

# CYBER SECURITY FOR INDUSTRIAL APPLICATIONS

A White Paper from



**GarrettCom**<sup>®</sup>

*Industrial Networking at Its Best*<sup>SM</sup>

**October 2010**

[www.GarrettCom.com](http://www.GarrettCom.com)

# CYBER SECURITY FOR INDUSTRIAL APPLICATIONS

By Howard Linton - Director of Technical Services

With the recent proliferation of cyber attacks, it has become increasingly clear that no business or industry is safe from attack. It is well documented that cyber security threats continue to rise. While these threats once seemed to be mostly limited to attempts to access financial data, recent data indicates that cyber attacks now cut across all business sectors. Security vendor Symantec recently revealed that 75% of enterprises on a global basis witnessed some form of cyber attack during 2009.

As the threat becomes more apparent for industrial applications, what can factory operations and IT management do to prepare for and fend off attacks resulting from unauthorized network access, cyber theft, and cyber attacks where malicious invaders destroy or corrupt important monitoring and/or control data? It also pays to look at the ways that cyber security and physical security can merge into an integrated security solution targeted using IP. An integrated solution strategy can make sure that only authorized employees have access to sensitive equipment and information, as well as monitor the actions of employees who may be security threats either through intention or human error.

In their excellent article posted December 1, 2009, in Control Engineering, [bloggers Matt Luallen and Steve Hamburg](#) state, “While many industrial control systems are becoming commercially available with various integrated cyber security controls, the reality is these systems are still susceptible to many types of threats. Consequently, they should not be deployed in isolation, at least from a cyber security perspective. The question that system owners and implementers raise is, ‘How do we maximize the assurance that our industrial control systems will be sufficiently resilient against cyber attacks once deployed?’ The answer is defense-in-depth.”

Defense in Depth offers a powerful approach to industrial cyber and physical security – and its basic tenets go back at least as far in history as the famous Sun Tzu’s “Art of War”: use a layered defense that provides multiple and varied defense strategies against any attack vector rather than relying on a single line of defense.

## Network Security using Defense in Depth

Defense in Depth is a layered security approach that uses several forms of network security to protect against intrusion from physical and cyber-borne attacks. The layers are setup to work in parallel, one technology overlapping, in many cases, with another; together they form a significant safeguard against attack.

Traditional examples of layering technologies include

- Firewalls and DMZs (Demilitarized Zones)
- VPNs (Virtual Private Networks)
- VLANs (Virtual Local Area Network)

- Secure Access Manager and Authentication Systems
- Centralized Logging and Auditing
- Video Surveillance Technologies and Physical Access Control

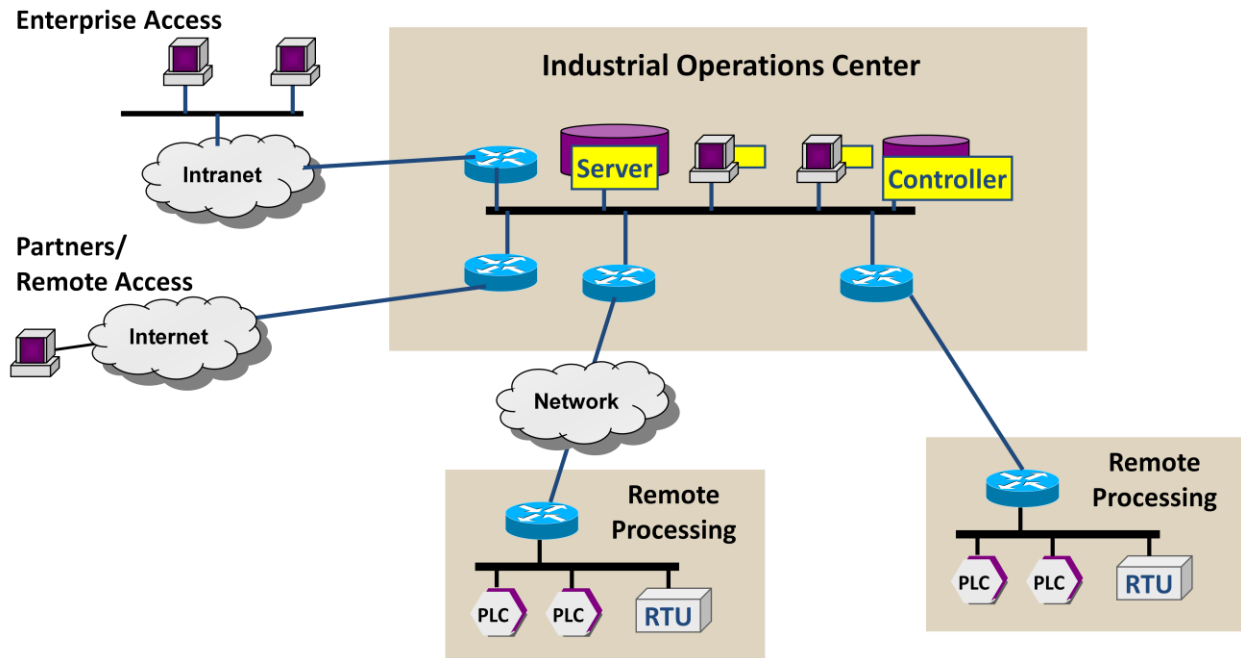
Additional information on Defense in Depth may be found in two publications from the National Institute of Standards and Technology: “Recommended Security Controls for Federal Information Systems—Special Publication 800-53” and “Guide to Industrial Control Systems Security—Special Publication 800-82”.

### General Industrial Network Topology

Here is a simplified look at a general-purpose industrial network, where the key network components include

- Main industrial campus and/or facility control center
- One or more remote locations
- Enterprise access portal
- Partners and remote access portal
- Multiple public and private transit networks (intranet, internet, etc.)

With multiple access points and multiple network hops (private and public), the following diagram illustrates a network that is wide open to abuse from cyber or physical attacks. This paper features a number of simple steps that can be taken to better secure this type of network using a Defense in Depth approach.



## **Firewall/NAT**

Firewall functionality is usually an option available on routers that are installed in the network. A firewall is typically located at the entry points to the core network and to all remote facilities, where it acts like a gate to protect and ensure that nothing private goes out and nothing malicious comes in. A firewall's value is its ability to regulate the flow of traffic between computer networks of different trust levels, thus it inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Typical examples are the Internet, which is a zone with no trust, and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized Zone (DMZ). Modern firewalls target packet information for Layers 3 and 4 (transport and link layer) and are often called 'Stateful' firewalls: they provide an additional level of security by examining the state of the connection as well as the packet itself.

A firewall can be an excellent choice as the only cyber perimeter protection for a site or as a player in a more complex network environment.

In addition to the basic firewall functions, a second layer of abstraction involves hiding inside IP addresses from the outside world by invoking a network address translation (NAT) functionality. In this case, the hosts protected behind a firewall commonly have addresses in the "private address range". Originally, the NAT function was developed to address the limited number of IPv4 routable addresses, however its facility for hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

## **VPNs**

Once the firewall has filtered out unwanted or unauthorized traffic, the next step is to make sure that the connections going outside of the firewall are protected. Secure access should be used whenever control messaging, protection messaging, configuration sessions, SCADA traffic, or other secure data will traverse networks where security could be compromised. Interception, or worse, unauthorized introduction of mischief into such traffic, could severely impact critical infrastructure operation with potentially disastrous results. For many applications, ensuring authenticity and security of networked connections is critical.

Of the various technologies used for secure access, VPNs include the most widely used and most broadly applicable set of standard protocols for creating secure connections across networks that can conceivably be compromised. Secure VPN protocols include L2TP, IPsec, SSL/TLS VPN (with SSL/TLS) or PPTP (with MPPE).

A virtual private network, or VPN, is a network that is layered onto a more general network using specific protocols or methods to ensure "private" transmission of data. VPN sessions can be established using various techniques and then tunneled across the transport network in an encapsulated, typically encrypted and secure, format, making it "invisible" for all practical purposes. The level of security obtained in a VPN network depends on the protocols used, the methods of

authentication used in establishing the connection, and the presence and strength of any encryption algorithm used.

The term VPN can be used to describe many different network configurations and protocols. Non-secure VPNs can be used to transport, prioritize and allocate bandwidth for various customers over a multi-purpose transport network. Secure VPNs, however, use transport and session negotiation protocols, as well as authentication and cryptography, to create secure connections over “exposed” (public, semi-public or otherwise accessible) communications paths.

The most common use for secure VPNs is to establish remote access sessions between a VPN device, or endpoint, on one end of the “exposed” network, and another VPN device on the other end (for example across the internet). VPN sessions can be established as end-point to end-point sessions to create a secure path between two devices or applications or to establish a secure tunnel between two locations that can be used by many devices or end points. These alternatives are configurable in rich VPN solution implementations.

### **Virtual LANs**

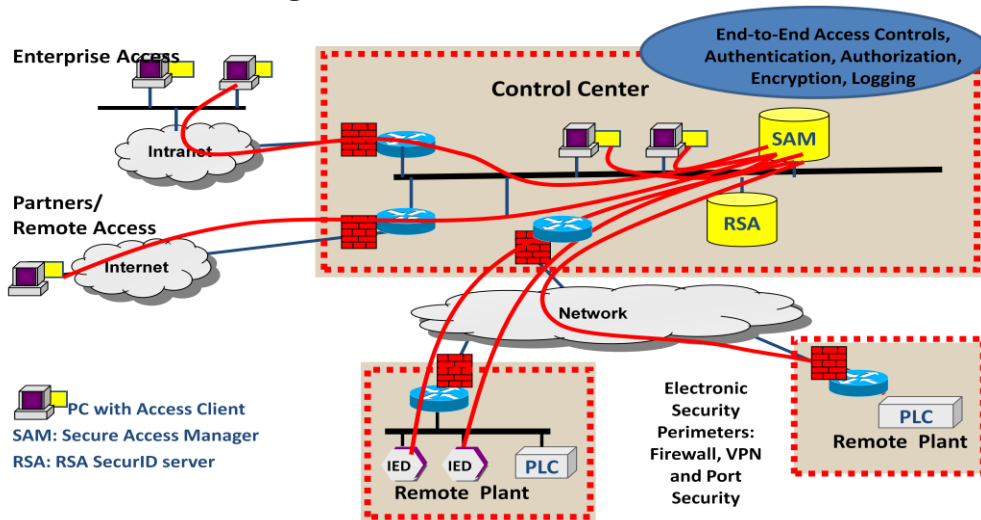
Virtual LANs or VLANs can add another layer of defense. VLANs make it possible to segregate the different traffic flows (such as VoIP, video, management, and control applications) into separate broadcast/multicast domains. Not only does this segregation keep the applications more secure by limiting where the applications reside, but it can also provide damage control. If one of the applications is compromised, the VLANs will keep the other applications isolated and safe.

### **Secure Access Manager (SAM)**

Secure Access Management systems are another mechanism in the arsenal of protecting the network and sub-systems. SAMs enforce “Triple A” security (authentication, authorization and accounting) by ensuring that only specifically authorized people are able to electronically access the control system components or other devices that are part of the network. Further, a SAM also makes sure that any actions or changes that are made are comprehensively logged for later retrieval and analysis. An insider attack can be malicious in nature or simply a careless act carried out by an employee that is “just trying to get the job done” and, in so doing, circumvents security. The Secure Access Manager shortcuts these types of threats by enforcing security policies.

When a remote or local operator tries to connect to a system, the user is transparently connected to an Access Management System (AMS) server. An AMS server obtains credentials from the end user and then can interrogate other security systems such as Microsoft’s Active Directory or two-factor authentication systems, such as RSA SecurID servers, as well as gather information from its own profile data base. It can authenticate (or disallow access to) the user, as well as determine whether or not to authorize target devices the user was trying to access. Once authorization is successful, the user is connected through the various secure active firewalls and VPN tunnels to the actual devices.

## Secure Access Manager



## Centralized Logging and Auditing

Key to all of the systems providing layered security is the ability for all network components to enter comprehensive logging and reporting information into a common repository. Recording and tracking “when, where, what” in a central system supports real-time detection and correlation of security threats. When something looks wrong, the information is immediately transmitted as an alert to IT departments and personnel so that they can shut down services and/or modify security policies. The information is also useful for detecting incident trends and other forensics. Protocols such as SNMP, SNTTP for time synchronization as well as Syslog provide simple tools to support forensic research.

## Secure Network Management

Another aspect of securing the network is to ensure that the networking components themselves are secure. Secure Network Management requires each network element to implement secure management interfaces requiring rigorous authentication/authorization, as well as both local logging and remote event notification regarding status, configuration changes and network security events. Many of the traditional access methods, such as HTTP and TELNET, have open security and passwords in plain text; they should be replaced by more secure methods, such as SSH/SSL(HTTPS) for console access, SNMPv3, secure FTP, and Syslog remote logging.

## Video Surveillance Technologies and Physical Access

Physical security normally means building “six wall” physical barriers around the facility. However, in most cases, someone has to enter the building at some time, so methods such as electronic card readers can be used to authenticate a person against data in a server running Radius or another type of authentication application. Physical access can be logged manually as well as by electronic logs. Video cameras and pixel-based systems that focus on certain parts of the video frame and send an alert if there is movement detected are powerful new security tools. Additionally, the use of PoE (Power over Ethernet), which supports both network access and power to remote monitoring devices,

makes digital video security and access control easier and less expensive to deploy than older analog-based systems.

Another component of physical security is protecting access to the networking equipment itself. A secure system can be compromised if it is possible to maliciously or inadvertently plug an unauthorized device into an Ethernet switch or router, or into a terminal server. Technologies such as VLAN, static MAC security, and 802.1x can provide Ethernet port security, while static Serial-IP and filters, serial-port SSL and serial-port VLANs can provide serial-port security. Firewall technology and/or SSL can be extended within a local site to ensure end-to-end connection security.

### **Defense in Depth in Action**

To really understand Defense in Depth, it is important to see how some companies have developed layered cyber security strategies. Companies of all sizes are evaluating options and requirements when addressing various levels of security access from field hardware (IEDs) to human machine interfaces, workstations and SCADA systems. Access to the industrial communications network, remote vendor access and support, and key databases and historical records are all areas where Defense in Depth decisions need to be made.

Each industrial facility will address its own needs in its own way, and most agree that a cyber security program is an incremental process.

Many industrial facilities are watching what is happening in the power utility industry because of stringent NERC mandates. The experience of one utility company is instructive. As a rural electric power cooperative, “Ridgmont Utility” does not yet fall under NERC mandates, but a security audit several years ago convinced them it was time to take security more seriously. Their Defense in Depth strategy followed the thinking below.

The first decision was to develop and maintain two separate networks – one corporate and one on the SCADA side. This limits the ability of incursions in either network to affect the other. The corporate network is concerned with standard business operations including contracts, accounting and filing systems. The SCADA network, on the other hand, uses secure measures to protect the control of the system – and access into the control system. In fact, the SCADA system is designed in a way that allows security personnel to isolate the SCADA network in a very short period of time without impacting its ability to run operations.

The philosophy of running separate networks for separate functions goes even deeper in the operating philosophy of the company. Firewalls are in place at every remote location and at every site where Ridgmont’s networks come into contact with the outside world. Firewall equipment in a clustered environment with hot-standby firewalls for failover protection guards gateways between networks, and is backed by redundant switching behind firewalls and redundant links. VLANs, which are run over point-to-point VPNs between firewalls, as well as different logical and physical networks for different functionalities, make it difficult for intruders to penetrate the system, even while authorized users can move easily among networks to get what they need. Even links running across leased circuits between outposts and the main office use point-to-point VPNs.

Ridgemont, which is in transition between serial and IP-based communications, use serial tunneling devices to run certain SCADA operations through the network, utilizing routers designed to support serial and IP in the same box.

Another philosophy is to block every port that is not necessary within a network. Realizing that many network switches and other IEDs come with all ports available for access and default passwords in place, the co-op shuts down all ports and removes all default passwords so that security is built from the bottom up. The operations manager would rather have access blocked by a firewall after a port had been connected to a new piece of equipment, and fix it, than take the easy approach and leave everything open and available for potential attack. To foil intruders, Ridgemont uses NAT functionality to change port numbers from their default programming to make it more difficult for unauthorized access.

Ridgemont has defined policies that determine what user will have access to which net, and which specific resources on that net. When outside access to a network is necessary, it is passed through a connection using SSL and both per-port and per-user authorization. The authentication process uses Active Directory, and is performed on the local level, not from a central location.

Everything that can be password protected is – often down to a different password for each piece of equipment. As mentioned earlier, a first order of business for Ridgemont when installing any piece of equipment is to discover and change default passwords. There is no standardization on passwords, which are randomly generated and require a minimum of eight digits, including at least one special character, number and letter per password. With thousands of pieces of equipment within the system, password management is difficult, but deemed essential. IP addresses are removed from equipment to protect the network in case of physical breach.

A Syslog server and SNMP management allow Ridgemont to track who is logging into the IP-based equipment—and when (legacy serial connectivity does not afford that luxury, and is being replaced). A next order of business is installing secure access software that will enable management to know *what* has been changed as well as *who* and *when*.

WiFi is carefully isolated on a separate network that links directly to the cable company. Access is offered as a convenience for sales people, customer representatives, repair crews and other outside visitors. Internally, employees need to access the internet through VPN appliances using SSL. Ridgemont ensures that firmware and software are kept up to date and have deployed the latest security patches.

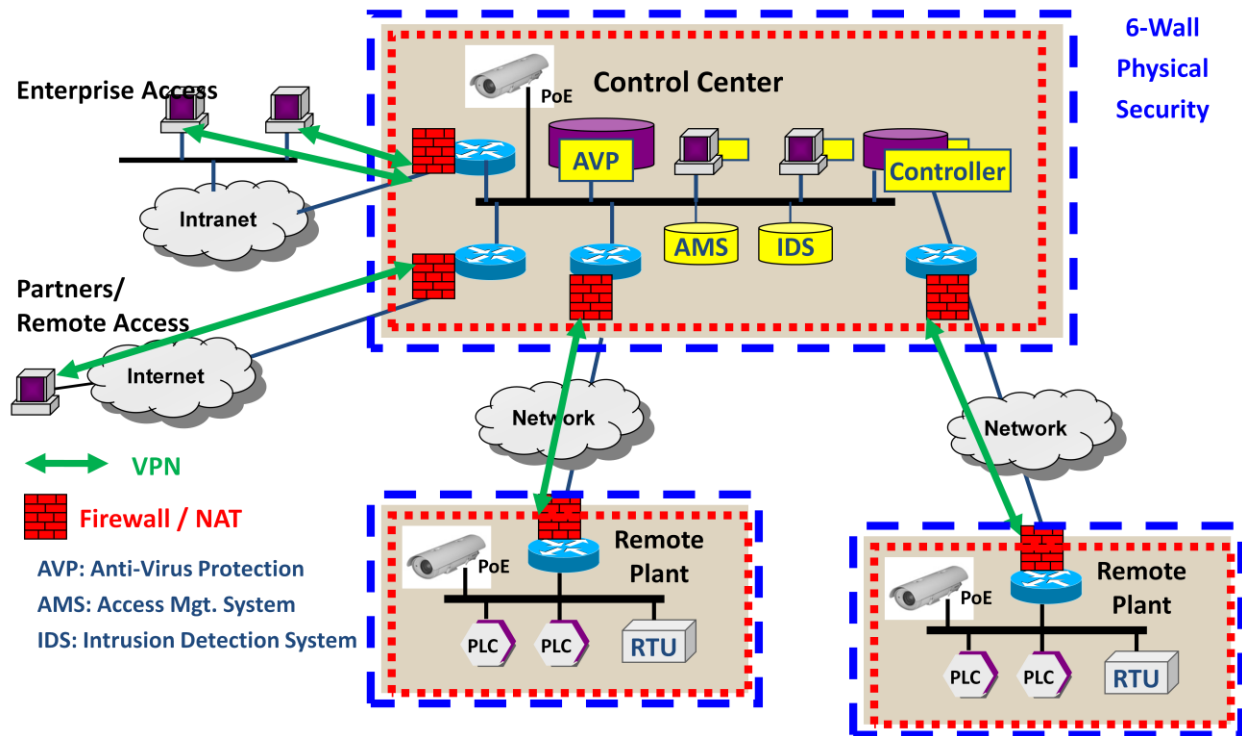
Recommended security practices generally recommend using outside security experts as well as internal teams. An affiliate utility, which is under NERC mandates, helps Ridgemont with the details of its security system. Like most fields, expertise and daily exposure provide a level of sophistication not possible when security is only “part of the job”.

Ridgemont’s operations manager notes that maintaining security can be very difficult. “You do due diligence; you do the best you can.” But, a key component to any security system is alert and educated employees.

“We talk about security at staff meetings and employee meetings. We remind people to leave their PCs at home and not plug them into the co-op network – ‘don’t bypass everything we have done!’. We have a good employee base and not a lot of turnover, and that makes our job easier,” he says.

## Conclusion

Introducing a number simple security elements into an industrial network will significantly reduce the risk of physical or cyber attacks. The resulting network topology should look very much like this:



The clock is ticking. IT groups and operations managers in industrial networking applications must come to the realization that it is a matter of when, not if, a physical or cyber attack will occur in their industry – and possibly their plant.

Fortunately there are readily available, off-the-shelf, industrial-strength networking equipment, and cost-effective tools, systems, and partners to work with to deploy Defense in Depth protection for any type of industrial network. Defense in Depth is not a one-time goal but a continual process of assessing network vulnerabilities, updating security policies and adding emerging technologies in a continues cycle in order to protect valuable cyber and physical assets.