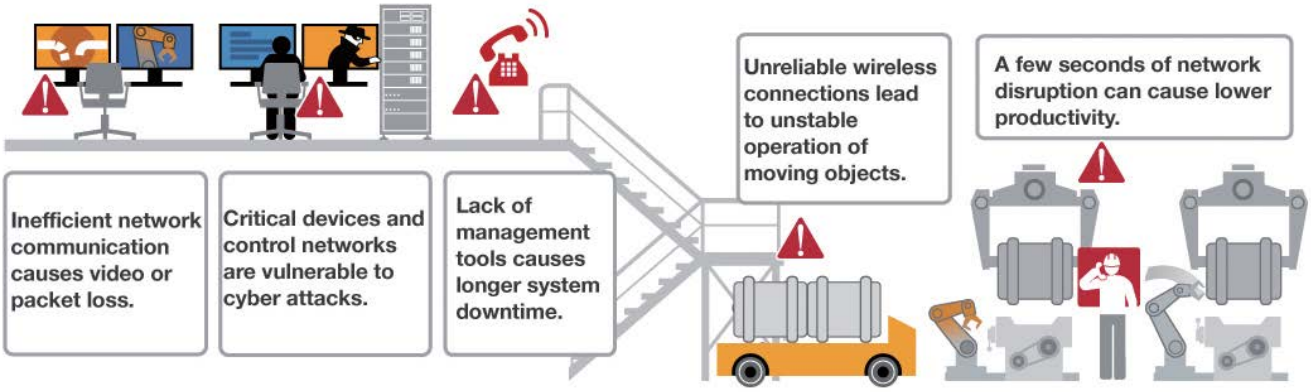
Is Your Network Infrastructure Ready for the IIoT?

Answers to Five Common Questions

The Industrial Internet of Things (IIoT) trend aims to improve efficiency and productivity for industrial automation by connecting different devices together as well as collecting and analyzing large volumes of data to offer accurate information, and in turn allows user to make better decisions. However, before implementation of the IIoT can begin and users are able to reap the benefits, they need to ensure that they have the correct infrastructure in place in order to get the most out of their networks. To make sure your network is ready for the IIoT, check out five of the most frequently mentioned questions below.



Q1: How Can You Ensure Smooth Video or Data Transmission on a Quad-Play Network?

It is becoming increasingly common for converged quad-play services (data, voice, video and control) to form a part of modern industrial networks. For example, video surveillance is fast becoming an essential component and thus industries are including this on their networks. As a result, network transmission has become more complex and requires larger bandwidth to transmit the different types of data, especially video. When building a network for bandwidth-hungry applications, don't forget to ensure the following:

a) Sufficient bandwidth for smooth operations

b) Cutting-edge technology that optimizes network performance

For quad-play networks, choosing large bandwidth availability, such as a Gigabit/10Gbe solution, or a wireless 802.11n solution, is a sensible option that generally supports smooth network operations. As the amount of devices that are deployed on industrial networks may change over time, what may be required at the start may differ significantly to what is required two years later, so sufficient bandwidth availability will ensure you don't experience network instability issues.

Bandwidth aside, transmitting video streams presents different challenges compared with data transmission. Typically, to reduce bandwidth consumption, automation engineers use multicast transmission over a fast redundant ring. However, different protocols are

used to transmit video packets. For example, the IGMP protocol updates multicast group tables every 125 seconds, so if a network cable becomes disconnected or an Ethernet switch loses power, your multicast video streams will not be immediately redirected to the backup path, which is why you lose the video frames.

Now, cutting-edge technologies are available to overcome the current limitation of video transmission. For instance, Moxa's latest V-ON™ technology ensures millisecond recovery on Layer 2 and Layer 3 networks, which keeps your video application up and running and avoids losing any critical video frames. Find out more about V-ON™ technology and how it is helping businesses solve these problems.

Q2: How Can You Make Your Industrial Network Safer?

Industrial control networks help facilitate efficient and safe operations in vital sectors such as utilities, oil and gas, transportation, and manufacturing. A resilient control network must be able to effectively detect and filter unwanted traffic. If an industrial network does become compromised, the network might have back doors that allow hackers and unauthorized personnel to gain access to the network. In short, a clear understanding of network security for industrial control systems is essential.

One of the options that can be used when making your network more secure is a defense in depth approach. This security approach uses a zone and conduit model, which means that within any particular zone, communications can happen quite freely. However, when different zones are required to communicate with each other, they are only able to communicate through a conduit. The conduit is protected by a firewall and only allows information that is specific to that zone to be communicated: any other information will be blocked. The defense in depth approach can be applied to industrial control systems to protect critical equipment and expand security coverage on automation networks at various locations, device cells, function zones, and factory sites.

A conventional network firewall is blind to the contents of industrial communications protocol packets (such as Modbus TCP). This is a particularly critical problem since industrial communications protocols generally have very poor security and often simply respond to any packets they receive without checking where the packet has come from or what information it contains, including read queries, shutdown commands, firmware updates, and control commands. The potential for this to wreak havoc with your system is clear, so stronger firewalls with added security functions, such as Deep Packet Inspection, are required to ensure your network isn't compromised.

Furthermore, within IIoT environments, especially water treatment, oil and gas, and ITS applications, the networks are often connected to remote applications. For such requirements, businesses can use IPsec or open VPNs functioning as encrypted data tunnels for secure data transmission and remote access. Find out more about Moxa's cybersecurity strategy.

Q3: How Can You Maximize Network Management Efficiency to Increase Network Availability?

As a network becomes more converged and complex, you need to find an easy way to monitor and manage devices to ensure that the network runs smoothly and is not hindered by network downtime. Generally speaking, the network management life cycle contains installation, operation, maintenance and diagnostics. At each stage, network administrators face different complex and time-consuming tasks. For example, at the installation stage, manually configuring and testing the network device could take several days to complete. Another concern is that the manual configuration of multiple devices might lead to input errors and subsequently delays while the errors are being rectified.

Frequently Asked Qs

Enterprise network management software, which supports complex features and sophisticated user interfaces, may not be helpful in industrial automation. To serve automation-specific purposes, the management software should allow network administrators to perform real-time monitoring on a user-friendly interface and support historical event analysis. In addition, the industrial network software needs to be able to collaborate with existing SCADA systems, so that it is easier for engineers to run and manage the entire operation on a single platform.

For administrators who are away from the control room, checking the network status on their mobile phone app allows them to instantly respond to events on the network. Some of the latest network monitoring apps even support a quick search function for field devices, saving network maintenance staff a lot of time locating specific devices on the factory floor. Find out more about MXstudio network management suite and MXview ToGo remote monitoring app.

Q4: How Can You Ensure Your Moving Objects Maintain Their Wireless Connection?

Wi-Fi networks have limited signal coverage, so multiple access points are necessary for full coverage throughout an entire warehouse. It is critical to ensure that the clients can roam smoothly between these access points with minimal handover time. Old-fashioned Wi-Fi devices commonly experience a 3 to 5-second disconnection time as they move between access points, causing severe disruption to operations. If this happens to a client device installed on an Automated Guided Vehicle (AGV) for example, the vehicle might simply stop until it re-establishes its network connection, causing production delays that could lead to an increase in operation costs.

Furthermore, users will often experience limited bandwidth availability across the different channel frequencies. In order to overcome this difficulty, system integrators must use multiple frequency channels to avoid channel congestion. System integrators will configure the roaming parameters to allow location-based load balancing, ensuring clients are connected to the closest access point to avoid network traffic congestion. In order to minimize wireless security risks, encryption protocols must be used. However, when security features such as WPA/WPA2 have been enabled, roaming performance can be affected. Moxa's Turbo Roaming provides millisecond-level handoff times and adjustable roaming parameters for wireless clients, which ensures a fast, stable, and flexible network suited for industrial environments.

Within factory environments, the automated storage and retrieval system and AGV system are constantly mobile to supply materials to the production process and to store finished goods. Devices that can be confidently deployed in industrial environments must be tested against the IEC 60068-2-6 standard, which specify the guidelines that wireless devices should adhere to in order to ensure protection against high levels of vibration and shock. In addition, electrical disturbances can damage wireless devices through their vulnerable power and antenna ports and that is why most system integrators use additional power and antenna-isolator accessories to strengthen their system. However, a negative consequence of this type of deployment is that it increases the system cost and also requires extra installation space. As Moxa's devices support a dual isolation design, system integrators who use Moxa's products are able to save on money and space, while deploying a secure industrial-strength product. Find out more about Moxa's reliable mobile Wi-Fi solution.

Frequently Asked Qs

Q5: How Can You Reduce System Downtime to Prevent Production Loss?

In Industrial Internet of Things (IIoT) applications, system downtime causes loss of productivity and significant financial losses so users demand system uptime that approaches 100%. However, industrial environments are often located in remote areas and connected to a distant control center, making on-site maintenance and troubleshooting more challenging and more expensive. Two critical factors affect network performance at field sites: network recovery time and the quality and design of the network devices.

Industrial networks are often deployed in harsh conditions, where electronic interference is caused by field devices, or environmental conditions, such as shock and vibration, humidity and erosion, or extremely hot and cold temperatures, which can all have a detrimental effect on devices. Therefore, when choosing an industrial network device, you need to consider its design and quality. In certain industries such as power, oil & gas or rail, the conditions are even more extreme, and require adherence to specific industrial certifications.

Industrial automation requires extremely fast recovery times to ensure smooth operations. Using industrial-grade redundancy protocols, which achieve millisecond-level recovery, users are assured of network reliability. Similarly, for wireless communications, it is highly recommended that engineers deploy wireless devices that support millisecond failover time. Besides recovery time, you have to consider the deployment scalability, the maximum number of devices that can be supported on a network, and last but not least, the cost. Find out more about Moxa's wired redundancy technologies such as Turbo Ring, Turbo Chain, and PRP/HSR, as well as our wireless redundancy technology AeroLink Protection.