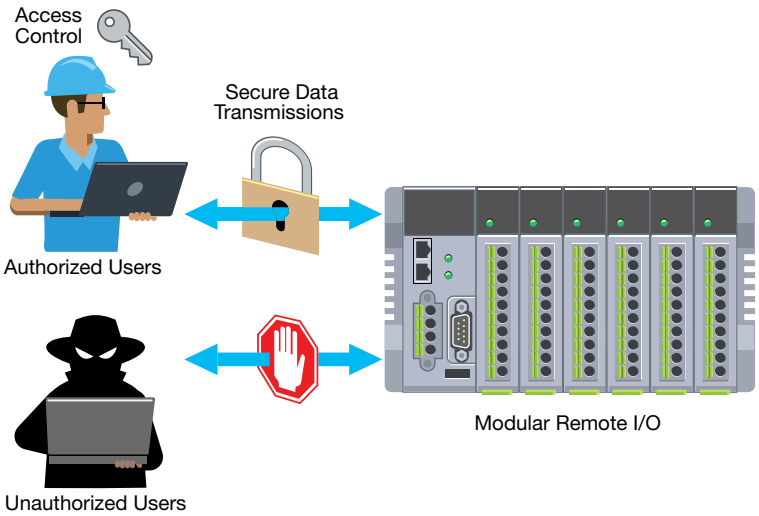



Modular Remote I/O

Key Criteria 3

## Don't Forget About Security

Cybersecurity concerns are inevitable whenever devices are connected over a network as in the case of any IIoT application. Remote I/O devices are no different. You'll need to carefully manage the accessibility and data confidentiality of the devices on your network. Making sure the security policies enforced within your organization is as important as making sure your devices are equipped with necessary security features. Ensure devices have the ability to **block unauthorized access** and control the traffic that is allowed. In addition, enabling **secure data transmission** for communicating sensitive data on the network protects your valuable information. When selecting modular I/O solutions, cybersecurity is definitely a consideration you want to take into account.




**Learn More**

Want to know how other companies secure their I/O data? Read our case study to learn more.

Case Study

Applying the above considerations when choosing your remote I/O solutions can ultimately make data collection easier and ensure your daily operations stay smooth and secure. In anticipation of new demands on I/O connectivity, Moxa has developed a **future-proof modular remote I/O device** that delivers more value with less effort for IIoT data acquisition.


"A future-proof modular remote I/O device should keep data acquisition easy and secure for both OT and IT engineers."

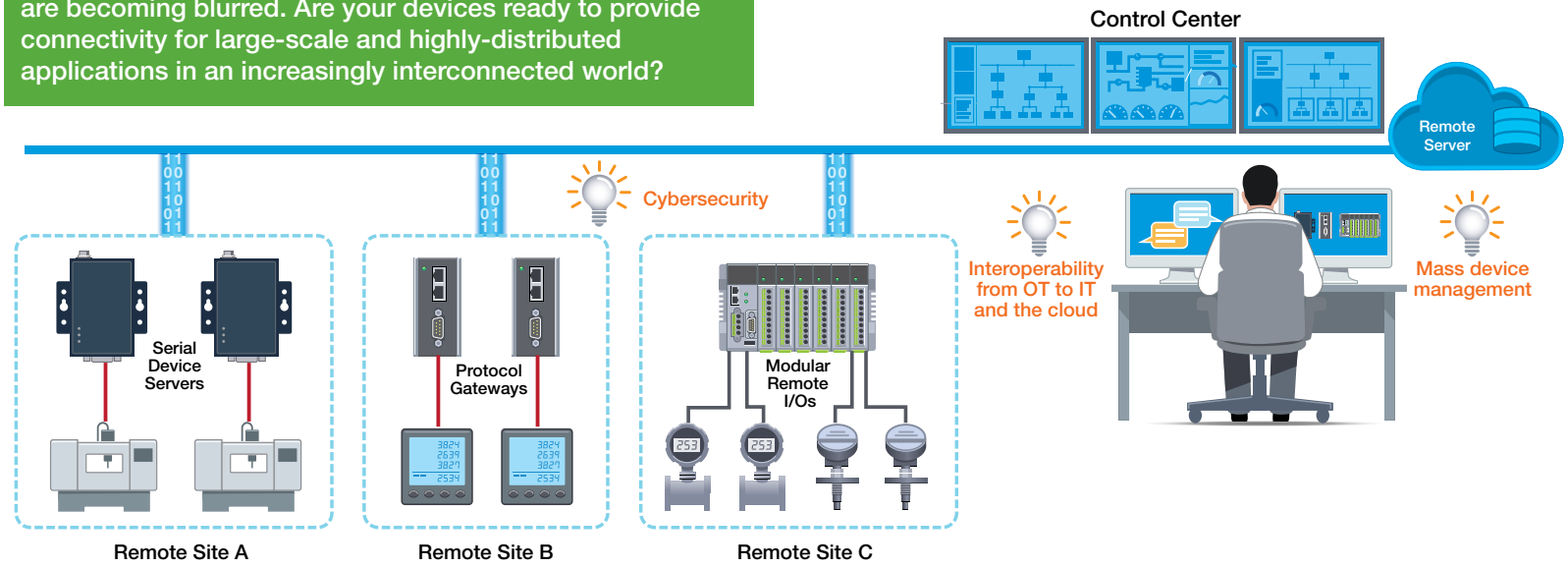
# What's Next for IIoT Device Connectivity?

Now that you've equipped your legacy serial devices and remote I/O systems with network connectivity, all your field data will instantly transform into brilliant business insights and boost your productivity, right? Not so fast! Choosing and deploying the perfect device server or remote I/O solution may be enough for relatively simple or small-scale IIoT applications. But what happens when you need to connect many different kinds of devices into a single network for both OT and IT engineers to access? Moreover, what if all these different devices are distributed around the world?

## Key Question

With widespread adoption of the IIoT, the traditional boundaries between OT and IT in industrial automation are becoming blurred. Are your devices ready to provide connectivity for large-scale and highly-distributed applications in an increasingly interconnected world?

The IIoT has not only blurred the lines between OT and IT disciplines, but also led to the increasing prevalence of **large-scale and highly-distributed applications** where field devices are dispersed over a wide area and need to communicate directly with remote servers. This means that where your data is going to and from, how you manage all your different devices, and how you keep your data safe matter even more than before. In this section, we provide three additional tips you should keep in mind for selecting device connectivity solutions that can meet the demanding requirements of large-scale and highly-distributed IIoT applications in our connected world.



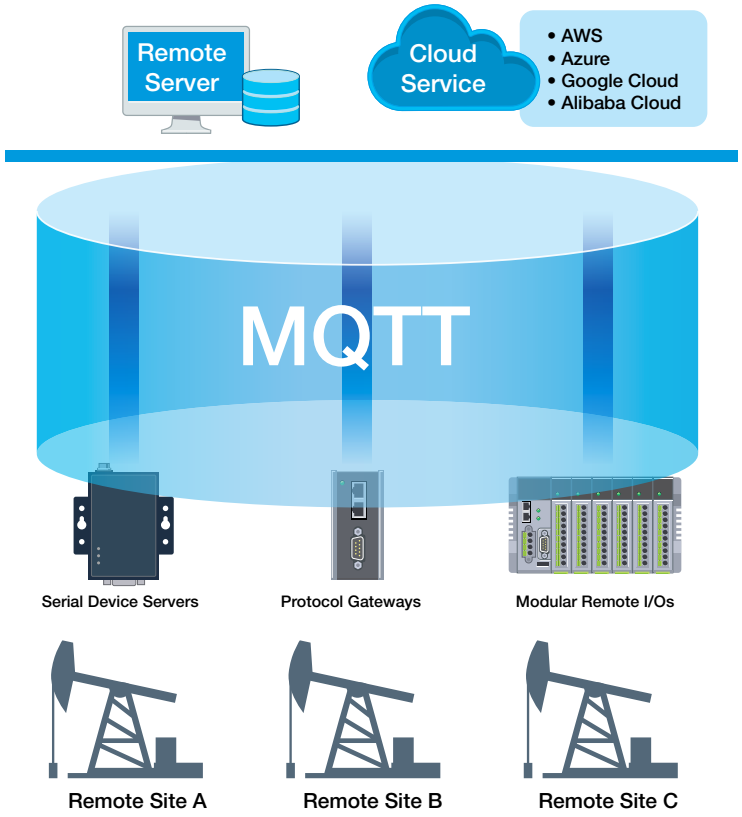
Expert Tip 1

## Know Where Your Data Goes

Large-scale and highly-distributed IIoT applications need to collect data from many different sites. Just imagine all the wellheads in a typical oil-drilling application that could be spread out over a massive desert. All the data from each wellhead not only needs to be collected and constantly monitored and controlled from afar, but also needs to be sent somewhere to process all the digital bits of information into human-readable insights. You could deploy an edge computer at each field site to collect, locally preprocess, and transmit your data to a remote server for more advanced analysis. However, some applications may only need to enable connectivity and be able to sufficiently process their data on a cloud server.

Using connectivity devices at each IIoT field site to transmit your OT data to a remote server could save you unnecessary time, effort, and costs. That is because many distributed applications such as oil drilling only require collecting relatively small amounts of data from each field site, so the costs and programming effort associated with deploying edge computers at multiple locations may not be justified. Instead, connectivity devices can usually do the trick and be more cost-effective and efficient too.

You'll also want to consider the type of remote server you're working with. For private servers, **MQTT** is one of most commonly used protocols to bridge the data between OT and IT systems. As for public cloud servers—such as Microsoft Azure, Amazon Web Services (AWS), or Google Cloud—each service provider has its own methods and protocols for collecting data. Before you choose your connectivity devices, **you should know (or decide) whether your applications use private or public servers**, and then find the connectivity devices that support related protocols or SDKs to save you time and money in the development stage.

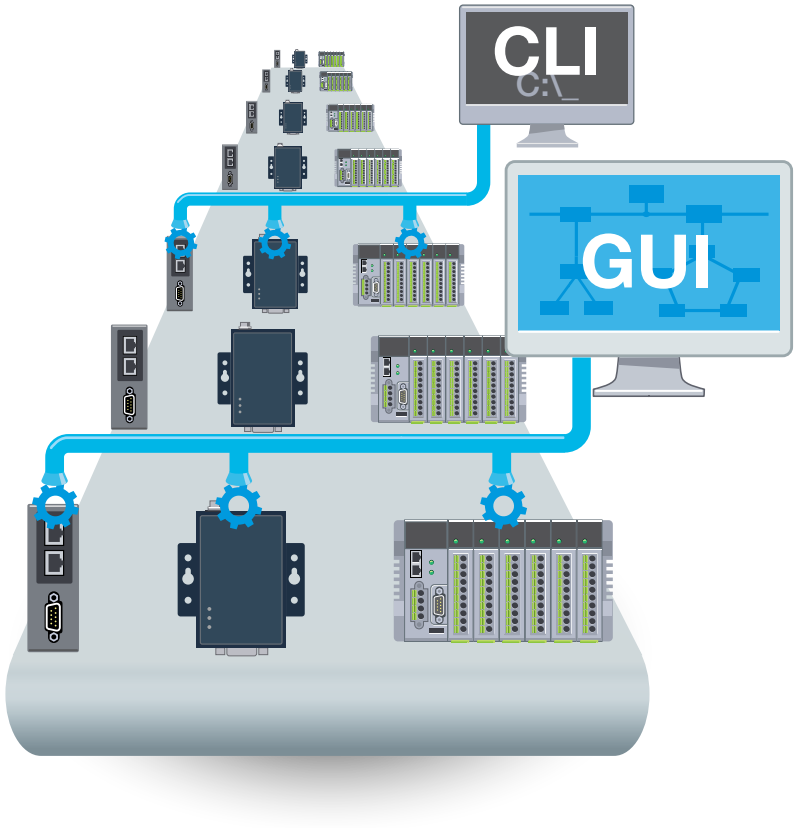


Expert Tip 2

## Stay on Top of Device Management

When you finally get all your field devices with multiple communication interfaces connected, another big question arises. How do you manage dozens or hundreds of different kinds of connectivity devices? During your daily operations, you need to monitor your connectivity devices to keep them up-to-date with the latest firmware and minimize unauthorized access and potential intrusions by updating device logon credentials for every user. Such tasks might not be an issue when there are only a few devices and one type of connectivity device. However, it can be a huge burden if dozens of different kinds of connectivity devices are used in your IIoT application.

Having a software tool or utility that can help you manage large amounts of different kinds of connectivity devices can make daily operation much easier. With the lines between the IT and OT worlds becoming increasingly blurry in the IIoT era, management tools need to be flexible enough to serve users from both domains. Besides mass device management capabilities, the connectivity device you choose should have both **a GUI for OT users** and **CLI for IT users** to optimize IIoT system maintenance.



Expert Tip 3

## As Always, Cybersecurity Matters

This isn't the first time we've mentioned cybersecurity—and it won't be the last! The truth is, the diversity of end devices in industrial field sites, distributed architectures, and legacy systems increases the security risk of your IIoT applications because most of these devices are not designed with cybersecurity in mind. As a result, it is essential to select connectivity solutions with built-in security features to place in front of your end devices. But with so many connectivity solutions on the market to fulfill the communication demands of different edge devices, how can you ensure your field data are well protected? Enter the **IEC 62443** standard, a set of global security guidelines that list specific security requirements for device manufacturers to follow to ensure the device you choose meets the latest cybersecurity standards.

When you choose a connectivity device, use the following checklist to make sure the devices support sufficient security features and allow you to define and control user access to your IIoT applications.

- ☑ Identify and control who can log on to devices
- ☑ Increase password complexity to enhance access control
- ☑ Verify authorized devices before the devices gain access to the network and communicate with other devices
- ☑ Encrypt confidential serial interface data on the network to ensure data integrity
- ☑ Encrypt configuration data to increase confidentiality
- ☑ Select device vendors that respond quickly to and fix reported vulnerabilities

Keep the above three tips in mind so that enabling device connectivity for your IIoT applications can be easier, more secure, and more efficient. To help you get started, Moxa has developed a series of device connectivity solutions—including **serial device servers**, **protocol gateways**, and **remote I/O devices**—that are capable of connecting your field data to private or public servers securely and efficiently.


"Enabling device connectivity for large-scale or highly-distributed IIoT applications in an increasingly connected world requires smooth communications between OT and IT systems, powerful device manageability, and uncompromised cybersecurity."

# Industrial Networking Needs—Now and in the Future

In the previous chapter, we discussed how to enable connectivity for industrial field devices so that your IIoT applications and previously unconnected OT assets can benefit from data acquisition, data transformation, and data analysis. However, connecting all of these field devices also requires building a network that can support information flows among multiple interconnected devices, systems, and even remote sites.

Consequently, you may want to consider incorporating the following elements into your industrial network infrastructure.

## Ethernet Network Nodes

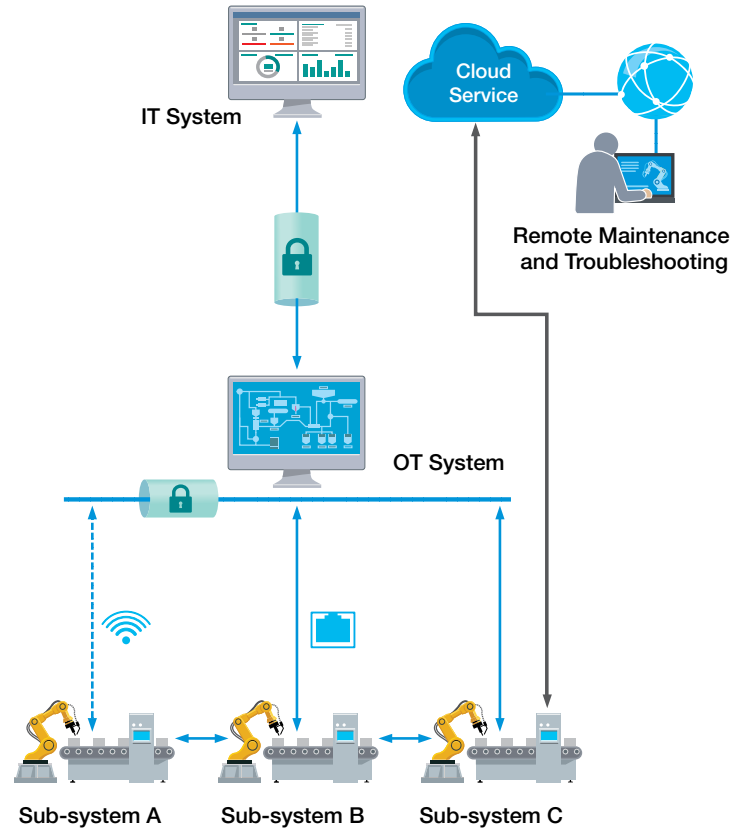
A wide variety of managed or unmanaged Ethernet switches are available for building the Ethernet foundation of your LAN, integrating remote edge systems, and connecting the overall network.

## Wireless Network Nodes

For hard-to-wire applications or those that require greater mobility, wireless LAN technologies can provide more cost-effective and flexible options instead of, or in addition to, wired Ethernet networks.

## Network Gatekeepers

Connecting field devices and OT assets to the Internet exposes your network to new cybersecurity risks. Secure routers and firewalls provide an excellent first line of defense that you will also want to consider.




## Future-ready Industrial Networks

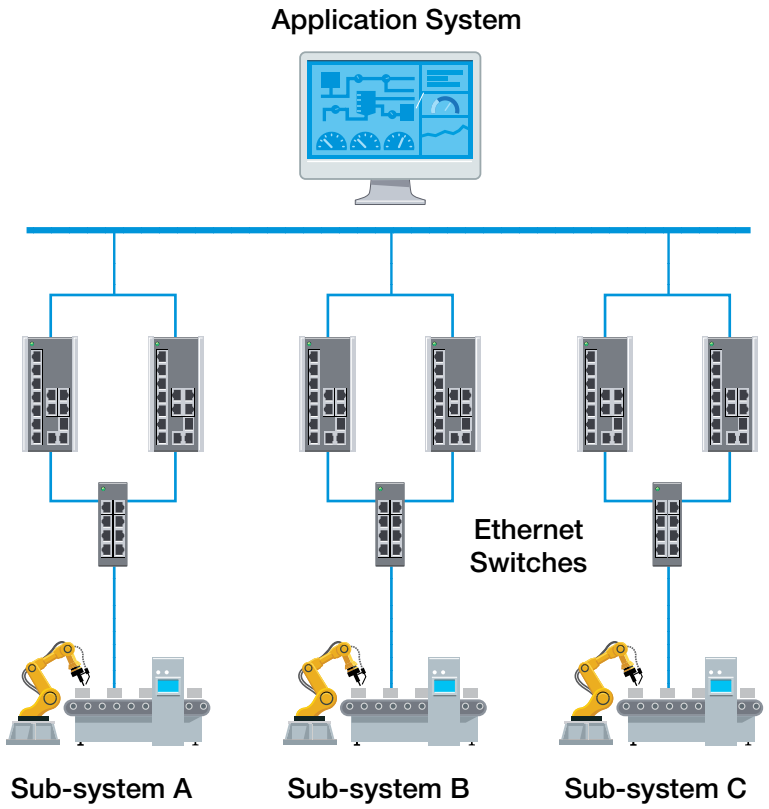
Many IIoT applications not only bring business opportunities, but also require more out of our existing network infrastructure. To win a long-term game, it is essential to ensure your industrial networks can take on future challenges and opportunities.

The following chapter presents key considerations to help you plan ahead when deploying Ethernet switches, wireless devices, secure routers, secure remote access, and network management for your current and future industrial networking needs.

# Gear Up Your Ethernet Switches for Edge Networks

Connecting a limited number of equipment in just one system can be hard enough. For a single automated production line, you may only need one or two Ethernet network nodes to enable connectivity so that operators located in the control center can monitor the system status and respond to incidents. Now imagine the headache of connecting a growing number devices from multiple systems into a single network. Every issue and challenge is multiplied. This is the reality faced by industrial automation engineers tasked with integrating several automated production lines across different factories. How do you ensure all of these devices and Ethernet nodes are connected and that operators receive the critical data they need to maintain continuous operations?

One solution is to deploy more managed Ethernet switches, which would allow you to manage your network transmissions and set related parameters according to your needs. Although managed Ethernet switches offer greater control and granularity, maintaining multiple managed switches could take a lot of time and effort. What's more, increasing the number of manageable network nodes may increase configuration and maintenance effort. Indeed, careful network planning and design are essential so you don't outgrow your network too quickly. Alternatively, using unmanaged switches at some network nodes may also improve overall network efficiency and reduce maintenance effort.

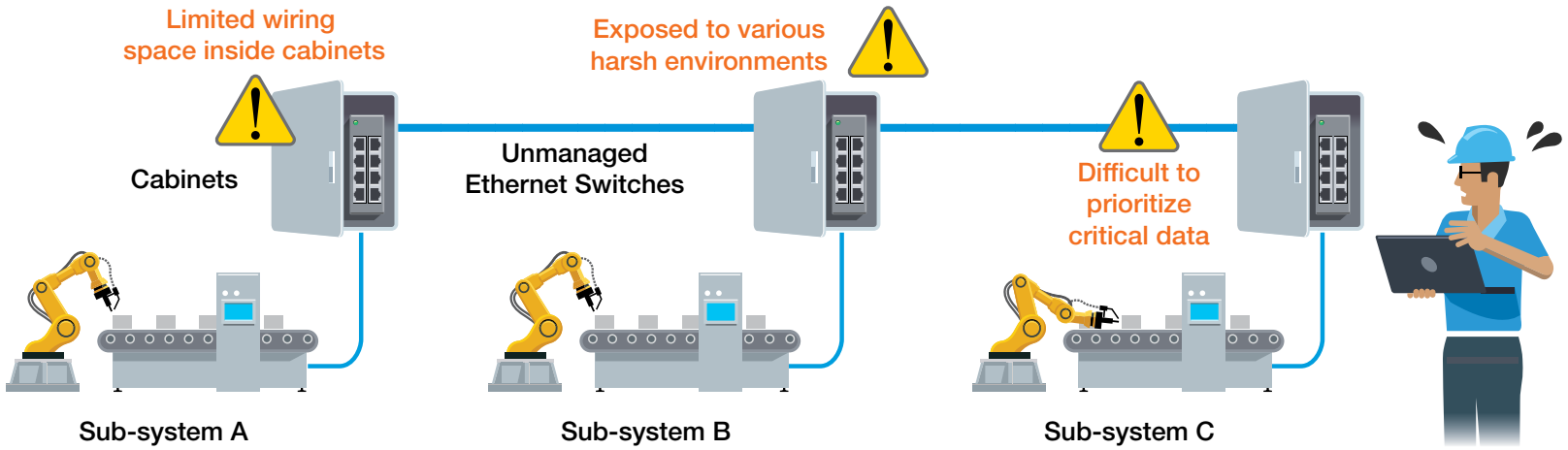


# Key Criteria for Choosing Unmanaged Ethernet Switches

Industrial operators often regard unmanaged Ethernet switches as simply network hubs for connecting field data to IP networks. When industrial operations are up and running, operators may even forget that they have unmanaged Ethernet switches on their networks. However, when more and more devices are connected to generate business insights, industrial operators may become overwhelmed by unexpected network instability. To satisfy increasing complex network requirements, unmanaged Ethernet switches need additional features. Here are some key criteria to help you choose which unmanaged switches best suit your IIoT applications.

## Key Question

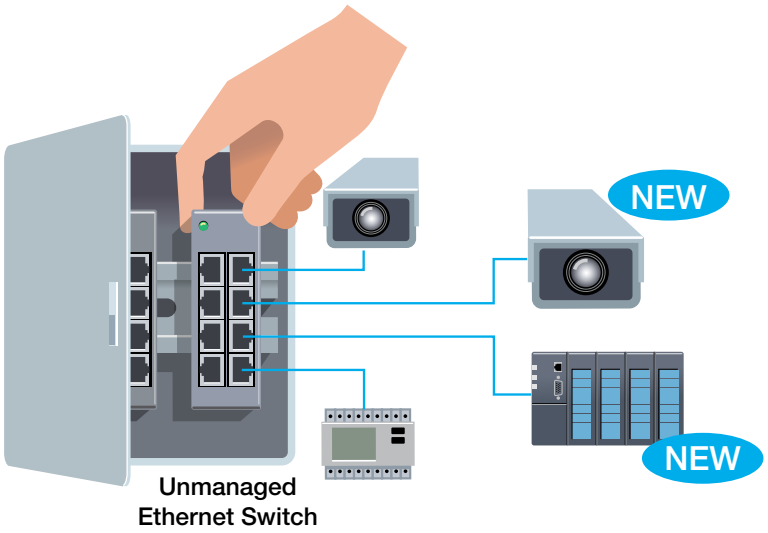
How can you squeeze an unmanaged Ethernet switch into a space-limited control cabinet that is already filled with multiple industrial devices, and still make it easy for engineers to check device and network status during operations and maintenance?



Key Criteria 1

## Plan for Expansion

The basic requirement for ensuring your network can support a growing number of connected devices is to use unmanaged switches that have a sufficient number of ports and enough bandwidth for high data volumes. Unmanaged switches are usually installed in space-limited cabinets so using a **compact yet high port density solution** can also save you trouble on future expansion. Another major consideration is network speed and transmission distance. Today, there are various types of data, such as video streaming, that use a lot of bandwidth and affect overall transmission speed. Unmanaged switches with Gigabit ports or fiber ports can ensure sufficient network speed for data uplinks, now and in the future.

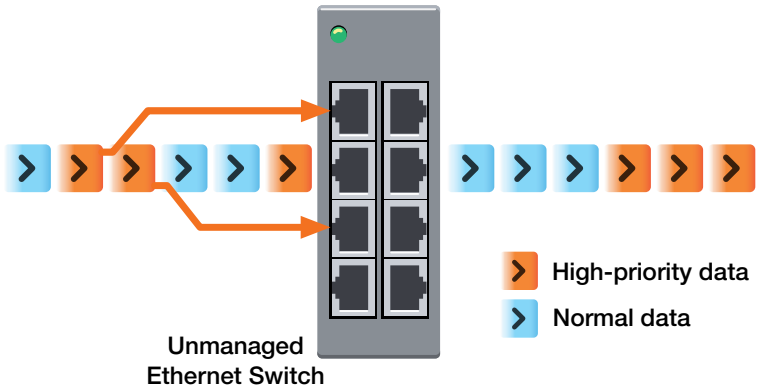



Key Criteria 2

## Prioritize Packets at Each Node

**Quality of Service (QoS)** is a common function used to ensure that critical data is always sent with high priority. Without QoS, critical data may be delayed during transmission if the network is congested. QoS is usually supported by managed switches or certain controlling equipment, such as PLC devices, but is rarely seen on unmanaged switches. With growing demand on network nodes to transmit multiple data types from field sites, it seems reasonable to also have this function on unmanaged switches to ensure that critical data can be transmitted in time without spending extra effort and money to deploy managed switches at every node.

When choosing unmanaged switches, check if they have QoS or similar functions that can prioritize critical data control so that you can keep your network simple and avoid spending too much time and effort on operating managed switches with unnecessary functions.



Key Criteria 3

## Verify Reliability for Any Environment

Choosing unmanaged switches that have industry certifications for your specific application requirements is the simplest way to verify reliability. However, not all industrial applications require certifications. Nonetheless, two commonly seen environmental conditions you should be aware of are extreme temperatures and high electromagnetic interference. Unmanaged switches featuring **wide operating temperature** and **redundant power inputs** can ensure your network operation stays up and running under harsh conditions.

In the event of an emergency, such as a power or port failure during operation, the unmanaged switches should also be able to send alerts to operators so that they can respond immediately.

**Learn More**

Looking for examples of how to achieve reliable operations? Download our application notes to learn more.

Using the three aforementioned criteria to evaluate your options can help you find the right unmanaged switches for your industrial applications. To address the needs of rapidly-expanding industrial networks, Moxa has developed a new series of industrial unmanaged Ethernet switches—EDS-2000-EL Series and EDS-2000-ML Series—that provides an extra-small footprint and reliability, easy deployment, and flexibility for a variety of industrial applications.

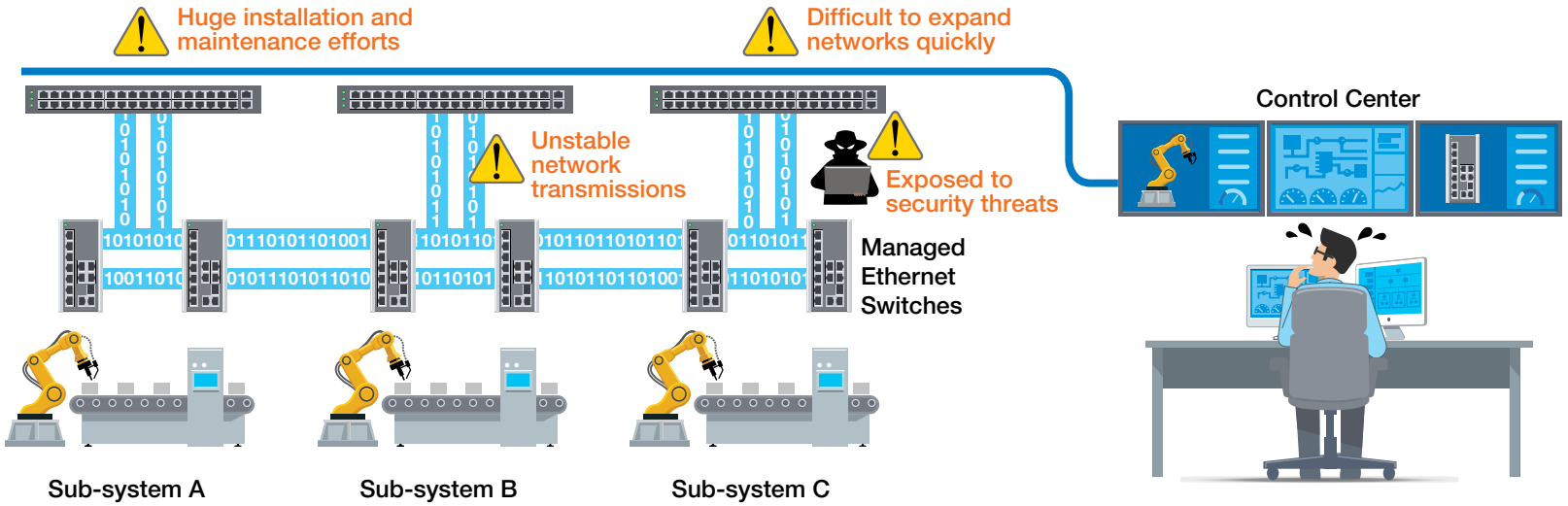

"Unmanaged switches with an extra-small footprint and managed functions such as QoS can help keep your network under control."

# Key Criteria for Choosing Managed Ethernet Switches

The increasing demand on network nodes to enable connected systems has become inevitable with the trend towards Industry 4.0 and IIoT transformation in full swing. Although some network nodes can use unmanaged switches that feature basic managed functions to minimize network complexity and administration effort, other situations may still require managed switches, which continue to play an important role in large-scale integrated networks. Your managed switches need to be smarter and more versatile than before to adapt to new changes and ensure that data can be delivered to the right place at the right time. Here, we look at three key criteria to help you identify a suitable managed switch for modern automation.

## Key Question

Digital transformation relies on reliable networks to maintain system uptime and reduce risk and errors. Are your current managed switches powerful enough to take the heat?



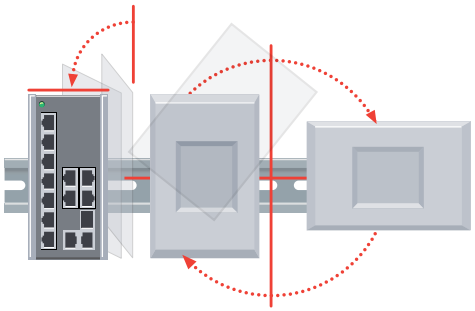
Key Criteria 1

# Easy to Use, Easy to Operate

Good usability is essential for any networking solution. What makes this more important than ever for industrial automation is the large number of network nodes that appear on a single industrial network. From installation to daily operation and maintenance, the following managed switch functions can help keep things manageable.

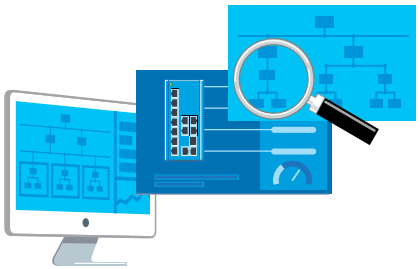
## Various Mounting Options Simplify Installation

Each node may have different requirements depending on where it is installed. Having various mounting options can make installation easy.



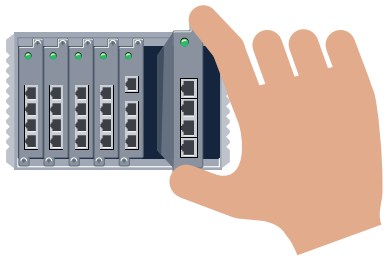
## A Glimpse at the Network Status

Tracking the status of network nodes is just one of the hundreds of tasks engineers need to juggle. Consequently, choosing managed switches that have user-friendly interfaces allows you to quickly check the status and make changes easily.



## Easy-to-maintain Hot-swappable Design

Device maintenance is unavoidable. Choosing a modular managed switch allows you to hot-swap a power or line module during routine maintenance without affecting overall operations.

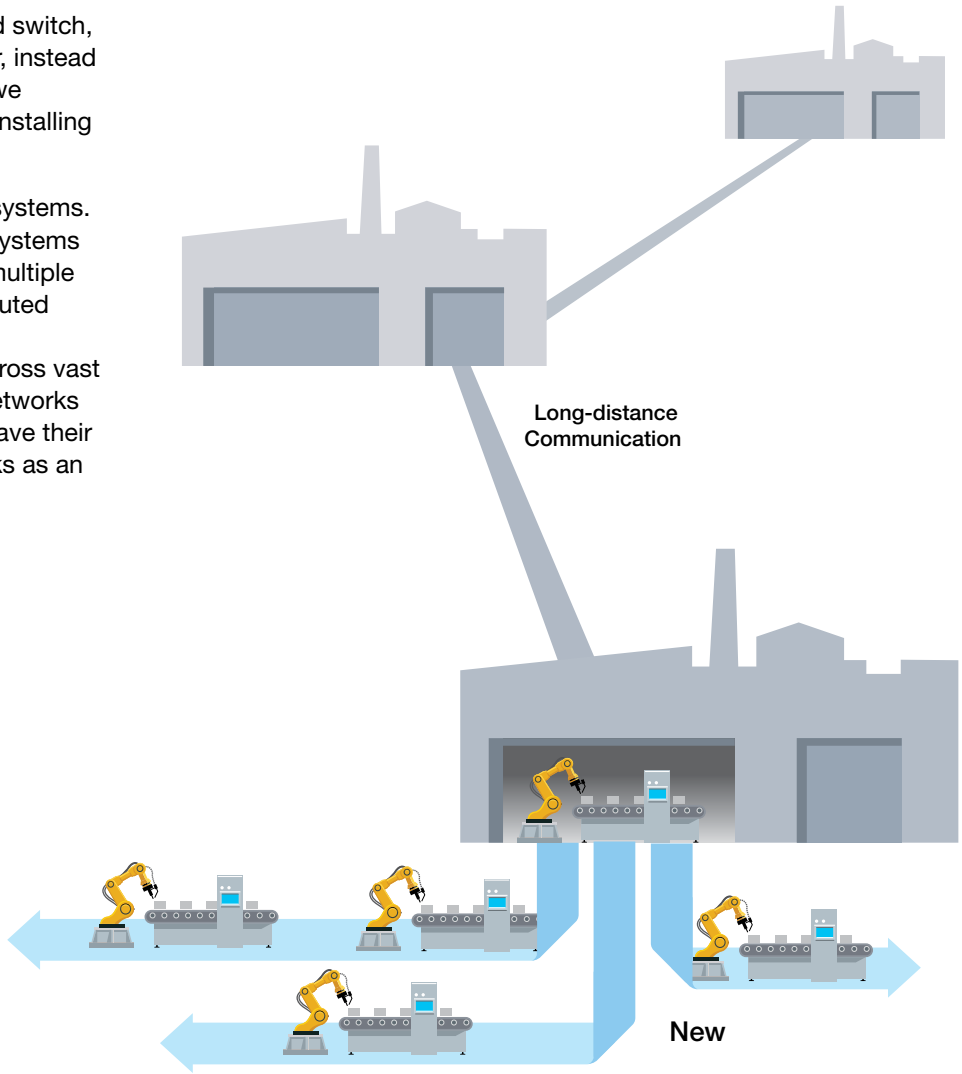


Key Criteria 2

## Ready to Scale

As with unmanaged switches, when choosing a managed switch, you need to consider future network expansion. However, instead of looking for a compact and high port density solution, we recommend choosing a modular design to save time on installing additional systems when the need arises.

Another consideration is the location of your connected systems. This might not be an issue when you enable connected systems within a single factory. But what if your project includes multiple factories or facilities in different places? For highly distributed networks, managed switches that support **optical fiber transmissions** can ensure reliable data transmissions across vast distances. Indeed, environmental limitations can make networks difficult to connect. Although wired cabling options still have their benefits, you may also need to consider wireless networks as an alternative in hard-to-wire applications.



Key Criteria 3

# It's All About Availability and Security

Connecting industrial systems with each other substantially increases network complexity and can affect your day-to-day operations. Any single point of failure can cause network downtime, and critical data can be lost or tampered with. To avoid network node failures, your managed switches need redundant mechanisms and security functions.

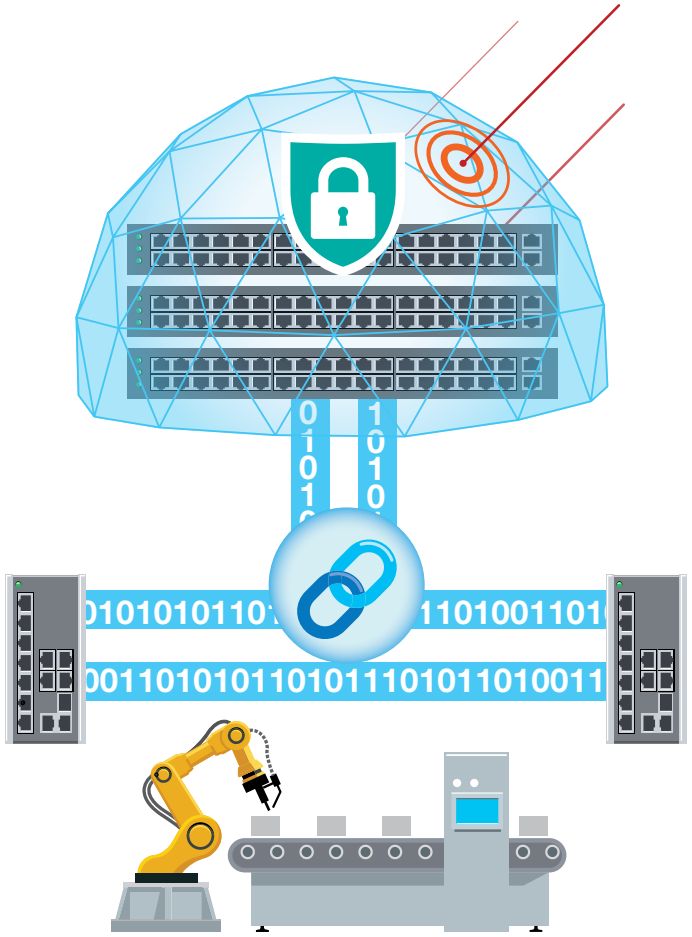
## Redundant Mechanisms

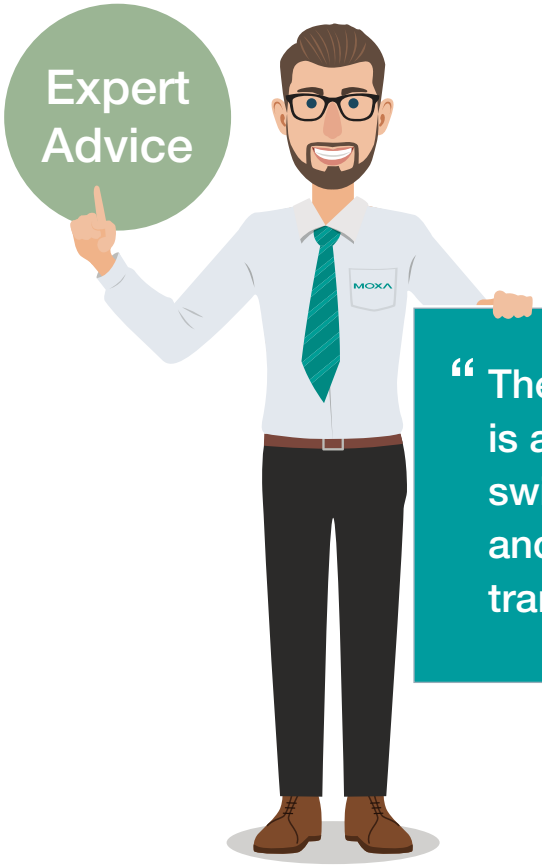
Network redundancy is an advanced function we have seen on managed switches. The idea is to prevent the loss of critical data if a network node fails. A redundant backup path can be enabled to bypass the failed node and recover the data transmission within seconds or even faster.

## Security Functions

Another potential risk for increasing the number of network nodes and connectivity is greater exposure to unauthorized access and vulnerabilities. Security concerns should not be overlooked, so we suggest choosing networking devices with security features based on the IEC 62443 standard to protect your network node from unwanted access. For additional peace of mind, you may even want to choose a vendor that has its own cybersecurity response team to ensure networking devices are protected from any vulnerabilities.

Using the three key criteria above to evaluate your options for managed switches can help you find the most suitable solution for automating your industrial network. In response to rapidly changing network requirements, Moxa has developed a new series of industrial managed Ethernet switches—the MDS-G4000 Series—with a scalable modular design that offers cost-efficient usability, security, and network availability for a variety of industrial applications.






"The key to developing reliable networks is a powerful managed Ethernet switch that is scalable, easy-to-use, and capable of keeping your data transmissions on time and secure."

# Get Unwired to Unleash More Possibilities

It's not always possible or ideal to pull wires in every industrial application. In situations where it's hard to wire or reconfigure industrial operations to ensure time to market, industrial wireless LANs (WLANs) can provide an ideal alternative to traditional wired Ethernet LANs. Indeed, recent advances in wireless technology have also contributed to industrial WLANs becoming commonplace solutions in various applications, such as automotive, logistics, and transportation systems. These industrial applications usually require automated equipment that is constantly moving and difficult to wire. The growing adoption of industrial WLANs enables these systems to be connected for enhanced operational efficiency.

With so much potential waiting to be unlocked by cutting free from wires, it's no wonder the popularity of industrial WLAN applications has grown so rapidly in recent years. For instance, you can use WLAN technology to deploy automated forklifts in a smart warehouse or overhead transfer system to increase efficiency and productivity, making the best use of limited manpower.

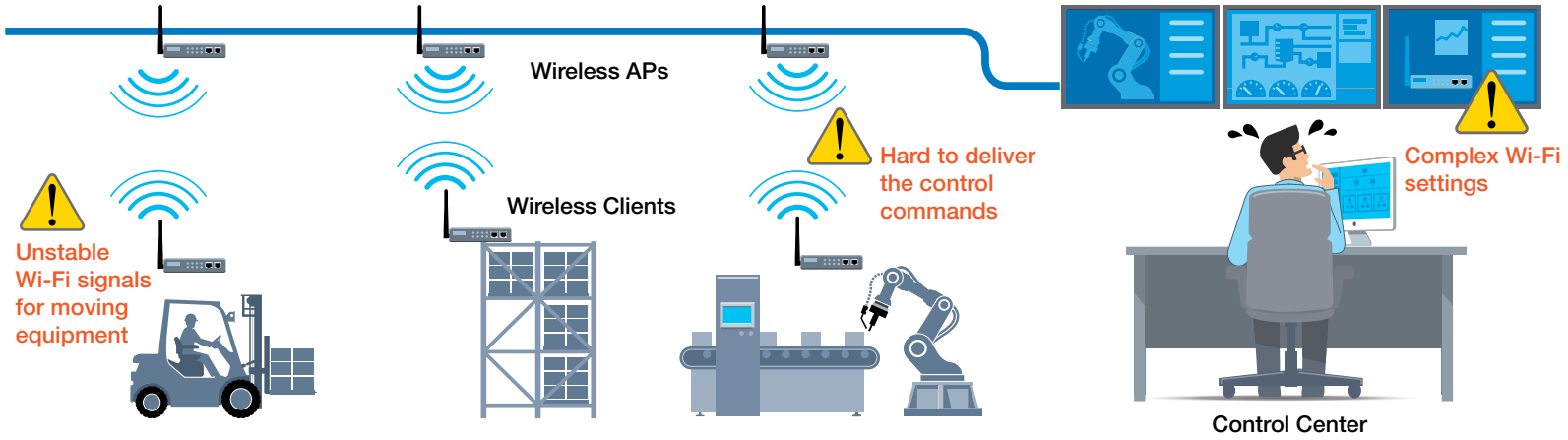
As endless as the possibilities may be, going wireless isn't always a clearcut choice. Even if you've decided on a wireless LAN, how do you choose the right solution for your industrial requirements? Consider the following criteria.

# Key Criteria for Choosing Industrial WLAN Devices

Without a doubt, industrial wireless LANs can extend connectivity beyond traditional physical limits and boundaries, unleashing new possibilities. However, industrial engineers may hesitate to embrace wireless applications due to a number of different hurdles. How do you confirm that the network is indeed connected when wireless connections are invisible? How do you troubleshoot when these invisible connections go down? Such concerns can be more vital than ever since IIoT applications require systems to be connected into one converged network. Any single point of failure can be fatal for the entire network. Besides **thoroughly planning your wireless network design**, here are some key criteria for choosing industrial WLAN devices and suggestions for how to address common concerns.

## Key Question

When taking advantage of WLAN technologies, can your WLAN devices ensure data transmission over Wi-Fi networks and still meet your expectations?



Key Criteria 1

## Wi-Fi Availability Is the First Priority

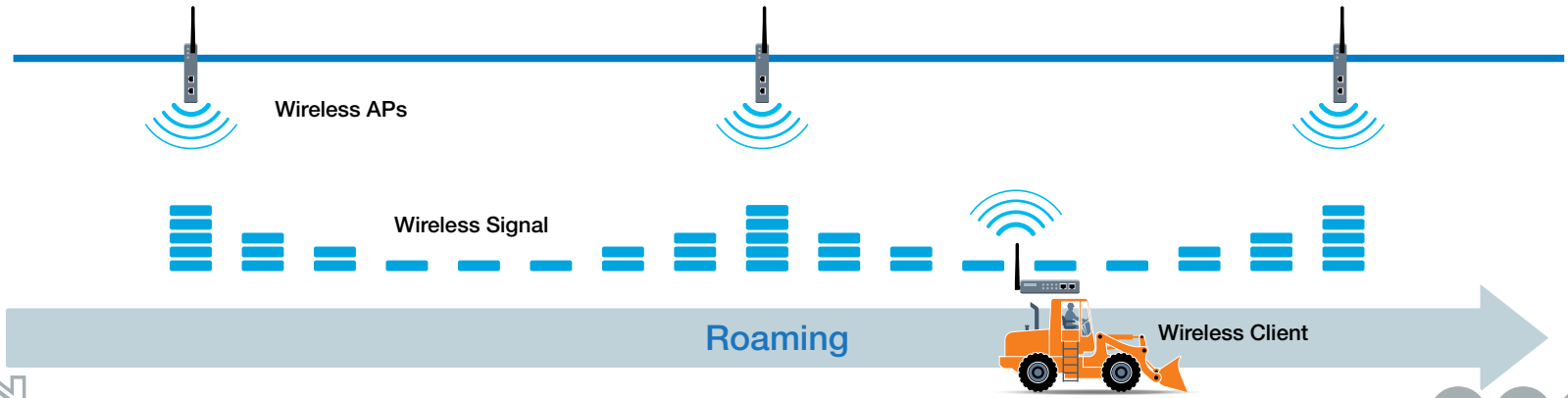
Industrial WLAN devices require specialized technology to establish and ensure reliable wireless networks. This is because wireless connection quality can be affected by many different issues, such as radio frequency (RF), interference in an industrial environment, incorrect antenna configuration, signal strength over long distances, and so on. Failing to properly design your system to avoid such issues can result in unstable communications, or even permanently damage your devices and cause a complete shutdown of your system.

In addition, constantly moving equipment requires extra attention to roaming requirements. For example, even if you have a strong wireless signal on your AP, moving devices to a different location may require a greater transmission signal, resulting in slower Wi-Fi connections or even network failures. Since slow or failed connections are unacceptable in industrial environments, consider **advanced wireless roaming technologies** that can achieve millisecond-level roaming to ensure reliable wireless connections.

### Learn More

You can't be too careful when it comes to wireless network design, especially for moving equipment in AS/RS. Download our white paper to learn more.

White Paper



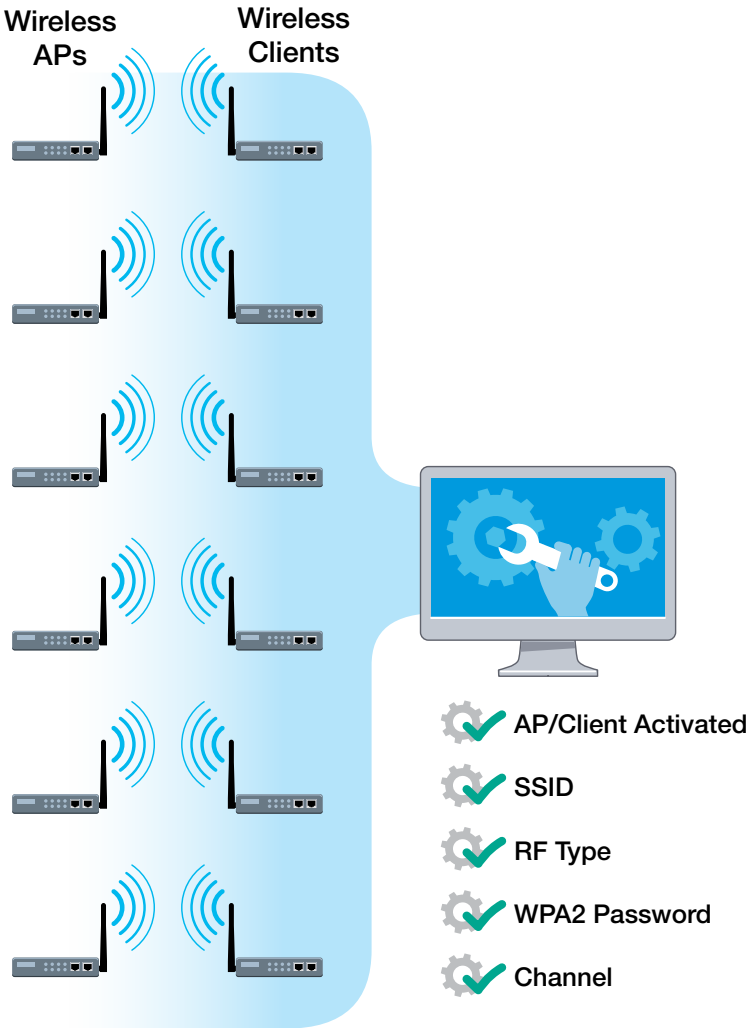
Key Criteria 2

## Minimal Effort on Wi-Fi Settings

Whether you are implementing a wireless network for the first time or have numerous WLAN deployments under your belt, you always want to choose easy-to-use solutions. Although wireless connections make constructing network infrastructure more convenient, network setup and long-term maintenance can also have a big impact on user experience. When it comes to basic device configuration during the initial setup stage for deploying or maintaining a network, a powerful software tool can save you significant time and effort. Once the networks are up and running, a software tool that can configure all your devices easily and find the best Wi-Fi channels to use on your environment with a click of a mouse can help keep your wireless connections stable and take the headache out of network administration.

### Learn More

Watch our video to learn more about fast and easy Wi-Fi network deployment.



Key Criteria 3

## Don’t Let Protocol Compatibility Issues Hold You Back

Many WLAN devices are deployed in various industrial applications, including **automatic guided vehicles (AGVs) and forklifts in logistics systems**. These systems require sophisticated devices such as sensors and PLCs to determine the location of moving vehicles. It is essential to ensure seamless communications between PLCs and control centers for safety reasons. When industrial equipment such as PLCs connect to a wireless client, a common issue is whether the wireless client device can support certain industrial protocols, such as **PROFINET**. To ensure seamless industrial protocol communications, consider the following requirements:

1. Layer 2 transparency over WLAN
2. Communication latency that meets your application requirements

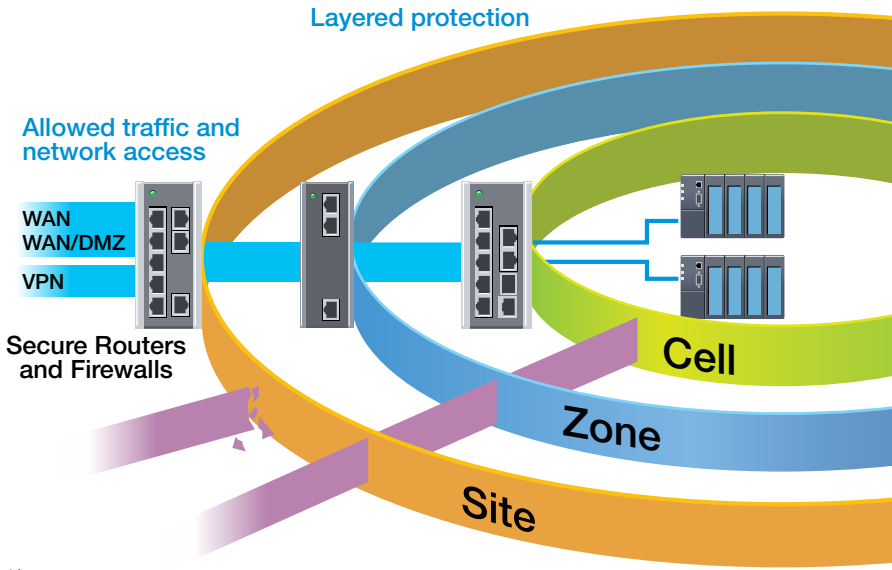
These three key criteria have been distilled from our many years of experience in enabling industrial connectivity for customers around the world. To learn more about industrial IEEE 802.11n wireless AP/bridge/clients specifically designed to overcome the challenges of industrial applications, visit the **Moxa website**.


"Reliable wireless networks require an industrial WLAN solution that can ensure connection availability, communication interoperability, and ease of use at every stage of operation."

# Your First Line of Network Defense

Hundreds of thousands of people left without electricity[1]. Global supply chains screeching to a halt[2]. These are just some of the devastating effects of cyberattacks on critical infrastructure and manufacturing in recent years. In fact, the past 10 years have seen more cybersecurity incidents involving industrial control systems than ever before[3]. Some of these incidents were targeted attacks, such as Stuxnet, which crippled the Iranian nuclear program, whereas others were non-targeted incidents where malware spread to industrial control systems by infecting a network computer.

In the IIoT era, previously unconnected systems are now connected over private or public networks in order to gain more insights and improve productivity. The downside of greater connectivity is that industrial networks are no longer immune to cyberthreats. The good news is a growing chorus of experts is also calling for industrial networks to shore up cybersecurity. Generally speaking, there are two methods for implementing industrial cybersecurity. One is to secure the foundation of your network infrastructure and only allow authorized traffic to flow to the proper places. The other involves identifying critical assets and applying layered protection. Industrial secure routers and firewalls are essential to both of these methods as they are deployed at the front lines to prevent unauthorized access and traffic to your industrial networks.



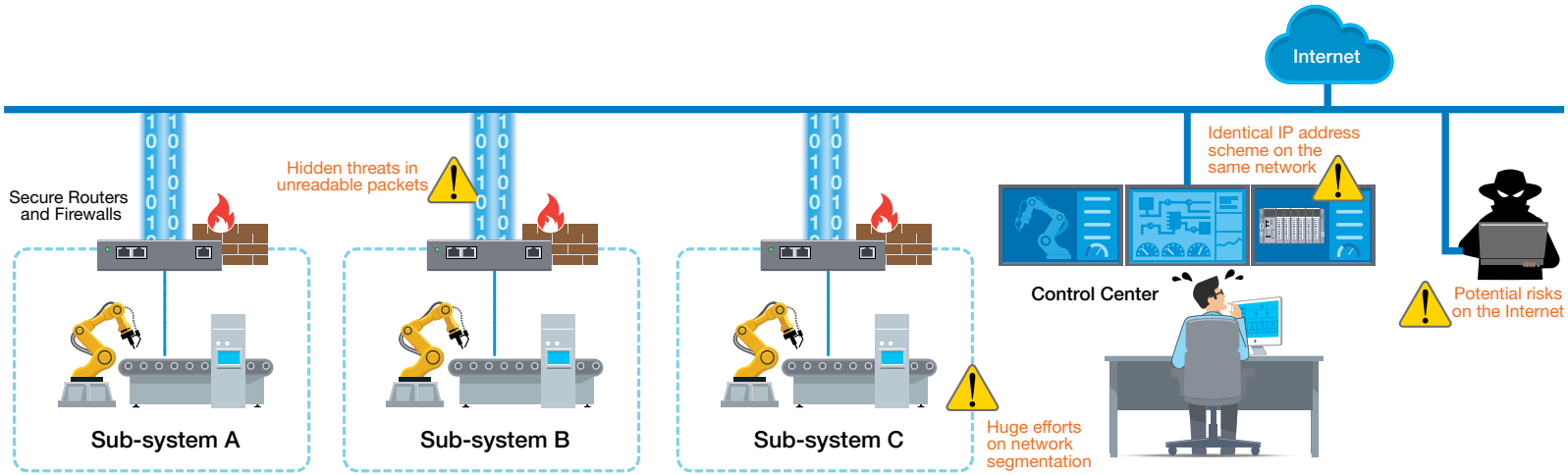

1. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
2. https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-march-26/
3. According to ICS-CERT Advisories from the United States Cybersecurity and Infrastructure Security Agency (CISA). https://www.us-cert.gov/

# Key Criteria for Choosing Industrial Secure Routers and Firewalls

Industrial control systems can apply a “defense-in-depth” approach to protect critical equipment and secure various locations, device cells, function zones, and factory sites on your automation network. Defense-in-depth cybersecurity includes three types of controls: physical, technical, and administrative. First, implement physical controls by segmenting your network and creating boundaries between each segment. Next, apply technical controls by securing network traffic or filtering data packets. Lastly, enhance administrative security by managing IP addresses and adopting strong security policies. Secure routers and firewalls provide an excellent way to achieve defense-in-depth cybersecurity on your network, but how do you choose the right router or firewall for your industrial application? Consider the following criteria.

## Key Question

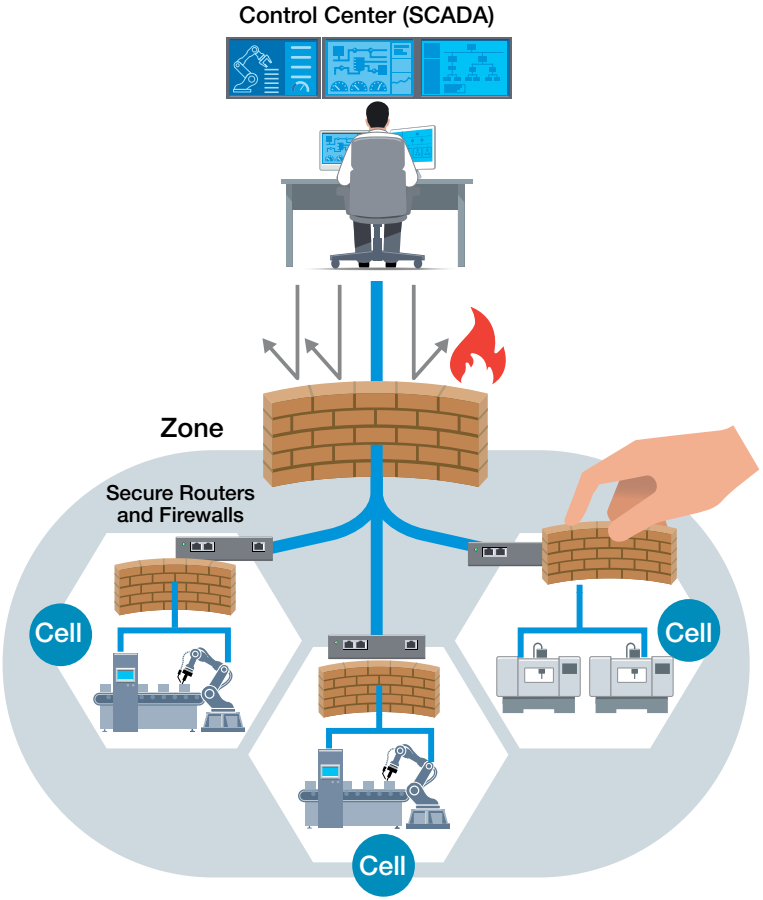
Shoring up security on your industrial automation network is no longer a choice; it is a must. How do you protect your business and assets from cyberthreats while keeping industrial operations up and running?



Key Criteria 1

## Adding Firewalls Without Changing Your Network

Network segmentation involves breaking down the network into physical or logical zones with industrial firewalls. A firewall is an access control device that looks at the IP packet, compares the packet with preconfigured policy rules, and decides whether to allow, deny, or take some other action on the packet. Generally speaking, firewalls can be either “routing” or “transparent”, and the type you will need depends on application requirements. Unlike routing firewalls, **transparent firewalls** allow you to keep the same subnet so that you can easily add firewalls to an existing network. With transparent firewalls, you also do not need to change the network topology. Transparent firewalls are suitable for protecting critical devices or equipment inside a control network where network traffic is exchanged within a single subnet. Furthermore, you do not need to reconfigure IP subnets because transparent firewalls do not participate in the routing process.




### Learn More

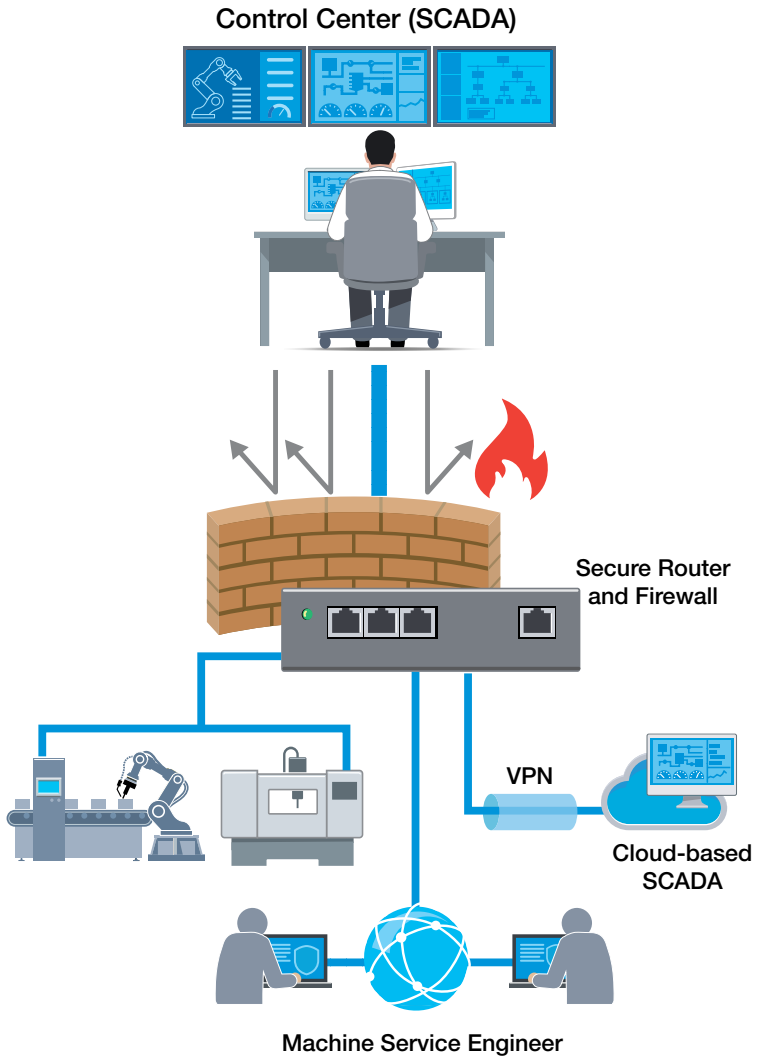
To learn more about how to choose the right industrial firewalls, download our white paper.

White Paper

Key Criteria 2

## Detect Threats and Protect Critical Data

Firewalls are akin to gatekeepers. Unfortunately, determined intruders may still be able to get through the gates on a segmented network. That's why you need to constantly check the traffic that passes through the gates you have established. One way to achieve this is to filter out unwanted commands such as write or configure commands that could cause industrial processes to fail when needed or unnecessarily trigger a safe state during production. Therefore, it is important for industrial secure routers and firewalls to support **industrial protocol filtering** at the command level (read, write, etc.) for more fine-grain whitelisting control. If you want to secure transmission of confidential data, you may also consider building secure tunnels for site-to-site communications. In some scenarios, communications over public or untrusted networks will definitely require secure encrypted data transmission. Under such circumstances, you may also want to consider **VPN capability** when choosing your industrial secure routers and firewalls.



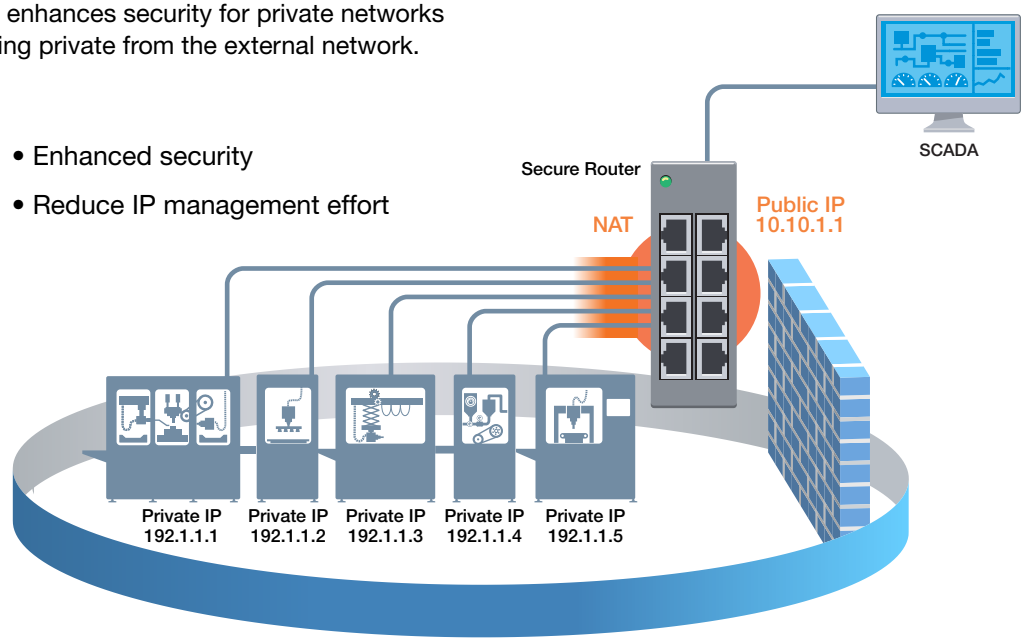
Key Criteria 3

## Getting Your Firewalls and Network Under Control

In industrial applications, there could be hundreds or thousands of firewalls installed to control data traffic and protect field equipment from malicious attacks. There could also be even more IP addresses on your network. As networks continue to expand, the more complicated it becomes to manage all of the devices, firewall rules, and IP addresses. Therefore, **Network Address Translation (NAT)** provides a very important function when you deploy industrial secure routers and firewalls. NAT allows you to reuse machine IP address schemes on the same network and connect multiple devices to the Internet, using a smaller number of IP addresses. This not only significantly reduces maintenance effort and administrative overhead, but also provides simple network segmentation. In addition, it enhances security for private networks by keeping internal addressing private from the external network.

Finding the right secure router or firewall for your application is the first half to successfully beefing up your industrial network security. Using these three criteria to help you choose can remove some of the guesswork. For instance, a highly integrated industrial multiport secure router with firewall/NAT/VPN and managed Layer 2 switch functions, such as the **Moxa EDR-810 Series**, could provide everything you need. Nevertheless, whatever solution you ultimately choose should fit your specific application requirements.

- Enhanced security
- Reduce IP management effort



Expert Advice


"Network segmentation and traffic filtering are the fundamentals to building secure industrial networks."

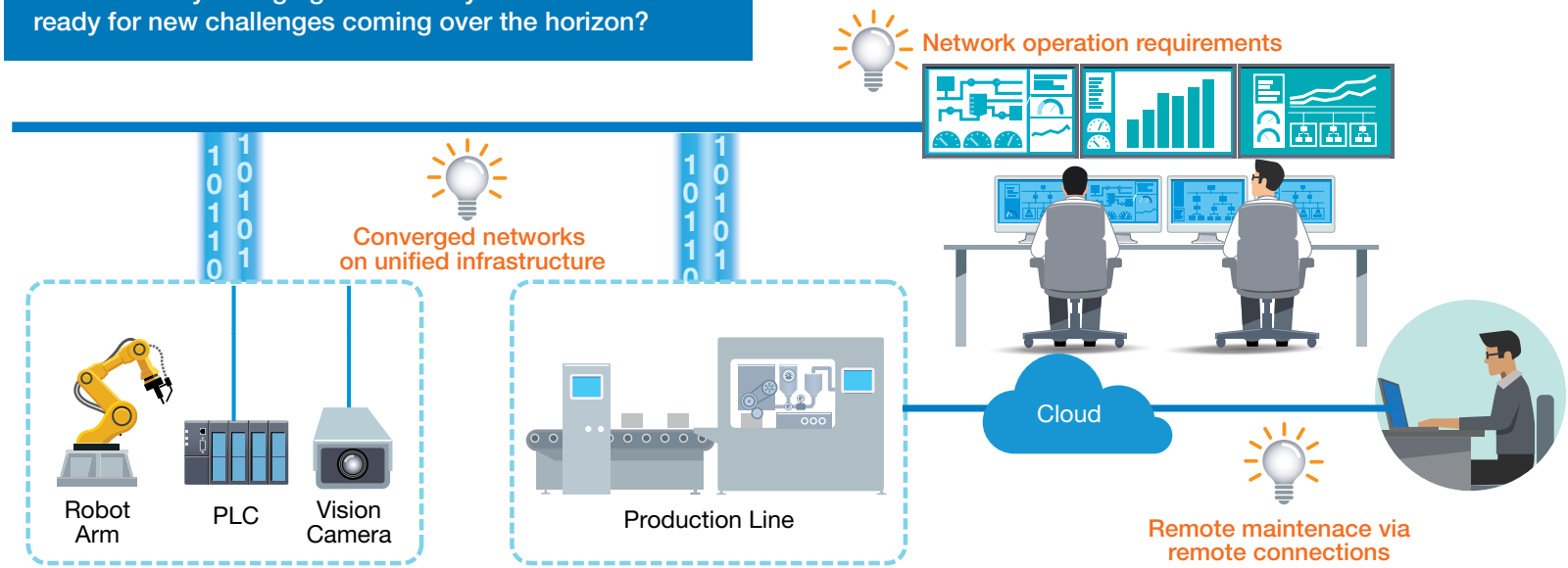
# Getting Your Networks Ready for the Future

When you finally get your IIoT networks up and running, it may be tempting to rest on your laurels. Nonetheless, change remains the only real constant in life and the world of industrial networking is no exception. Your IIoT network may be sufficient for your current needs. It may even be ready for your foreseeable application requirements over the next several years. But what about the next decade or more? Change is always in the air, and we need to be prepared.

## Key Question

Staying agile in the face of new demands has become a key criteria to maintaining a competitive advantage in our constantly changing world. Will your IIoT network be ready for new challenges coming over the horizon?

Since the early days of industrial automation, manufacturers have adopted a variety of purpose-built protocols and systems, instead of standard Ethernet technologies, for highly specialized industrial control applications. However, as the IIoT market is expected to grow at a CAGR of 24.0%[1] by 2023, industrial networks in the future will likely require the capability to transmit large amounts of data between interconnected devices or collect data from remote devices. With these growing demands on the horizon, how well-prepared you are for the future of industrial networking may determine your success in tackling new challenges. This section provides three considerations to help you prepare your IIoT-ready industrial networks for the future.



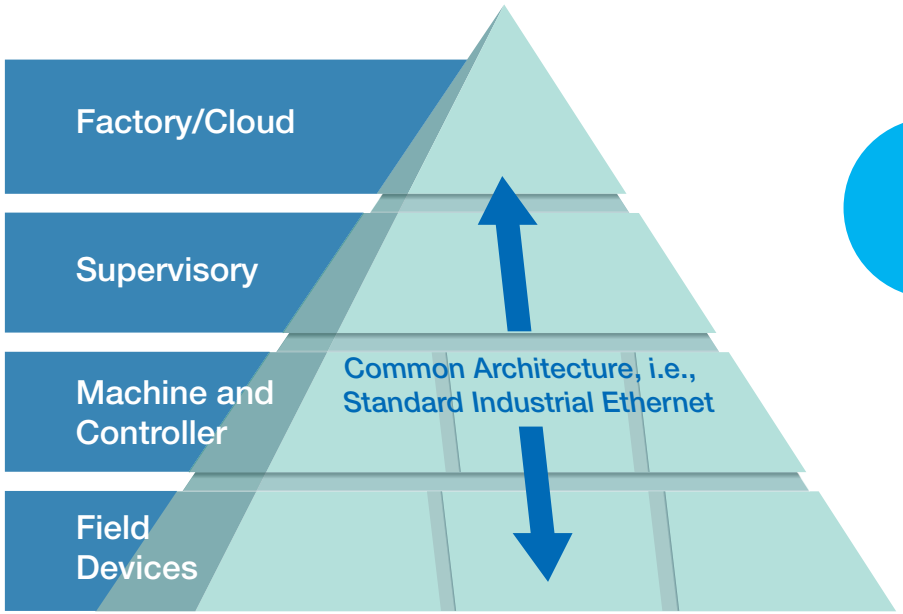

1. The Industrial Internet of Things Market Forecast, MarketWatch, March 2019

Consideration 1

## Achieve Greater Integration With Unified Infrastructure

Over the years, various devices using different industrial protocols have been deployed on industrial networks to provide diverse services. Under these circumstances, network integration usually costs more than expected or becomes more difficult to achieve. Manufacturers can either choose the status quo, that is, maintain their pre-existing isolated automation networks with numerous purpose-built protocols of the past, or alternatively **seek solutions to provide deterministic services** and integrate these "islands of automation".

If our goal is to be ready for growing demands on our IIoT network in the future, the choice is obviously the latter. The rule of thumb is to take potential industrial protocols into consideration and ensure you can redesign your networks in case any new demands arise in the market. Time-sensitive networking (TSN) is a set of new standards introduced by the IEEE 802.1 TSN Task Group as an advanced tool box. With TSN, you can build open, unified networks with **standard Ethernet technologies** that reserve flexibility for the future. Furthermore, you may consider selecting solutions offered by the key players who are advocating this new technology because they actively participate in TSN plugfests to complete the ecosystem and ensure compatibility among different vendors.




**Learn More**

To understand how time-sensitive networking transforms industrial automation, download our white paper.

White Paper

Consideration 2

## Anywhere Access to Your Remote Machines With Hassle-free Cloud Services

Cloud-based remote access offers many benefits to IIoT customers, such as reducing the traveling time and expenses of sending maintenance engineers to multiple remote sites. Furthermore, cloud-based secure remote access can provide flexible and scalable connections to meet the dynamic, changing requirements of the future. However, operational technology (OT) engineers for water and wastewater treatment plants, machine builders, and other IIoT customers may find it cumbersome to set up and maintain their own cloud servers to provide new services and applications. Indeed, there is considerable effort associated with setting up new infrastructure, even if it is in the cloud. Fortunately, OEMs and machine builders can now deliver secure cloud-based services and remote access to their customers without having to maintain their own cloud servers.

One key issue you should definitely scrutinize is the **cloud server license scheme**. Often, upfront costs may seem low for limited server hosts. However, these apparent cost savings on server hosts may actually make your project uneconomical due to a limited scale of connections. Secondly, you may also need to consider **central management capabilities** in order to flexibly expand remote connections in the future. With this said, carefully weigh the costs and benefits of incorporating secure remote access to your industrial networks. Always select solutions that can eliminate the hassles mentioned and help you focus on delivering more value and benefits to your customers.

**Learn More**

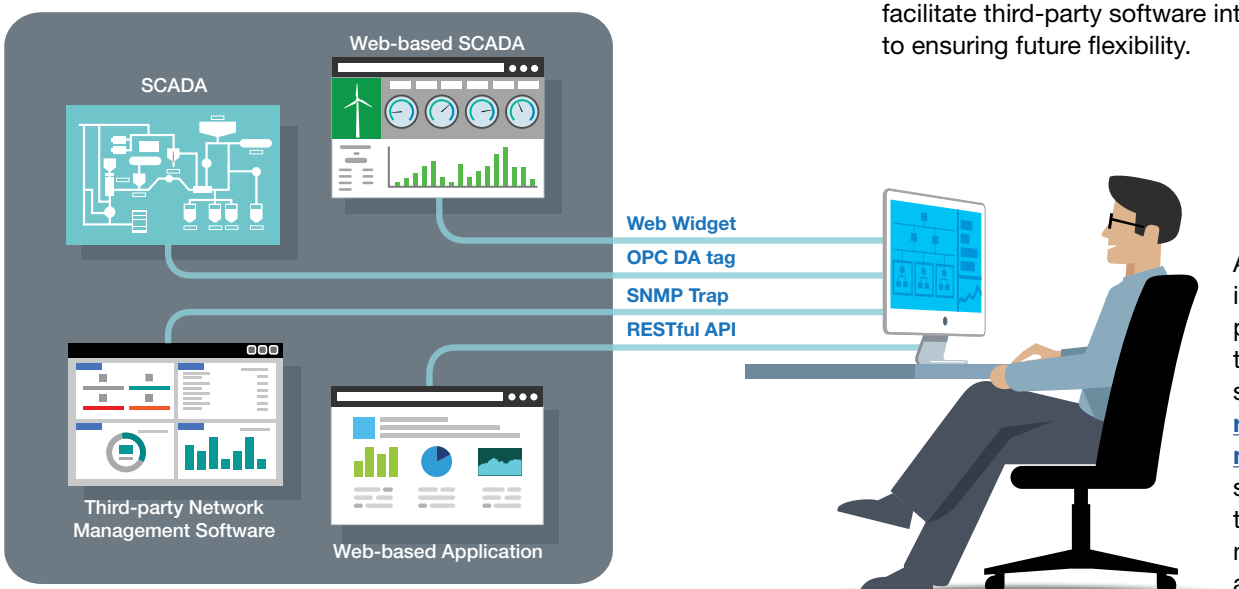
Visit our website to see how easy it can be to develop cloud-based secure remote access.

Consideration 3

## Visualize Your Network Status for Both OT and IT Professionals

You may have seen the following scene in a movie or photograph in the news. The control room of a metro system contains a group of monitors showing the current status of each metro station in the system, the locations of all the moving trains, and so on. Managers or operators need to quickly judge the current situation and take action according to the information aggregated on the screens in front of them. This visibility helps them keep everything under control. When complexity increases with greater connectivity on industrial networks, it can become very difficult to identify the root cause of problems and maintain sufficient network visibility. Control engineers often have to revert to trial and error to get the system back to normal, which is time-consuming and troublesome.

Therefore, in order to facilitate and manage growing industrial networks, network operators need an integrated network management software to make more informed decisions throughout network deployment, maintenance, and diagnostics. In addition, as your systems continue to grow, you will need to pay attention to a number of network integration concerns. First, only managing industrial networks in local control centers may not be feasible three or five years later, especially when existing systems need to be integrated with new ones. It is therefore important to use **network management software with integration interfaces**, such as OPC DA tags for SCADA system integration or RESTful APIs for external web services. Furthermore, an interface to facilitate third-party software integration is also a key criteria to ensuring future flexibility.




As a pioneering expert in industrial networking, Moxa provides a number of innovative technologies and solutions, such as secure cloud-based remote access and a network management tool, that already satisfy the above three factors to help you accelerate your network readiness for future IIoT applications.


"Future-proof IIoT networks require a unified network infrastructure, the ability to handle more and more remote access applications, and easy-to-use and powerful management tools to be ready for the future."

# Conclusion

For many industries, the IIoT presents as many challenges as opportunities. Nonetheless, this uncharted frontier in industrial automation where traditional OT and IT silos converge is clearly the way of the future. Successfully deploying an IIoT application requires careful planning and attention to detail from the moment you decide to begin your journey. From enabling device connectivity to ensuring your current and future networking needs are met, we hope the key factors discussed in this guidebook will embolden you as you embark on your own IIoT transformation journey. After all, connecting the world has always been part of our DNA.

With more than three decades of industry experience, Moxa offers myriad solutions for serial connectivity, remote I/O connectivity, and IIoT device connectivity that enable device connectivity for your trusted legacy devices and machinery. We also provide a wide array of managed and unmanaged Ethernet switches, wireless LAN technologies, secure routers and firewalls, and future-ready networking solutions to support information flows among multiple interconnected devices, systems, and even remote sites for all your newly connected OT assets. No matter how labyrinthine your IIoT application may be or where it may lead, know that Moxa stands ready to help you at every step of the way.

# Your Trusted Partner in Automation

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 65 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.


## Moxa Americas

**USA**
Toll Free: 1-888-MOXA-USA
Tel: +1-714-528-6777
Fax: +1-714-528-6778
usa@moxa.com

**Brazil**
Tel: +55-11-95261-6545
brazil@moxa.com

## Moxa Europe

**Germany**
Tel: +49-89-37003-99-0
Fax: +49-89-37003-99-99
europe@moxa.com

**France**
Tel: +33-1-30-85-41-80
Fax: +33-1-30-47-35-91
france@moxa.com

**UK**
Tel: +44-1844-355-601
Fax: +44-1844-353-553
uk@moxa.com

## Moxa Asia-Pacific and Taiwan

**Asia/Japan/Taiwan**
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
asia@moxa.com
japan@moxa.com
taiwan@moxa.com

**India**
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045
india@moxa.com

**Russia**
Tel: +7-495-287-0929
Fax: +7-495-269-0929
russia@moxa.com

**Korea**
Tel: +82-2-6268-4048
Fax: +82-2-6268-4044
korea@moxa.com

## Moxa China

**Shanghai**
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
china@moxa.com

**Beijing**
Tel: +86-10-5976-6123/24/25/26
Fax: +86-10-5976-6122
china@moxa.com

**Shenzhen**
Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
china@moxa.com