Industrial Ethernet Security:
Threats & Countermeasures

Matthew Franz (mfranz@cisco.com)
Darrin Miller (darrimil@cisco.com)
Critical Infrastructure Assurance Group
Cisco Systems, Inc.

July 2003

A version of this white paper first appeared in Issue 15 of *The Industrial Ethernet Handbook*.

INTRODUCTION

The integration of IT and control system networks using Industrial Ethernet has the potential to increase efficiency and enhance productivity for manufacturing and other process control operations. However, it is important to plan for new vulnerabilities that could be introduced by integrating these formerly separate networks. For example, the lack of authentication and authorization in Industrial Ethernet protocols (i.e. Modbus/TCP, Ethernet/IP, Fieldbus/HSE, etc.) and in end devices (PLCs and remote IO) could allow attackers to steal or alter data or conduct denial of service attacks. Fortunately, proper deployment of security features in switches, routers and dedicated security devices such as firewalls, VPNs, and intrusion detection can provide or the multiple layers of defense necessary to mitigate most likely attacks.

It is too soon to tell whether Industrial Ethernet will suffer from the same sort of well-publicized vulnerabilities that have plagued other technologies during their initial deployment. Given the lack of plant floor incident data or published security advisories in network-enabled industrial products, it is difficult to judge the true extent of threats and vulnerabilities—and therefore the risk—to manufacturing networks. Recent worms targeting Windows operating systems seriously impacted large IT networks and to a lesser extent, the Internet. They also may have resulted in outages on the plant floor, but few manufacturers are willing to admit these or other security breaches. Although there are still many unknowns, using a little common sense and experience from securing other network protocols, we can make an educated guess regarding security risks of Industrial Ethernet adoption.

Apart from insider attacks, probably the greatest risk to the plant floor is likely to be attacks that migrate from corporate IT networks. Despite tantalizing accounts of Al Qaeda interest in SCADA networks and other critical infrastructure targets, there actually appears to be relatively little interest among the hacker community in developing tools and exploits for PLCs or industrial protocols such as Modbus/TCP or Ethernet/IP. Unlike IT products, tools for automatically "hacking" PLCs, remote IO devices, robots, or Ethernet-based sensors are not readily available.

The vast majority of likely adversaries (that have little to no knowledge of automation systems) are, in reality, unlikely to cause deliberate harm. The chance is far greater for an insider (or security consultant, conducting a penetration test) to gain unauthorized access or conduct a denial of service attack against a plant floor network. However, new technologies mean new ways for hackers to make a name for themselves and to learn new skills. It is only a matter of time before independent security researchers become interested in devices and protocols used in manufacturing and other automation networks. Given that the majority of control systems need to interact with higher level networks that have IP connectivity regardless of what protocols are actually used in the factory floor, it is becoming increasingly important that the manufacturing engineering community begins to put in place best practices for securing the industrial networks.

Although it is tempting to conclude that most plant networks are safely behind the corporate Internet firewall (and therefore immune to the sorts of outsider attacks that target corporate mail and web servers) it is not that simple. Insecure wireless access points, long-forgotten dial-up modems directly attached to PLCs (or PCs or perhaps even RAS servers directly connected to plant network) can provide easy access for determined outsiders. Direct Intranet connections with business partners, suppliers, system integrators, or vendors within the plant provide ample opportunities for attackers to gain access--without having to breach the Internet firewall or the firewall between the IT and plant network. And once access is gained, attackers will find a large number of familiar targets (namely Windows-based workstations and servers) that can be compromised with existing tools and techniques. Many plant PCs and applications have not been upgraded with the latest security patches, which makes these even vulnerabilities worse.

Another area of concern is the protocols used for industrial communication. Since the majority of industrial Ethernet protocols simply encapsulate existing protocols (Fieldbus H1, CIP, MODBUS, etc.) over TCP/IP, they provide even less security than many “insecure” Internet protocols such as Telnet or HTTP, which at least provide *weak* authentication. Few of the current versions of Industrial Ethernet protocols provide any means of authenticating devices or users, let alone encrypting messages in transit. Also, many devices are simply unable to implement even basic network filtering to block unauthorized access attempts--making it unnecessary for attackers to even spoof or forge messages. They can simply contact the device across the network. Although applications (HMIs or programming software) may provide password authentication or forms of role-based access control, the underlying protocols do not. Embedded web servers on Ethernet-devices seldom have authentication by default and frequently provide information to whet a would-be PLC-hacker’s appetite.

While this may paint a frightening picture, it doesn’t have to. Security is never foolproof, but the majority of these threats and vulnerabilities can be addressed with existing security tools and

techniques—much of what has successfully been used to secure E-commerce or Enterprise networks can be used to reduce vulnerabilities and mitigate the threats to the plant floor.

BUILDING YOUR SECURITY TOOLKIT

Now that you know there are security issues, what can you do about them? And what does security mean in the context of the plant floor? Security is typically defined by three attributes: confidentiality, integrity, and availability. To be secure, assets (whether information or equipment) should only be accessible by authorized users, modifications should be prevented, and they should be there when you need them. These concepts hold true for both PLCs and PCs and for both physical and cyber security. Although there are countless ways of achieving confidentiality, integrity and availability, security measures can be grouped into several categories: device hardening, access control and authentication, intrusion detection, and secure connectivity.

Device Hardening

End-devices such PLCs, remote IO, HMIs, or engineering workstations are the mostly likely targets, because they contain sensitive data or allow attacker to gain control of an “interesting” process that could lead to the greatest physical damage. Unfortunately, many of these devices do not yet have adequately security features and contain applications and services that may be unnecessary or impossible to disable. For example, on many PLCs it is difficult or impossible to turn off the embedded web server. Also many systems may need to run continuously, making the frequent software upgrades necessary to keep most operating systems in a secure state, difficult or impossible to achieve. Virus software may not be compatible or may reduce performance so much that it must be turned off. All of these factors make it difficult to harden the end devices. For now, the best way to overcome this limitation is to provide security within the network.

Access Controls and Authentication

Network-based access controls are the most common form of security that is currently deployed and is typically implemented using firewalls. However, access control technology is not limited to just to dedicated firewalls devices. Any device that can make decision to permit or deny network traffic can be part an integrated access-control solution. Filtering decisions based on a variety of criteria: typically an IP address or TCP/UDP port number. Some managed Industrial Ethernet switches (such as the Cisco 2955) provide this sort of intelligent filtering as well as the ability to enforce policy decisions based the IP or MAC address of a laptop or PLC. Additionally, virtual LANs (VLANs) provide the ability to create multiple IP subnets within an Ethernet switch. This allows can be used to separate low priority end devices (office automation) from high priority devices. Additionally, access control technology can be utilized connect these separated VLANs. Access controls can also include some form of device or user authentication. 802.1x provides

port-based authentication so that only legitimate devices can connect to switch ports, complementing physical security measures that may be present in the plant.

Intrusion Detection and Prevention

Intrusion detection systems analyze network traffic order to determine if malicious activity is present, whether reconnaissance, denial of service attempts or application attacks such as buffer overflows or Trojan activity. Intrusion prevention takes this idea one step further and not only detects the vulnerabilities, but prevents the application traffic from either accessing the vulnerable host or stops the effects of the exploits when it reaches the vulnerable host. Both intrusion detection and intrusion prevention can be deployed in the network or on clients and servers. Both have their advantages and disadvantages in a manufacturing environment. For instance, network based IDS cannot see encrypted traffic that transverses the network and currently does not yet understand automation protocols. Host implementations must go through the same rigorous system compatibility and performance testing as security patches. However, it should be noted that host intrusion prevention systems can potentially mitigate the risk when a security patch can't be implemented due to system incompatibility.

Secure Connectivity and Management

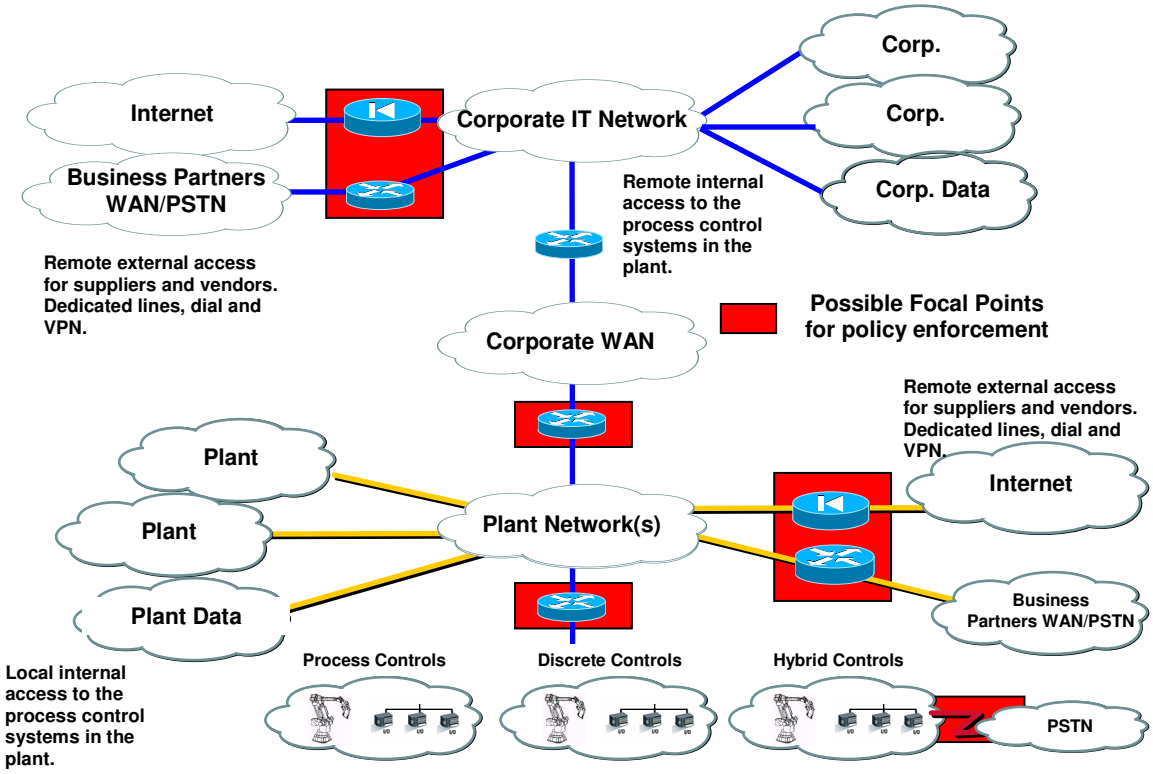
Several approaches are available for authenticating and encrypting TCP/IP traffic, which normally provides no confidentiality, integrity or authenticity. Secure sockets layer (SSL) is most commonly implemented in HTTPS protects only application layer data, while IPSEC encrypts and authenticates the entire packet, effectively defeating common attacks such as sniffing and spoofing. Since many automation devices do not yet support secure management protocols, VPN client software in conjunction with Remote Access VPNs can be used to encrypt device monitoring and programming sessions and also support strong authentication. Secure shell (SSH) is always preferable to telnet for remote terminal logins on network devices. The same is true for SNMP: with SNMPv3 providing encryption and authentication of management commands and data.

PUTTING IT ALL TOGETHER

Although this article focuses primarily on security technology, security cannot be bought off the shelf and simply plugged in—despite the claims of many security product vendors. It must be grown within the organization and built upon a sound corporate security policy that is based on a risk analysis of an organization’s assets. Stakeholders identify critical assets, elaborating threats and vulnerabilities, and decide where countermeasures can best be deployed. This sort of careful analysis must drive secure network design and deployment of any security technology. Plant networks should be designed with security in mind from the ground up, with the

acknowledgement the fact compromises may be necessary to come up with scalable solution. Industrial Ethernet deployments may provide the opportunity to “get it right the first time” and build rings of multi-layered defenses that were not possible with serial, DeviceNet, or Fieldbus networks.

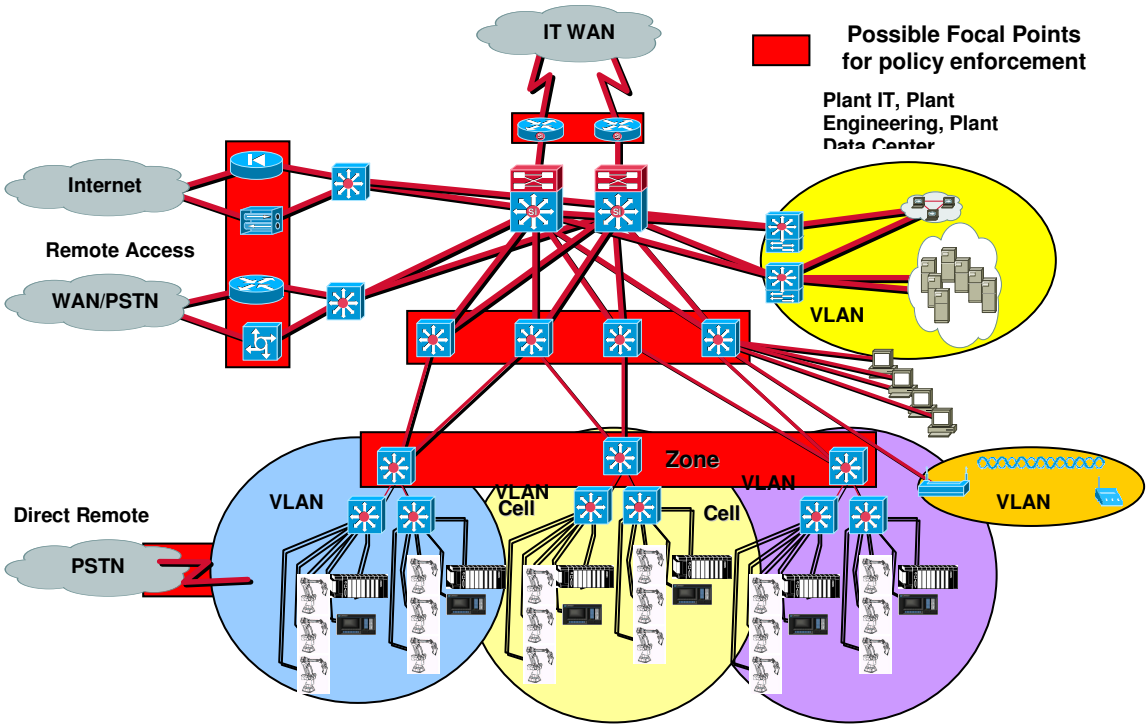
This type of approach is often referred to as defense in depth and is considered the best practice for implementing security solutions. In order to assess the threats you must understand the existing environment in as much detail as possible. This analysis assumes a security policy is in place and assets have been prioritized and likely threats have been identified.



Securing the Enterprise

Although it is out of scope of this article to discuss Enterprise security best practices and deployment guidelines, it goes without saying that if a manufacturer’s Internet connectivity has not been adequately secured, it will be difficult to secure the plant network. For the purpose of our analysis we assume that Corporate IT and Internet has been properly securely. Redundant stateful firewalls inspect inbound traffic ensuring that only allow applications are permitted. Network address translation has been deployed to hide internal address space. Host and network

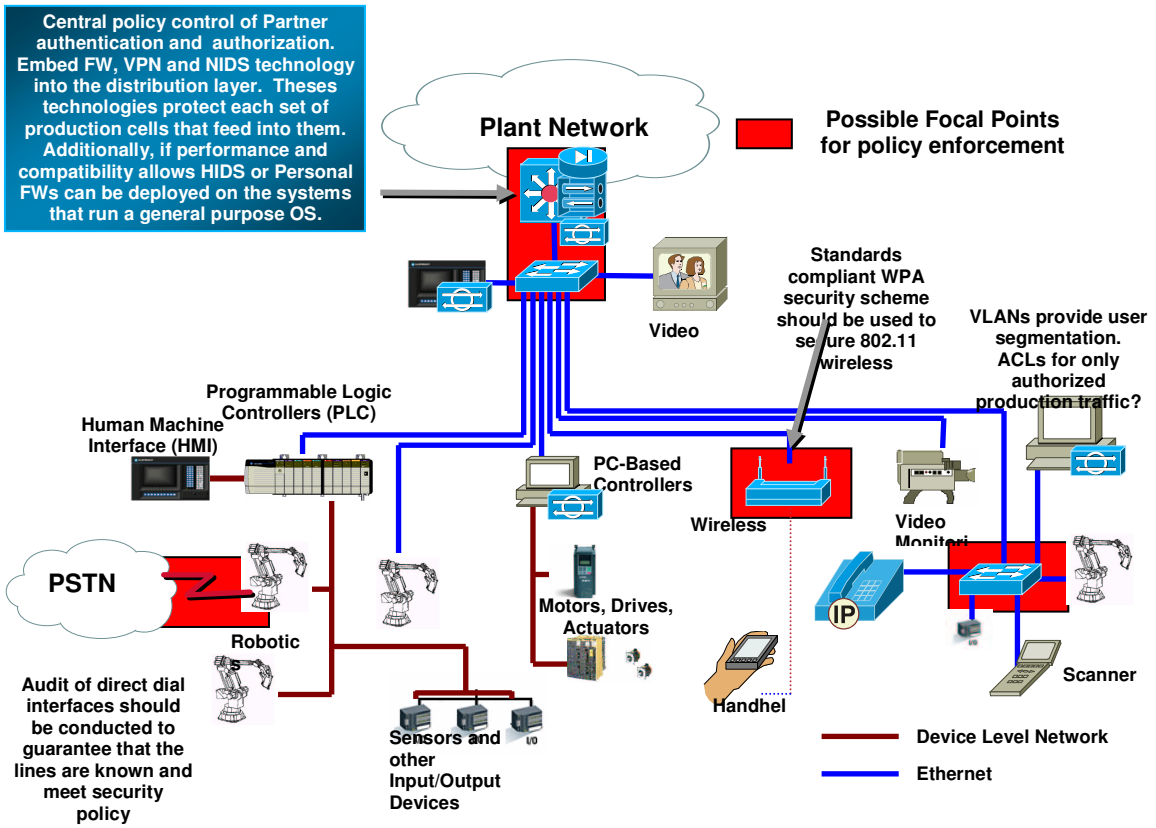
based IDS protects critical servers on the DMZ and within corporate data centers. Internet VPNs have been established with business partners and smaller campuses. Remote Access VPNs have largely replaced direct-dialups. Finally periodic security audits and vulnerability assessments ensure that networks and host comply the recommended security posture. Corporate IT security personnel have incident response plans in place.



Securing the Plant

Having created a first layer of defense, now we must consider how to protect the plant networks that have integrated with the corporate IT network. This layer of security focuses on authenticating and authorizing external entities before they can access the automation network. Two paths of connectivity should be considered for remote access to the automation network, external network access and internal network access. External network access is characterized as network traffic that originates outside the corporation. This can include providing network access for vendor support or information sharing. It is recommended that the external remote access be consolidated in a plant DMZ to allow the access to be centrally administered in order to facilitate consistent implementation and scalability. In the DMZ you can use the appropriate technology outlined above to provide access control and secure connectivity while a network IDS can provide monitoring of the externally originating traffic. In some instances, direct dial access to a device may be required. In this event, it is highly recommended that the device should

implement device based user authentication and also have the ability to generate logs that account for remote access. Internal network access is characterized as network traffic that originates on the corporations private network, but is not considered totally trust worthy. A firewall or router with access control lists should filter the majority of the inbound traffic to the plant according to the security policy. This access control can be implemented at the plant's WAN edge router or at an aggregation layer above the automation network as depicted in the above diagram.



Securing the Automation Cell

We now must focus on layers of defense with the automation cell. The layers of defense in this are of the network concentrate on device hardening, authorized network access, traffic separation and access control. Within the automation cell it is recommended that the each device be audited and tuned to only allow applications and services required for the automation cell to operate. Additionally, it is recommended that general purpose OS devices have host IDS/IPS and anti-virus software implemented when possible. At a consolidation point before gaining access to an automation cell you may implement access control on a Ethernet switch or a router. Additionally, you can require that a user authenticate via a RAS VPN device before access the

automation cell. A network IDS device can also be deployed at this point to monitor traffic that enters and leaves the automation cell. Access control within the automation network can be supplied by Ethernet switches that have the capability to define ACLs on MAC address, IP addresses, and IP port numbers. If a WLAN is required in the automation cell, it is highly recommended that it be deployed with equipment that can provide network authentication, network integrity checks, and network confidentiality. For example, 802.11 devices that meet the Wireless Protected Access (WPA) testing standard from the WiFi Alliance will provide all of the above security protections.

CONCLUSION

In conclusion, proper deployment of security features in switches, routers and dedicated security devices such as firewalls, VPNs, and host/network based intrusion detection deliver today the level or protection required and provide multiple layers of defense against possible attackers. Factory floor and IT management must work together to establish company-wide security procedures and set "best practices" for securing industrial Ethernet networks.

REFERENCES

Modbus/TCP – The Modbus Organization (http://www.modbus.org)
Ethernet/IP – The Open DeviceNet Vendor Association (http://www.odva.org)
Fieldbus/HSE – The Fieldbus Foundation (http://www.fieldbus.org)