Reliable Networks Sincere Service

An Insider's Guide to Bringing Your Serial Devices to the IIoT

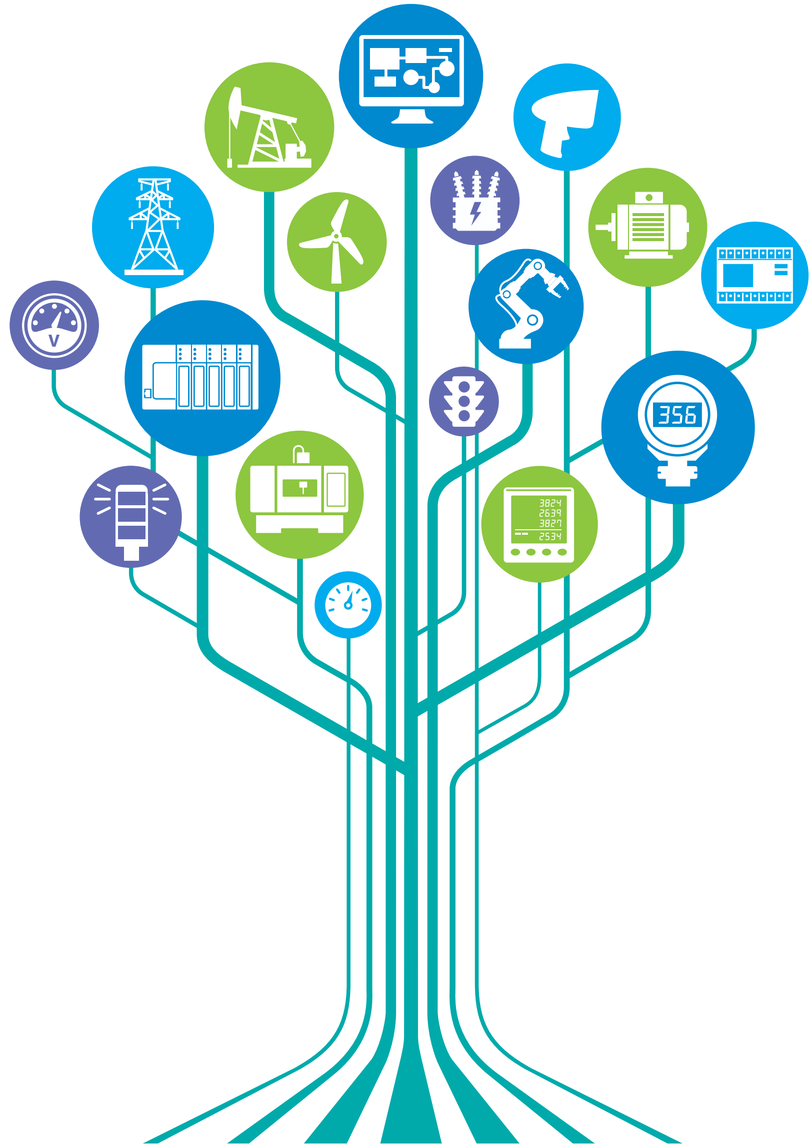
Table of Content

Introduction

The Importance of IIoT Connectivity

The Industrial Internet of Things (IIoT) offers businesses the opportunity to transform their operation and increase profits by providing a better understanding of how assets are performing, or even better, how their assets will perform in real time. The results that drive investment in the IIoT include an increase in productivity, operation efficiency, and reduced operational costs. Many businesses also sees IIoT investment as a means to gain a competitive edge over their competitors.

The ultimate goal of almost every IIoT deployment is to get actionable insights from industrial data sources for better and precise business decision-making. A number of use cases serve as examples where the IIoT has benefited numerous businesses. One shining example is where predictive maintenance has thwarted unplanned downtime in order to optimize the supply chain and asset management to maximize equipment usage and production performance.



The effectiveness of a business decision will depend on the accuracy of data acquired from field sites. For IIoT applications to reap benefits, it's essential how data has been collected and processed. A simplified data processing model in IIoT applications includes at least three layers: edge devices, interconnectivity devices (such as gateways) and a backend data server.

Edge devices encompass the industrial equipment that collect and provide data that offers valuable insights when unlocked. The interconnectivity devices aggregates collected data from the edge layers, process or even analyze it, depending on the requirements of the applications. Then, the data is transferred to the backend data server for storage or further analysis as actionable insights.

The importance of bridging the edge devices and data server makes interconnectivity devices indispensable in IIoT applications. To choose a suitable solution for your application, you need to know what kinds of devices you need to connect in the field sites.

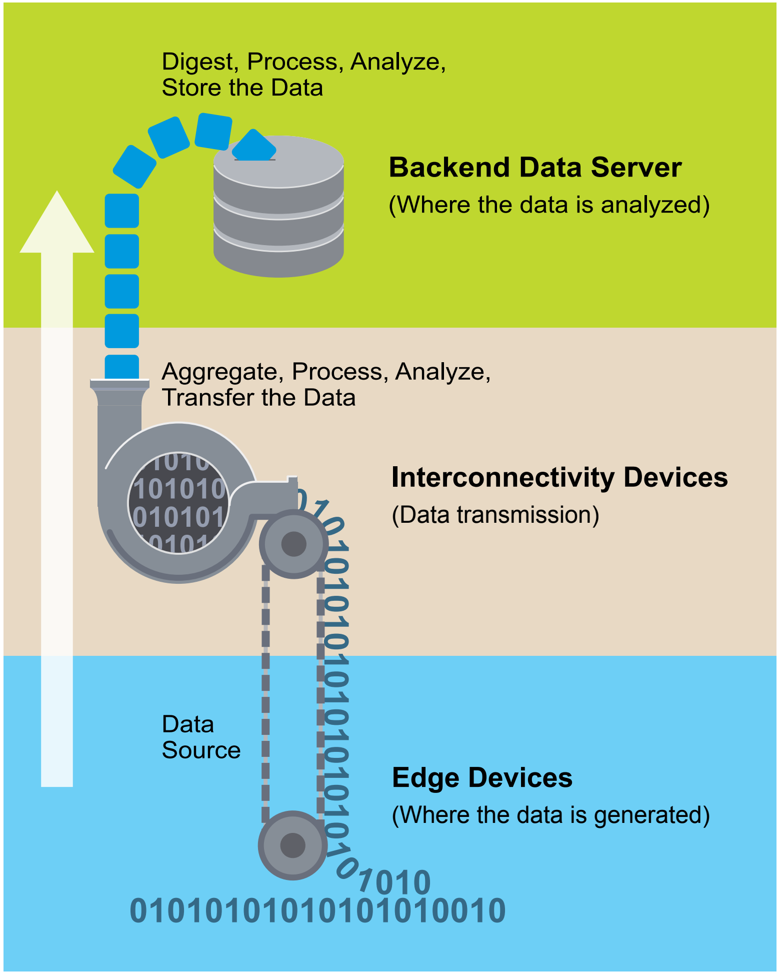
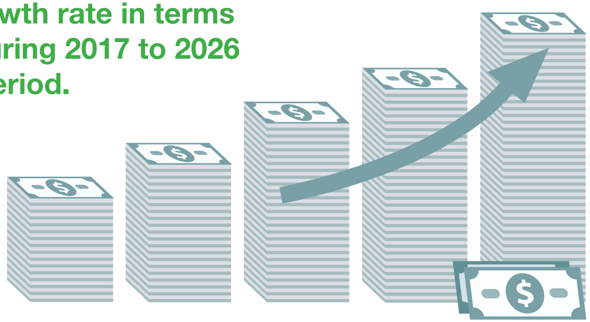


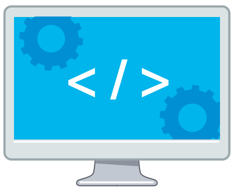
Figure 1: Data processing model for IIoT applications

Why Serial Connectivity Matters?

You may surprised to find that even today a large number of serial-based devices still exist in industrial applications, where operators are trying to collect and leverage data. According to MarketResearch.Biz, the growth rate of the global serial device server market is projected at 6.2% in terms of value from now to 2026. A number of reasons support the still wide usage of this communication technology, although it is considered as old-fashioned.

Over 6 %
annual growth rate in terms of value during 2017 to 2026 forecast period.



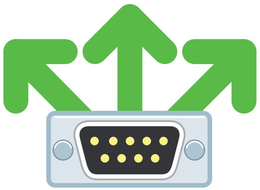


Easy to Develop: Serial application software is a lot easier to program compared to communication technologies such as USB, Ethernet, Bluetooth, or Wi-Fi, which requires a complex software stack.

The learning curve is also easier for a programmer. We are talking about the difference of a program size , for example, a couple of lines of coding versus a thousand lines of coding, or the difference between a couple days or months to develop software.

Cost-effective: In most cases, serial is cheaper to implement compared to parallel. Many ICs have serial interfaces that are built-in CPUs, which will reduce material costs.

What's more, only three wires are needed to achieve your communication purposes. The difference in cost is also significant.



Easy to Deploy: Over short distances, as well as with low-speed communication, cables are usually less sensitive to noise, so the quality of the cable material, the necessity of terminators (for long-distance communication and multidrop application only) will not easily affect communication. As long as you match the pin assignments correctly, communication will work.

Easy to Maintain: Debugging is relatively easy if there is a communication problem. The root cause might be nothing more than a wiring error, serial parameter setting error, or protocol setting error (for example, Modbus setting). Most communication problems can be addressed by fixing these errors.

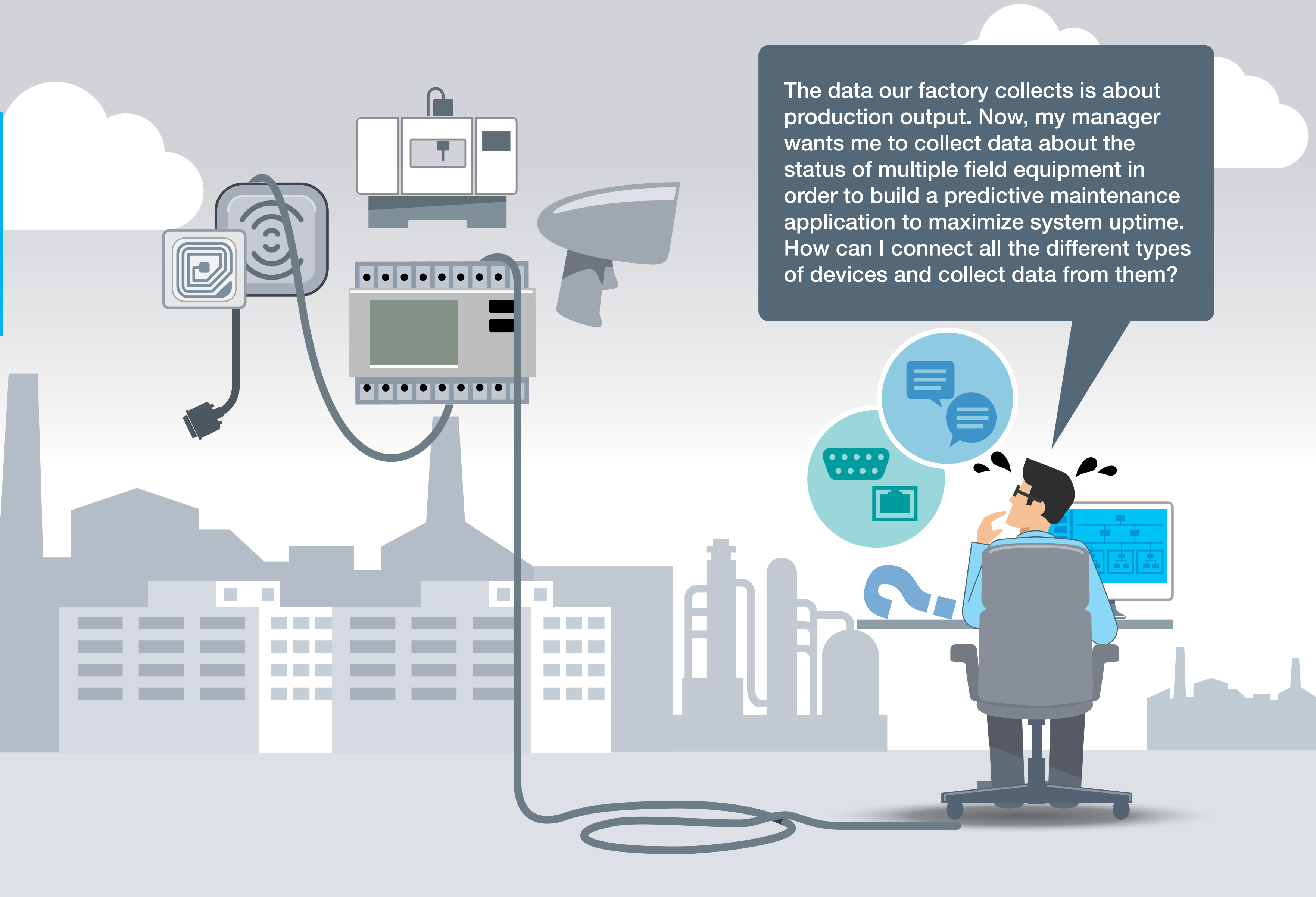
The aforementioned four reasons make serial-based devices commonly seen in various industrial applications. When you choose the interconnectivity devices for your IIoT applications, it's imperative to know how to enable connectivity for serial-based devices.

In this guide, we illustrate four practical challenges you need to know about and useful tips on how to choose the most suitable interconnectivity devices to bring your serial devices to IIoT applications.

Four Considerations to Develop Connectivity for Your Serial Devices

Interconnectivity devices need to ensure that the right data is delivered from the edge devices to the data server, without delay, tampering, or loss. To make this happen, you should take note of four considerations when developing connectivity for your IIoT applications.

Consideration One



Consideration One: Don’t Let Complex Connectivity Make You Fall Short

Overview

The complexity of connectivity in IIoT application can be attributed to edge devices, because a wide variety of device types need to be integrated into a network, and a large portion of them are legacy devices (serial) that are probably older than most of our current-day mobile phones or laptops. What makes things even more complicated is that these devices are communicating through a variety of protocols.

Data from different devices and different protocols needs to be converted in a centralized device so that an enterprise can collect and compile data through out an application field, and use this data to generate actionable insights. This is where interconnectivity devices become extremely important, as they have to enable and ensure connectivity.

Quick Tip

Taking Stock of Serial Devices

The first crucial step in any IIoT project is to understand what edge devices you need to connect in order determine the suitable interconnectivity devices to access data and transmit it through the network to where it will be analyzed. Figure 2 shows the types of serial devices commonly found in various industrial environments.

These serial devices either speak in proprietary protocols or in standard fieldbus protocols such as Modbus, PROFIBUS, etc. Even though there is a common goal to bring these serial devices to a network, the handling and converting of serial data to Ethernet can be very different for each type of serial device.

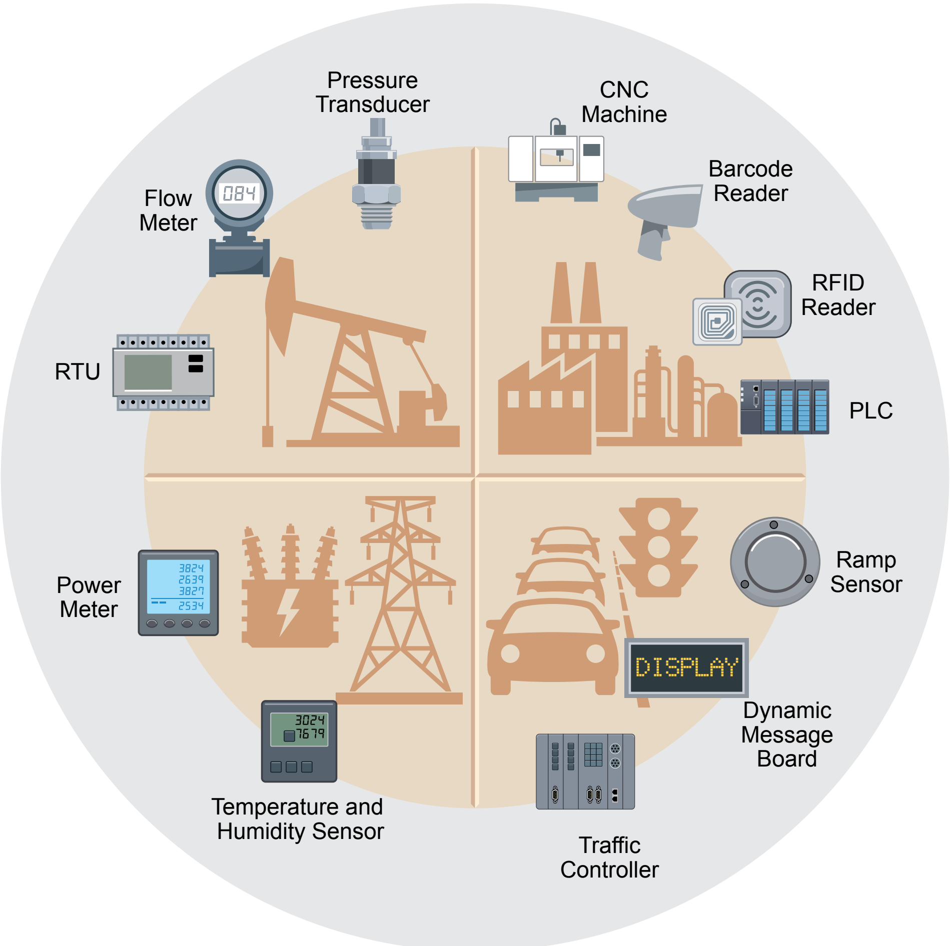


Figure 2: Common serial devices in various industries

Quick Tip

Proprietary Protocol Communications

In general, if your device uses a proprietary protocol, then you need to convert serial data into an acceptable packet format to transmit it to the Ethernet-based network. It is otherwise known as serial tunneling.

If your serial devices use proprietary protocols, serial tunneling is required to bring the serial device data to an Ethernet-based network.

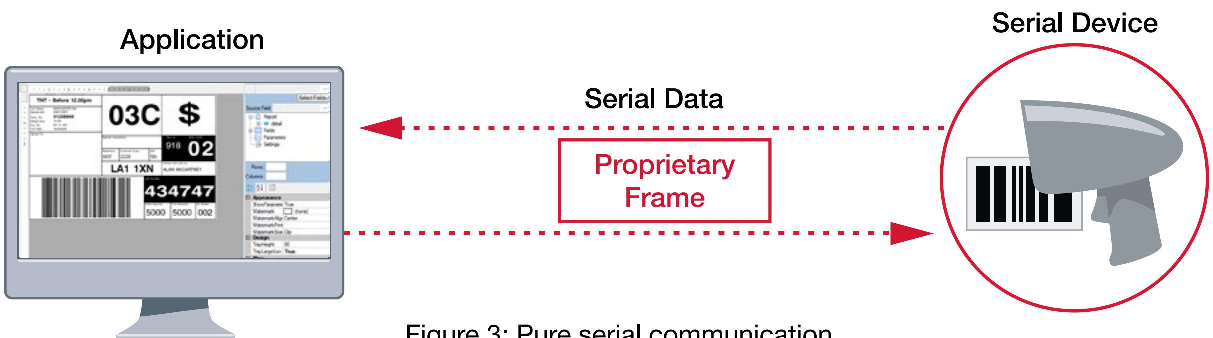


Figure 3: Pure serial communication

Serial-to-Ethernet devices handle serial tunneling along two major scenarios. Behavior at the host's end determines the operation mode to achieve serial-to-Ethernet communications. Virtual COM is commonly used if users wish to keep the serial application program while TCP socket mode is used if users prefer to deal with a TCP header on its own or redevelop the application program.

Quick Tip

Serial Tunneling (Virtual COM/TTY)

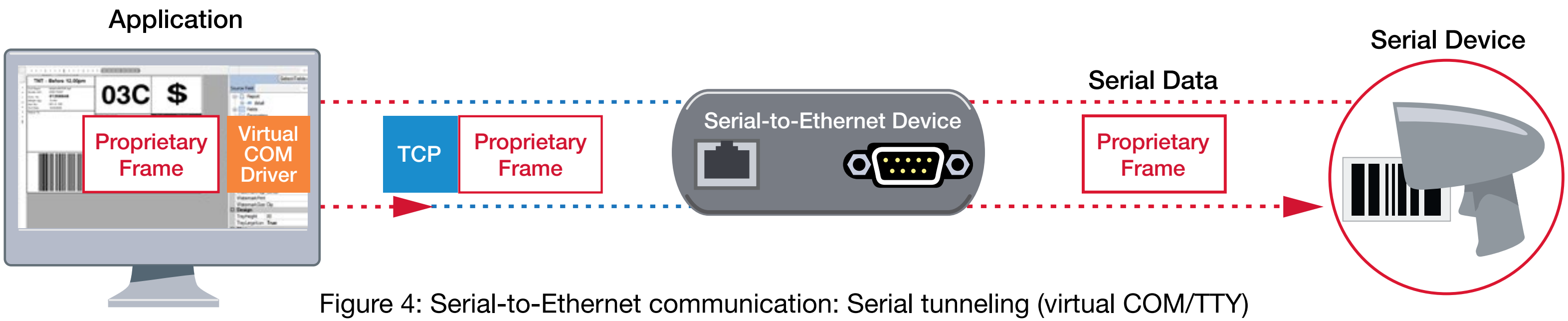


Figure 4: Serial-to-Ethernet communication: Serial tunneling (virtual COM/TTY)

Application Scenario

- The driver provided by the vendor of the device can read the proprietary frame, but the driver supports serial interfaces only.
- Serial-to-Ethernet solutions provide a virtual COM driver that helps to unpack the TCP frame.

Quick Tip

Serial Tunneling (TCP Socket)

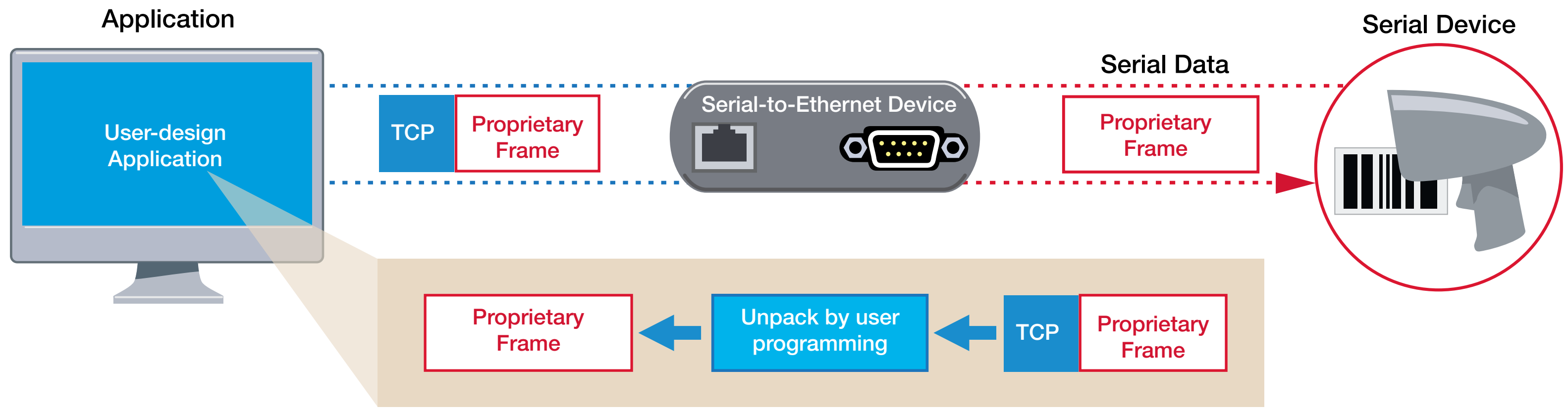


Figure 5: Serial-to-Ethernet communication: Serial tunneling (TCP socket)

Application Scenario

- The design engineer knows how to deal with the proprietary frame.
- The TCP frame is unpacked by programming and applied to other applications.

Quick Tip

Industrial Protocol Communications

If your device uses standard industrial serial protocols, such as Modbus RTU, and needs to convert to an Ethernet-based protocol, such as EtherNet/IP, then things become a bit complicated. This calls for data reformat in order for the protocol to be redefined so that it can be transmitted through the network as an Ethernet-based protocol.

> Things become a bit complicated when you have to convert the industrial protocols that your serial device use to Ethernet-based protocols.

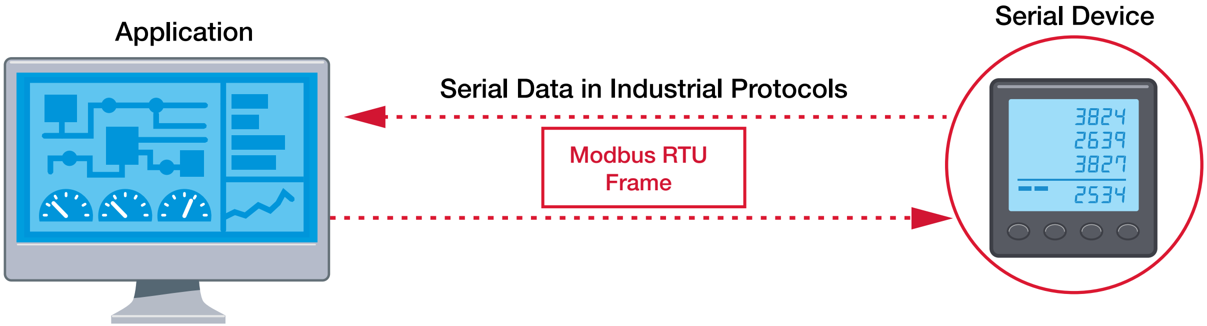


Figure 6: Pure serial communication with industrial protocols

Serial-to-Ethernet gateways handle protocol conversion along two major scenarios. If the industrial protocols that are being converted are technically similar, for example, Modbus RTU and Modbus TCP, then a transparent gateway is needed. If they are poles apart, then an agent gateway is needed to handle the protocol conversion.

Quick Tip

Transparent Protocol Conversion

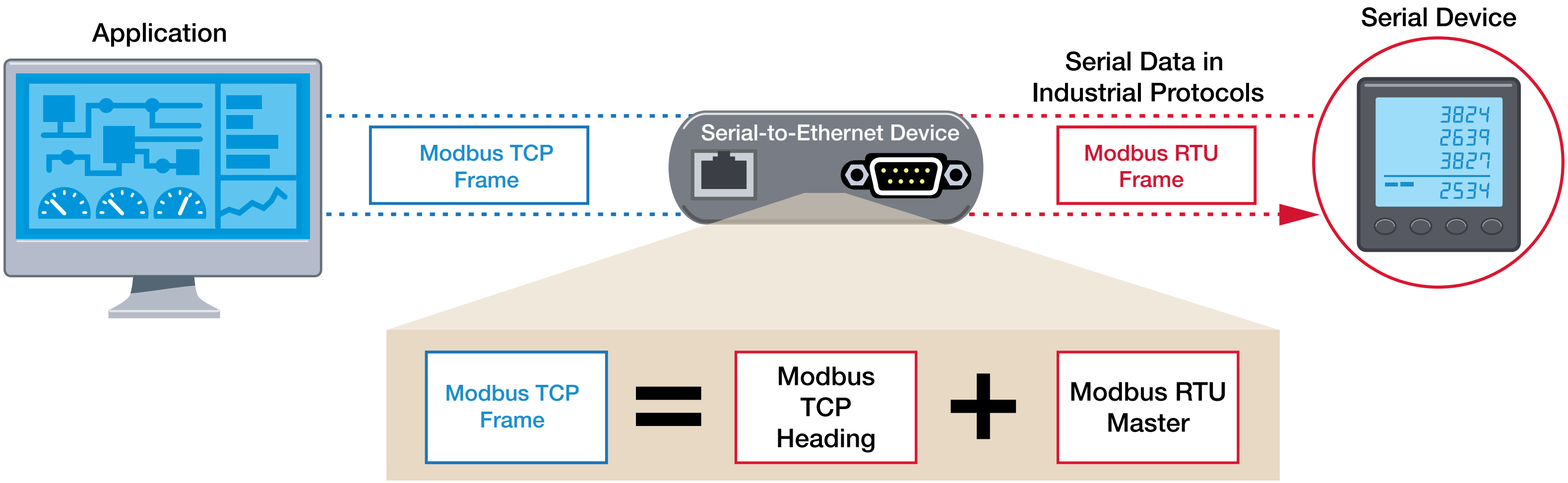


Figure 7: Serial-to-Ethernet communication: Transparent protocol conversion

Application Scenario

- Standard protocols can be read by standard third-party application such as SCADA.
- The converted protocols are similar from one another (e.g., Modbus and DNP3.0), so it can be changed quickly.

Quick Tip

Agent Protocol Conversion

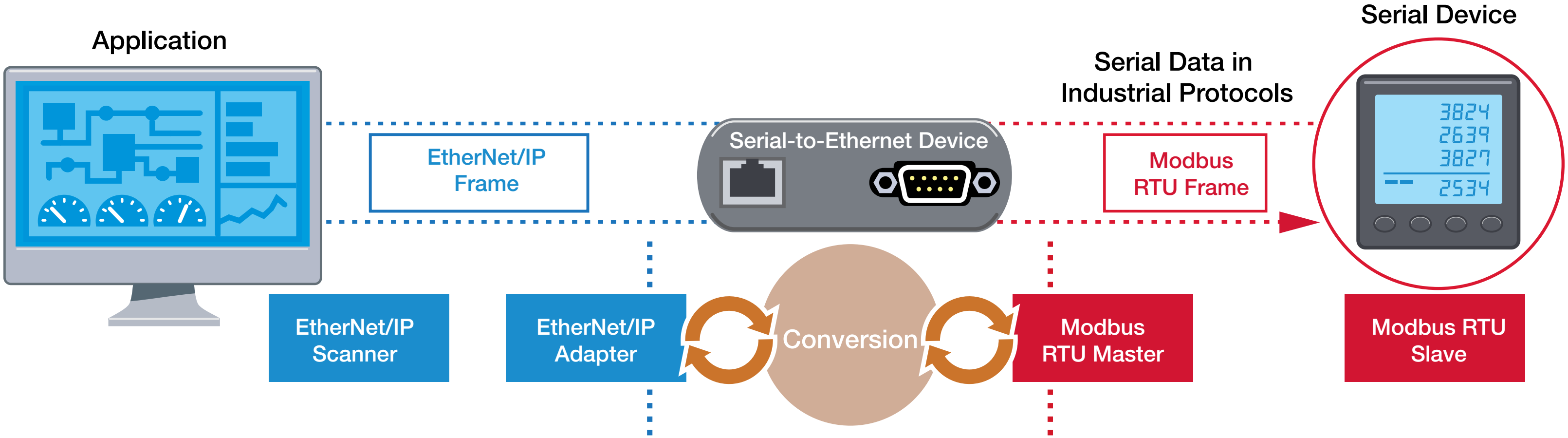


Figure 8: Serial-to-Ethernet communication: Agent protocol conversion

Application Scenario

- The converted protocols are totally different from one another.
- The gateway plays two roles to communicate with both sides of the device.
- It is mainly required when connecting serial devices to SCADA or PLC.

Moxa's Solutions

When using the right solution, getting multiple types and a large number of serial devices connected can be easy. Moxa has a comprehensive serial-to-Ethernet product portfolio to simplify and execute any of your connectivity demands.

NPort Serial Device Servers
Proprietary Serial-to-Ethernet Solutions

MGate Protocol Gateways
Serial-to-Ethernet Protocol Conversions

Find out more…

As mentioned previously, many types of serial devices can be found in field sites, as well as various types of data behaviors. How well can a serial-to-Ethernet solution cover diverse application scenarios? Download to learn more.

- NPort Operation Modes Guidance
- Serial-to-Ethernet Q&A
- Finding a Better Protocol Conversion Solution Between PLCs and Devices
- How to Optimize SCADA Systems Through a Modbus Gateway

Originally, the purpose of collecting data from wellhead applications was to understand production output. Now, my manager wants me to collect more data from field-site sensors such as RTU or meter in order to build an application to increase OEE. Would it be more effective to send field data to the cloud and analyze it through cloud systems?

Consideration Two: To Cloud or Not to Cloud

Overview

Is the cloud necessary in IIoT applications? We have learned that behind the rationale of IIoT deployment is the collection of data from end devices to get actionable insights. However, where do we store these huge amounts of data? As data users, we need to ask ourselves some key questions:

- Is my field of application mostly distributed?
- Does my organization have the ability to maintain our own data server, which means do I have the money and expertise to either keep up the computing power that my application requires or ensure data storage capacity for my field data.
- Will my application need the ability to access field data from anywhere anytime?
- Will my application need to be scaled up with time?

If your answers are mostly “Yes” to the above questions, then it is a good idea to get your devices connected to the cloud.

But then an all-too-familiar problem sticks out its head again: many edge devices do not speak a language that the Internet understands. The ability of interconnectivity devices to connect to the cloud is key should you choose the cloud as your backend data server.

Quick Tip

In addition to the southbound (supporting protocols for your device) and northbound (supporting cloud connections) capabilities of your network, data integration is another factor that needs to be considered. In some applications, data analysis or network integration tasks may take place on the edge, and in others, it may happen in the cloud. This will greatly impact the interconnectivity devices you choose for your IIoT deployment. Figure 9 shows the Interconnectivity Devices Capability Metrics, outlining the suggested interconnectivity devices by mapping your data integration needs and the selected backend data server.

As you can see from Figure 9, for applications where data integration does not need to take place at the edge, a simple ready-to-run serial-to-cloud device could save a lot of effort and front-end costs.

Choose the interconnectivity devices wisely based on your application scenarios.

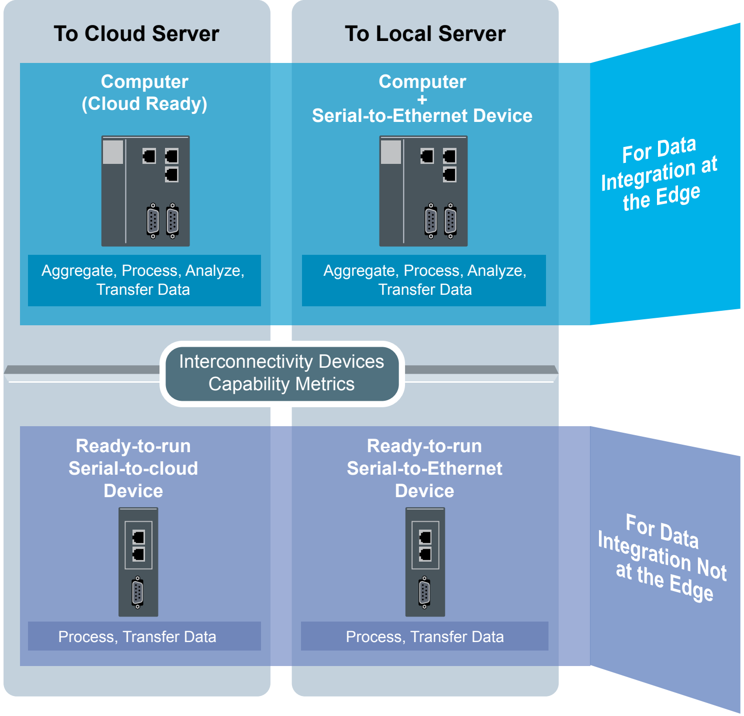


Figure 9: Interconnectivity devices capability metrics

Moxa's Solutions

As an expert on serial-to-Ethernet communication, Moxa's NPorts and MGates bring their easy-to-use and reliable DNA to ready-to-run serial-to-cloud devices, which supports multiple choices of cloud connectivity, such as Microsoft Azure, Alibaba Cloud and generic MQTT for private clouds.

Find out more…

As mentioned previously, getting your cloud system can be easy with Moxa's solutions. Watch our video to learn more.

Getting Onto the Cloud is Easy With Moxa's Solutions

For Proprietary Serial Data to Cloud

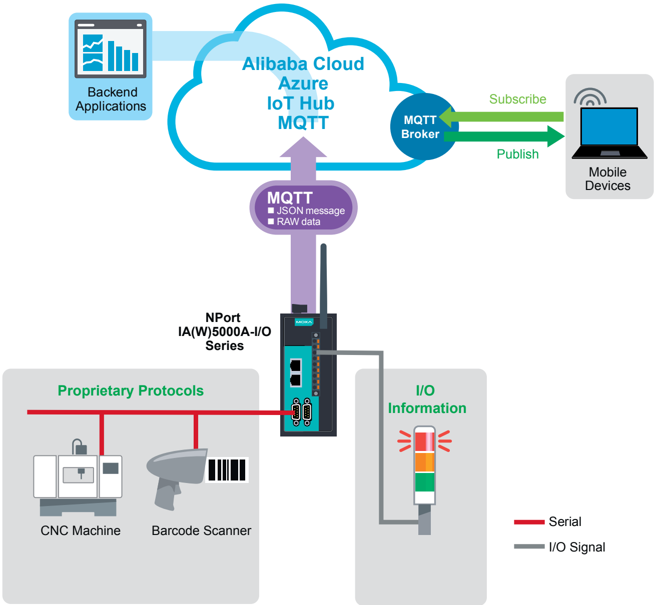


Figure 10: Cloud connectivity capabilities of the NPort IA(W)5000A-I/O Series

For Industrial Standard Protocol Data to Cloud

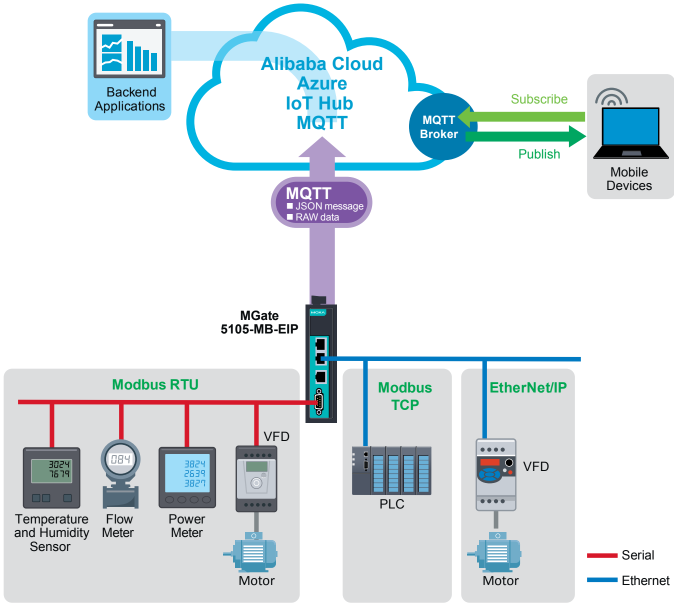


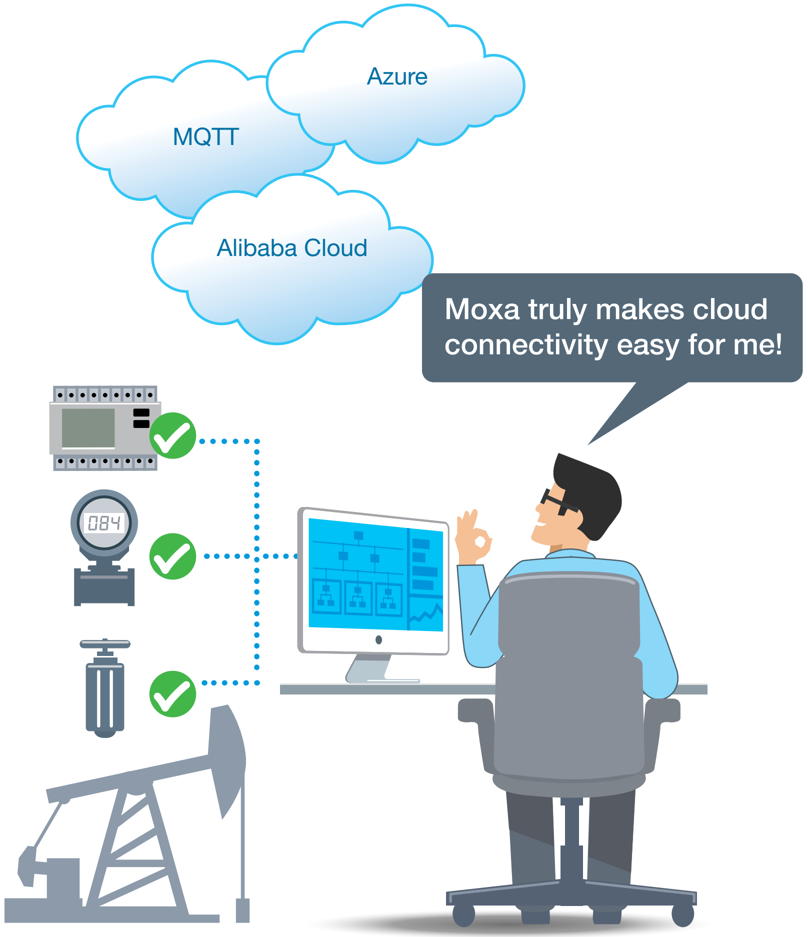
Figure 11: Cloud connectivity capabilities of the MGate 5105-MB-EIP Series

Moxa's Solutions

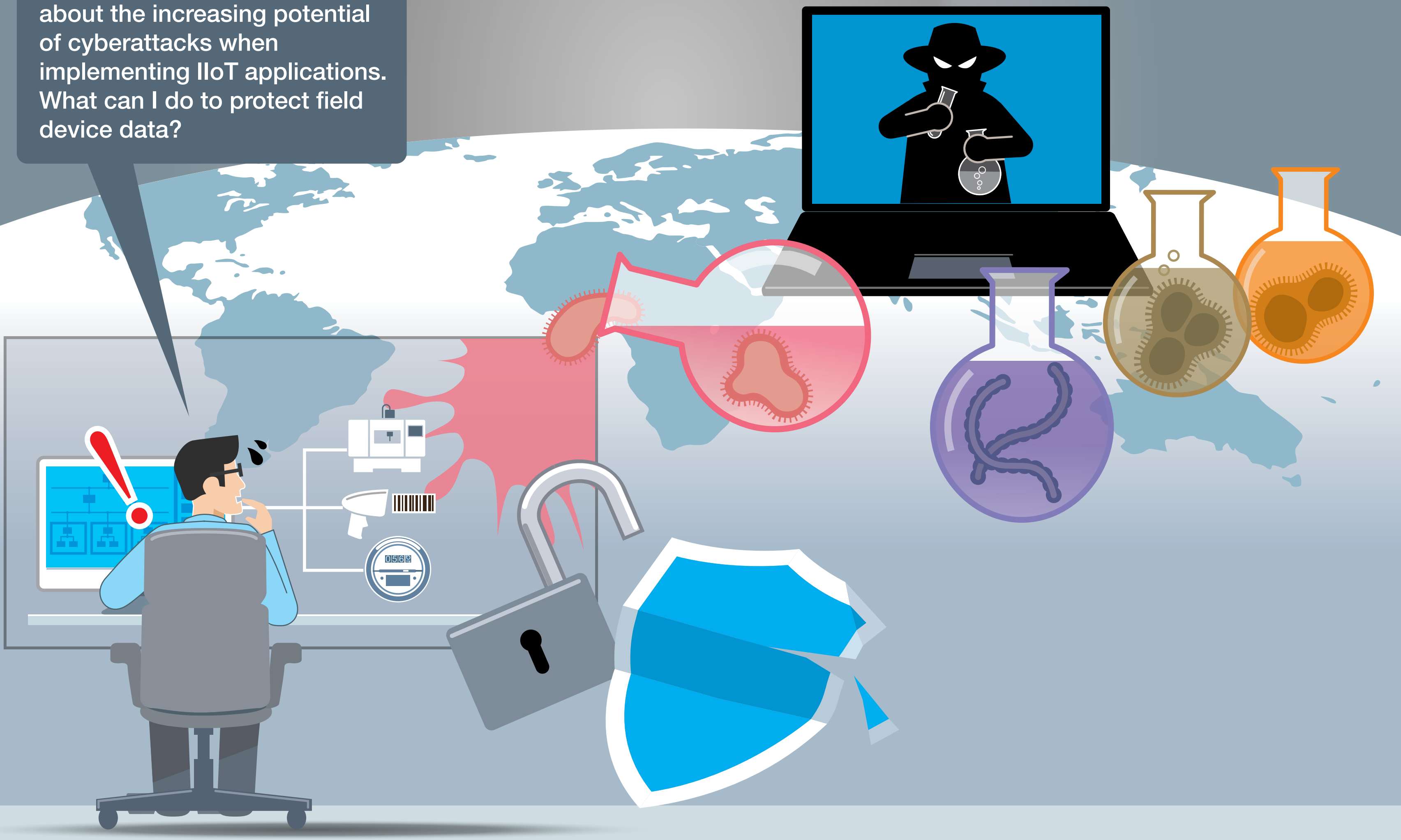
Featured Products

NPort IA(W)5000A-I/O Series
Serial to MQTT/Azure/Alibaba Cloud

MGate 5105-MB-EIP Series
Modbus and EtherNet/IP to
MQTT/Azure/Alibaba Cloud



Business owners are worried about the increasing potential of cyberattacks when implementing IIoT applications. What can I do to protect field device data?



Consideration Three: The First Line of Security Defense

Overview

Security becomes a crucial element when it comes to data ingestion and transmission in IIoT applications. IIoT security considerations certainly need to address all edge devices, the network in which the data is being transmitted, and the locations where the data will be processed and analyzed, no matter whether it is an interconnectivity device or the backend data server. IIoT security guidelines have to apply appropriate controls to the device(s) or a segmented network to ensure proper protection for data with regards to:

- **Confidentiality**: Protecting data from being disclosed
- **Integrity**: Protecting data from being altered
- **Availability**: Allowing only intended use of the data for defined purposes

However, the diversity of end devices in industrial fields, distributed architectures, and legacy end devices make it even more difficult to secure deployment, because these devices were not designed with cybersecurity in mind and lack an encryption or authentication mechanism.

Quick Tip

Interconnectivity devices undoubtedly are central in collecting data in a connected system, as they act as a gateway between edge devices and the backend data server. Therefore, the security of these devices is crucial to ensure the robustness of the entire IIoT environment. If not enough security measures are in place, then the potential for risks, such as cyberattacks, increases. For example, if an interconnectivity device is interfered with during communications, then the whole IIoT ecosystem is jeopardized.

Ensure your interconnectivity devices is secure as they might jeopardize the entire IIoT ecosystem.

To find secure interconnectivity devices, the following checklist sets you on the right path:

- ☐ Identify and control who can log in 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 to ensure data integrity
- ☐ Encrypt configuration data to increase confidentiality
- ☐ Select device vendors that respond quickly to reported vulnerabilities and fix them

Moxa's Solutions

As edge devices feature user authentication, data integrity and confidentiality, network access control abilities, the design of Moxa's serial device servers or protocol gateways is based on the IEC 62443 standard to provide frontline protection.

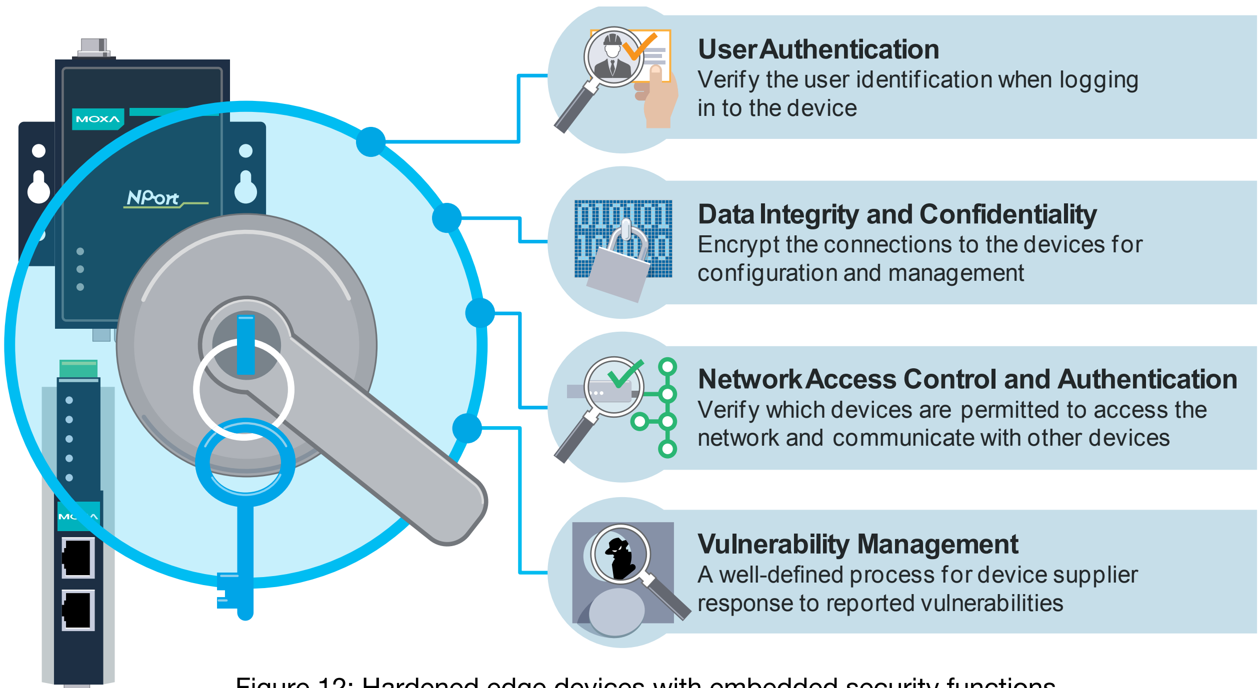


Figure 12: Hardened edge devices with embedded security functions

Moxa's Solutions

Product Features Based on IEC 62443-4-2 Standard

Serial Device Severs

- NPort 5400 Series
- NPort 5600 Series
- NPort 5600-DT Series
- NPort 5600-DTL Series
- NPort 5100A Series
- NPort P5150A Series
- NPort 5200A Series
- NPort IA5000A Series
- NPort 5000AI-M12 Series
- NPort 6100/6200 Series
- NPort 6400/6600 Series
- NPort S9450I Series
- NPort S9650I Series

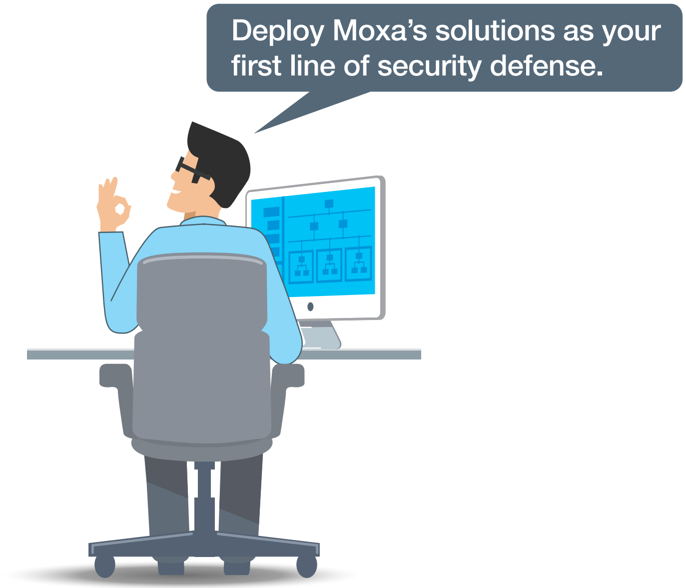
Industrial Protocol Gateways

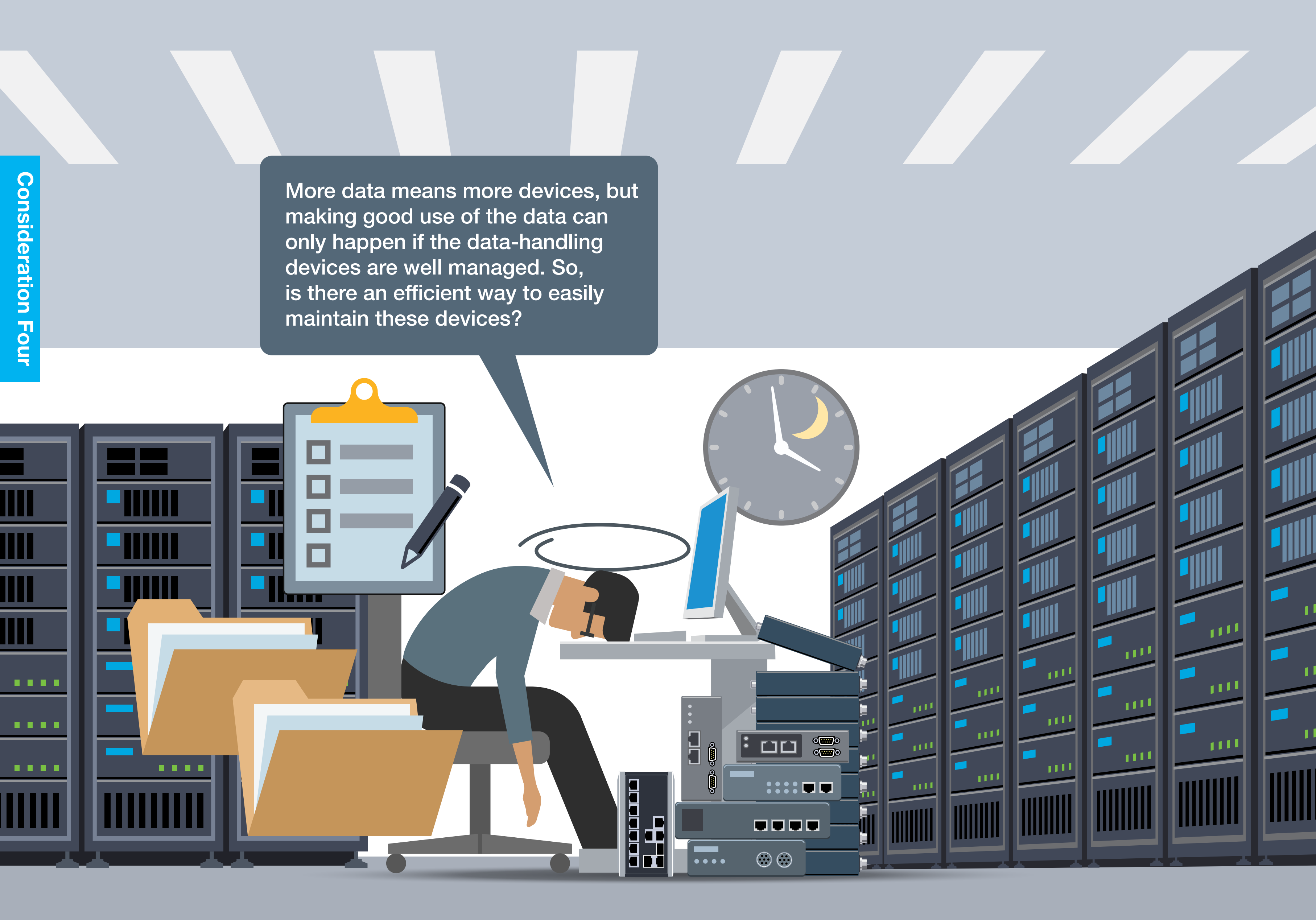
- MGate MB3170/3270 Series
- MGate MB3180/3280/3480 Series
- MGate MB3660 Series
- MGate 5101-PBM-MN Series
- MGate 5102-PBM-PN Series
- MGate 5103 Series
- MGate 5105-MB-EIP Series
- MGate 5109 Series
- MGate 5111 Series
- MGate 5114 Series
- MGate 5118 Series
- MGate W5108/W5208 Series

Find out more…

If you are looking for more information about device security and Moxa's solutions, download our whitepaper or watch our video to learn more.

- Tips on How to Ramp Up the Security of Industrial Networks
- Ramp Up Your Network Security




More data means more devices, but making good use of the data can only happen if the data-handling devices are well managed. So, is there an efficient way to easily maintain these devices?

Consideration Four: The Heavy Workload of Mass Device Management

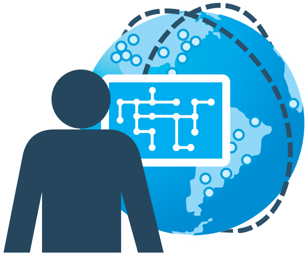
Overview

The complexity of scale and heterogeneity in networks increases the risk of security breaches when IIoT technologies are being adopted. Device management and security are inseparable. Organizations that intend to implement IIoT applications must carefully consider the range of vulnerabilities they are opening themselves up to during the early planning stages. It is essential for IIoT users to know how many devices are connected to the network, what is the status of each device, what software these devices are running on, are any unintended user activity taking place, etc. Furthermore, any outdated firmware or software on edge devices may expose networks to a security vulnerability that can lead to password theft and loss of key.

The fundamental management requirements for interconnectivity products are:

Security-related Actions	Why
Patch Management (Report firmware versions and upgrade firmware)	New firmware often fixes bugs, contains new features, and protects from security vulnerabilities, making patch management a requirement whenever there is a firmware upgrade.
Password Update	For security purpose, passwords need to be changed periodically in order to comply with company policy.
Configuration Backup	Device settings need to be archived periodically in case of failures in the field and for audits if these settings are being altered.

The IIoT presents many opportunities to business. But, many things about the IIoT is not so straightforward even though at first glance it might seem easy. A number of issues are challenging for users:



Scope of Implementation

Common IIoT deployment includes hundreds to thousands of devices. What's more, most of them are located in distributed networks.

Corporate Policies

As organizations require regular password updates and configuration backups for security purposes, network management becomes more burdensome.

Diverse Device Utilities

Different device manufacturers offer different types of management utilities and support various OS platforms. Users need to constantly change management tools from utility to utility between different brands or even products.

Frequent Security Patches

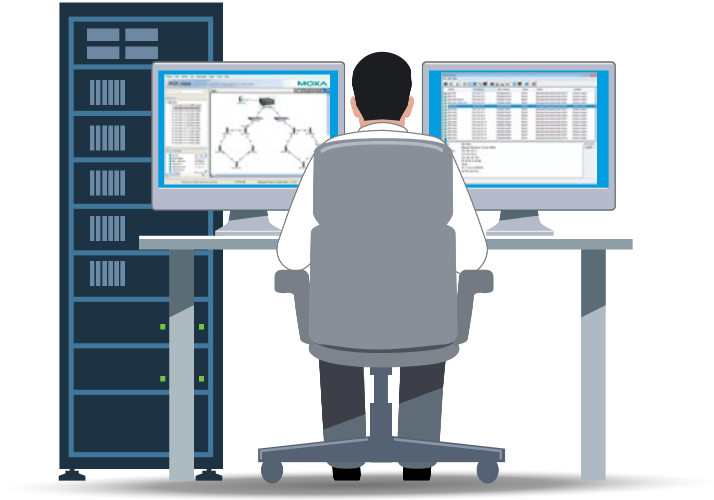
The growing number of cybersecurity threats increases the frequency that devices users must perform firmware upgrades in order to avoid potential vulnerability risks.

Quick Tip

To overcome the aforementioned challenges, finding solutions that make your mass device management easy is essential. Moreover, with the line between the IT and OT worlds becoming increasingly blurry in the IIoT era, management tools need to flexible enough to serve users from both these domains. Choosing an interconnectivity device that has mass device management capabilities, for both GUI and CLI, is the best solution when it comes to IIoT system maintenance.

> To survive under the complexity scenario for IIoT applications, you need a easy-to-use and flexible mass device management tool.

OT Favorite GUI



IT Favorite CLI

Moxa's Solutions

Moxa provides different types of management utilities that are user-friendly for both GUI or CLI users.

GUI Type of Utility Tool

MXconfig and MXview are industrial network management software that enables mass configuration and network visualization for efficient monitoring. Mass firmware patches, password updates, and configuration backups can be completed within a few clicks, saving network administrators time and effort.

Find out more…

See how fast our MXconfig tool takes to complete dozens of device settings.

- MXconfig Mass Network Configuration vs One-by-One Setup

Serial Device Severs

NPort 5400 Series	NPort IA5000A Series
NPort 5600 Series	NPort 5000AI-M12 Series
NPort 5600-DT Series	NPort 6100/6200 Series
NPort 5600-DTL Series	NPort 6400/6600 Series
NPort 5100A Series	NPort S8000 Series
NPort P5150A Series	NPort S9450I Series
NPort 5200A Series	NPort S9650I Series

Industrial Protocol Gateways

MGate MB3170/3270 Series	MGate 5109 Series
MGate MB3180/3280/3480 Series	MGate 5111 Series
MGate MB3660 Series	MGate 5114 Series
MGate 5101-PBM-MN Series	MGate 5118 Series
MGate 5102-PBM-PN Series	MGate W5108/W5208 Series
MGate 5103 Series	MGate EIP3170/3270 Series
MGate 5105-MB-EIP Series	

Moxa's Solutions

CLI Type of Utility Tool

Moxa CLI Configuration Tool (MCC Tool) is another useful tool to manage mass field serial-to-Ethernet devices, and it is especially handy for those with an IT background. Besides that it can perform similar tasks as MXconfig and MXview, CLI command can be scripted and repackaged into user-defined programs and is suitable for management tasks that have repetitive characteristics.

Find out more…

See how fast our MCC tool complete dozens of device maintenance tasks

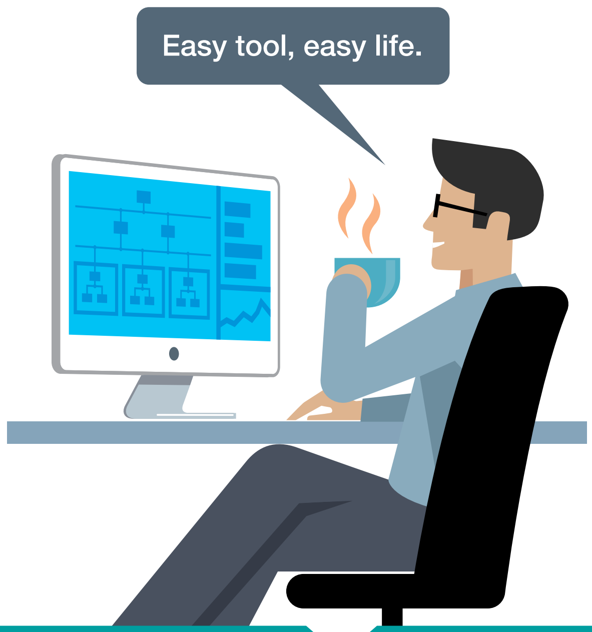
MCC Tool Demo for Fast Device Maintenance

Serial Device Severs

NPort 5100A Series
NPort P5150A Series
NPort 5200A Series
NPort IA5000A Series
NPort 5000AI-M12 Series
NPort 6100/6200 Series
NPort 6400/6600 Series

Industrial Protocol Gateways

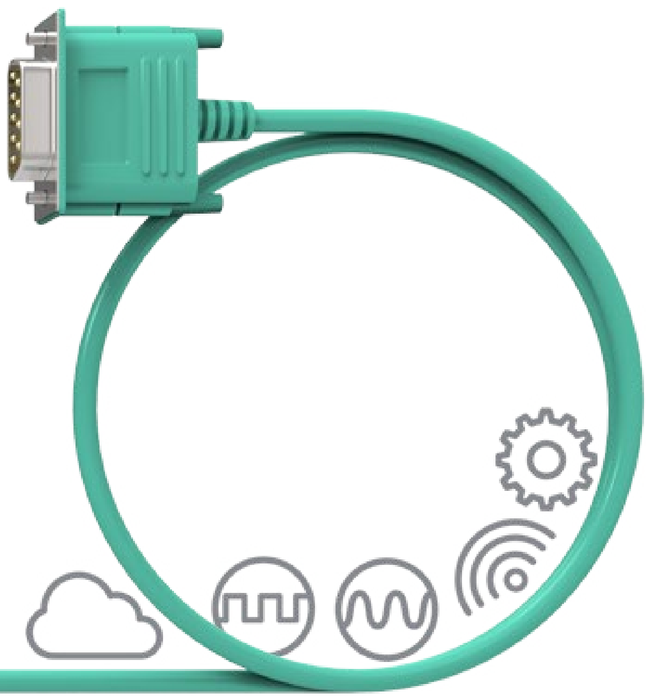
MGate MB3170/3270 Series
MGate MB3180/3280/3480 Series
MGate MB3660 Series



Conclusion

To enable IIoT applications, you need to know how to bring different devices and data formats into one integrated system to unlock insights for your business. To find the most suitable connectivity solutions for you, take a close look at the tips provided in this insider guide. They can help you determine whether your current solutions make your IIoT applications simple and secure, or complex and vulnerable.

Moxa, the industrial leading networking solutions providers, has over 30 years of experience and expertise on how to enable industrial connectivity for our customers in various industries. We have the comprehensive serial-to-Ethernet solutions that not only simplify your IIoT connectivity, but also secure your data during transmissions. Check out our product solutions to find the solutions that fit you the most.



NPort Series
Serial Device Servers
Learn More ▶

MGate Series
Protocol Gateways
Learn More ▶