WHITE PAPER

Three Aspects to Consider When Securing Industrial Automation Control System Networks

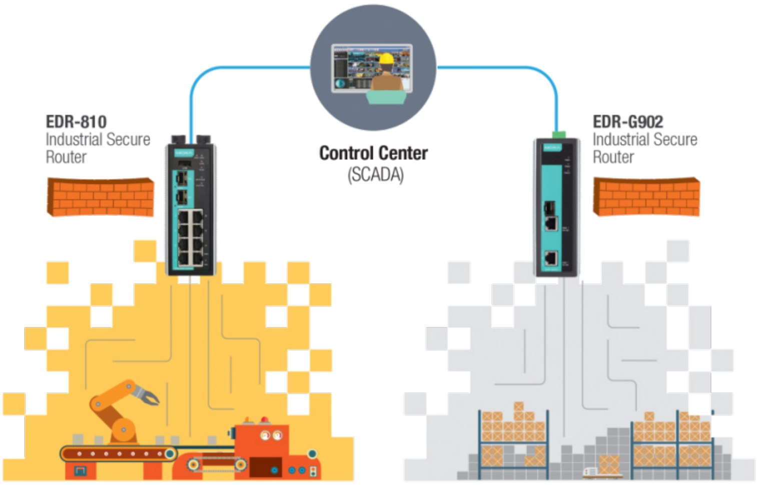
Alvis Chen
Product Manager at Moxa

MOXA®

Introduction

Operational technology (OT) consists of a combination of hardware and software to monitor and control physical devices on a network, such as valves or pumps. OT is facilitating the expansion of the industrial Internet of things (IIoT) by ensuring that different hardware and software can communicate in industrial environments. The most common examples are programmable logic controllers (PLC) in factory automation, distributed control systems (DCS) in the manufacturing industry, and SCADA systems in process automation industries such as oil & gas. When a network includes controllers and motors managed by a SCADA system as well as industrial technologies it is known as an IACS (industrial automation control system). The main benefit of an IACS is that it allows greater efficiency by facilitating remote management and more automated processes. However, the vulnerability of an IACS network increases as it expands and more networks require access to the IACS network, which is common within the IIoT.

For many years, industrial networks were isolated from enterprise networks, which meant that cybersecurity was not a primary concern for system operators as the networks were well protected due to their isolation from other networks. However, as this is no longer the case, system operators must not use out of date security practices if they want to keep their networks secure. The focus of this white paper will be to analyze why cybersecurity is of paramount importance for IACS networks and what has to be achieved in order to build, manage, and maintain secure IACS networks.



Released on June 30, 2017

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 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 industrial communications infrastructures. 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

Challenges That Must be Overcome to Increase the Cybersecurity of IACS Networks

As no networks are exactly the same and the risks posed by each threat are unique, there are numerous possible cybersecurity threats facing system operators. Before an IACS network can be deemed secure, it is essential that system operators have a thorough understanding of all of the risks. The challenges system operators face will now be explored in as much detail as possible, which will assist them to implement successful solutions to address these challenges.

How to design and deploy a secure network

- Typically, parts of an industrial network and certain devices are secure from the threats that are posed to them. However, in order to violate the security of the entire network, all that is required is to infiltrate one device or area of the network. Once someone with malicious intent has gained access to a single device on the network, it is very easy to corrupt and control other areas and devices on the network. Most network designs are intended to stop unauthorized users from gaining access to the network, but once a device on the network has been infiltrated, it is very difficult for other devices within the network to understand that it poses a security risk. As IACS networks become less isolated by adding more devices and networks to the originally closed network, they become more vulnerable to attacks. System operators that only previously managed isolated networks often have insufficient knowledge about how to ensure that an IACS network is kept secure.

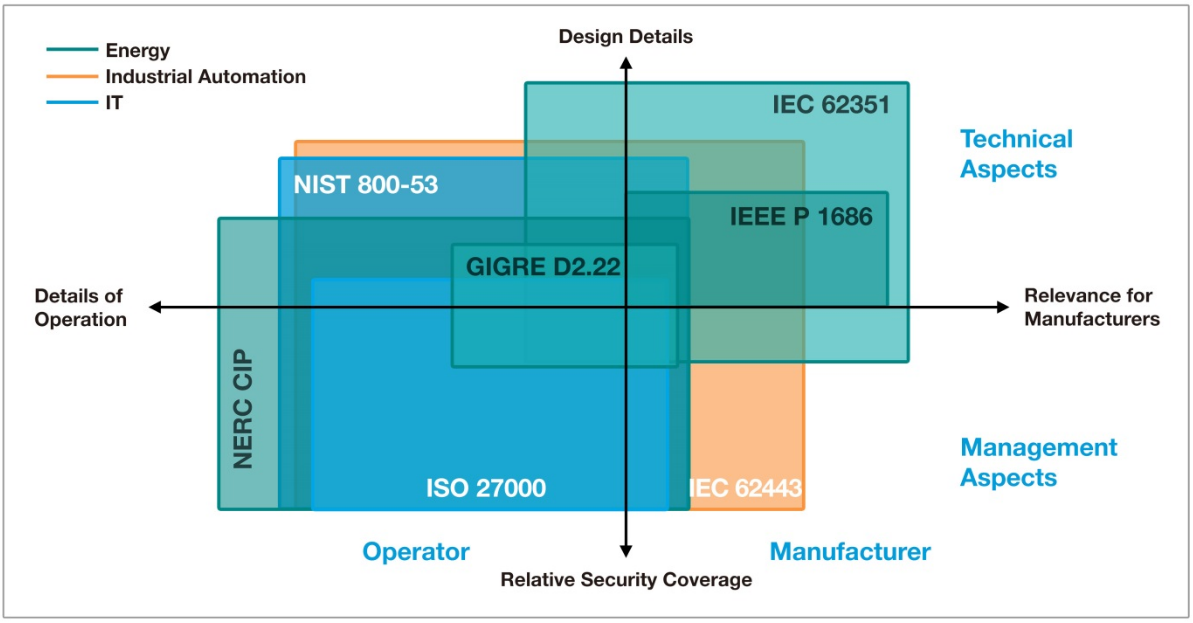
How to prevent cyberattacks against industrial network devices

- All it takes is for one device on the network to be corrupted, and it is very easy for those who have control over a single device to modify the configurations of any device located on the network. The effect that this can have on IACS networks can be devastating. In addition, as industrial networks continue to evolve to keep pace with modern trends, there are still some legacy features that need to be updated. Previously, isolated industrial networks did not know who accessed a device or from which location, but only knew that the automation process had been logged into. However, as modern industrial networks frequently converge with other networks, this makes them more susceptible to hacking. In order to combat this threat, the devices on industrial networks must record and keep log files that are capable of determining when an event with a potential security risk occurs on the network. This can include events such as a firewall blocking communications or a user unsuccessfully trying to log in three times. Another countermeasure to ensuring network devices are not affected by cyberattacks is data encryption. Previously, system operators rarely encrypted sensitive data because industrial networks used to be isolated from enterprise networks. However, as modern industrial networks continue to expand, there is a high chance that data will be stolen or corrupted as it is transmitted outside of the closed network. It is for these reasons that data encryption is essential for modern networks.

How to manage network security throughout the entire system lifecycle

- Modern industrial networks are continuously evolving. This means that the security settings need to be constantly reviewed to ensure that the network remains secure for its entire deployment. Many cybersecurity experts have observed that as an IACS network adds more devices and connects other networks for IIoT opportunities, it requires more maintenance and firmware upgrades. The more changes that happen on the network increases the chance that a vulnerability will occur that allows someone with malicious intent to gain access and corrupt the network. An example that frequently occurs is when a new device is added to the network and the default password settings are not changed. As soon as default passwords for devices are used on a network, it is much easier for hackers to gain access to a device, which puts the entire network at risk. In addition, as networks expand over the duration of their lifecycles, they often require new types of connections with different networks or devices that the system operator has not encountered before. When this scenario occurs, the system operator will often be unaware of what needs to be done to ensure these new connections are secure. This will increase the number of potential weaknesses and open vulnerabilities on the industrial network.

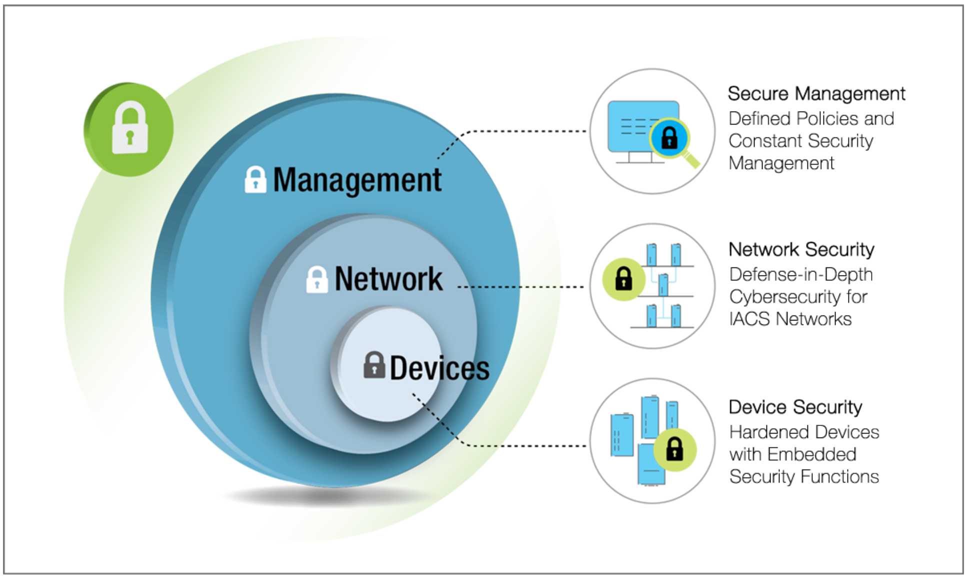
There are a wide range of options available in order to counter the numerous cyber threats posed to industrial networks. Solutions tend to focus on hardware and software that allows system operators to build secure IACS networks. In addition, there are cybersecurity guidelines developed by leading professionals, such as the IEC 62443 standard, NERC CIP, and NIST 800-53 that advise system operators on how to protect their networks. Each of these standards focuses on specific parts of a network for those who perform maintenance there. Even though there are multiple security standards that address different security areas, this white paper will focus on the guidelines set out by the IEC 62443 standard as they contain the most relevant details for the security of industrial networks.



The IEC 62443 standard covers the most basic challenges of industrial cybersecurity.

Three Factors that Help Ramp Up the Security of Industrial Networks

Industrial networks must be protected from unauthorized access that could damage industrial networks and decrease the productivity of the network. Many cybersecurity experts believe that in order to ramp up the security of industrial networks, there are three aspects that need to be addressed. These aspects will be briefly introduced before being considered in detail.


Management
Network
Devices
Secure Management
Defined Policies and Constant Security Management
Network Security
Defense-in-Depth Cybersecurity for IACS Networks
Device Security
Hardened Devices with Embedded Security Functions

- **Device Security:** This section will focus on how the evolution of industrial networks over the past few years has changed the procedures system operators must perform in order to secure network devices from cyberattacks. The first concern that will be considered is device authentication and access protection. The second concern is how to utilize an easy-to-use, effective password policy when system operators have hundreds of devices installed on their industrial network. Finally, it addresses how to ensure that all devices have the ability to collect and store event logs. Event logs alert the system operator to what happened on the network and why it happened, which will allow them to fix the problem as quickly as possible.

- **Network Security:** In the network security section, the focus will be on which devices or systems need to have the highest levels of protection. In addition to this, an explanation of the defense-in-depth approach will be given that includes examples of why it should be utilized in order to ensure that the network remains secure. Finally, the challenge of how to ensure secure remote access through the use of firewalls and VPNs will also be explored.

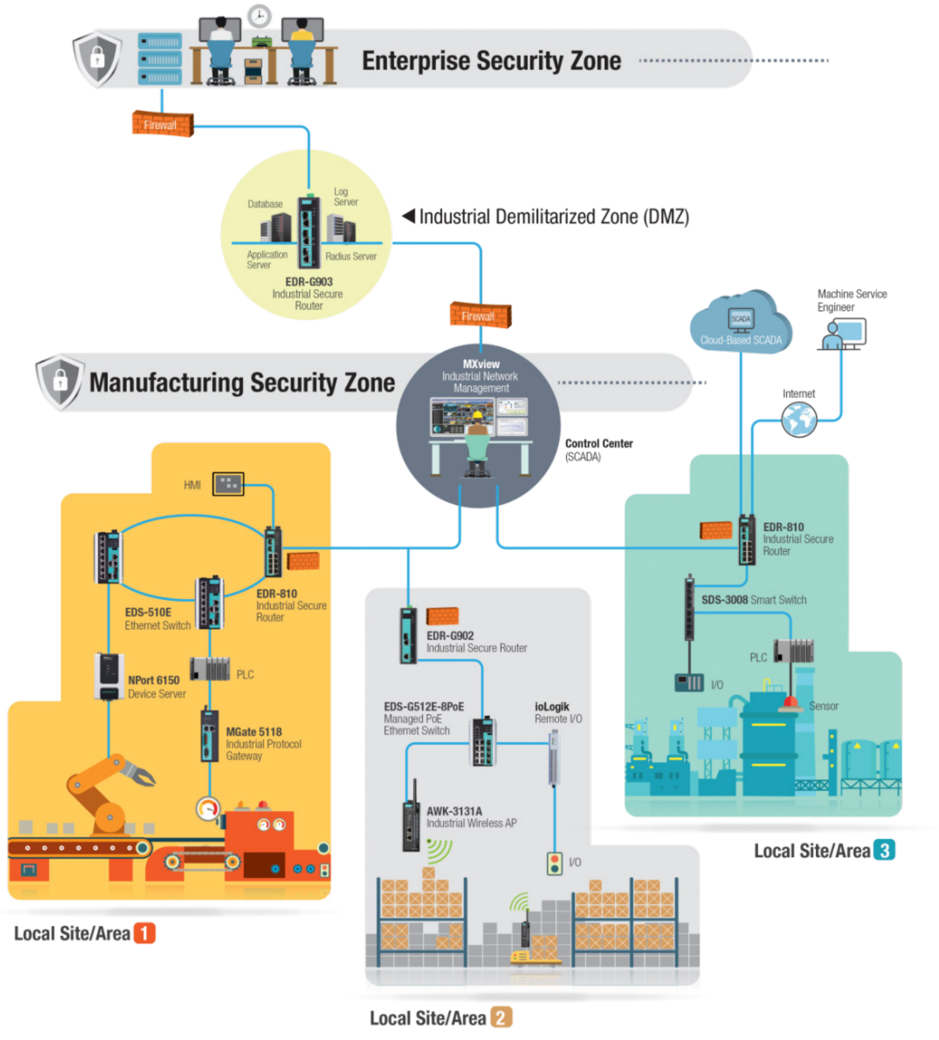
- **Secure Management:** The secure management section will consider a list of the recommended procedures for security policies and guidelines developed by experts in order to ensure that the network is protected throughout the entire network lifecycle. This section will also consider device security and how to manage the security of the entire network. Finally, this section will consider how to simplify the configuration and management of security settings. When security settings are too complicated, as is often the case on industrial networks, system operators will tend to ignore recommended guidelines and not implement security settings.

How to Implement a Secure Industrial Network

This section will give system operators a step by step overview of the three aspects that need to be considered in order to implement a Defense-in-Depth security architecture.

Defense-in-Depth Security Architecture

When designing a network, many system operators have stated that the best way to secure a network is to use the defense-in-depth security architecture, which is designed to protect individual zones and cells. Any communication that needs to take place across these zones or cells must be done through a firewall or VPN. Deploying this type of architecture reduces the chance that the whole network will fail because each layer is able to address a different security threat. It also reduces the risk to the entire network; if a problem occurs in one part of the network, there is a higher chance that the problem can be contained within that layer and will not spread to other layers. Experts have identified three steps that should be taken in order for a reliable defense-in-depth cybersecurity architecture to be deployed, which will now be considered in detail.


Enterprise Security Zone
Firewall
Database
Log Server
Application Server
Radius Server
EDR-G903 Industrial Secure Router
◀ Industrial Demilitarized Zone (DMZ)
Firewall
Cloud-Based SCADA
SCADA
Machine Service Engineer
Manufacturing Security Zone
MXview Industrial Network Management
Control Center (SCADA)
Internet
HMI
EDR-810 Industrial Secure Router
EDS-510E Ethernet Switch
NPort 6150 Device Server
PLC
MGate 5118 Industrial Protocol Gateway
EDR-G902 Industrial Secure Router
EDS-G512E-8PoE Managed PoE Ethernet Switch
ioLogik Remote I/O
AWK-3131A Industrial Wireless AP
I/O
EDR-810 Industrial Secure Router
SDS-3008 Smart Switch
PLC
I/O
Sensor
Local Site/Area 1
Local Site/Area 2
Local Site/Area 3

Step 1: Network segmentation

Network segmentation involves breaking down the network into physical or logical zones with similar security requirements. The benefit of segmenting the network is that each section can focus specifically on the security threats that are posed to that section of the IACS. Deploying the segmentation approach is advantageous because each device is responsible for a particular part of the network, as opposed to being responsible for the security of the entire IACS.

Step 2: Define zone-to-zone interactions in order to scrutinize and filter network traffic

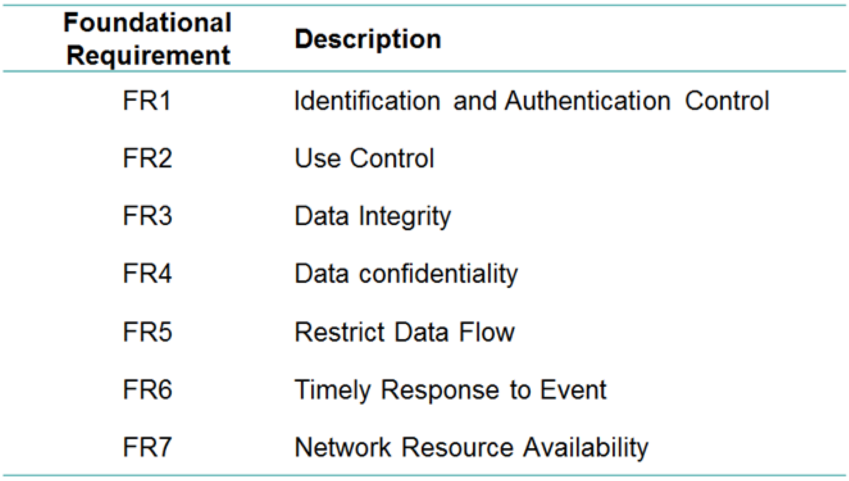
In order to enhance network security, the traffic that passes between zones in the IACS must be scrutinized and filtered. Cybersecurity experts believe that one of the best methods to filter traffic is for the data to pass through a demilitarized zone (DMZ). By utilizing a DMZ, there is no direct connection between the secure IACS network and the enterprise network, but the data sever is still accessible by both. Eliminating a direct connection between secure and enterprise networks significantly reduces the possibility that unauthorized traffic can pass to different zones, which has the potential to jeopardize the security of the entire network.

Step 3: Support secure remote access on industrial networks

Finally, within the IACS industry there is a growing need to provide access to remote sites where functions such as maintenance can be performed. However, this significantly increases the risk that someone with malicious intent can access the network from a remote location. For networks that require the remote site to be constantly connected to the IACS, it is advised to use a VPN that supports a secure encryption method such as IPsec, which prevents unauthorized users from accessing the network. There are three main advantages of using a VPN that supports IPsec. The first is that the data will be encrypted when it is transmitted. The second is that it forces the sender and recipient to authenticate who they are, which ensures that data is only passed between verified devices. The third is that by enforcing encryption and authentication, integrity of the data can be ensured. For many experts, data integrity is the most crucial aspect for system operators to use their data reliably. IPsec ensures that security keys must be between 20 and 40 characters in length, which is considered strong enough encryption to transmit data securely on an IACS. In order to ensure data is complete, system operators need to use secure transmission methods that ensure data is encrypted and authenticated at all times.

Secure Industrial Network Devices

After the network has been secured, the next step is to consider how to ensure that users cannot adversely change settings by accident or on purpose. This problem can arise from users who operate and manage the network, third-party system integrators, and contractors that are required to perform maintenance on the network. The best way to secure against this threat is to enhance the network devices' cybersecurity to ensure that they cannot have their settings altered in a way that puts the devices or the network at risk. Many cybersecurity experts view the IEC 62443 standard as the most relevant publication for how to secure devices on industrial networks. This standard includes a series of guidelines, reports, and other relevant documentation that define procedures for implementing electronically secure IACS networks. The IEC 62443 standard contains seven foundational requirements for device security on industrial networks, which will now be listed and their relevance explained.



Foundational Requirement	Description
FR1	Identification and Authentication Control
FR2	Use Control
FR3	Data Integrity
FR4	Data confidentiality
FR5	Restrict Data Flow
FR6	Timely Response to Event
FR7	Network Resource Availability

The IEC 62443 standard lists seven foundational requirements for device security.

1) Identification and Authentication Control: Public key authentication should be used in order to ensure server-to-device and device-to-device connections are secure. In order to ensure identification and authentication control, each network device must be able to validate security certificates by checking the authentication of the signature as well as the revocation status of a certificate.

2) Use Control: Every device that appears on a network must support login authentication. To restrict unauthorized users from gaining access to devices or the network, the application or device must limit the number of times a user can enter the password incorrectly before being locked out.

3) Data Integrity: Across all IACS networks, the integrity of the data is very important because 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 supports encryption between a web browser and a server.

4) Data Confidentiality: When data is stored or transmitted across networks, it has to be safe and secure. The data should be protected from all types of threats ranging from very basic ones to highly sophisticated attacks. Data must be secured at all times from those who wish to eavesdrop on communications, alter settings, or steal data.

5) Restrict Data Flow: One of the most effective methods of restricting the flow of data is to split the network up into different zones. Each of the different zones utilizes specific security features to ensure that only those with authorization can access and send data from a specific zone. Another benefit is that if a zone is infiltrated, the threat cannot easily spread to other parts of the network, which helps limit the damage caused by the security breach.

6) Timely Response to Events: It is essential that system operators are able to respond quickly to security incidents that happen on the network. In order to facilitate this, the network must support the features needed to alert system operators if a problem occurs and also keep a record of any abnormalities that happen on the network. All of the events that happen on the network should be processed in real time or at least fast enough to ensure system operators can respond quickly enough to prevent further damage being caused to the IACS network.

7) Network Resource Availability: Devices on IACS networks must be able to withstand denial of service attacks from people with only a basic understanding of IACS networks or who are presented with an opportunity due to operator error. Devices must also be able to withstand attacks from entities that have high motivation and high levels of IACS specific skills. The important point is that the network must not experience downtime regardless of who is attacking the network.

Now that the security requirements have been outlined, three examples will be explored in order to demonstrate how the fundamental requirements of the IEC 62443 standard can help protect against security threats.

The first example involves the importance of strong password-based authentication, which relates to the first foundational requirement.

- Most devices on industrial networks still use default passwords that make them vulnerable to security breaches. The reason why some engineers prefer to use default passwords is because it simplifies their work processes. However, this puts not only the devices but also the entire network at risk. In order to overcome this security issue, the devices located on industrial networks must enforce password policies that are based on a minimum password length and a variety of character types. The password policy should also include guidance for the user in the event that a password is input incorrectly. Passwords that adhere to a strong password policy will help protect against brute force attacks as they are much harder to guess.

The second example explains the importance of why devices on the network must be able to protect the integrity of transmitted data, which relates to the third foundational requirement.

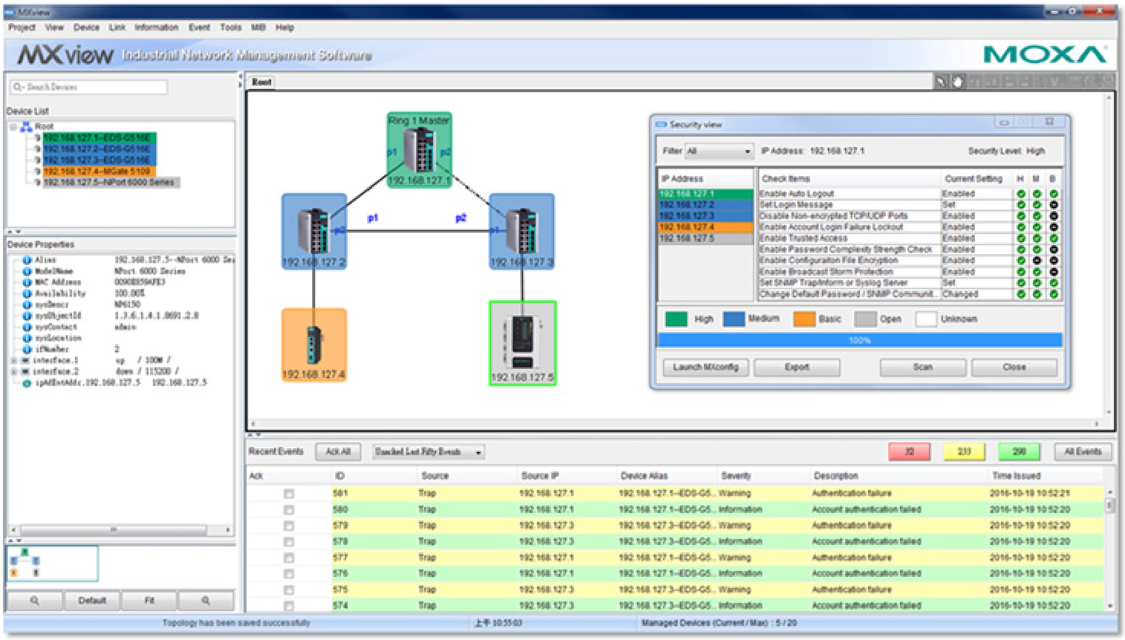
- The best way to enhance the security of the industrial network devices is by ensuring they support secure communication protocols such as SSL, SSH, or alternatively password protection for device configuration through HTTPS. However, most of the devices on IACS networks still use non-secure plain text communications. If secure communication methods are not used, system operators leave their devices vulnerable to being hacked. Another more dangerous scenario is when operators continue to use devices on the network and are unaware that their data has been corrupted. This can lead operators to making operational decisions based on inaccurate data, which has the capability to wreak havoc on the network.

The third example is that all devices on the network must support a method to retrieve critical information if the network fails, which relates to the seventh foundational requirement.

- In order to do this successfully, devices must be able to verify that the data has been backed up reliably and accurately. All network devices must utilize appropriate mechanisms to ensure that once the data has been backed up, it is stored reliably and can be retrieved when it is needed. It is not only the data on the devices that is important to keep secure but also the configuration settings. As there is a very real risk that an industrial network will be attacked, it is highly advised to use devices that can back up network settings and device configurations. On IACS networks with thousands of devices, this can save system operators many hours by allowing configurations to be uploaded automatically as opposed to entered manually.

Secure Monitoring and Management

After determining that the network devices and the network topology are secure, a network management policy needs to be established to ensure that the network remains secure throughout the entire network lifecycle. In order to achieve this, system operators should have a series of guidelines to follow. This will allow them to implement procedures that follow best practices to ensure that secure monitoring and management of the network takes place as smoothly and reliably as possible.



Device List

- Root
  - 192.168.127.1–EDS-G516E
  - 192.168.127.2–EDS-G516E
  - 192.168.127.3–EDS-G516E
  - 192.168.127.4–MGate 5109
  - 192.168.127.5–NPort 6000 Series

Device Properties

Alias	192.168.127.5-–NPort 6000 Se
ModelName	NPort 6000 Series
MAC Address	0090E859AFE3
Availability	100.00%
sysDescr	NP6150
sysObjectId	1.3.6.1.4.1.8691.2.8
sysContact	admin
sysLocation	
ifNumber	2
interface.1	up / 100M /
interface.2	down / 115200 /
ipAdEntAddr.192.168.127.5	192.168.127.5

Filter: All IP Address: 192.168.127.1 Security Level: High

IP Address
192.168.127.1
192.168.127.2
192.168.127.3
192.168.127.4
192.168.127.5

Check Items	Current Setting	H	M	B
Enable Auto Logout	Enabled	✓	✓	✓
Set Login Message	Set	✓	✓	●
Disable Non-encrypted TCP/UDP Ports	Enabled	✓	✓	●
Enable Account Login Failure Lockout	Enabled	✓	✓	●
Enable Trusted Access	Enabled	✓	✓	✓
Enable Password Complexity Strength Check	Enabled	✓	✓	●
Enable Configuration File Encryption	Enabled	✓	●	●
Enable Broadcast Storm Protection	Enabled	✓	✓	●
Set SNMP Trap/Inform or Syslog Server	Set	✓	✓	✓
Change Default Password / SNMP Communit...	Changed	✓	✓	✓

🟩 High 🟦 Medium 🟧 Basic ▨ Open □ Unknown

100%

Ack	ID	Source	Source IP	Device Alias	Severity	Description	Time Issued
□	581	Trap	192.168.127.1	192.168.127.1–EDS-G5...	Warning	Authentication failure	2016-10-19 10:52:21
□	580	Trap	192.168.127.1	192.168.127.1–EDS-G5...	Information	Account authentication failed	2016-10-19 10:52:20
□	579	Trap	192.168.127.3	192.168.127.3–EDS-G5...	Warning	Authentication failure	2016-10-19 10:52:20
□	578	Trap	192.168.127.3	192.168.127.3–EDS-G5...	Information	Account authentication failed	2016-10-19 10:52:20
□	577	Trap	192.168.127.1	192.168.127.1–EDS-G5...	Warning	Authentication failure	2016-10-19 10:52:20
□	576	Trap	192.168.127.1	192.168.127.1–EDS-G5...	Information	Account authentication failed	2016-10-19 10:52:20
□	575	Trap	192.168.127.3	192.168.127.3–EDS-G5...	Warning	Authentication failure	2016-10-19 10:52:20
□	574	Trap	192.168.127.3	192.168.127.3–EDS-G5...	Information	Account authentication failed	2016-10-19 10:52:20

Topology has been saved successfully 上午 10:55:03 Managed Devices (Current / Max) : 5 / 20

Moxa's MXview network management software helps users quickly check the security level of their industrial networks and set up security-related parameters.

Maintenance of an industrial network

Throughout the automation system lifecycle, maintenance will often need to be performed by local engineers or system integrators. This maintenance will typically include changing, replacing, or updating devices located in the network. It is important to note that whenever a device has some of its setting modified, there is a possibility that it is no longer secure and is now vulnerable to cyberattacks. As networks, especially IACS networks, continuously evolve and change, there needs to be constant monitoring of the network and all the devices located on it. As there are almost always a large number of service personnel who are responsible for monitoring and maintaining different devices on the network, it is not a good idea for all of them to perform security settings based on their own knowledge or experience. For this reason, a good standard operating procedure that clearly defines how to configure device settings should be adhered to at all times. It is important to ensure that constant monitoring of the network takes place to ensure that no errors occur and that the network can be kept safe from all security threats. In addition, system operators will often ask their device suppliers how long it will take to have a firmware upgrade in the event of a vulnerability being discovered on the network. A quick response time to this type of request is very important for ensuring the security of the industrial network. Therefore, network operators should know how long they need to wait for a firmware upgrade or device replacement if a security risk occurs.

Operating an industrial network

Now that some of the best practices have been established for ensuring IACS networks remain secure, the question of how to simplify this process will be considered. On almost every IACS network, there are multiple security setting options for all of the different devices located on the network. Therefore, it is very challenging for system operators to monitor the security status of every device. In order to overcome this difficulty, one method that is frequently employed by system operators is to export all of the devices' configuration settings to a storage device. When a device needs to be replaced or reset, all the system integrator has to do is import the device's settings from the storage device directly into the network device. This avoids the aforementioned problem of engineers relying on their own experience or knowledge to configure device settings as well as saving time and avoiding human error. System operators must choose a suitable device that will securely store configuration settings and reliably upload configuration settings to devices without any errors.

It is important to remember that industrial networks are only secure when all the network devices support the necessary security features and when these features are adhered to throughout the entire network lifecycle. In addition, the system operator must be able to respond very quickly to any event that occurs on the network and ensure that any configuration changes are done securely and accurately. Being able to efficiently maintain and operate a network will greatly assist system operators to monitor and manage their network in a secure manner throughout the whole network lifecycle.

Conclusion

Ensuring that a network and the devices installed on the network are secure is not easy because the threats posed to industrial networks are constantly changing and evolving. In order to protect the network as well as possible, system operators should adopt the defense-in-depth network architecture. Aside from a good overall network design, system operators should select hardened devices that are compliant with the IEC 62443-4-2 standard. Overall, system operators should have a thorough understanding of the possible threats facing their network as well as detailed knowledge of the best practices for designing and maintaining networks. Finally, ensuring that the network is constantly monitored throughout the network lifecycle will mitigate any security risks that arise as the network evolves.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.