WHITE PAPER

Protecting Industrial Control Systems with Gigabit Cybersecurity

Li Peng
Moxa Inc. Product Manager

MOXA®

Executive Summary

An Industrial Control System (ICS) needs the type of network security that takes into consideration its central role in industrial applications. Problems that arise in ICS operations can result in losses on many different levels, including costs incurred from equipment damage, and even loss of life. Although ICS networks may use some of the same technology and devices as enterprise IT systems, from a hands-on practical point of view, ICS network security differs in three aspects: protecting devices, content for filtering, and operating environment.

With ICS networks now joining the converged network revolution, video, voice, and data are being transmitted over the same network infrastructure, and as a result, it takes more bandwidth to perform non-stop data communications. For example, the HD IP cameras that are now being used with centralized management systems to monitor ICS networks create a demand for higher bandwidth over the network.

In this white paper, we first outline three key distinguishing characteristics of ICS networks, and the unique network security requirements of ICS networks compared to IT networks. Next, we summarize the best practices of ICS cybersecurity, which uses a "defense-in-depth" design recommended by the American National Standards Institute (ANSI) and the International Society of Automation (ISA). And then, we identify key hurdles that must be overcome to achieve these best practices. Finally, we present solutions that forward-thinking ICS operators have deployed to realize robust cybersecurity on their ICS networks, including an ICS cybersecurity case study from an oil & gas pipeline monitoring application.

Understanding the Unique Needs of ICS Network Security

ICS networks may have characteristics in common with IT networks and use similar equipment, but the two types of network differ in three important ways. Understanding these differences and the key characteristics of an ICS is the first step to building a robust network security solution.

Fact 1: Critical devices and SCADA systems on ICS networks require more protection than can be provided by an IT firewall.

Enterprise IT networks and ICS networks operate in very different worlds. Whereas an IT network is concerned primarily with PCs, servers, smart phones, and even printers, an ICS network's core responsibility is the very physical world of automation devices such as PLCs,

Released on August 26, 2013

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 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. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

I/O devices, analyzers, and SCADA systems. An important consideration is that the IT firewall rules that restrict access to TCP/IP and TCP/UDP ports do not apply to industrial protocols, which are not Ethernet-based. In fact, one of the main requirements of ICS network security is understanding the data type used by the industrial devices on the network, since this knowledge is needed to prevent unauthorized control packets from crippling the operation. You should also keep in mind that some industrial protocols, such as Modbus TCP, do not support security mechanisms, which makes Modbus devices susceptible to both intentional attacks and unintentional abnormal operation.

Fact 2: ICS networks place greater emphasis on system availability.

Security priorities for IT networks are expressed as CIA: *confidentiality*, *integrity*, and *availability*, with the greatest emphasis placed on "confidentiality." In contrast, security priorities for ICS networks are expressed as AIC: *availability*, *integrity*, and *confidentiality*, with the greatest emphasis placed on "availability." This is because ICS networks are used to manage and synchronize physical operations, such as production or assembly lines in a factory, and delays in transmitting data to mission-critical controllers can result in huge financial losses, or even endanger human life.

Fact 3: ICS networks face a different set of threats.

Both IT and ICS networks must defend against intentional hacker attacks as well as worms or viruses introduced unintentionally by authorized users. However, ICS networks have the added complication that in addition to managing security issues from personnel, they must also focus on the machines themselves. For example, out-of-order machines may produce unexpected broadcast storms of Ethernet packets that disrupt the operation of other machines. In addition, both industrial PCs infected with viruses as well as devices that are not working properly can easily compromise the performance of an ICS network, and in this way affect availability.

Deploying ICS Network Security: Challenges and Criteria

Deploying ICS network security involves a tradeoff between cost and risk management. For example, critical infrastructures such as national utilities naturally demand higher levels of protection, leading to higher costs. Attacks from malicious malware are easier and less costly to defeat, whereas it is more difficult to protect against human hackers. The most common counter measures for protecting ICS networks are to increase vigilance, and introduce measures that complicate the attack process so much as to dissuade hackers from even trying. These measures are at the heart of the so-called "defense-in-depth" strategy recommended by industry experts.

Defense-in-Depth Cybersecurity

Recognizing the unique security challenges facing ICS networks, the American National Standards Institute (ANSI) and the International Society of Automation (ISA) have promulgated the ANSI/ISA-99 (IEC 62443) standards, which describe best practices for ICS security. Central to the ANSI/ISA-99 standard is the "zone and conduit" security model, which is implemented with a "defense-in-depth" strategy.

In the ANSI/ISA-99 model, ICS devices are segmented into independent "zones" composed of interconnected devices that work closely together to achieve a specific function. While communications within a zone are less restricted, different zones are required to communicate with each other through a single point called a "conduit," which is usually protected by a secure router or firewall. The conduits are robustly protected to only allow the specific data that is needed to coordinate the functions of the different zones. Any communications that are irrelevant to the function of a certain zone, such as http traffic to a Modbus TCP zone, will be blocked by the secure router.

Obstacles to Deploying a Defense-in-Depth Strategy

The most critical part of an ISA-99 security model is the "conduit," which is protected by a secure router and must handle a number of responsibilities:

- **High Network Performance:** As the point of contact between two network zones, the secure routers must have the level of network performance needed to filter and deliver all of the traffic in a timely enough manner so that network availability is not affected.

- **Deep Packet Inspection:** As the security guardian between adjacent zones, the secure routers must be able to accurately inspect the content of the packets of industrial protocols for abnormalities and security threats.

- **Deployment Complexity:** The high-density deployment of secure routers needed for well-protected ICS networks requires more effort to maintain both Ethernet switches (for the network infrastructure) and secure routers (for the firewall).

Let's examine the challenges of each of these responsibilities in greater detail.

High Network Performance

Any device that connects between subnets can expect to see a lot of traffic. ANSI/ISA-99 conduit devices are effectively "backbone" devices that connect different ICS subnets. Modern ICS systems also require more and more bandwidth to support sophisticated applications that they run, such as video. In addition, some DCS networks call for gigabit-based networks for efficient communication. In order to maintain network availability, a zone conduit must provide the service required, all while acting as a firewall and filtering inappropriate data without compromising performance.

Deep Packet Inspection

A conventional network firewall is not sufficient for the specified communications requirements of an ICS because the conventional firewall is blind to the contents of industrial communications protocol packets (such as Modbus TCP). This is a particularly critical problem since industrial communications protocols generally have very poor security. Industrial devices simply respond to any packets they receive, including read queries, shutdown commands, firmware updates, and control commands. The network conduit needs to know the contents of a packet to sort safe packets, such as read queries, from potentially unsafe packets, such as shutdown or wipe commands.

Deployment Complexity

The conventional way of deploying cybersecurity on an ICS network is to add secure routers or firewall equipment that act as secure conduits, which is in addition to the existing network hardware such as layer 2 switches. Protecting one factory site requires only one or two high-performance secure routers, whereas protecting network zones could require tens of secure routers. However, cybersecurity best practice dictates that security must be implemented at the device cell level, which could involve hundreds of secure routers or firewalls to be deployed at field sites. As you can easily surmise, installing and managing such a device structure would require both a high cost and herculean effort.

Overcoming the Challenges

Moxa's new EDR series of industrial secure routers gives managers of ICS networks all the tools they need to create the type of layered security that fulfills the guidelines set forth in ANSI/ISA-99.

High Throughput*:* Moxa's EDR family of secure routers has gigabit uplinks and easily supports large amounts of network traffic. Even when inundated with traffic, the EDR secure routers easily deliver enough throughput to provide seamless video support, as is demonstrated in the performance test available here: http://youtu.be/ZI6p9BHKQjk

Deep Packet Inspection: In addition to a firewall, VPN, and NAT security functionality, the EDR-810 also supports PacketGuard for deep packet inspection of Modbus TCP packets. Modbus TCP is a commonly used industrial communications protocol, but it is not secure. With PacketGuard, the EDR-810 can scrutinize the contents of Modbus TCP packets to identify potentially damaging commands and thus protect Modbus devices from the commands, regardless of whether they are intentional or unintentional. An explanation and demo of how PacketGuard works is available here: http://youtu.be/txn54clQanY

Integrated, Cost-Effective Solution: The EDR-810 has a built-in switch and includes all the security functionality needed to establish a secure zone. The EDR-810's 10 ports can be set to WAN mode (for communications outside the zone) or LAN mode (for communications inside the zone), with the firewall sitting between the WAN and LAN in the same box. This innovative integrated solution, which combines a secure router with switch functions in the same product, not only provides connectivity for devices but also protects them directly against external networks. More information about the EDR-810 is available here: http://www.moxa.com/Event/Net/2013/Gigabit_Cyber_Security/Products.htm

Typical Industrial Cybersecurity Applications: Secure Remote Access and Critical Device Protection

In the past, ICSs were isolated systems, and hence only minimal security measures were required. Today, however, ICSs often exist as extensions of corporate networks, making cybersecurity an absolute necessity to protect against malicious and skilled hackers operating over the Internet. Two specific applications are typically used to protect ICSs against Internet disturbances or disruptions from the internal corporate network.

Secure remote access for maintenance and monitoring

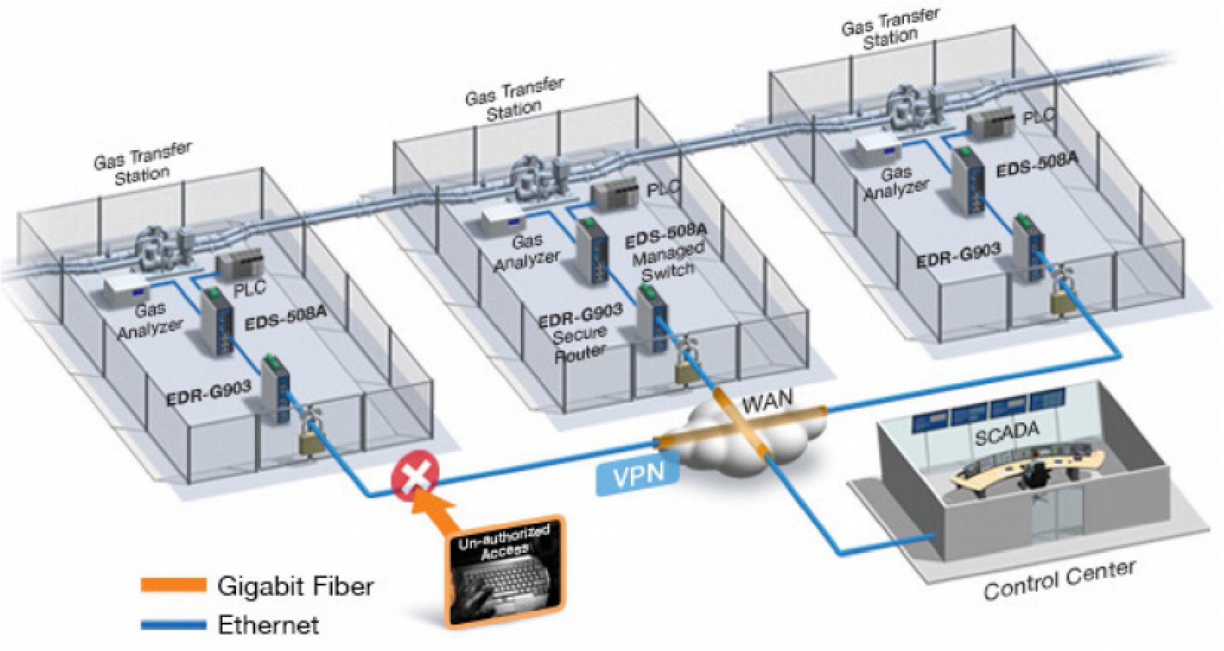
Many distributed industrial applications, including pipeline monitoring for oil & gas and water/wastewater processing, DCSs (distributed control systems) for power substations, traffic control for ITS applications, and factory automation, use the existing public network to provide remote access to controllers for monitoring and maintenance. The best and most common method of ensuring that control system devices are secure is to set up a VPN (virtual private network), which is an encrypted data tunnel that allows authorized personnel and remote connections to access the devices. NAT is another technology used to prevent exposure of devices' IP addresses to public networks.

Protecting critical devices provides greater availability

Since critical devices must be secure and able to withstand and rapidly recover from all hazards, a proactive and coordinated effort is needed to strengthen and maintain a secure, functioning, and resilient critical infrastructure—including assets, networks, and systems. A "firewall" is a common technology for protecting critical devices from any unauthorized connections or unexpected data commands. The best practice for ensuring the most availability is using the "while list" configuration of a firewall. This makes sure that only authorized connections or data are transmitted through the firewall.

Case Study: Secure Remote Pipeline Monitoring for Gas Transfer

Large gas pipelines use ICSs to remotely monitor and maintain pipeline assets and gas transfer stations. In the gas pipeline system illustrated below, each gas transfer station is a secure zone, the control center itself is also a secure zone, and secure conduits monitor the communications between each zone.



In addition to adhering to the ANSI/ISA-99 guidelines for strong packet authentication, encryption, and integrity protection, ICS security devices must also meet the following application-specific requirements:

- Be able to operate in outdoor environments and temperatures ranging from -40 to 75°C
- Gigabit, high performance fiber and copper connectivity
- Dual WAN port redundancy for greater reliability over public networks

By deploying Moxa's EDR-G903, the pipeline operator was able to create truly secure zones and confidently manage the gas transfer stations from a central control center, even when using the public Internet to connect the control center to the individual gas transfer stations.

Cybersecurity that Knows what ICS Networks Need

ICS systems are now increasingly connected to each other and even to the Internet, making the need for security more urgent than ever before. Moxa has combined a background in industrial automation with strong networking expertise to create extremely rigorous network security solutions that fulfill the unique operational, performance, and environmental requirements of ICS networks. Click the following link to download resources or request information: http://www.moxa.com/Event/Net/2013/Gigabit_Cyber_Security/index.htm.

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.