WHITE PAPER

Rethinking Connectivity: Considerations for Designing Industrial IoT Networks

Alvis Chen
Project Manager

Zig Stegner
Technical Writer

MOXA®

Many businesses around the world are developing strategies on how to embrace new trends such as globalization and digitization. As these trends continue to affect businesses more and more, they need to address the changes these trends are causing in order to stay competitive and profitable. However, working out how to effectively embrace emerging trends is not easy. Within the automation industry, most business owners are trying to understand the Industrial Internet of Things (IIoT) and adjust their production and services to ensure that they can reap the benefits of the IIoT now and into the future.

Key Insights

1. Provide business owners with a full picture of how to enable IIoT applications and explain the real and attractive possibilities that are available.
2. A full explanation of connectivity between Information Technology (OT) and Operational Technology (OT) systems, which is seen as the most important challenge when enabling IIoT applications.
3. An overview of several solutions that can be adopted in order to bridge the OT and IT worlds in an easy, smart, and efficient manner.

The IIoT – A Creator of Global Trends

Global trends, such as globalization and digitization, have highlighted how the opportunities and limitations of future business development depend on how business owners address these trends now. As of 2018, the Industrial Internet of Things (IIoT) is one of the leading initiatives that have the potential to increase business opportunities by connecting related products and systems together. This convergence of devices and systems allows for significantly more data to be gathered, which in turn empowers business owners to make more informed decisions.

Most business owners are aware of the benefits of the IIoT and have started to incorporate IIoT strategies into their business plan. All predictions state that by 2020, there will be tens of billions of devices connected. If these devices have the capability to communicate effectively, the potential to enhance efficiency, and therefore profits, is a very real and attractive prospect. In order to achieve this, devices must be smart enough to understand what data is useful and only send the relevant information to IT systems that can then interpret this data quickly, as opposed to forcing operators to sift through masses of unfiltered data.

The IIoT concept is causing business leaders to give thought and consideration to how to produce a comprehensive solution to make these visions a reality. In broad terms, IIoT

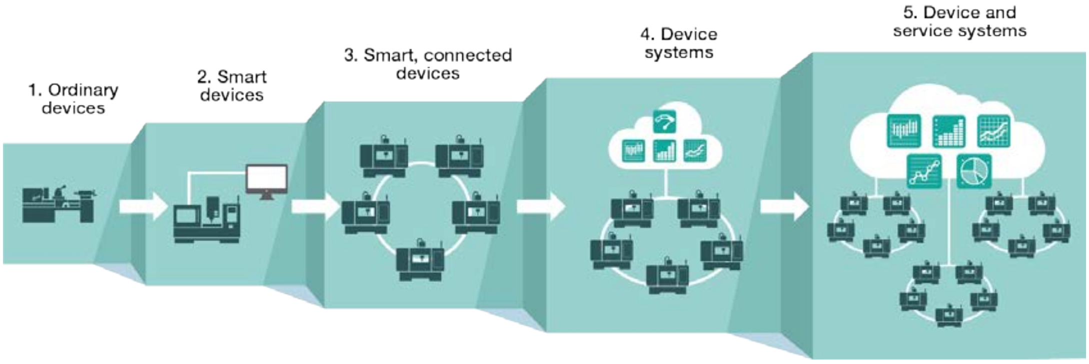
Released on March 19, 2018

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and 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 industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

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

MOXA®
Reliable Networks ▲ Sincere Service

applications are made up of four key components: hardware, software, services, and connectivity. For this white paper, the focus will be on connectivity and how it relates to the other components, especially in the industrial automation world.



Before IIoT applications become a reality, devices and systems must become smarter in order to facilitate continuous improvements to productivity and efficiency.

The Importance of Connectivity for the IIoT

For business owners in the industrial automation world, the first question they often ask is: how can I apply the IIoT concept to my business model? Typically, the first challenge that they encounter relates to connectivity, due to the fundamental differences between Information Technology (IT) and Operational Technology (OT). This hurdle is one of the most difficult to overcome, but the benefits make the effort worthwhile.

In order to demonstrate the benefits of enhanced connectivity, here is an example that illustrates how smart, connected products make solutions more competitive. Previously, John Deere only manufactured agricultural vehicles. However, as more systems and products became connected because of the IIoT trend, John Deere was presented with an opportunity to diversify and expand. John Deere is now able to connect systems that were previously disparate, which has enabled them to offer enhanced solutions that connect irrigation systems and soil and nutrient sources with weather information, crop prices, and commodity futures. These new connections allowed John Deere to optimize overall farm performance as opposed to just offering agricultural machinery. The result was a much more competitive solution that significantly enhanced efficiency and increased profits. This example clearly highlights the tremendous benefits that can be reaped once connectivity in IIoT applications is enabled.

Considerations for Enabling Connectivity on IIoT Networks

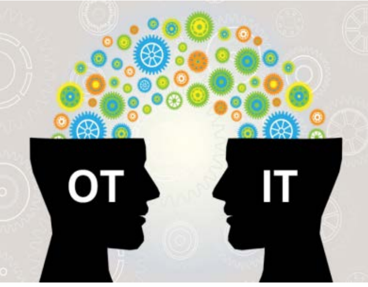
Before businesses start their IIoT journey, they need to be aware of how the IIoT will change their business operations and what changes need to be made to their networks. The four main points that business owners need to consider are as follows: the changes that occur when connecting devices that were previously unconnected, how devices that use different protocols can communicate with each other, minimizing network downtime, and cybersecurity concerns. These four points will be considered in detail before looking at some of the solutions that are currently available.

1. Issues with Connecting the Unconnected

Within the automation industry, companies typically purchase equipment that they will use for decades. When new trends evolve, such as the IIoT, business owners do not want to replace their existing equipment, but rather want solutions that allow them to incorporate their unconnected legacy devices into modern solutions. There are, broadly speaking, two options available: connecting legacy devices directly to the expanding network, or extracting information from the legacy devices to send to other systems. Connecting legacy devices directly to an expanding network can be difficult; many systems and devices use different protocols, which makes communication problematic and requires solutions to simplify communications. Extracting information from legacy devices becomes increasingly difficult as more and more devices are added to the IIoT network, as the sheer volumes of data that are harvested make it time consuming for human operators to process the information. The challenge for business owners is finding smarter and more efficient ways of extracting useful data from all of the devices deployed across their networks.

2. Problems with Facilitating Communication between the OT and IT Worlds

Most people are at least peripherally familiar with IT systems, as they generally use them during their work or personal life. On the other hand, people are often not familiar with OT systems. Within OT systems, proprietary protocols have been developed to perform very specific tasks at field sites. As a result, OT systems are less open, less accessible, and are not readily able to connect to devices or networks that do not support their proprietary protocols. The need to integrate incompatible subsystems in an OT setting is a situation unfamiliar to most IT engineers. If IT engineers are unable to interpret the various OT protocols they encounter, they will find it very difficult to convert the data that has been harvested into useful information. An example that frequently occurs in the industrial automation world is that OT uses fieldbus protocols for real-time purposes and IT uses protocols such as Restful API, MQTT, and AMQP. Previously, there was no need for OT and IT networks to communicate directly, so there was no reason why these separate protocols needed to communicate with each other. The ultimate goal is to ensure that the foundations are laid to ensure these networks are IIoT-ready and that business owners can reap the benefits that come with enhanced connectivity.



Close cooperation between IT and OT professionals is fundamental to leverage any smart application's IIoT platform. For example, when building a smart factory, OT and IT approaches to problem-solving may differ vastly, but they are both working towards a common goal: optimized production. To be successful, both domains need access to industrial data. IT departments, which oversee Enterprise Resource Planning (ERP) and sometimes MES, need to review this data to form the bigger picture and then develop solutions for each of the issues that hamper an operation's reliability. OT professionals are more closely involved with the physical operations on the factory floor and have to figure out how to make all the divergent systems, fitted mostly with proprietary technologies, work together. Business owners must find a suitable solution to allow these two groups of people and two different sets of protocols to work together.

3. Network Requirements for Real-Time Data Connectivity

As networks begin to converge, more devices become reliant on the network. Although this is advantageous as efficiency can be enhanced and new possibilities emerge such as mass customization, it also means that the IIoT network no longer uses simple logic to enable controllers to connect to devices. Because the converged network now carries connections between different systems, it means that the repercussions of the network failing are more severe. One of the primary motivating factors for business owners to embrace the IIoT trend is that having multiple communication methods on a single network offers convenience and flexibility that are not possible when networks and systems operate independently of each other. Therefore, business owners need to ensure that their personnel have a sufficient understanding of converged networks that utilize different protocols so they reap the benefits of an expanded network without getting caught in one of the various issues that can arise. In addition, as more devices are now dependent on the IIoT network, it is of paramount importance that the network does not experience downtime, as this will cause the system to crash and will almost certainly cause the business to incur financial losses. Understanding how to guarantee network uptime on IIoT networks is essential for success in the IIoT.

4. The Evolution of Network Security from LAN-centric to LAN / WAN Convergence

As more and more OT systems are being connected to IT networks, understanding how to ensure network security is of paramount importance. In the past, less emphasis was placed on network security since OT data was transmitted via fieldbus or closed proprietary systems that were not directly connected to the Internet. Now, overseeing the security of heterogeneous networks requires both OT and IT know-how to ensure success. Whereas IT engineers are well-versed in security protocols and security policies, OT engineers provide expertise in production processes and machine deployment to ensure that their production systems operate at peak performance. Furthermore, to minimize costs, it is important to implement such systems without making huge changes to existing network environments and legacy equipment.

As multiple devices are now connected on the same network, all entry points to the network present the possibility of unauthorized access if proper security measures are not taken. This problem is exacerbated by the fact that many industrial protocols were not designed with cybersecurity in mind. These protocols were originally designed at a time when devices were expected to be physically connected to each other, and preventing unauthorized access was a matter of restricting physical access to those devices. As devices now frequently connect to the Internet, they can be open to remote access over that network. This is an issue because legacy protocols rarely support encryption or user authentication. Those devices are therefore susceptible to access and control by anyone able to gain access to the network. This is a serious concern for public utilities and other critical infrastructure. The problem business owners need to overcome is how to ensure that their networks are protected now and into the future as networks continue to evolve.

Migrating to an IIoT Network Seamlessly

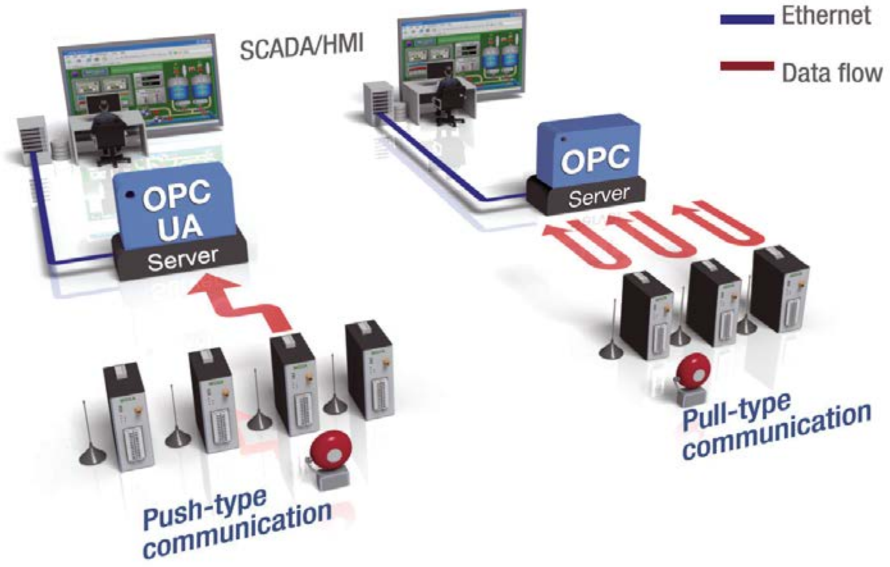
Now that attention has been given to the problems business owners face when attempting to migrate to an IIoT network, consideration will now be given to some solutions that are available as well as some of the best practices that can be followed to ensure that business owners can reap the benefits of the IIoT.

1. Connecting Legacy Devices to IIoT Networks

IIoT networks need to ensure that all devices can communicate with each other. The biggest issue that is often encountered is how to connect legacy devices to IIoT networks. There are currently two common approaches available based on typical operating scenarios.

The first approach is choosing industrial protocol gateways that can convert and connect legacy equipment with one unified communication protocol before transporting this data to IT systems. For example, converting the different proprietary industrial protocols used by legacy devices into one more common protocol, such as Modbus/TCP, Ethernet/IP, or PROFINET. This simplifies OT engineers' efforts when they need to extract data from multiple sensors and machines that use different communication protocols.

The second approach for getting legacy OT device data into an IIoT network is leveraging a traditional OPC (OLE for Process Control) solution for industrial automation telecommunication. OPC architecture uses a polling model (pull-type) to get device data from devices such as PLCs, RTUs, motor drivers, and remote I/Os, and passes data and commands to and from SCADA (Supervisory control and data acquisition) servers and devices. However, with the number of devices/sensors increasing in IIoT applications, this polling method will cause a huge increase in the bandwidth needed by the network. To address this issue, the OPC Foundation standardized a new methodology called OPC Unified Architecture (OPC UA for short), which provides additional "subscription and monitored item" and "report by exception" push-type models, where communication data will be sent only if the data changes. This increases the efficiency of the operation and minimizes the amount of network bandwidth required.



2. Making Devices Smarter via an IIoT Gateway

IIoT gateways are frequently used in order to create a data transmission bridge between devices in the OT and IT worlds. As almost all IIoT networks do not currently utilize a set of universal protocols, IIoT gateways are going to play an important role on IIoT networks for the foreseeable future. On these networks, direct transmission of vast amounts of data across networks can lead to network latency and IT personnel are required to use a lot of effort to identify useful data, which results in delayed data analytics. To deal with this, there are some features that gateways should support to make the process more effective.

Smart Processing Capabilities: As gateways are deployed across many different applications, each gateway should have specific rules so that only the information useful to that application is passed to the cloud where the data will be analyzed. For example, there could be an acceptable temperature range of -40 to 70°C, and only when the sensor records temperatures outside of this range will the data be passed to the cloud for further analysis.

Secure Remote Communication: One of the most beneficial features that gateways can support is remote monitoring. IIoT networks often require multiple gateways, which makes remote monitoring crucial as it can remove the need for site visits if a problem can be rectified remotely. In order to prevent data stored on the gateway from being tampered with, it should be secured with a file protection system such as TPM (Trust Platform Modules). For remote connections, a VPN (Virtual Private Network) should be utilized to connect the control center and the gateway.

Simplify Data Acquisition: Another feature that operators find useful because it helps reduce their workload is for gateways to support multiple protocols. This overcomes one of the main problems of bridging the divide between the OT and IT worlds, where engineers often only specialize in one of these technologies. For example, devices that can automatically translate protocols that OT engineers use such as Modbus/TCP and EtherNet/IP, and protocols that IT engineers often use such as SNMP and RESTful API, will simplify communication between devices that have different interfaces. They can also remove the need for engineers to learn about protocols they are not familiar with as the conversion is done automatically.

3. Networks with Sufficient Bandwidth and High Availability Avoid Interruptions, Downtime, and Failure

As IIoT networks host more devices compared to traditional networks, it is therefore even more important to enhance the reliability of the IIoT network. Although multiple networks converging to form an IIoT network brings numerous benefits, it is particularly troublesome for business owners if the network experiences any interruptions, downtime, or failure, as this would mean the entire system would go down, whereas previously, only a small part of the system failed. One method to enhance the reliability of IIoT networks is to ensure network availability and high bandwidth. High availability means the network is designed with redundancy to prevent having a single point of failure to ensure that the network stays up and running. This type of redundant network design also minimizes the amount of downtime required when fixing issues on the network. As IIoT networks add more and more devices, it is important that these devices and applications can operate without experiencing latency and without overloading the network and causing it to crash.

Network Bandwidth: For IIoT networks that use wireless technologies, the 802.11ac and 4G LTE standard provides throughput and transfer speeds significantly better than previous standards, which make them suitable for use on converged industrial networks. It is also highly recommended to use 10G for networks that utilize wired Ethernet in order to ensure sufficient bandwidth availability. Even though 5G may be sufficient most of the time, there is a much higher chance that network downtime will occur, which will almost certainly be more expensive than choosing 10G over the course of the network lifecycle.

Network Redundancy: As networks expand to include more devices and applications, network redundancy is frequently utilized as it helps networks avoid dropping data packets when a single point of failure occurs. Network redundancy ensures that when a single point of failure occurs on the network, data is rerouted through a point that is currently active, preventing both data loss and network downtime.

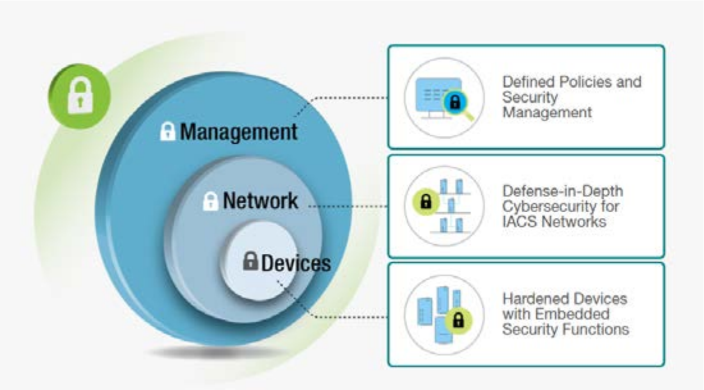
To summarize, business owners should future-proof their networks by deploying networks that support sufficient bandwidth and smart redundancy to ensure that their network does not experience any interruptions, downtime, or failure.

4. Ensuring Network Security Now and Into the Future

Many system operators have stated that the best way to secure a network against cyber-attacks is to use the defense-in-depth security architecture, which is designed to protect individual zones and cells. Any communication that needs to take place across these zones or cells must be done through a firewall or VPN. Deploying this type of architecture reduces the chance that the whole network will fail due to an attack because each layer is able to address a different security threat. It also reduces the risk to the entire network; if a problem occurs in one part of the network, there is a higher chance that the problem can be contained within that layer and will not spread to the other layers.

After the network has been secured, the next step to consider is how to ensure that users cannot adversely change settings by accident or on purpose. This problem can arise from users who operate and manage the network, third-party system integrators, and contractors that are required to perform maintenance on the network. The best way to secure against this threat is to enhance the network devices' cybersecurity to ensure that they cannot have their settings altered in a way that puts the devices or the network at risk. Many cybersecurity experts view the IEC 62443 standard as the most relevant publication for how to secure devices on industrial networks. This standard includes a series of guidelines, reports, and other relevant documentation that define procedures for implementing electronically secure IACS (Industrial Automation & Control Systems) networks.

Throughout the automation system lifecycle, maintenance will need to be performed by local engineers or system integrators. As networks, especially IIoT networks, continuously evolve and change, the network and all the devices located on it need to be constantly monitored to ensure they are properly protected against cybersecurity threats. As there are almost always a large number of service personnel who are responsible for monitoring and maintaining different devices on the network, it is not a good idea for all of them to perform security settings based on their own knowledge or experience. For this reason, a good standard operating procedure that clearly defines how to configure device settings should be adhered to at all times. It is important to ensure that constant monitoring of the network takes place to ensure that no errors occur and that the network can be kept safe from all security threats.


Management
Network
Devices
Defined Policies and Security Management
Defense-in-Depth Cybersecurity for IACS Networks
Hardened Devices with Embedded Security Functions

Conclusion

It is clear that there are multiple benefits for business owners that deploy solutions and products that follow the IIoT trend. However, there are several obstacles that need to be overcome. Of these obstacles, connectivity between OT and IT systems is seen as the most important. Therefore, business owners must pay significant attention to whether their current connectivity solution is ready to be used with IIoT applications. Below are four takeaway tips that every business owner should consider as part of their IIoT connectivity development plan.

1. Choose a smart, efficient solution to collect and deliver data from unconnected legacy devices to the systems on your IIoT network.

2. In order to accelerate convergence of OT and IT systems, deploy an IIoT gateway that makes your devices smarter.

3. Ensure your network design has sufficient bandwidth and supports network redundancy to allow data to be transmitted without latency now and into the future.

4. Ensure sufficient network security when transmitting data between OT and IT systems.

Business owners that have implemented these four suggestions are on the right track to successfully migrate to IIoT applications.

As Moxa has embraced the IIoT trend over the past few years, we have developed edge-to-cloud connectivity solutions that support comprehensive industrial connectivity and have also developed computing solutions that help business owners deploy IIoT applications in an easy, fast, and intelligent manner.

For more information about deploying edge-to-cloud connectivity solutions, visit:
https://www.moxa.com/support/request_catalog_detail.aspx?id=3608

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.