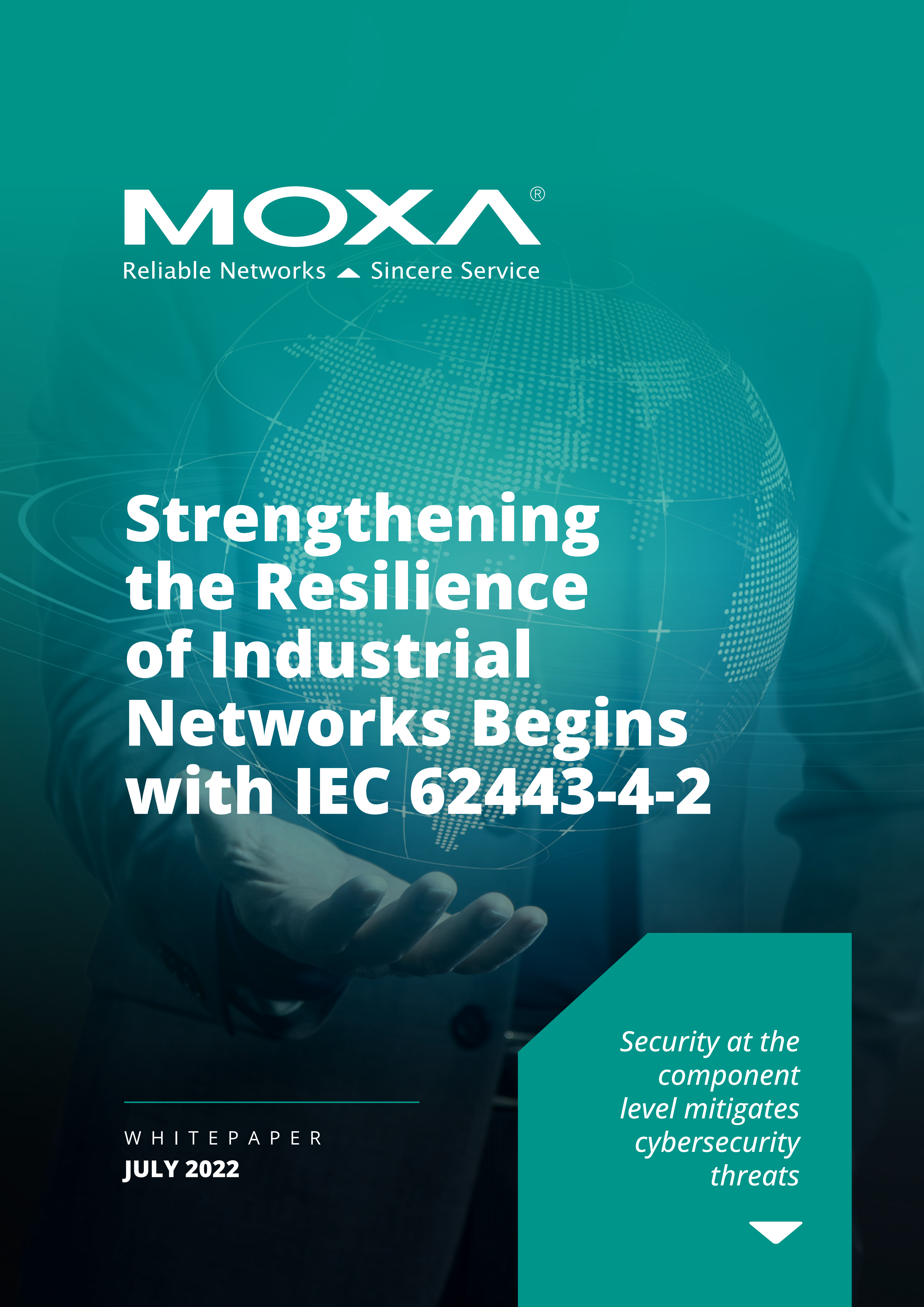


MOXA®

Reliable Networks ▲ Sincere Service

Strengthening the Resilience of Industrial Networks Begins with IEC 62443-4-2

WHITEPAPER

JULY 2022

Security at the component level mitigates cybersecurity threats

To capture, transmit, and ultimately transform data into meaningful insights, manufacturers are implementing innovative networking technologies to speed up their digitalization journey. Unfortunately, all this connected equipment poses new cybersecurity risks to industrial control systems and therefore requires security features at the component level to mitigate them.

There are many standards that outline the security framework for industrial control systems. One of the most prevalent and frequently adopted by industrial organizations is IEC 62443 developed jointly by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA). Basically, this refers to industrial control systems and the cybersecurity of BMS, SIS, PLC, SCADA, DCS and similar non-IT systems that monitor and control industrial plants (i.e., chemical processing, discrete manufacturing, oil and gas), buildings, utilities, electrical grids, and railways, marine and other transportation systems. While IEC 62443 is not mandatory, it represents best practices for automation and control system cybersecurity.

In this whitepaper, we address a subsection of that standard, IEC 62443-4-2, which issues guidelines for suppliers of industrial automation and control system supplies. We will also look at the world's first IEC 62443-4-2 certified managed Ethernet switch, the Moxa EDS-4000/G4000 Series, which was engineered from the ground up to help accelerate IT/OT convergence with an emphasis on network security.

Cybersecurity and the IIoT

Until the 1990s, manufacturing largely occupied two separate universes: Information Technology (IT) and Operation Technology (OT). The OT universe was composed of heavy machinery, electrical devices, processing systems, and other industrial equipment ranging from pumps and heat exchangers, to pressure vessels and mixers. The IT universe is more recent. Born of the information age, IT relies on servers, storage, networking and PCs running applications and processing data. Like two ships passing in the night, IT and OT occupied separate silos, shared little data or control, and relied on oversight from staff with divergent skill sets and agendas.

With the advent of the IIoT, these two worlds have converged, resulting in productivity gains on a scale never seen before. Data gathered from sensors and actuators deployed throughout a plant collect equipment and environment data, leading to better informed decision-making, improved employee safety, streamlined supply chains, cost-saving predictive maintenance, and reduced waste. Amidst all this excitement, however, a new danger has emerged posing far higher stakes: cyberattacks.

Here is the problem: With all its connectivity and devices, the IIoT makes an appealing target for cyberattacks. The expanded attack surface gives bad actors the opportunity to move laterally across a network, jumping across IT and OT systems to conduct industrial espionage, intellectual property theft, IP leakage, or even production sabotage. Any point in the infrastructure that a hacker can use to gain unauthorized access is an attack vector, including devices, software, machines, input touchpoints, displays, sensors, and even people. Humans are fallible and are often exploited by attackers through "Phishing" schemes to gain unauthorized access. The hacker only needs to identify the weakest link in the system. In contrast, the network operator must protect every link to block malicious entry.

The Cost of Cyber Attacks

Cyberattacks are very costly. According to the Global Cybersecurity Outlook 2022 report from the World Economic Forum (WEF), the cost of cyberattacks has grown to an estimated $3.6 million per incident. The study also found that it takes, on average, 280 days to identify and respond to an attack. Consulting firm Deloitte US went further to point out additional "hidden" costs that need to be calculated to determine the total price of a security breach. In its report "Beneath the surface of a cyberattack: A deeper look at business impacts," Deloitte listed seven "hidden" costs:

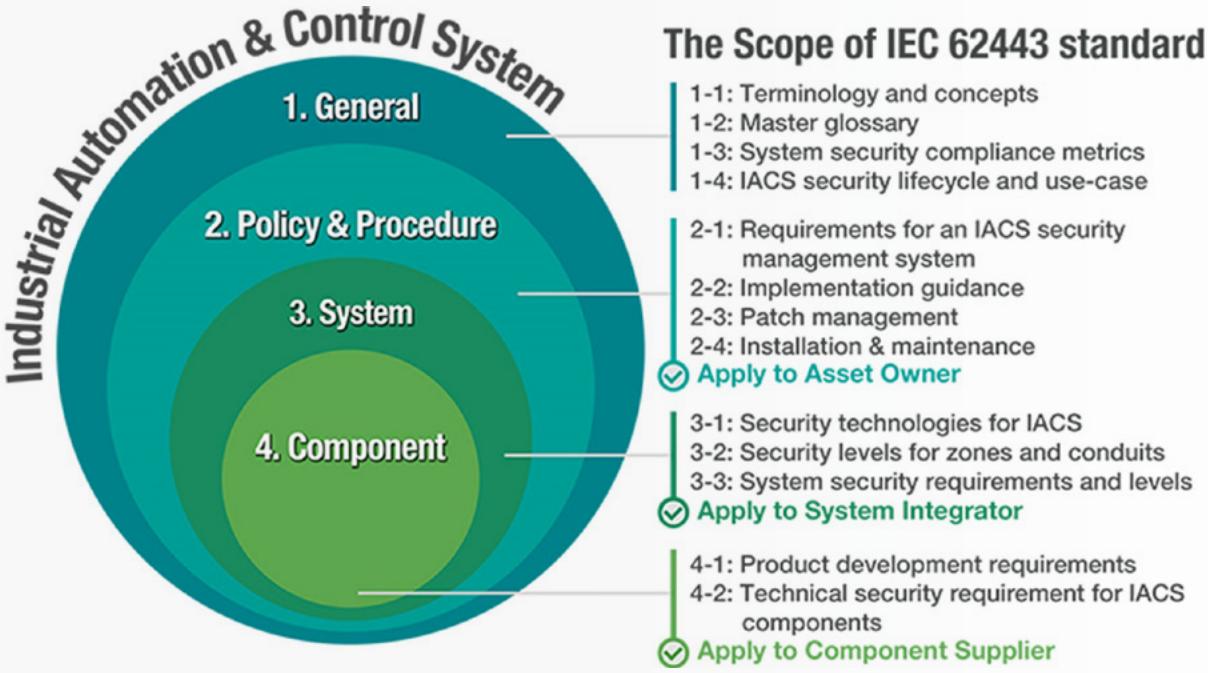
- Insurance premium increases
- Increased cost to raise debt
- Operation disruption or destruction
- Lost value of customer relationships
- Value of lost contract revenue
- Devaluation of trade name
- Loss of intellectual property.

One of the more common complaints against cybersecurity is that it is too expensive, yet that argument fails to address the other side of the equation: the cost of cyber attacks. In its report "The Hidden Costs of Cybercrime," security software maker McAfee tallied up and estimated that monetary losses from cybercrime reached nearly $1 trillion in 2020. McAfee's report also found that of the 1500 companies it surveyed, more than half said they did not have plans to both prevent and respond to a cyber attack, and that among those that did, only 32% said the plan was actually effective.

IEC 62443 Security Guidelines

To help prevent cyber attacks, IEC 62443 includes guidelines that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS) for different parts of a network.

In addition, the standard has guidelines for those who perform automation control and different responsibilities on the network. Nowadays, system integrators (SIs) often require component suppliers to comply with the subsection of the IEC 62443 standard that pertains to their devices. The figure below provides an overview that includes the scope and the roles and responsibilities for those who must ensure secure operations of a network during each stage.



The Scope of IEC 62443 standard

1-1: Terminology and concepts
1-2: Master glossary
1-3: System security compliance metrics
1-4: IACS security lifecycle and use-case

2-1: Requirements for an IACS security management system
2-2: Implementation guidance
2-3: Patch management
2-4: Installation & maintenance
✓ Apply to Asset Owner

3-1: Security technologies for IACS
3-2: Security levels for zones and conduits
3-3: System security requirements and levels
✓ Apply to System Integrator

4-1: Product development requirements
4-2: Technical security requirement for IACS components
✓ Apply to Component Supplier

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 hacking, 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.

What is a Network Component?

The part of IEC 62443 that deals with security program requirements for suppliers of industrial automation and control systems components is IEC 62443-2-4. A product is considered to be a “component” if it satisfies one or more of the definitions in IEC 62443-4-2. Those definitions are:

- **software application** one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian).
- **embedded device** special purpose device running embedded software designed to directly monitor, control or actuate an industrial process.
- **host device** general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers.
- **network device** device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process.

IEC 62443-4-2 Requirements

Now that we’ve had an introduction to IEC 62443, let’s focus on the details of the security requirements that component suppliers must meet when designing devices for deployment on automation networks, per IEC 62443-4-2. Although this subsection is meant for use by suppliers, it can be suitable for the asset owners who purchase the equipment, machinery or plants that automation systems control. IEC 62443-4-2 provides asset owners with a handy list of demands that must be satisfied by automation vendors and system integrators. That list is:

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:

- The password composition must state what type of characters are allowed, and the number of characters required before a password will be accepted as valid
- 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: This 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.

Moxa EDS-4000/G4000 Switches

Last year, with the launch of its EDS-4000/G4000 Series, Moxa became the first manufacturer to bring to market an IEC 62443-4-2 certified managed Ethernet switch.

As outlined earlier, certification to the standard required EDS-4000/G4000 switches to be engineered with hardened cybersecurity protection developed by the IEC including:

- account, identifier, and authenticator management
- password-based authentication
- public key authentication
- use control
- data integrity and confidentiality
- backup for resource availability.

Since that time Moxa has introduced 68 separate EDS-4000/G4000 switch models that meet IEC 62443-4-2 certification across seven series with options ranging from 8 to 14 ports. Secure by design, these futureproof level 2 Ethernet switches feature embedded security functions such as secure boot, device access control, user authentication and authorization, vulnerability management, and device access control.

And yet Moxa did not compromise performance for security. For example, to reduce installation and operational complexity, EDS-4000/G4000 switches can meet multiple requirements with their easy-to-use design, advanced UX, and certifications for railway, marine, power, ITS, and similar use cases in operating temperatures as wide as -40°C to 75°C. The compact dimensions are 31% thinner than the previous generation so each switch takes up less space on a DIN Rail, plus their modular power design provides the option of connecting from either the side or the top. For power- and bandwidth-hungry devices, such as PTZ cameras, EDS-4000/G4000 switches offer 90W 802.3bt PoE and support 2.5 GbE multi-gigabit fiber unlinks. Network operations are simplified further by the intuitive interface of Moxa MX-NOS and MXview software.

Although Moxa added the capabilities required in IEC 62443-4-2 to these hardened switches, the onus is on network operators to utilize these features across their network. Furthermore, network operators must ensure that everyone granted access to the network is familiar with the best procedures and guidelines outlined within the IEC 62443-4-2 subsection. Choosing not to follow the guidelines could have negative consequences, which will make the network less secure and leave it vulnerable to attack from those with malicious intent.

Why It Matters

When network components manufacturers do not diligently work to analyze device vulnerabilities, they leave their customers’s networks open to attacks. Adherence to every guideline set out under the IEC 62443-4-2 subsection — as demonstrated with Moxa EDS-4000/G4000 switches — will result in several positive outcomes that go a long way towards enhancing network security.

With more than 35 years of industry experience and a deep understanding of OT networks, Moxa is committed to helping industrial networks take the leap towards the new generation of networking. Moxa’s futureproof networking solutions are designed to help businesses seamlessly merge their IT and OT systems and prepare them for transitioning to a digitalized future.

MOXA®

Reliable Networks ▲ Sincere Service

www.moxa.com