A Checklist for Building a Secure Industrial Network

Secure digital products are a must for asset owners and industrial operators to build secure OT products and industrial systems. To assist in this, the Cybersecurity and Infrastructure Security Agency (CISA) collaborates with several authorities worldwide to release "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products," a guideline for OT operators in selecting digital products. Networking devices are one of the essential components of OT digital products. As an expert in industrial networking, we have created a checklist to help you choose the right networking devices, establish layered security, and efficiently manage networks. This will help you select the best solutions for building a secure industrial network for your OT systems and products.

Considerations for Choosing Secure Devices

- □ Provides **strong authentication** for identity verification and access control. Also, uses role-based access control (RBAC) to assign permissions based on different levels
- □ **Disables insecure default settings and unused services**, including default passwords, insecure protocols, and unused interfaces
- □ Provides a **security hardening guide** for networking devices to ensure they are used securely
- □ **Encrypts configuration data** to increase confidentiality and reduce the risk of unauthorized changes
- □ **Verifies authorized devices** before allowing access to the network and communication with other devices
- □ **Select device vendors** that securely distribute updates for products to fix or promptly mitigate vulnerabilities

Expert Tips for Choosing Secure Devices

Look for a device vendor that implements a secure development life-cycle and designs their networking devices referencing industrial cybersecurity standards such as IEC 62443-4-2.

Considerations for Securing Network Infrastructure

- □ **Segment networks** into smaller subnetworks to isolate and contain potential issues, preventing disruptions affecting the entire system
- □ **Create a DMZ** to control and limit external connections, safeguarding sensitive OT data from external threats
- □ **Filter out unauthorized traffic and block unauthorized access** to enhance network security
- □ **Create a secure tunnel for encrypted data transmission** to ensure data integrity
- □ **Prevent** potential attacks from **known threats** to minimize security risks
- □ **Perform virtual patching** to safeguard legacy devices are not physically updatable

Expert Tips for Securing Network Infrastructure

Adopt defense-in-depth strategies to minimize security risks for your networks. Build layered protection and implement security measures to reduce the impact of threats on systems.

Considerations for Managing Network Security

- □ **Ensure all network devices** are configured to **the required security level**
- □ **Notify** users when device on the network have **insecure configurations**
- □ **Regularly monitor the network** to see if any unknown devices were added
- □ **Perform security assessments** of all connected devices periodically to maintain overall network integrity
- □ **Log critical events**, such as restarts, logins, or configuration changes on the network, as well as security events
- □ **Compare the network configurations** before and after incidents to find the root cause of the problem
- □ Provide **authenticated backup** for configuration settings for fast restoration after security incidents
- □ **Update security patches** timely and allow users to deploy them easily and securely
- □ Use a secure and efficient mechanism to **restore your system database** after an attack for quick recovery

Expert Tips for Managing Network Security

Maintaining daily network security and preventing threats is a huge undertaking for network administrators. Use a network management tool to help you easily plan, deploy, monitor, and maintain your network security.

MOXA®

For more information about Moxa's secure networking solutions, visit www.moxa.com/security.

Moxa's Secure Networking Solutions

Select Secure Devices

You need security-hardened networking devices to build a secure network foundation

Continuous Secure Development

Secure Software Development
Moxa's PSIRT enables swift responses to newly reported Moxa device vulnerabilities.

Vulnerability Management
Moxa devices provide high-quality performance and minimize cybersecurity risks through strict software version control and regular firmware security scans.

Embedded Security Functions

Device Integrity and Authenticity*
Validates the integrity and authenticity of device firmware and boot processes (Secure Boot)

Device Least Functionality
Provides hardening guides to restrict the use of unnecessary services

User Authentication and Authorization
Verifies the user identification when logging into devices based on various privileges

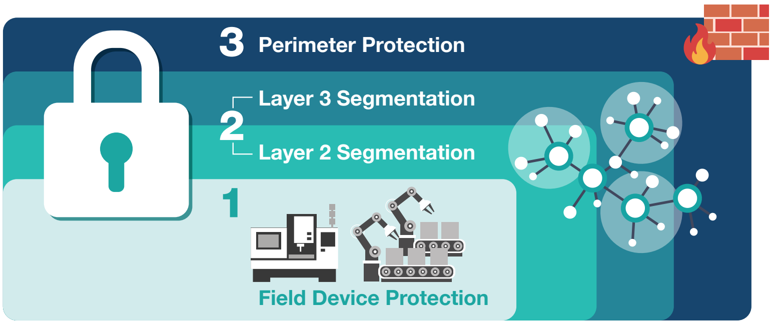
Network Access Control and Authentication
Verifies which devices are permitted to access the network and communicate with other devices

Communication Integrity
Encrypts connections with devices for configuration and management

* Only available for selected models.

Build Layered Protection

Implement a layered protection to mitigate security risks for your industrial networks



3. Perimeter Protection
Deploy boundary firewalls to block cyberattacks from outside networks, ensuring reliable operations.

2. Layer 2 and 3 Segmentation
Implement VLANs and network subnetting to virtually isolate different system zones, ensuring only trusted communications through controlled network access and traffic flow.

1. Field Device Protection
Deploy an industrial IPS for your critical assets. It safeguards legacy devices from malicious actions through threat prevention and virtual patching.

Identify Network Status

Visibility empowers you to secure and control your industrial control systems

Security Add-on Tool
Centrally manages firewall policies and monitors network security using a security dashboard.

Centralized Account Management
Centrally manages accounts and passwords for multiple networking devices on one platform.

Device Security Monitoring
Visualizes device security levels and provides secure setting suggestions.

Network and Traffic Monitoring
Monitors the traffic between devices on your network and triggers events for specific traffic conditions.

Rogue Device Detection
Identifies connected devices that are not in the current topology.

Centralized Device Management
Manages networking devices easily and securely with configuration backup and firmware patch management.

MOXA®

For more information about Moxa's secure networking solutions,
visit www.moxa.com/security.

Disclaimer

This document is provided for information purposes only and does not constitute any compliance advice. Contents hereof may be changed by Moxa without any further notice to you. By this document, Moxa does not provide any representation or warranties of any kind, whether express or implied, including but not limited to warranties of merchantability or fitness for a particular use, or that the products will be error-free. We specifically disclaim any and all liability with respect to this document and no contractual obligations are formed, directly or indirectly, through this document.

MOXA®

For more information about Moxa's secure networking solutions,
visit www.moxa.com/security.