WHITE PAPER

Industrial Networking Security Best Practices

Jim Toepper
Product Marketing Manager

MOXA®

Executive Summary

Protecting network-enabled industrial control systems from both external and internal threats is critical to preventing costly intellectual property theft and ensuring cybersecurity. In this white paper, we discuss five major categories of hacking afflicting today's industrial control systems, and identify some simple hardware devices and settings that can help protect against these threats. Although no piece of hardware can protect your systems from the most advanced hackers, using the "right" hardware in tandem with comprehensive security policies can significantly reduce your risk.

Overview

Most industrial engineers are unaware of the importance of network security in today's industrial market. With recent events bringing to light that foreign governments are funding hackers whose sole mission is to target industrial control systems, we now know that cybersecurity and network security are absolutely critical. In fact, the Department of Homeland Security says "[cybersecurity is] one of our country's most important national security priorities," and has established an entire division, called ICS-Cert (Industrial Control System-Cyber Emergency Response Team), which is dedicated to securing industrial control systems.

In this white paper, we explore the following five important topics related to cybersecurity.

- Protecting against EXTERNAL hackers who want to cause a disruption
- Protecting against EXTERNAL hackers who want to steal information
- Protecting against INTERNAL employees who accidentally cause a disruption
- Protecting against INTERNAL hackers who want to cause a disruption
- Protecting against INTERNAL employees who want to steal information

Most people think that the majority of hackers are out to disrupt or cause general mayhem on various systems, such as the traffic sign hacking and similar incidents that can be seen on YouTube clips. Although such incidents are a cause for concern, there is something much more valuable worth protecting on your industrial network—your IP. This is where "IP" does not refer to IP address, but instead stands for your company's **Intellectual Property**. With

Released on August 20, 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 or Allied Automation

Tel:	1-714-528-6777	317-253-5900
Fax:	1-714-528-6778	317-253-5901

MOXA®
Reliable Networks ▲ Sincere Service

millions of dollars at stake, it is no wonder cybersecurity has recently become a major concern within our own government. In fact, recent events have caused such a concern that President Obama has signed an executive order that requires federal agencies to share information about cyber threats with private companies. This is thought to be a first step in REQUIRING private companies to comply with future cybersecurity laws where critical infrastructure is involved.

Protecting against EXTERNAL hackers who want to cause a disruption

Many Hollywood movies have depicted hackers as young kids snooping around in computer systems for fun or even out of curiosity. In these depictions the young hackers are never the "bad guys," but instead are portrayed as "curious youths" just poking around and causing insignificant disruptions. While this kind of behavior does occur, it does not represent the most significant threat to networks today. The reality is that there are a small number of "experienced" hackers, or black hats as they are known, whose goal is to gain illegal access to computer systems and networks.

Generally, black hats are the reason we believe we need to use routers with firewalls within our industrial networks to protect ourselves. Firewalls provide the most basic protection from EXTERNAL threats, and are NOT considered optional if your company has an Internet connection. Although firewalls and routers do a great job of weeding out the hackers who are just poking around, such incidents do not represent the majority of unauthorized traffic attempting to gain access to your systems, and while the majority of all threats may be protected against by simple routers and firewalls, the most significant threats are those with malicious intent. That is, those who attempt to gain access for the specific purpose of causing harm to computers and network systems. We should also keep in mind that although no piece of hardware can protect your systems against the most advanced hackers, using the "right" hardware, together with comprehensive security policies, can significantly reduce your risk.

Consider a simple analogy: Leaving your car unlocked on the street with the windows down is tantamount to inviting thieves to steal the contents of, if not the entire car. Believe it or not, there are thousands of corporate systems out there that fall into this category. Locking your car doors provides at least some security, and would be equivalent to a company implementing a firewall. Locking your doors, rolling up your windows, and installing a car alarm, which makes it much less likely that the vehicle or its contents will be stolen, is equivalent to a company using the right hardware at every level and the right security policy. Unfortunately, fewer industrial control systems fall into the high security category than the low security category. In fact, while doing research for this white paper, I discovered thousands of Internet connected industrial devices that were not protected by any significant amount of security. This figure is from the U.S. alone. Open this search up to the rest of the world and it becomes apparent that there is a serious lack of security in the industrial market.

In general, treating network security the same way we treat automobile or home security would be putting network security in the appropriate context. It is difficult though, since network security may not seem absolutely necessary until something bad happens.

We should adopt security measures that protect the entire network, just in case a hacker actually makes it through the front lines. Critical considerations include:

- Segmentation with multiple firewalls and NAT
- Password management
- Deep packet inspection
- VPN when using remote access
- Network management software

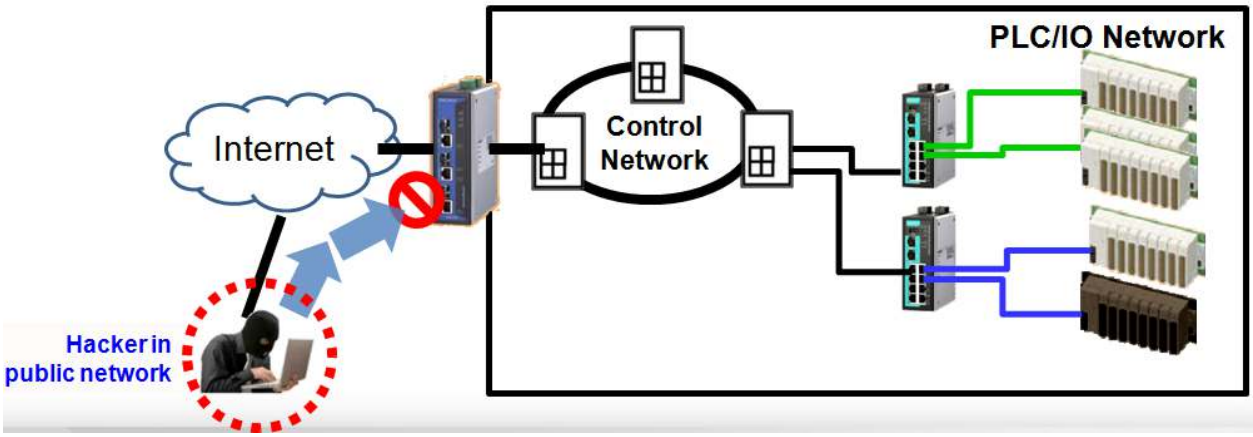

Figure 1: A firewall can provide protection against hackers on the Internet.

Protecting against EXTERNAL hackers who want to steal information

Recently, it was reported that intellectual property theft costs the United States as much as $300 billion and 1.2 million jobs annually (Commission on the Theft of American Intellectual Property). The majority of this lost revenue can be attributed to a lack of security within our networks and communications systems. In fact, a well documented report titled APT1 by Mandiant shows that a significant amount of IP was stolen from industrial control systems that were network-enabled. In many cases, cyber attacks were as simple as hacking into a network and downloading CAD files for very specialized patented designs. Once the files were stolen, the product plans could be easily copied, allowing imitation products to flood the market and destroy the advantage innovative companies reap from large investments in R&D.

In most cases of intellectual property theft, the IT network and the industrial automation network were tied together. In addition, it is equally likely that the security policies between the two groups diverged. To hedge your bets, you should at the very least use a firewall/router to separate the IT network from the automation network. No one from the office side should have access to proprietary design files, even IT administrators. For example, would you allow an industrial engineer to access employees' personally identifiable information from the human resources department? Although the IT networks for both sets of information are valuable, they need not—and should not—be conjoined.

Your second layer of defense is to make sure any WAN connection also has a firewall separating the WAN from the LAN side. Additionally, remote access should only be allowed by, at the very least, a 128-bit encrypted VPN to protect your data and manage access to your industrial control network. Besides incorporating encryption and authentication, VPN access should also be subject to strong user passwords to prevent unauthorized access to your network. Such passwords can be derived using a password generator that helps create

passwords that conform to best standards. This is the primary means of setting passwords, and is recommended by the NIST (National Institute of Standards and Technologies).

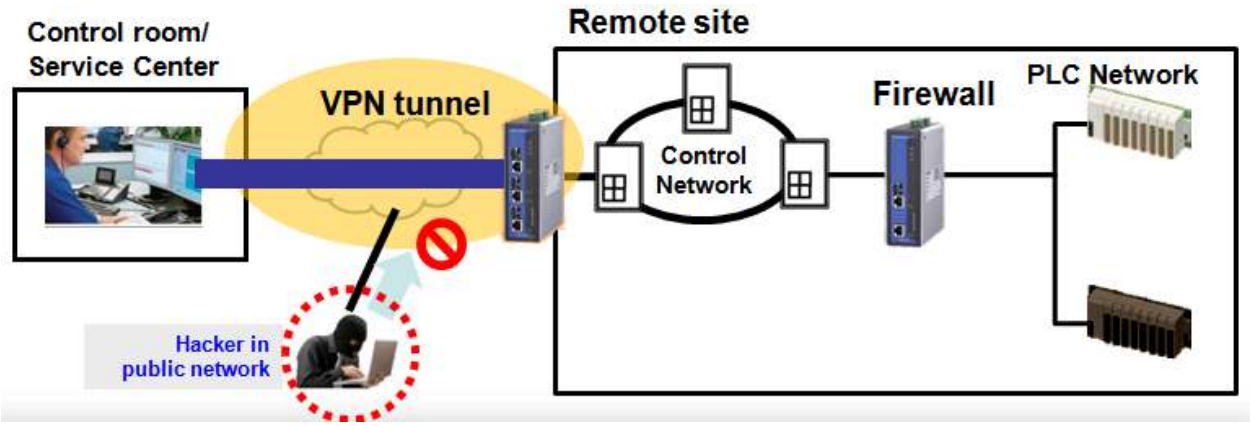

Figure 2: A Firewall with VPN capability provides protection against unauthorized entry into your network.

Protecting against INTERNAL employees who accidentally cause a disruption

Once you have shored up your defenses to the outside world, you will want to address users within your own company. Unintentional hacking is probably the most common cause of network disruption and is often caused by devices that are not configured properly. Most employees are not extremely tech savvy and the last thing they want to do is harm anyone or any system within their own company. Despite the absence of malicious intent, it is still best practice to use simple subnet segmentation. In other words, each cell should have its own small, protected network. More specifically, this network should prevent accidental entries by requiring purposeful intent to access. Furthermore, segmentation protects against broadcast storms or broadcast data produced by a misconfiguration outside of that cell. Segmentation can be achieved with a simple router in each cell.

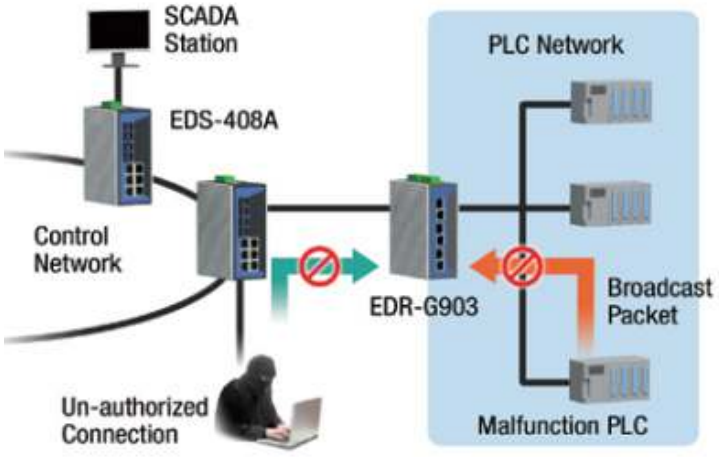

Figure 3: An example of one cell in a segmented network. The blue rectangle represents a segmented network subnet.

Protecting against INTERNAL hackers who want to cause a disruption

Although the vast majority of employees do not wish their employer any harm, there are always exceptions. For example, disgruntled contractors or recently laid off employees may hold a grudge. To prevent any critical device interruption, it is good practice to place industrial firewalls in front of your most important equipment. An example might be to place a firewall between the rest of the network and a manufacturing cell, or a group of critical control PLCs as shown below in Figure 4. By placing a firewall at this section of your network, you can ensure that only industrial control messages get through. For example, you can configure the firewall to only allow EtherNet/IP communication, and only from specified senders. Although this would normally be accomplished by simply segmenting the network with subnets, this method alone is not nearly as effective as incorporating both segmentation AND firewall protection.

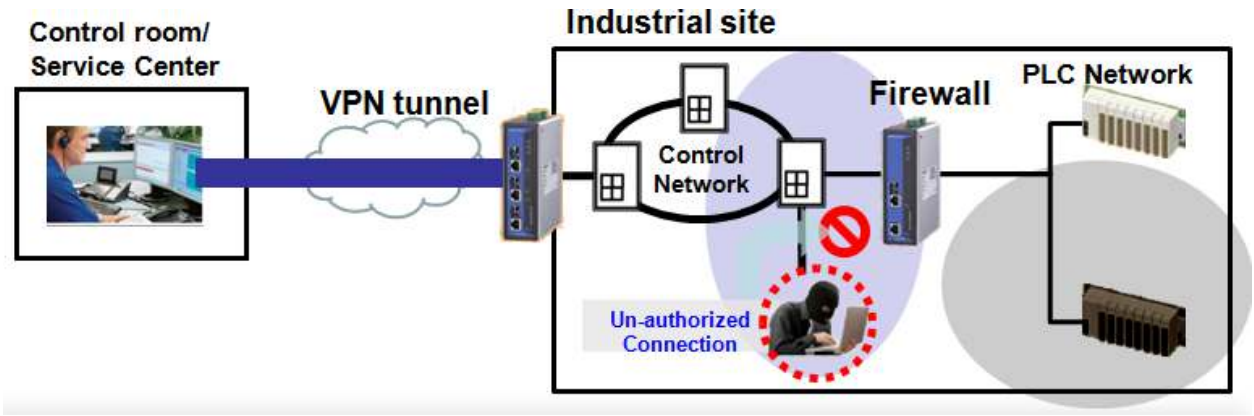

Figure 4: Protect your critical devices from internal threats by using firewalls.

Protecting against INTERNAL employees who want to steal information

In addition, disgruntled employees may want to take some parting gifts as they leave a company for a competitor. In this case, the stealing of IP may result in the loss of significant amounts of revenue. Proprietary design files are very valuable and could bring a company to bankruptcy if they end up in the wrong hands. Here, a firewall in front of your critical devices that is capable of **deep packet inspection (DPI)** could really save the day. DPI basically looks at the actual data itself (which could be specific commands and requests) to determine whether it should be allowed to pass through the firewall.

Example: *A malicious industrial engineer is trying to steal a design file from a CNC/DNC machine. He sends a MODBUS request to download this file. If configured properly, the firewall would see that he is not just requesting machine status as usual, and would deny his request.*

Allowing basic non-harmful commands may be necessary on a day-to-day basis. But with deep packet inspection, you can protect against unauthorized engineers issuing commands they should not be using. Some industrial firewalls already have DPI capability, which can be best utilized if deployed in a manner similar to the setup in Figure 5.

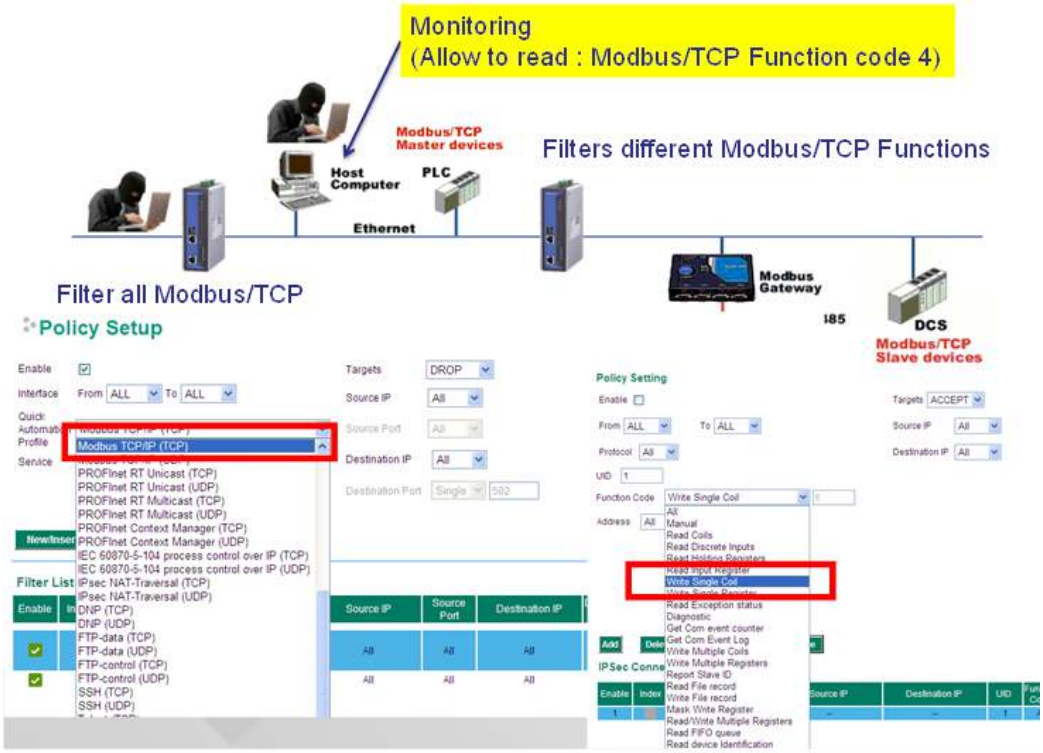

Figure 5: Deep packet inspection can help prevent unauthorized users from issuing damaging commands.

Additional Suggestions for Increasing Network Security from a General Network Sense

There are countless devices connected to industrial control networks, and these devices also play an important role in your security policy. From a best security practice standpoint, it is important that each connection follows the guidelines listed below:

Disable Telnet on any network attached device (make sure you have another way into the device first). Use SSH instead if available.

Telnet transmits characters in plain text. If someone is using a software network sniffer, this can be a major security risk. SSH connections accomplish the same thing but encrypt traffic so that it is not easily readable.

Disable HTTP web access to web servers built into Ethernet attached products, and use HTTPS instead.

HTTP is the web access version of Telnet. HTTPS is the encrypted version. You should not use HTTP for the same reasons you should not use Telnet.

If you really want to ratchet down security, you can disable Telnet, SSH, HTTP, and HTTPS and rely instead on the serial console port for direct connection to a computer. But be sure to verify that all configurations required can be made through the console port before disabling the above services.

Disable ports that are not in use.

If you have ports that are not being used on an Ethernet switch, disable them so that any Ethernet devices plugged into the ports will not be able to communicate over the network.

Enable MAC address filtering on Ethernet ports.

You should enable MAC address filtering for each Ethernet switch attached to your network. This means that ONLY specific MAC addresses can connect to specific ports on the switch. Unauthorized devices plugged into the switch will not be allowed to communicate.

Enable 802.1x authentication.

Before being allowed to communicate past an Ethernet switch, a credential check must be done with an authentication server (RADIUS and TACACS are common types). If you are not on the list of authorized users, you will not be able to get on the network.

Change default passwords; use best security practice passwords.

NEVER leave the default user name and password on your device. Default usernames and passwords are just an Internet search away from being discovered.

Conclusion

We have looked at several categories of hacking that take place today in industrial control systems, and have identified some simple hardware devices, settings, and methodologies that can help protect against these threats. Integrating firewalls and routers at multiple points in your network can indeed help protect you against both intentional threats and unintentional threats, whether they originate from inside or outside your organization. Using strong passwords and segmentation further augments your security efforts.

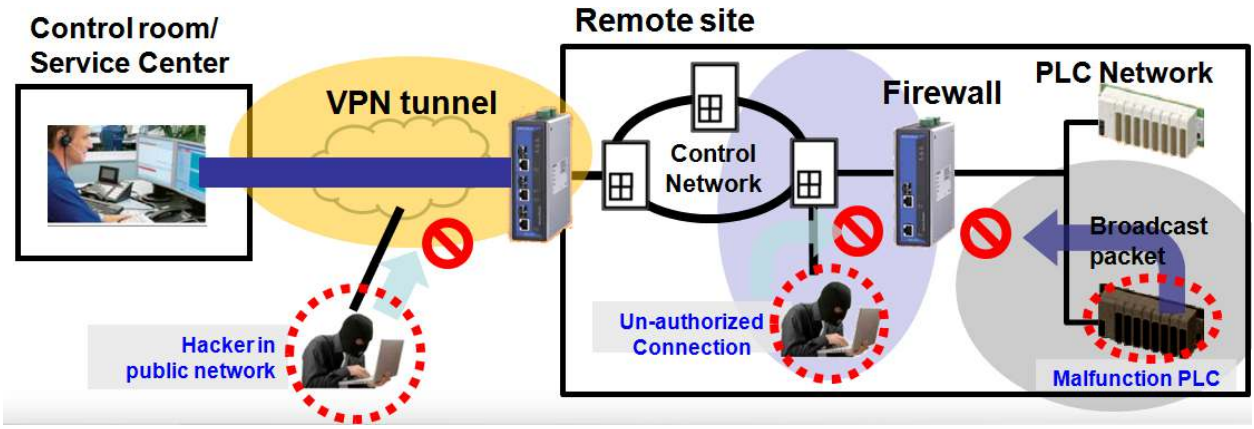

Figure 6: From a hardware perspective, multiple routers and firewalls bolster security.

While secure industrial hardware devices and basic methodologies can help, they are not the only safeguard you should take in shoring up your security. In order to truly protect against hackers and security threats, you will need to take a holistic approach.

As a whole, what can you do to help protect your industrial systems from both INTERNAL and EXTERNAL hackers?

There are many things you can do to protect against hackers. The very first initiative is to create a **comprehensive security policy**. This policy should include the following:

1) **Physical security**: Make sure only authorized users have access to sensitive systems and data.

2) **Technology usage policies**: Train your employees to steer clear of malicious web sites, disallow the use of unofficial USB drives (which was how Stuxnet spread), and do not give out administrator rights too readily.
3) **Secure password policies**: Ensure that user passwords are complex and changed on a regular basis.
4) **Internal network security**: Utilize firewalls, routers, VLANs, and network segmentation appropriately. Use firewalls in front of critical systems, not just as a filter for connections to the Internet. In addition, using deep packet inspection and network management software adds an additional layer of security.
5) **External network security**: Utilize firewalls at every WAN connection, close unauthorized and unused ports, always use a 256-bit encrypted VPN for remote access, and monitor unauthorized connection attempts.

For additional help securing your network, contact Allied Automation 317-253-5900 or call 714-528-6777 or email sales@moxa.com

References

1. **ISC-Cert:** http://ics-cert.us-cert.gov/
2. **CIO.com:** http://www.cio.com/article/728758/Obama_signs_cybersecurity_order
3. **Fortune Magazine:** *"The CEO Who Caught the Chinese Spies Red-Handed,"* by Nina Easton, July 22, 2013
4. **The IP Commission Report:** The Report of the Commission on the Theft of American Intellectual Property, May 22, 2013
5. **APT1:** Exposing One of China's Cyber Espionage Units, A Report by Mandiant, Inc.
6. www.mandiant.com
7. www.RSA.com
8. www.Shodanhq.com