Hands-on Advice for Your First Step towards IIoT Field Connectivity

Casper Yang, Charles Chen, Harry Hsiao
Moxa Product Managers

MOXA®

Introduction

The Industrial Internet of Things (IoT) is more than a trend—it is now a way of life. More and more, people are embracing this concept by connecting all types of devices to the Internet. The thing is, though, implementing the Industrial IoT is not always that straightforward: the tricky part is bringing all the different pieces of the Industrial IoT puzzle together. Needless to say, companies need to overcome many challenges before putting their IoT strategy into action. The first step to an effective implementation strategy revolves around your organization's operational environment, made up of devices, applications, and processes. In this article, we put ourselves in your shoes. We have come up with three scenarios to point out key factors you need to look out for when making your first foray into the Industrial IoT. Remember, doing it right the first time will save you both time and money.

Scenario 1: Managing Heterogeneous Networks at Field Sites

Scenario 2: Configuring, Deploying and Troubleshooting, and Maintaining Devices on a Large Scale

Scenario 3: Devices Are Damaged by Extreme Temperatures and Other Environmental Interference

Scenario 1: Managing Heterogeneous Networks at Field Sites

In industrial automation applications, collecting data from field devices will become more important than ever. Temperature, motor speed, start/stop status, or video footage, can be used to gain new insights to increase competitiveness. For example, you can determine how to optimize your energy usage, production line performance, and even when to do preventive maintenance to reduce the amount of downtime. However, these devices often speak different languages: some use proprietary protocols, whereas others use open standard protocols. Whatever the case may be, you will need to find an efficient way to convert back and forth between one or more protocols.

Hands-on advice:

- *Selecting suitable protocols*

- *Integrating different media and protocols effectively*

- *Handling proprietary protocols*

Released on February 15, 2016

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution field service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

Hands-on Advice: Selecting Suitable Protocols

Many different protocols are used in different field devices, and each protocol has unique features to meet specific purposes. For example, Modbus RTU/ASCII is simple, easy to use, and cost-effective. If you just need to collect data every few seconds or even longer, then Modbus will be more than sufficient to do the job. But if you want to exchange data every 10 milliseconds, then PROFIBUS is a better solution. It's more expensive, but it's extremely reliable in time-critical applications. Your requirements should determine the solution best suited for your operation. Because Ethernet is now well established, Ethernet-based protocols are being used more frequently at field sites. Most Ethernet-based protocols are open standard protocols, such as Modbus/TCP, PROFINET, OPC UA in automation, or ONVIF in video. When you design a new system, or upgrade an existing one, make sure your field devices support open standard protocols so that they will be interoperable with devices from other vendors.

Hands-on Advice: Integrating Different Protocols and Media Effectively

In the field, the entire network can be separated into a field layer, a control layer, and a supervisory layer. Each layer has a different response time and environmental factors. You may then use different protocols to meet the requirements of each of the three aforementioned layers respectively. After choosing the right protocol, the next step is to collect the applicable information from these devices with different protocols. A protocol gateway is usually the best solution for this integration. For example, it can convert a field layer protocol (e.g., Modbus RTU meter) to a control layer protocol (e.g., EtherNet/IP or PROFINET PLC in control layer).
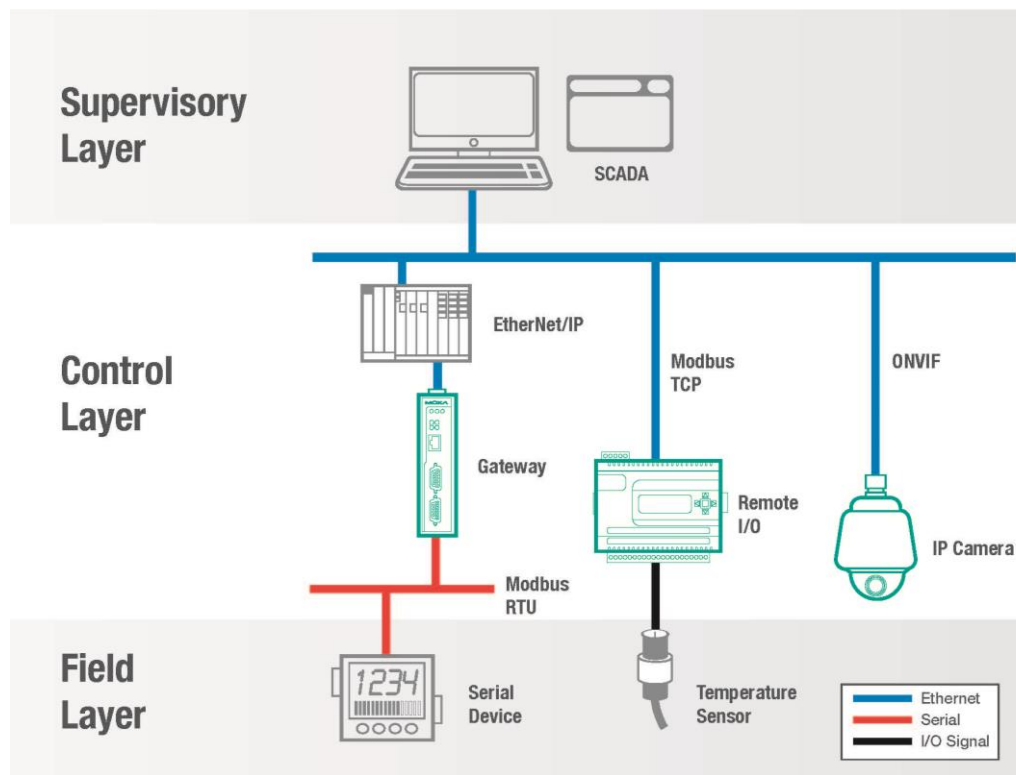

To meet industrial environment requirements, different transmission media can be used to build the most reliable communications system. For example, fiber-optic cable is used for Modbus RTU communications because it can extend over a long distance. In cases of excessive

electronic noise, fiber-optic cable is also the default choice. So, when you plan your system, it is important to make sure the vendor can provide a foolproof solution with regard to any communications issue. This includes different device interfaces (e.g, RS-232/RS-485, remote IO), different network interfaces (e.g., optical fiber, Ethernet, Wireless), and support for different protocols (e.g., fieldbus, OPC UA, ONVIF). A complete solution can save lots of valuable time in system integration.

Hands-on Advice: Handling Proprietary Protocols

We have already talked considerably about standard protocols. However, a large number of existing devices use proprietary protocols. In most cases, the interface is serial. For some reason, however, Modbus RTU or DF1, which are very popular on the serial market, are not used. These devices can range from a power meter to a barcode reader. To connect them to an Ethernet network, you can use a serial-to-Ethernet converter, referred to in the industry as a serial device server. Two interfaces are supported: a serial interface on one side, and an Ethernet interface on the other side. Serial device servers can support virtual real COM ports so that they work as a legacy COM port in your SCADA system; you can even use the existing SCADA system without any redevelopment. Serial device servers also support the so-called "raw socket" mode, which can transfer serial data to TCP or UDP packets transparently. Most SCADA or OPC servers support special drivers or libraries to work with serial device servers to receive this proprietary protocol. You still have to handle the protocol manually as before, but serial device servers can help you transmit the data to an Ethernet network.
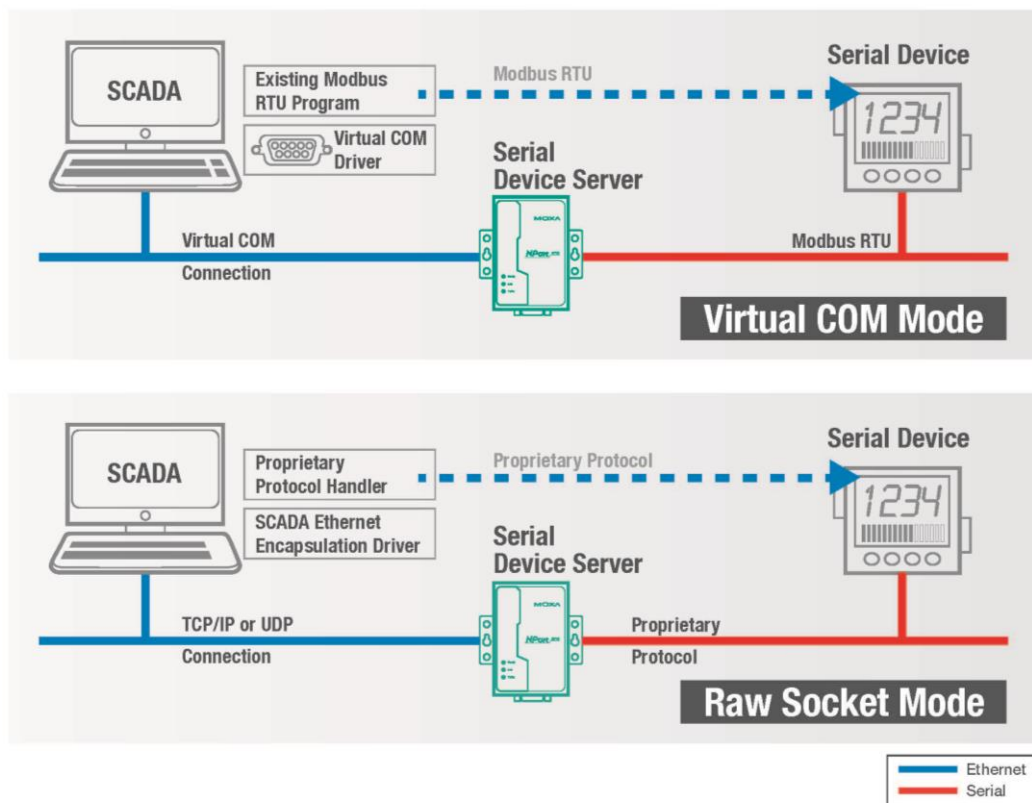
Scenario 2: Configuring, Deploying and Troubleshooting, and Maintaining Devices on a Large Scale

Before taking the first step into the IIoT, one defining question needs to be answered first. How do I manage different devices from different sources on the same network? The acquisition of devices—to collect data from field sites—usually goes smoothly. It's the management of the whole kit and caboodle that makes things complicated. Take note: the possible deployment of hundreds or even thousands of devices—most probably sourced from different vendors—on your site will most certainly bring about a complex situation. Let's talk about what you need to do after buying your devices. These tasks may include but are not limited to device provisioning, testing, configuration file backup, deployment, troubleshooting, remote access and upgrade, and device monitoring.

If these devices are installed at remote sites, operation and maintenance costs could increase tremendously. Therefore, extensive and time-consuming planning and testing are essential before any deployment of devices to ensure lower maintenance costs in future operations. The good news is that there is a better solution that is less cumbersome and time-consuming. Industrial IoT solution providers can help end users manage massive numbers of devices by offering a handy configuration tool, device management software, or troubleshooting utilities, which help lower the total cost of ownership of the entire Industrial IoT system. To give you an overall concept about what software can be used to easily manage these devices, we will elaborate on some tips to evaluate different IIoT vendor solutions.

Hands-on advice:

- *Use a user-friendly web console and a utility for faster configuration*

- *Deploy and troubleshoot large numbers of devices efficiently*

- *Monitor and maintain multiple devices at remote sites*

Configuration
User-friendly web console and utility

Deployment
Handy troubleshooting tool

Maintenance
Handy device management tool
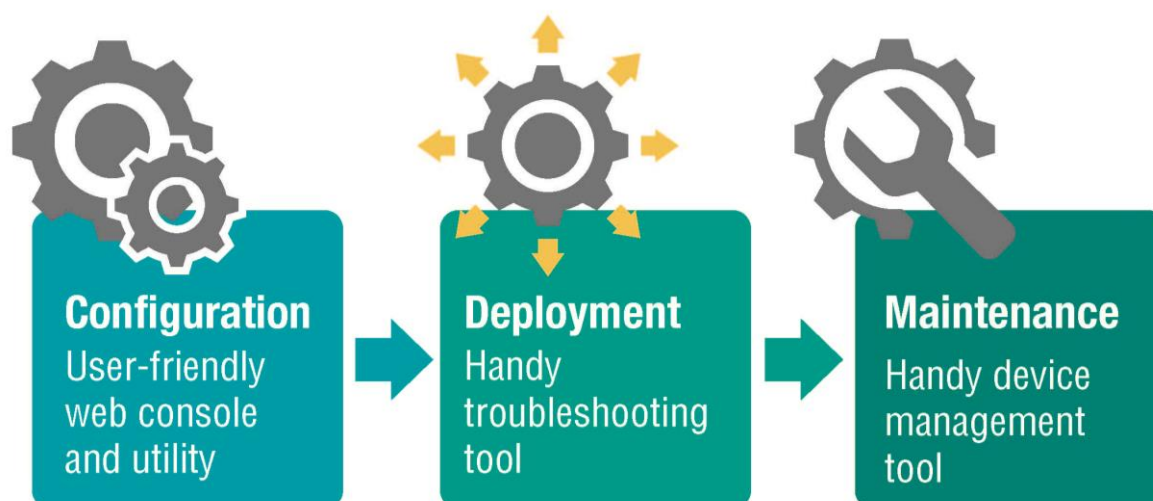
Hands-on Advice: Use a User-Friendly Web Console and Utility for Faster Configuration

Configuring a single device is easy, but it is another story when it comes to configuring multiple devices. A web console is a good and important configuration tool, not only for configuration but also for maintenance purposes. A user-friendly web console walks you through the entire setup process on a single device; all that is needed is a computer equipped with Ethernet and a web browser. When conducting a maintenance task, a field engineer can simply bring along a laptop computer and Ethernet cable, without installing any software, to easily check and configure a device at a remote site. A Windows-based utility is useful when multiple devices need to be configured simultaneously. The utility should provide an autosearch function to search for devices already connected to the network. Furthermore, it should be able to duplicate a configuration as a template for multiple connected devices, where different settings could simply be an IP address or a device name.

A user-friendly utility should also provide a quick protocol mapping function, which can save engineers time since they won't need to reference registered addresses in different vendors' user's manuals. An offline configuration tool offers a ready-to-configure feature that does not require you to first buy a device. Users can simply download an offline configuration tool from a vendor's website, install it on a PC, and start configuring the device right away. It can help users determine whether a device's functions are sufficient for their applications without spending money unnecessarily by blindly buying devices. Let's take a controller, which provides control logic capabilities, as an example. It is difficult for users to ensure, by reading a datasheet or user's manual, whether the control functions meet the requirements. An offline configuration tool should provide a simulation function to test whether the configuration is correct before updating it on the device to prevent any disasters or fatalities at a remote site.

Hands-on Advice: Deploy and Troubleshoot a Large Scale of Devices Efficiently

Installing a device at a remote site is pretty easy, but confirming that the device is running correctly is easier said than done. Sometimes the configured devices pass tests with flying colors in an office environment, but then issues may occur at a remote site. It may be an issue related either to the hardware or the software, and a field engineer may not have enough knowledge to immediately clarify and fix the issue during the installation process at a remote site. A handy troubleshooting tool can help diagnose the issue on a device or record all commands and responses that pass through the device, assisting engineers in determining the root cause of failures. If the issue can be solved quickly, it will mean fewer man-hours and savings on labor costs. Also, speeding up the installation process would deliver the required results sooner to the end user.

Hands-on Advice: Monitor and Maintain Multiple Devices on a Remote Site

How can we ensure that hundreds or thousands of devices always run smoothly and correctly at a remote site? Accidents and breakdowns may happen and cause a system error. Engineers in control rooms need to be alerted immediately so they can react promptly to mitigate the impact. Even better, the ideal solution is that engineers should have ample warning that a stress situation is building up in a system so that they can enact a contingency plan in advance to keep the main system running. SCADA software is designed for remote monitoring and controlling your main system—but not for all of your IIoT devices. A handy device management tool should provide integrated status overview for all the connected devices at a

remote site, such as running status, firmware version, and configuration settings. It should also provide settings that can be configured from a central site to fine-tune the device without sending engineers to a remote site. Furthermore, it should also be able to update a device's configuration from the central site without disrupting its operation. In addition, the device management tool should provide reliable remote access and software upgrade capabilities from a central site to reduce maintenance labor costs. It also should help manage device firmware and configuration versions to keep the device's software current and reliable.

Scenario 3: Devices Are Damaged by Extreme Temperatures and Other Environmental Interference

Lots of Industrial IoT devices are located in harsh environments with extreme weather and installation conditions, such as high temperatures, high electromagnetic interference, excessive vibrations, enormous dust storms, high humidity, and many more factors, all of which can have a big impact on devices' reliability and longevity. Therefore, it is important to choose fully rugged devices that are highly reliable to ensure operations are not disrupted due to devices breaking down or being damaged.

Hands-on advice

- *Evaluate the installation environment to choose the optimal industrial-grade devices*

- *Review test reports and master manufacturing processes*

- *Evaluate MTBF and ask for RMA rates*

Hands-on Advice: Evaluate Installation Environments to Choose Optimal Industrial-Grade Devices

Many industrial-grade devices are available on the market right now. Most of them feature a rugged design specifically for industrial system applications; they are also industry approved and certified. The dilemma now is to choose the one that will optimize your operations the most as each has its own design and features. Because devices' performance and reliability impact your costs and the efficiency of long-term operations, making the right choice is vital.

The first thing to consider is the type of environment in which a device will be installed. What is the temperature range? What is the electromagnetic/surge protection? Will the device be installed outdoors or indoors? Is water or dust present? Do vibrations occur? From these details, you can get a clear picture of what environment specifications are required for a device. Usually, devices with higher rugged design specifications, such as -40 to 75°C operating temperature range, IP66/67/68 water and dust protection, and EMI/surge level 4 are suitable for most outdoor environments. But these rugged design specifications also mean these devices don't come cheap. Then again, it is important to remind yourself that choosing devices for their optimal rugged-design specifications based on the installation environment can maximize your ROI for the industrial system.

Hands-on Advice: Review Test Reports and Master Manufacturing Processes

Are you sure the devices you choose are really industrial-grade? To be sure, you need to do two things before you buy them: one is to read test reports, and the other is to evaluate the manufacturing process. These rugged design specifications usually have different criteria for

different environments, and are endorsed by different certifications and standards. Let's take UL certification as an example. UL 60950-1 applies to devices used indoors, while UL 60950-22 is specific to devices used outdoors. This is standard in the industry, and most industrial devices should have this kind of information in their datasheets or user's manuals. Furthermore, we recommend reviewing the device's test report or certification by a third-party to confirm that the device satisfies all of the test criteria. Moreover, it is also important to know what manufacturing processes are involved to test these rugged-design specifications as not all of the components assembled in these devices are industrial-grade. Therefore, special manufacturing processes, such as hi-pot and chamber burn-in, to name a few, are required to filter out those devices with weak components. Implementing such a process guarantees that mass-produced devices really come with these rugged design features.

Hands-on Advice: Evaluate MTBF and ask for RMA rates

Maintenance is also a key issue in industrial systems. Therefore, device reliability and longevity needs to be considered. Currently, the most popular method to evaluate a device's reliability is MTBF (mean time between failures). Obviously, the device with the highest MTBF values should be more reliable than those with lower MTBF values. However, when comparing the MTBF values between different devices, you need to verify whether the calculation standard and profile of the devices are the same. Also, keep in mind that MTBF is a theoretical value: it does not mean the device will not fail in the period indicated by the MTBF. Hence, we recommend asking the supplier for the RMA rate as a reference.

Moxa Solutions

Moxa provides complete solutions for device connectivity, including device servers, fiber media converters, remote I/Os, and IP cameras. These solutions are designed to meet industrial environment requirements, for example, high electronic noise protection, wide temperature ranges, and DIN-rail mounting design. The standard protocols are also supported, such as Modbus TCP, PROFIBUS, PROFINET, EtherNet/IP, OPC UA, and ONVIF for IP cameras. Moxa provides the OPC UA server software to simplify SCADA system integration. Also, the ActiveX control SDK for IP cameras, together with a video gadget, provides an easy and simple integration process for live displays and video recording in SCADA systems. All Moxa solutions provide a user-friendly web console or utility that can help you finish the configuration quickly and easily.