

Providing Access to Your Manufacturing Data – Securely

By Mike Miclot, Vice President of Marketing, Industrial Solutions Division at Belden® Americas Group and Jeff Cody, Industrial Ethernet Technical Support Engineer, Hirschmann®, A Belden Brand

Table of Contents

Introduction 1

A Changing Landscape: 1
The Genesis of Industrial Ethernet

A Different Animal: 2
The Need for A Special Kind of Protection

Ways and Means: 3
Building Protection Into the Network

Beyond the Basics: 4
Putting it All Together

Go the Extra Mile: 5
Developing Defense-in-Depth Security

Introduction

The proliferation of industrial Ethernet today is putting manufacturing at risk for inadvertent and deliberate intrusions. Security measures tailored specifically for production environments are imperative for keeping operations protected...and profitable.

Security today is a necessary part of every manufacturing operation that expects to run smoothly, efficiently, safely, and profitably. But protecting the industrial environment is far from an easy job. As production equipment and the systems that connect and control it grow increasingly more complex and sophisticated, the measures needed to protect them become more critical as well.

Fueling these developments in large part is the recent evolution of Ethernet technology from the office enterprise to the industrial environment. Once thought to be insufficiently robust and lacking in functionality, industrial Ethernet (standardized Ethernet communications over a hardened networking infrastructure) has advanced remarkably, becoming, in a few short years, the communications staple of manufacturing and production, of automation and control.

Although it offers many benefits, industrial Ethernet is not without issues, especially in terms of security. It typically must carry signals between devices on a precise, exacting schedule. While standard Ethernet in the office environment may be unharmed by a signal transmission fault, it is a different story in the industrial world. Networks here must be able to withstand harsh and hazardous environments with little margin for error. Downtime caused by a security breach on the manufacturing side—whether it is from an inadvertent or unintentional error or from a deliberate cyber attack—is always expensive and can put assets at risk.

**A Changing Landscape:
The Genesis of Industrial Ethernet**

Before the advent of industrial Ethernet, industrial networks were not as susceptible to cyber security incidents as their enterprise brethren. Security flaws inherent initially in enterprise infrastructures made them prime targets of the cyber underworld. However, relying predominantly on such fieldbus network protocols as FOUNDATION Fieldbus, Modbus, or Profibus that used proprietary RS-232 or RS-485 serialized communications, industrial networks were essentially closed with minimal connection to the outside world. They were rarely affected by the network vulnerabilities and attacks that plagued enterprise environments. Isolated and independent, the industrial world rarely shared a common communications path with the enterprise environment, and even rarer was the person skilled enough to attack both realms.

When industrial companies began seeking a common networking platform that could be leveraged for office and plant floor alike, Ethernet seemed the likely prospect. In fact, it wasn't long before Ethernet became the *de facto* standard for the company striving to modernize its business by incorporating the power of computing into their business models.

In particular, two developments accelerated the growth of industrial Ethernet:

- Operating system vendors used Ethernet to create networks that united once-isolated clusters of information (standalone personal computers and servers); and
- Software vendors developed applications that allowed this information to be shared over a common network resource.

Once industrial automation developers saw how flexible and reliable Ethernet networks had become in the enterprise world, they started looking at how they might capitalize on Ethernet technologies as well. The result was an industrial automation revolution that used Ethernet networks as the core technology to drive increased productivity, reduce costs, and integrate real time data from manufacturing to the front office.

Using common protocols over standardized networking equipment brought many advantages to industrial and enterprise networks. Thanks to interconnected enterprise and industrial networks, seamless interoperability from the shop floor to the front office made multi-network connectivity, anytime, anywhere, a reality.

Corporations with multiple geographical locations could be united as if in a single building. Multi-faceted organizational and commercial entities could more easily collaborate, simplifying inter-system relationships. Yet these advantages are the very cause of the vulnerabilities and weaknesses that expose industrial networks to many of the same security woes of the enterprise network. In some cases, even more.

A Different Animal: The Need for a Special Kind of Protection

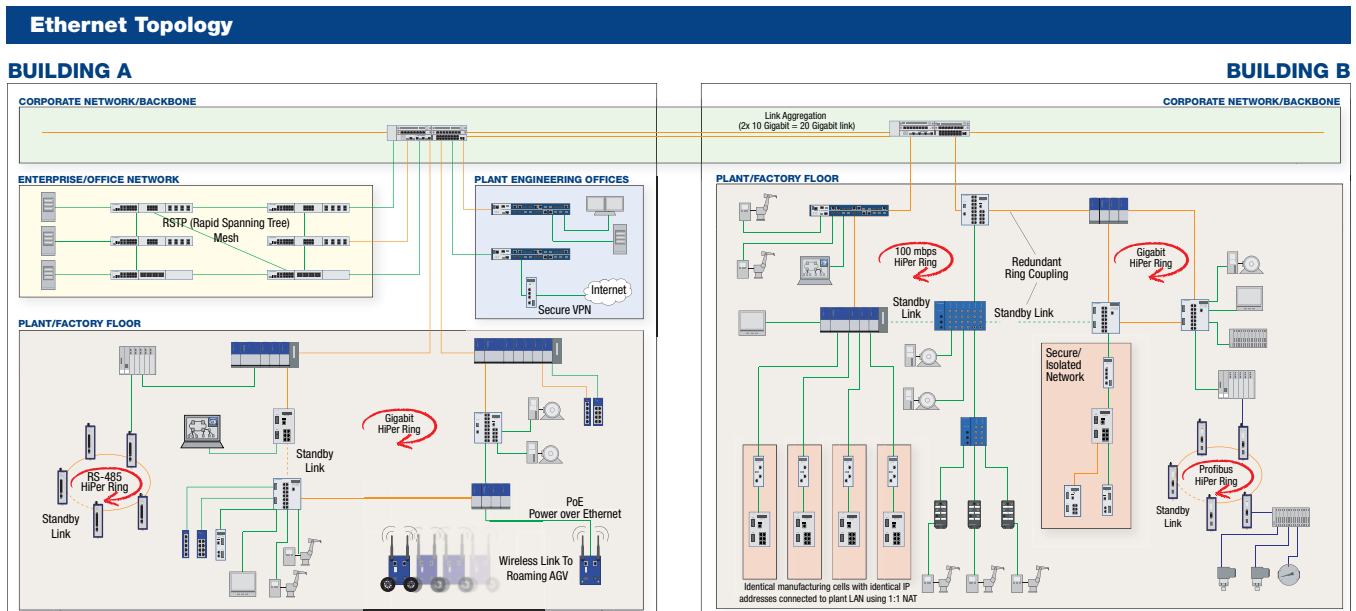
The security mechanisms and controls used to protect enterprise networks are, quite simply, insufficient or ineffective for industrial networks. Although they use the same types of networking equipment and protocols, industrial and enterprise networks have different characteristics, adhere to different performance criteria, and can be affected in dramatically different ways by the same types of events.

Enterprise networks usually can withstand periodic network outages anywhere from a few minutes to a couple of hours, depending on the type of failure. Firewalls and proxy servers protect them from external threats. Operating system patches, intrusion detection mechanisms, and anti-virus software keep them safe from internal threats. In addition, they are continuously scanned by designated security systems, operate in a relatively controlled environment, and are cared for by a dedicated, trained technical staff. Communications on enterprise networks are rarely time sensitive and the traffic often comes in bursts, as, for example, when data files or documents are transferred from one server to another. Many mechanisms used by today's popular operating systems rely heavily on broadcasts and multicasts to resolve network resources and establish communications with peer systems.

Industrial networks are a different animal. They have a more specialized nature, with environments

ranging from climate controlled clean rooms to hazardous manufacturing environments. Rarely is a dedicated staff on hand to monitor and maintain an industrial network. Its care becomes one more duty for plant, production, or control engineers who are already maintaining high production rates on lean budgets within stringent timelines.

Deterministic control networks usually operate within strict timing constraints and sustained rather than intermittent traffic. Outages are intolerable. Any disruption is too long, and can lead to waste or contamination of raw or in-process materials or goods. It might also mean an entire process needs to be restarted. Unplanned disruptions can pose risks of all kinds to manufacturing assets. The capability must be there to restore a system to operation as quickly as possible. Further, production machines rarely can be secured with a software patch, anti-virus system, or intrusion detection mechanism. Most



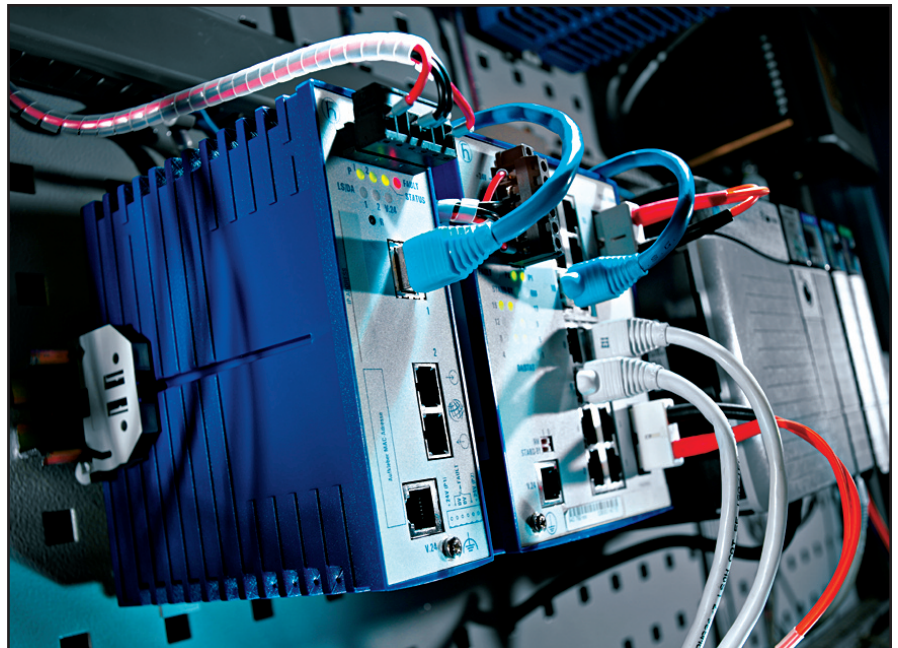
Ethernet topology showing integration of the corporate network with the manufacturing plant. Security is achieved through use of Hirschmann® Eagle Firewall/ VPN devices in three areas: at Plant Engineering (highlighted in light blue) and two areas of the plant floor in Building B (highlighted in light orange). Eagle VPN devices are ideal for remote, secure access – isolating a network by controlling what data is allowed to pass in either direction and to perform NAT (Network Address Translation).

of the time, they must be updated by the vendor, at significant cost in time and money.

Industrial networks vary widely in how they are linked to corporate networks today. Some are directly connected on the same enterprise domain. Others consist of segmented networks connected by routers or VLANs (virtual local area networks). Still others remain completely isolated while sharing common resources over the Internet. In too many instances, security measures for these networks mirror the controls and mechanisms used in the enterprise network...and subsequently fail to address the requirements of the industrial side. What is needed is a more robust method of securing the industrial network by adapting, modifying, and configuring tried-and-true security techniques developed by the enterprise for use in the industrial world. These adaptations must consider the differing security focus, performance requirements, production architectures, and risk management goals of the manufacturing processes, facilities, and networks.

Ways and Means: Building Protection into the Network

Let's look in more detail at these characteristics, at how they impact the development of a secure communications network, and at some of the measures, procedures, and devices that can be applied to provide protection. Just what are the needs of an industrial security network compared to the capabilities of an IT-system security network? The overall goal of any industrial network protection strategy should be to protect all sensitive areas of the production process while supporting the long-term integration of the office and industrial networks in the company-wide environment. Building such a system can be a delicate balancing act. On the one hand, the industrial network cannot merely copy the security measures used in the office environment. To do so will leave security gaps. On the other hand, care must be taken not to over-engineer network security. To do so might be too restrictive or make certain necessary actions prohibitive.



Hirschmann Eagle Firewall/VPN devices guarantee maximum protection of industrial cells and rule out accidental and unauthorized data manipulations.

The challenge to the manufacturer is to become familiar enough with the points of vulnerability of his operation, acquire an understanding of the security tools available, and then build a system that will provide adequate protection. A variety of security techniques and technologies exist today, and virtually thousands of products are available to help do the job. These include, but are not limited to, industrial networking firewalls and routers; security appliances; and VPN, authentication, and encryption devices discussed here. Properly applied and installed, these mechanisms and techniques can give your industrial network the security it requires for directly connecting either the network or individual production devices to the Internet, corporate or remote offices, remote production facilities, duplicate production cells, or other areas that need secure industrial Ethernet communications.

Firewalls...and Firewall/Routers. Firewalls come in many types; common among them are transparent products that operate out of the box.

Such plug-and-play devices can be installed anywhere on the network without the need to configure or re-configure end devices. No changes to the network settings (IP addresses, subnet masks, and default gateways) are required; networks do not have to be divided into separate IP subnets.

Firewall/routers usually are combination devices. They consist either of routers with some built-in firewall functionalities, or firewalls with routing functionalities built in. They excel at protecting the industrial network edge: the points of vulnerability where the industrial network meets the corporate network or Internet.

These devices can segment networks, be used as a gateway, and enable safe access to the Internet. Firewall functions include isolating critical devices from threat sources, separating the network into security zones, restricting communications between zones, and protecting controllers from known vulnerabilities.

In a typical firewall/routing operation, all IP (Internet Protocol) traffic sent from a secure network to an unsecured network or beyond is permitted to traverse the firewall/router. Traffic sent to the secured network from an unsecured network is blocked automatically. Replies from any secured traffic that establishes and maintains a TCP (Transmission Control Protocol) connection with an external host should be inspected against a *stateful inspection firewall* to ensure that the traffic is authorized and that it is not being spoofed or forged from an unknown or unauthorized external host.

The stateful inspection firewall feature is an important technology for industrial-grade firewalls/routers today as it analyzes the type of traffic going through the network. It tracks where it is coming from, where it is going, and, most importantly, examines packet characteristics. Rather than simply filtering data based on source and destination, it looks deeper into the packet. It not only tries to establish that the data are coming from an authorized source, but also that established connection rules were followed. Such capabilities help avoid "man in the middle" attacks, in which a hacker eavesdropping on the Internet hijacks a communication session between two parties and impersonates one of the parties.

Security Appliances. Security appliances are another type of in-line hardware intended to give a single device or a small group of devices real-time protection from unwanted and undesirable traffic. Among the newest types are those that offer zone level security, including deep packet inspection for groups of programmable logic controllers (PLCs), distributed control systems (DCSs), remote terminal units (RTUs), and human-machine interfaces (HMIs) and their industry specific communication protocols. These devices are usually simpler to install than many other security products, and can be installed and implemented on a live network with no special training, pre-configuration, or system downtime.

These types of products usually are offered as a distributed security solution. The central management software that accompanies the devices enables modular configuration, management, and monitoring of multiple appliances from a single management workstation. The management software allows a virtual model of an entire control network to be quickly developed; many offer drag-and-drop tools to simplify creating, editing, and testing the configuration of the appliances and devices deployed in your network. The status of an entire system is visible at a glance on a single monitor, providing real-time information about non-conforming events in your network.

VPNs, Authentication and Encryption Techniques. Secure communications can be extended beyond the network's edge, local security cell, or device level using remote user authentication or VPN (virtual private network) connections. Most firewalls can support the establishment of VPN connections using secured socket layer (SSL), pre-shared key (PSK) or X.509 certificates to provide encrypted access across intermediate or untrustworthy networks such as the Internet. Additional secured communications can be established using *user authentication* and user specific firewall rule bases. The firewall may be used on a network's edge between the office and the plant floor or duplicate production cells, or act as a gateway to the Internet.

For example, a VPN solution should create secure tunnels of communication over untrustworthy networks, including the Internet or corporate business network. It should be easy to deploy, test, and manage and should provide ways to build pre-configured installation files to help ensure that security is not compromised by configuration errors. In addition, it should support industrial automation devices and protocols, be industrially hardened, and be able to be combined with other equipment to create a comprehensive security solution.

Beyond the Basics: Putting It All Together

Choosing devices to secure the industrial communications network is only part of the challenge. Installing the right equipment properly also plays a significant role, with the volume of components and number of variables involved making for an often enormous task. And unfortunately, one size, system, or approach does not fit all, or even most. However, some general concepts and guidelines do apply.

Different products are intended for different purposes. For example, a security appliance protects at the device level and has no routing or network segmentation capability. For a small plant with no on-site IT staff that needs to link to the Internet to connect to its main corporate office, a firewall would be a better choice. The security appliance usually cannot act as a traditional firewall or router. It cannot construct separate network segments by creating an IP network segment on one interface and an IP network segment on the other. Although it will not modify or route traffic to a different network segment, it will, however, protect end-devices through comprehensive traffic monitoring and customizable granular firewall rule bases.

Because systems vary so widely, specifics are impossible to enumerate in this paper. In general, however, when putting together such a system, take time to answer such questions as:

- Does the device or system provide scalable security functionality?
- Is it easy to integrate into the existing architecture?
- Is it easy to install, operate, and maintain?
- Does it include comprehensive diagnostics, such as Web-based management and status LEDs?
- Does it support redundancy mechanisms?

When choosing protection, take time to determine whether the devices being considered were developed with your personnel in mind. Is the system designed so that your staff can use it effectively without needing to be an IT expert, or to call one at every turn? In addition, any industrial security device must be designed, approved, and hardened for harsh environments. It should include ruggedized housings, redundant internal power supplies, and a wide operating temperature range to enable installation wherever security is needed.

Most security systems accommodate a variety of network connectivity media, the most common being copper or fiber optic cabling, and wireless—or, in some cases, a combination. Although all provide optimum signal transmission performance, high-risk installations might lean toward fiber optics, which offers high bandwidth, is not susceptible to interference (EMI or RFI), and offers a more robust medium that is less prone to hackers. When fiber optic cable is chosen, however, some special installation concerns must be addressed—among them bend radius restrictions, maximum load, and certain environmental hazards, in particular moisture.

Overall, industrial Ethernet security devices should be capable of being managed individually using either your Internet browser of choice or with additional software from the device manufacturer. Multiple firewall configurations should be maintainable on the device or off-line, as required. Security equipment may be applied at the edge of the industrial network, the subsystem level, and/or the production cell or machine itself. Such umbrella protection offers simplicity and reliability, providing local security for a full range of control applications, remote operations and maintenance, and links to adjacent processes.

Go the Extra Mile: Developing Defense-in-Depth Security

Today's burgeoning technology, coupled with exploding industrial automation, is advancing the need for security. Industrial Ethernet unquestionably has brought innumerable benefits to control systems and to the plant floor. It has also opened the door to many problems. Protecting the industrial operation is not discretionary. Failure to safeguard it puts a company at risk for expensive and time-consuming downtime and damages.

No system should be installed and forgotten. Security is a dynamic process that involves, beyond the initial effort, regular maintenance and improvement; periodic evaluation and updates; and continuing education. Every facility should work with its security solution vendor to perform, at regular intervals, a security risk assessment and review the measures that have been put in place, especially in terms of process or production changes that may have been implemented. Be aware of modifications that may create new vulnerabilities, and know that products continue to evolve, offering improved performance and greater efficiency.

Further, no single source should ever be expected to provide all the answers. Take time to learn about security measures and advancements. Help is available: Ask your vendor, attend workshops and seminars, consult outside experts, and make use of online resources. Helpful U.S. government sites include the Department of Homeland Security's US-CERT (computer emergency readiness team), which makes available a variety of information online and through security publications (www.us-cert.gov). The Computer Security Division Computer Security Resource Center (csrc.nist.gov) of the U.S. National Institute of Standards and Technology

(NIST) is another good source. Helpful international organizations include the International Electrotechnical Commission, or IEC (www.iec.ch) and the International Organization for Standards, or ISO (www.iso.org). Independent organizations such as the Industrial Society of Automation, or ISA (www.isa.org), also offer materials and advice. Finally, check with your own industry associations to see what they offer. In all cases, search "security" on the home page of any of these websites to see what information might be available.

A system of well-placed security products and procedures—only a few of which have been touched upon here—is time and money well spent. Giving your manufacturing operation the defense-in-depth security it needs, tailored to its specific demands, precision levels, and rugged environments, requires careful planning, diligent installation, and continuing vigilance. A system design *must* take into account the industrial security focus, performance requirements, and risk management goals of the manufacturing process that standard IT solutions fail to provide. To do otherwise, is just risky business.