WHITE PAPER

Industrial Network Cybersecurity: Debunking the Myths and Adopting Best Practices

Alvis Chen
Project Manager

MOXA®

Executive Summary

Industry 4.0 or the Industrial Internet of Things (IIoT) are no longer buzz words. Many different industries including manufacturing, consumer and retail, energy and utilities, automotive, and the telecommunications sector are following the IIoT trend. In particular, manufacturers are embracing the IIoT faster than many other sectors, indicating the tremendous impact the IIoT and the realization of Industry 4.0 can have on manufacturing.

However, cybersecurity is still a major concern for managers before they can deploy IIoT or Industry 4.0 systems. One of the main reasons is that cybersecurity is not always the highest priority for traditional operational technology (OT) systems. As a result, when OT systems are connected to the Internet or connected to other IT systems, the OT system becomes a point of weakness for malicious attacks or accidental data loss. So why is cybersecurity so often overlooked by OT engineers? The answer can be traced to four common myths.

This white paper explains why these four misconceptions are no longer true in today's highly interconnected world, discusses the differences between IT and OT networks, and shares some best practice guidelines to help your organization successfully overcome these IT-OT differences and transition to IIoT or Industry 4.0 systems.

Four Common Industrial Cybersecurity Myths

Myth 1: My industrial network is physically isolated and not connected to the Internet, so my network is secure.

This statement may have been correct ten years ago. However, nowadays, many IIoT devices are already directly connected to the Internet, bypassing traditional IT security layers. A question that is often asked is: Why do so many IIoT devices need to connect to the Internet in the first place? The main reason is because IIoT or Industry 4.0 systems need to collect large amounts of data for further analysis. Since the data sources may not be in the same locations, it is necessary to send the data to a remote server by connecting your systems to the Internet.

Even if your industrial control systems (ICS) or industrial networks are not connected to the Internet, they may still be vulnerable to unauthorized connections. For example, a third-party vendor or an automation engineer may update systems by connecting unauthorized laptops or USB drives to conduct regular maintenance or troubleshooting, which opens the ICS up to insecure access and ultimately makes ICS devices more vulnerable.

Released on July 15, 2019

Moxa is a leading provider of edge connectivity, industrial networking, 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 57 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. 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

Myth 2: Hackers do not understand ICS, PLCs, and SCADA systems, so my network is secure.

Since 2010, there have actually been several sophisticated cyberattacks that targeted ICS networks, such as Stuxnet (targeting PLCs) and Industroyer (targeting circuit breakers). There has also been malware designed to target industrial control devices. This trend indicates that hackers are changing their focus to target industrial sectors, such as oil and gas, energy, and manufacturing, which suggests that attacks on industrial sectors are likely to increase in the future.

Figure 1. Notable cyberattacks that targeted ICS networks from 2010 to 2018.

Myth 3: My network is too small to be targeted, so my network is secure.

Internal breaches often come from trusted users, employees, and external contractors that have authorized access on a network. Often times, the unintentional breach is due to human error or a device that malfunctions, which is not relevant to the size of your company. Although these attacks are unintentional, they can still result in substantial damage and financial losses to your business.

Myth 4: I already have a firewall to protect my industrial network, so my network is secure.

Firewalls may provide the first level of protection but they are not 100% effective. Moreover, most firewalls are not designed for industrial protocols (for example, Modbus TCP, EtherNet/IP, and PROFINET), so without proper configuration, the firewall may block necessary industrial protocols and shut down industrial control systems. Simply put, implementing firewalls cannot guarantee complete protection for ICS networks. Instead, industrial firewalls should be utilized with layered defenses (the defense-in-depth approach) to protect critical control devices, production lines, and the entire factory. In addition, industrial devices should be frequently updated with security patches to protect against cyberattacks.

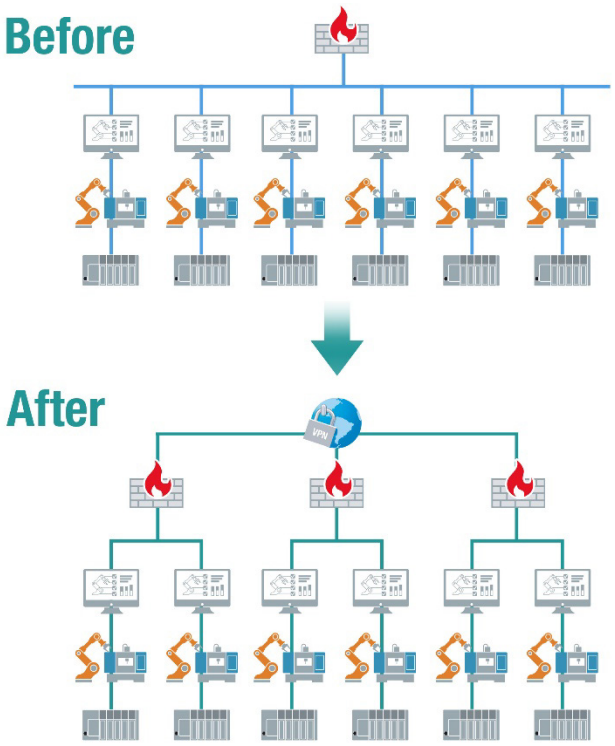
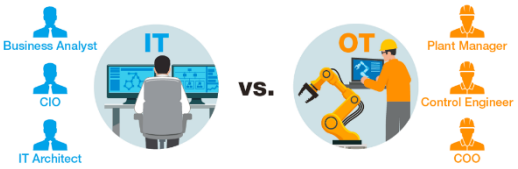


Figure 2. Firewalls for ICS networks should utilize layered defenses (the defense-in-depth approach) to protect critical control devices.

The Differences Between Industrial Networks and IT Networks

Industrial networks and IT networks actually have different business priorities, focus areas, protection targets, and even environmental conditions. Different priorities are also decided by different managers within the same organization. On the IT side, business analysts, CIOs, and IT Architects are the primary decision-makers that plan and manage the IT network and cybersecurity. From their point of view, confidentiality is the top priority. On the OT side, plant managers, COOs, and control engineers are the main decision-makers. From their point of view, production or system availability is the key concern. Therefore, in order for IT-OT integration to succeed, it is important to understand the different business priorities and needs of both IT and industrial control systems. The following figure describes these differences in greater detail.



	IT	OT
Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Zero downtime for control processes
Protection Targets	Windows computers, servers	Legacy industrial devices (PLC, HMI, meters)
Environmental Conditions	Air-conditioned	Harsh environments (extreme temperatures, vibrations, shocks)

Figure 3. Different priorities for IT and OT networks.

If not properly addressed, the different priorities of IT and OT networks may even interfere with each other. For example, industrial control systems (i.e., OT networks) are primarily concerned with minimizing system downtime because any downtime can cause significant losses to production. However, common best practices for IT networks include constant security patches and system updates to mitigate the risk of security breaches and data loss. However, constantly updating security patches may be undesirable for industrial control systems because each update disrupts real-time system operations and requires some downtime.

In the past, ICS networks were physically isolated and almost immune to cyberattacks so most legacy industrial devices did not have extensive security features. For example, a PLC or HMI may not have had their default passwords changed, which means they are vulnerable to cyberattacks. IT networks, on the other hand, already have very mature security features, such as account management and authorization mechanisms. However, it is difficult to apply IT security features to legacy OT devices because the OT devices were not originally designed to handle IT features.

Finally, industrial devices often do not operate in climate-controlled environments. Sometimes, the devices even operate in harsh environments with extreme temperature, strong shocks, vibrations, and high electrical noise interference. Enterprise IT equipment is not designed to operate in these environmental conditions for a long period of time (24/7 for several years), which may affect system reliability and increase the total cost of ownership.

Best Practices for Enhancing Your Industrial Network Security

Despite the big differences in priorities and techniques used to protect industrial control systems versus enterprise IT systems, several industrial associations have developed standards and security guidelines for connecting or converging ICS with IT systems. In particular, the Industrial Internet Consortium (IIC), National Institute of Standards and Technology (NIST), and International Electrotechnical Commission (IEC) focus on three major areas for improving ICS cybersecurity. These three pillars for securing industrial networks include:

- **Deploy defense-in-depth protection for industrial networks**
- **Enable security settings on your industrial networks**
- **Manage security through education, policies, and monitoring**

Based on these three pillars, we recommend the following best practices as the first step to shoring up your ICS cybersecurity.

Pillar I: Secure network infrastructure

Secure networks are made by design. Unfortunately, most automation networks have been deployed, added to, and modified slowly over several years or even decades. Many PLC networks and devices were never designed to be connected to a plant network or the Internet and often lack strong security features, if any at all. Since the priority was to keep the plant operating, networks were designed more with simplicity in mind than security.

In order to deploy a secure industrial network, the first thing you need to consider is a "defense-in-depth" network design. A defense-in-depth network design starts with segmenting your network into logical zones, each of which is isolated and protected by industrial firewalls. Between each zone, you can then set up conduits, which are firewall rules that filter or manage data communication across the zones in your network. In short, a defense-in-depth design seeks to protect your network from the inside out.

Consider the example of a smart factory. Although it is important to deploy a firewall between the IT network and the OT network, this is not enough. Within the OT network, additional firewalls for critical assets, such as a controller for a distributed control system (DCS), should also be installed. After all, the more critical the device, the more security protection it requires. This is the basic tenet of a defense-in-depth design. By making it harder for unauthorized personnel to access a critical system, you minimize the potential impact of a security breach by limiting access to a single zone rather than granting complete access to the entire network.

An intrusion prevention system (IPS) or intrusion detection system (IDS) is an advanced system you can consider for your industrial network system. The IPS/IDS will monitor network data for malicious activity. It is commonly used in IT/office networks. But it can also be used for industrial control system networks since there are more and more applications that are running on Windows-based industrial computers.

Another important factor in secure network design is secure remote access. Similar to using VPN software on your laptop to access a corporate network from home, you can also deploy encrypted VPN connections for remote monitoring or remote maintenance.

Best Practice I: Secure Network Infrastructure

- **Segment your ICS into several subsystems and define the data communication needs between subsystems**
- **Install industrial firewalls between each segment and configure the data communication policy properly (for example, block unnecessary data communication with protected subsystems)**
- **Install an intrusion prevention system (IPS) or intrusion detection system (IDS) to monitor malicious activity on your industrial network**
- **Set up VPN connections for any remote monitoring or remote maintenance access**

Pillar II: Hardened device security

Another best practice for shoring up industrial network security is device security, often referred to as device hardening. This refers to securing the network switches, routers, and other devices connected to your industrial control system. Some of the methods include user authentication, maintaining the integrity and confidentiality of data, and using authentication to control network access. These are all things you probably experience in daily life with your own personal devices.

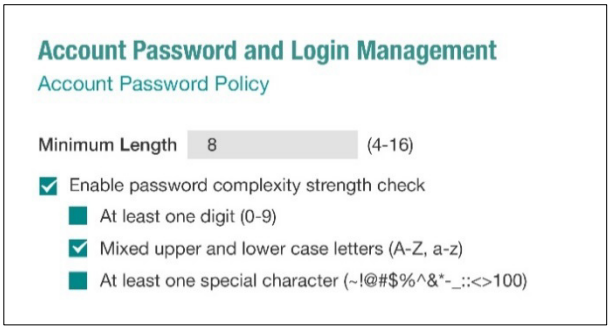
For example, online access to a bank or credit card account requires a strong password. And if you are unable to sign in after a certain number of failed attempts, you will probably be locked out and need to contact support to prove your identity. This is the basic concept behind user authentication.

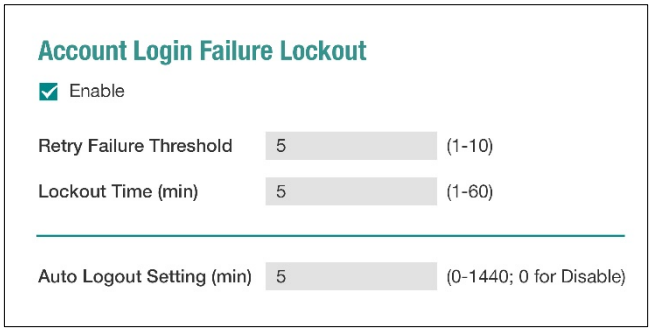
Another example is a web browser message that notifies you when your connection is not secure. That is because the site you are trying to access requires or recommends an encrypted web session using HTTPS. This is the basic idea behind data integrity and confidentiality.

To complete the analogy, have you ever tried to log in from a new device and had to validate the device through a registered email address or text message to a registered cell phone? This is concept of authentication and access control.

While these concepts are familiar to most people, it is quite common to see industrial devices in critical systems deployed with little to no configuration for security. In many cases they still have the default user name and passwords as shipped from the manufacturers.

Besides the previously mentioned security settings, you should also consider vulnerability management. If you have ever installed a Windows update on your computer, this is simply applying the patches to known vulnerabilities as they are discovered and fixed. Since vulnerabilities affect components from virtually every software and device manufacturer, working with vendors that have a well-defined response plan for patching vulnerabilities is more important than ever.





Base Practice II: Hardened Device Security

- **Confirm that you are not using default passwords on your equipment, especially network devices such as industrial Ethernet switches, routers, wireless access points, or cellular routers.**
- **Choose a strong password that has at least eight characters and is hard to guess.***
- **Enable access lockout features.**
- **Enable access control lists. This feature can pre-register device IP or MAC addresses on the industrial network device and only allow the devices that match the access control rules to use the network.**
- **Use a VPN or HTTPS session to encrypt communications for remote access to industrial devices through a web console. This helps prevent sensitive data, such as login account IDs and passwords, from being stolen.**
- **Check with your equipment vendor on how to get device security patches and updates within the shortest amount of time after they become available.**

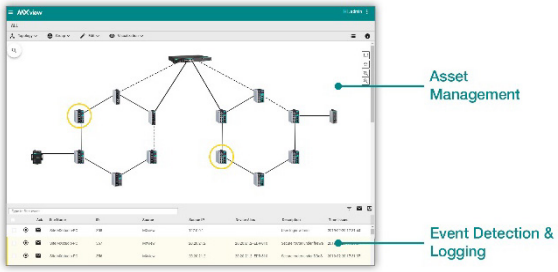
Pillar III: Security management and education

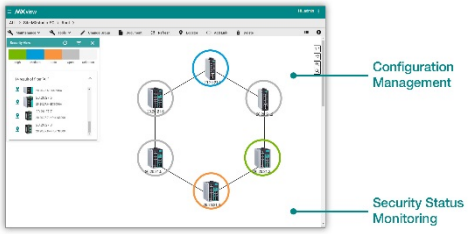
The third best practice is the concept of security management or monitoring your network security, which includes educating/training the engineers that use your ICS to comply with new security policies. Education to ensure cybersecurity policies and practices are followed through could be the most important best practice of all, as well as the most difficult to implement successfully. To facilitate compliance, you may also want to consider investing in specialized software tools to manage ICS security policies more efficiently.

In particular, some industrial network management software can help scan network devices, give you an inventory list so you can easily identify if something that should not be there is located, and remove it. Some tools can even help you consistently configure new devices to comply with the security settings you have selected, visually validate that the devices have been properly configured, and even back up configuration files to aid in network recovery if an incident occurs.

*For further reading please see: NIST Special Publication 800-63-3B: https://pages.nist.gov/800-63-3/sp800-63b.html#reqauthtype

Another important feature is real-time event notification and logging, which notifies you when there is a security incident, such as multiple failed login attempts, firewall rule violations, or a device configuration change. Logging can help pinpoint vulnerabilities and fix them before damage is done. Actually, security information and event management (SIEM) systems are very important components in IT network management. Consequently, some industrial network management systems also offer APIs (for example, RESTful APIs) or support for common network protocols (for example, SNMP) for ICS integration with existing SIEM systems.





Best Practice III: Security Management and Education

- **Develop security policies for the operators who design, operate, and maintain this system. Policies should also consider third-party contractors and equipment vendors.**
- **Train and educate system engineers to understand the importance of cybersecurity and become familiar with new policies.**
- **Develop security policies for endpoints, equipment, and network devices.**
- **Invest in security monitoring tools to monitor and back up security settings on your equipment and network devices.**
- **Record and back up event logs for industrial control system equipment and industrial network devices.**
- **Use an ICS that supports integration with existing IT SIEM systems (for example, systems that support RESTful APIs or SNMP).**

Conclusion: Industrial Cybersecurity Is Everyone's Job

Ultimately, the successful adoption of IIoT or Industry 4.0 systems hinges upon effective cybersecurity for industrial control systems that integrate seamlessly with the latest Enterprise networks. However, acknowledging that OT networks and industrial devices are no longer immune to cyberattacks is only the first step. Manufacturers also need to understand and balance the different priorities of their IT and OT departments in order to effectively break down organizational silos and implement best practices for strengthening industrial network security: deploying defense-in-depth protection, enabling security settings on industrial networks, and managing security policies through education and monitoring. As these guidelines suggest, the responsibility of ensuring cybersecurity for industrial networks falls on more than just one person in your organization. In the end, everyone in your organization has a crucial role to play when it comes to industrial cybersecurity and the successful transformation of legacy OT systems to Industry 4.0 in a future where everything is connected to the Internet.