WHITE PAPER

Tips on How to Ramp Up the Security of Industrial Networks

Yiwei Chen
Product Manager

MOXA®

It is inevitable that the adoption of the Industrial IoT (IIoT) is going to continue to grow, facilitating more and more devices to be connected to networks. The momentum driving this trend is a strong desire from asset owners to enhance operational efficiency. However, achieving enhanced operational efficiency is not without problems. It is forcing asset owners to start to give serious consideration to the dangers posed by cybersecurity threats.

Every device that is added to a network creates a potential weak point or vulnerability by providing attackers with a possible entry point to the network. The importance that companies and even governments are starting to place on cybersecurity is hard to overestimate. In July 2016, the European Parliament[1] published guidelines that should be adhered to in order to prevent cyber attacks. Asset owners are united in their demands for cybersecurity solutions that allow them to deploy secure devices and networks for industrial applications.

What is the IEC 62443 Standard?

The IEC 62443 standard is constantly evolving to provide up-to-date security guidelines and a list of best practices for different parts of a network. It also includes information for those who perform different responsibilities on the network in order to protect against known security leaks and unknown attacks. The ultimate goal of the standard is to help improve the safety of networks and enhance industrial automation and control settings security. At present, many system integrators (SIs) require component suppliers to comply with the IEC 62443-4-2 subsection of the IEC 62443 standard that specifically pertains to the security of end devices. The subsection is compiled from foundational requirements, including identification and authentication control, use control, data integrity and confidentiality, as well as backup for resource availability.

Understanding the Security Risks

There is a general consensus among security experts that there are six main cybersecurity threats that can affect internal networks, including unauthorized access, unsecure data transmission, unencrypted key data, incomplete event logs, lack of security monitoring, and human setting errors. It is paramount that network operators understand these threats so that they can deploy devices that have sufficient security features in place and ensure that their networks are safe from internal and external threats. Consideration will now be given to situations where these security risks can arise and some of the options that are available to network operators in order to neutralize threats to their networks.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Released on October 28, 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

Reliable Networks ▲ Sincere Service

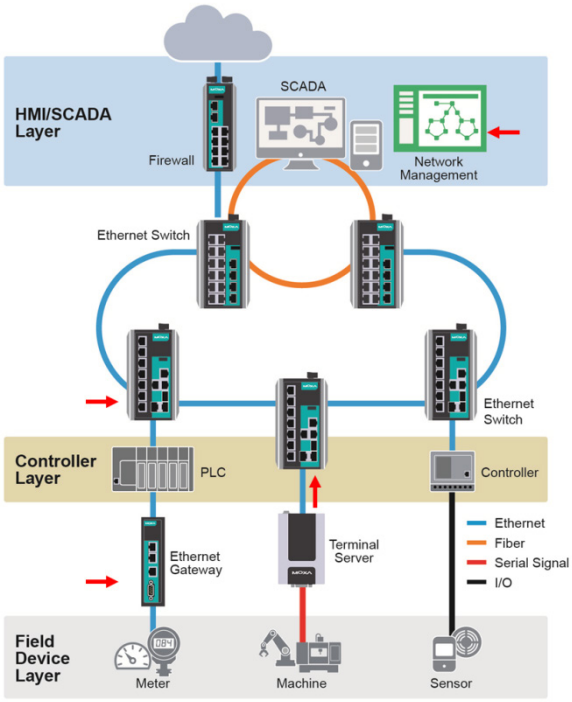

Diagram 1: Unseen security risks in industrial control system networks

Prevent Intrusions and Attacks

The first step to prevent unauthorized access to devices on a network is to implement a password policy. While password policies are effective to a certain extent, as the number of users and devices on a network increases, so does the possibility of the network being breached. It is frequently noted that one of the greatest risks posed to the security of the network is from a user who gains unauthorized access to the industrial control system and then exploits the network. A strong password policy is definitely a good starting point to prevent brute force attacks, but there are several other features that should be used in conjunction with a strong password policy in order to enhance the security of the network.

An identifier management policy will often include several parameters to further enhance the security of the network. These parameters will typically ensure that the accounts can only be used by the users they were created for, and that the users only have access to parts of the network that are required for them to fulfil their job roles. The devices deployed on the network should be capable of logging users out of accounts that they shouldn't have access to and alerting the network operator of any violations. This will further reduce the chances of someone gaining unauthorized access to the network or devices.

Protect Sensitive Data

All devices on the network must support and enforce data encryption when data is transmitted on the network. This will almost eliminate the risk of data being stolen during transmission. The reason why data integrity is so important is because it guarantees that data is accurate, and that the data can be processed and retrieved reliably and securely when it is needed. When data integrity is not guaranteed, network operators are unable to ascertain whether the data is accurate. When this scenario arises, the data becomes meaningless to network operators who require accurate data. It is even more troubling when the data is manipulated to provide false information, and causes network operators to adjust settings or make the wrong decisions that cause further damage to the network.

As well as the data collected from devices, another type of data that is hosted on IIoT networks is configuration data. The configuration of network devices in industrial control networks is highly important. If the configuration data is inaccurate, or is corruptible, it can cripple network operations. In order to reduce the risk of the configuration data being corrupted, it is essential for devices to support and enforce configuration encryption.

The Ability to Audit Security Events

Networks must constantly be monitored and every event that takes place on the network should be recorded for further analysis if required. Although several security precautions can be taken in order to prevent cyber attacks, in the event that an attack is successful, it is quite difficult to detect in real time. By utilizing data logs, network operators are able to track what activities took place before an incident occurred, and then analyze the data. This allows the network operator to effectively address the issue. Network operators can also use the valuable information that is provided by event logs to improve the design and security of the networks, and prevent networks from disruption in the future. Other counter-security measures include the ability to log users out, delete accounts, and restart devices.

Visualize the Security Status of the Network

Software that visualizes the security status of the network allows network operators to monitor any abnormal or potentially damaging activity that is taking place on the network. In addition, this type of software can help network operators prevent problems before they arise, by allowing the network operators to ensure the correct settings are applied to each device on the network at a quick glance. If a device isn't as secure as it should be, the network operator can identify the problem to reduce the risks that arise from the vulnerabilities. The security features that are typically covered can include password policies, encryption, login credentials as well as the integrity of the data.

Correct Configuration

Human error typically occurs when network operators inadvertently configure the settings inaccurately. This has the potential to cause a wide range of problems, including the network not functioning properly, data being lost, or even creating significant network vulnerabilities for attackers to exploit. When the configurations on a network are incorrect, it creates the possibility that the network can be manipulated by internal staff or those outside who have gained unauthorized access. For cyber attacks that are successful due to human error, the network operator will often not be aware that the network has been compromised for some time after the breach has occurred, allowing significant damage to be caused to the network. Cyber attacks that are caused by human error are the most common method that networks are compromised, so significant consideration should be given to preventing this type of attack.

Moxa's Solution

There is a common factor with the above six security risks that results in network operators losing the ability to control and manage their network. Moxa, along with many other security experts in the industrial automation industry, strongly believe that the best way to protect the overall security of networks is to start with ensuring the security of the switches as well as the serial-to-Ethernet solutions. In response to the security threats facing network operators, Moxa has started developing solutions that meet the technical security requirements of the IEC 62443-4-2 level 2 standard.

- Moxa's Industrial Ethernet switches include the new firmware Turbo Pack 3 in order to meet the technical security requirements of the IEC 62443-4-2 level 2 standard, and also support MAC Address and RADIUS authentication.
- Serial-to-Ethernet connectivity: Industrial secure terminal servers, NPort series, and industrial Ethernet gateways, MGate series
- Moxa's industrial network management software suite, MXstudio includes new functions that allow users to visualize the security status of their network so they can monitor events, and perform batch configuration.

If the security features that are discussed in this white paper are deployed on networks, and safety procedures are implemented correctly, it significantly reduces internal and external security threats. To find out more about how Moxa is enhancing device security please visit: www.moxa.com/Event/IES/Security