WHITE PAPER

# Securing Network Devices with the IEC 62443-4-2 Standard—What You Should Know

**Vance Chen**
*Product Manager*

MOXA®

## Industry Background

*As the Industrial IoT (IIoT) continues to expand, more and more devices are being connected to networks. This trend is seeing networks transitioning from closed networks to enterprise IT networks that are accessible over the public Internet. While this trend is enhancing operational efficiency, it is unfortunately causing asset owners to become increasingly concerned about the dangers posed by cybersecurity threats. The asset owners' concerns are justified. A recent report released by the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) calculated that investigators responded to 295 incidents in 2015 in the U.S., compared to 245 the previous year regarding cyber attacks on infrastructure. It is even more concerning for the critical manufacturing sector, which saw the largest increase proportionally from 27% of the overall total in 2014 to 33% in 2015. It is therefore unsurprising that asset owners are increasingly requiring cybersecurity solutions to allow them to build secure systems for industrial applications.*

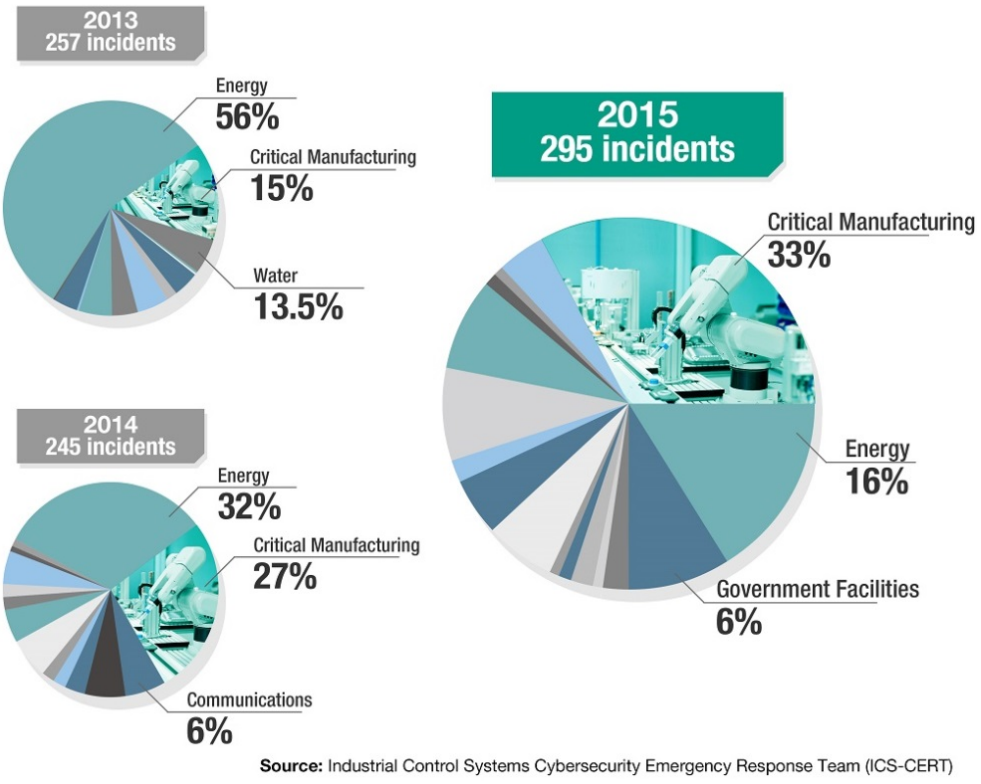


Fig. 1: Overview of cyber attacks affecting the critical manufacturing sector

Released on September 12, 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 40 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 automation systems. 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

## How Cybersecurity Standards Evolved

In 2002, the International Society for Automation (ISA) produced the ISA-99 document to advise businesses operating in the automation industries how to protect against cybersecurity threats. Fifteen years ago, cybersecurity wasn't the hot topic it is today. The ISA documents have been aligned with those more frequently used by the International Electrotechnical Commission (IEC) as the concerns around cybersecurity have grown since the conception of the ISA standards. Currently, the IEC 62443 standard constitutes a series of standards, reports, and other relevant documentation that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). If the guidelines within the IEC 62443 standard are followed, it significantly reduces the chances of a cyber attack affecting the network.

### A Quick Glance at the IEC 62443 Standard

The IEC 62443 standard includes guidelines for different parts of a network and those who perform different responsibilities on the network. In the past, asset owners relied on system integrators (SIs) such as Siemens, Honeywell, and ABB to provide the security solutions for the network. However, many SIs now demand that component suppliers comply with the subsection of the IEC 62443 standard that pertains to their devices. The diagram below provides a brief overview including the scope and the significance of each part for those who must ensure the secure operation of a network.

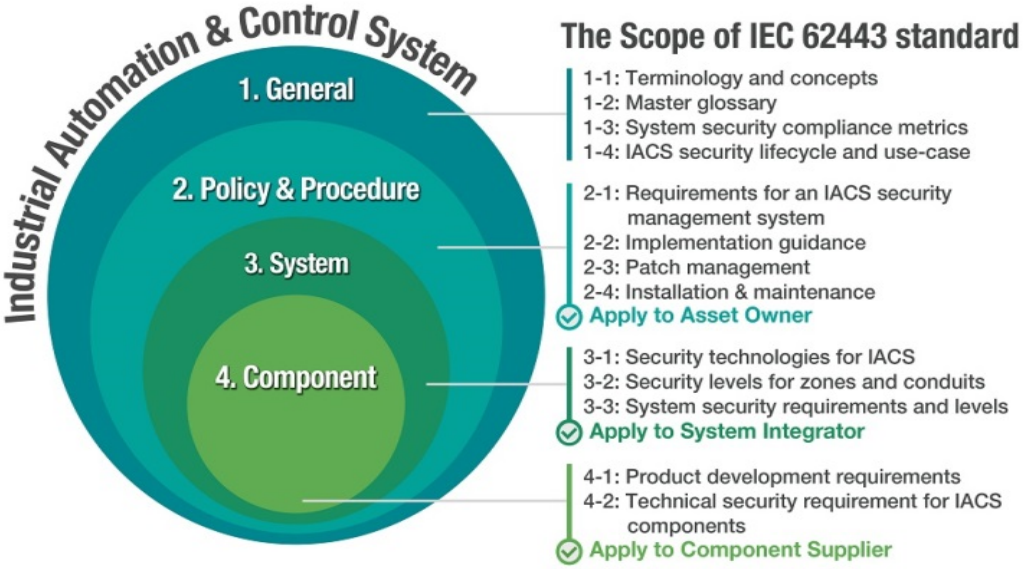


Fig. 2: Industrial Automation & Control System Overview

The IEC 62443 guidelines define four security threat levels. The security standard level 2 is the baseline requirement of the automation industry. It relates to cyber threats posed by hackers, which is the most common attack experienced by system integrators who secure industrial networks. Level 1 is to protect against accidental unauthenticated access and Levels 3 and 4 are against intentional access by hackers who utilize specific skills and tools.

## IEC 62443-4-2 Level 2: Baseline Requirements of the Automation Industry

Within the IEC 62443 standard are several subsections that relate to different parties. As SIs are demanding compliance with the IEC 62443-4-2 subsection, which issues guidelines for component suppliers, the subsection is becoming increasingly important. The component requirements are derived from foundational requirements, including identification and authentication control, use control, data integrity and confidentiality, as well as backup for resource availability. Due to the increasingly important role that component suppliers are playing on IIoT networks, the remainder of this paper will focus on the details of the security requirements that component suppliers must meet when designing devices for deployment on IIoT networks.

### Infrastructure

If a network component allows users to access devices or applications, the network component must be able to uniquely identify and authenticate all users, including humans, processes, and devices. This allows separation of duties and the principle of least privilege that ensures every user only has access to information and devices that are essential for the user to be able to perform their designated role within the network. It is essential to avoid the unnecessary security risk of granting users greater access to the network than is necessary for them to perform their roles. Avoiding this unnecessary security risk will restrict users with malicious intent from being able to cause greater damage to the network. Following this guideline will help secure the infrastructure of a network and provide a solid foundation to develop networks so that the networks are ready to meet the security challenges of today and tomorrow.

### Account Management

The capability to support the management of accounts, including establishing, activating, modifying, disabling, and removing accounts, must be supported across the network. This ensures that no accounts are created, modified, or deleted unless permission has been granted, and forbids embedded devices from making any unauthenticated connections. The management of accounts feature has several possible scenarios, which if not implemented could cause problems for asset owners. For example, a person who works on the network gets promoted, so they now require more access to devices and applications, and their privilege level must be adjusted accordingly. Another example that is frequently encountered is when an employee leaves the organization. As soon as they cease being an employee they must no longer be able to access the network and must have their network privileges revoked. It doesn't require a stretch of the imagination to envision the possibility of a disgruntled ex-employee who was recently dismissed accessing the network after his departure with malicious intent.

### Identifier Management

Any component of the network with a direct user interface must directly integrate into a system that identifies individuals by user, group, role, and/or system interface. This stops users from being able to access devices connected to the network that they haven't been granted access to. As those with different roles on a network have different privileges, a network administrator's account can often manage device configurations on a network, but someone who has guest level access can only view devices, but not alter configurations. In addition, there should be security procedures in place if an account hasn't been accessed for a

certain period of time that allows the account to be deactivated. The identifier management feature controls each user's account on the network and ensures that users are confined to the roles assigned to them by network administrators so that users can't accidentally or on purpose access parts of the network that they don't need to access.

### Authenticator Management

All devices on a network must be able to confirm the validity of any requests for system/firmware upgrades, and verify that the source isn't trying to upload any viruses or malware. This is achieved by requiring the use of tokens, keys, certificates, or passwords. If no authenticator management system is in place, anyone wishing to attack the network could very easily upload malware, allowing them to change settings or take over control of the network.

### Password-based Authentication

For network components that utilize password-based authentication, the network component must integrate a password policy that enforces the following:

A) The password composition must state what type of characters are allowed, as well as the number of characters required before a password will be accepted as valid

B) The frequency that the password must be changed

The advantage of using a password is that it is a simple way for network administrators to protect their network without requiring any additional work from system engineer. Utilizing an effective password policy will keep out the majority of hackers who gain access to networks by using brute force to break weak passwords. A network that doesn't support a password policy or a network that allows weak passwords to be used is at a much greater risk of hackers gaining access to the network.

### Public Key Authentication

Public key authentication should be used in order to build a secure connection between servers and devices, or device-to-device connections. In order to enable this function, each network component must be able to validate certificates by checking the authentication of the signature, as well as the revocation status of a certificate. In addition, it should construct a certification path to an accepted certification authority, or in the case of self-signed certificates deploy certificates to all hosts that communicate with the subject to which the certificate is issued. Public key authentication is important because it stops information from being sent to the wrong place, and also stops confidential information that should remain within the network from being transferred to unverifiable sources outside.

### Use Control

All of the devices that appear on a network must support login authentication. To restrict unwanted users from gaining access to a device or the network, the application or device must limit the number of times a user can enter the password incorrectly before being locked out. As the majority of attacks on industrial networks are performed by hackers using brute force attacks, login authentication is an extremely effective method of stopping hackers from gaining access to a network. In addition, the system or device must also be able to inform users whether their login attempt was successful or not. Informing users that they are logged into

the network allows them to confirm their current status and proceed knowing that changes or alterations they make to network settings or devices have been authenticated.

**Data Integrity**

Across all IIoT networks data integrity plays a vital role. It ensures that data is accurate, and that it can be processed and retrieved reliably. There are several security measures that can be utilized to protect the data, including SSL, which enables encryption between a web browser and a server. As data is constantly moving around a network, network operators need to be sure that the data is moving in a safe, reliable, and efficient manner. If the data is sent to unintended recipients, the network operators will not only lose control of their data, but also leave their networks vulnerable to hackers.

**Backup for Resource Availability**

All of the applications or devices that are found on a network must be able to back up data without interfering with network operations. The main advantage of performing regular backups is to ensure that no data is lost and that if the network experiences some problems the network can utilize the data that has been backed up to return the network to normal. In addition, the backup process must ensure that any private information that is on the network is stored in accordance with data protection policies and is not accessible by anyone who should not have access to that information. In some cases this means that data can't be stored outside the network. Any data breach containing users' personal information is extremely damaging to network operators as well as to those whose data has been accessed by those it shouldn't be accessed by.

**Conclusion**

As more devices are constantly being added to networks, the security of these devices is of paramount concern to asset owners. It is acknowledged throughout the industry that adopting the best practice approach to security gives asset owners the best chance of protecting their network from those with malicious intent. To enhance component-level cybersecurity, Moxa has introduced the latest switch firmware, called Turbo Pack 3, which is not only compliant with the IEC 62443-4-2 level 2, but also supports other security functionalities, such as enhanced MAC Address and RADIUS authentication to ensure the integrity of data and the network from known security leaks and unknown attacks.

Learn more about Moxa's latest switch firmware functions:

http://www.moxa.com/news_events/New_Switch-Firmware.htm