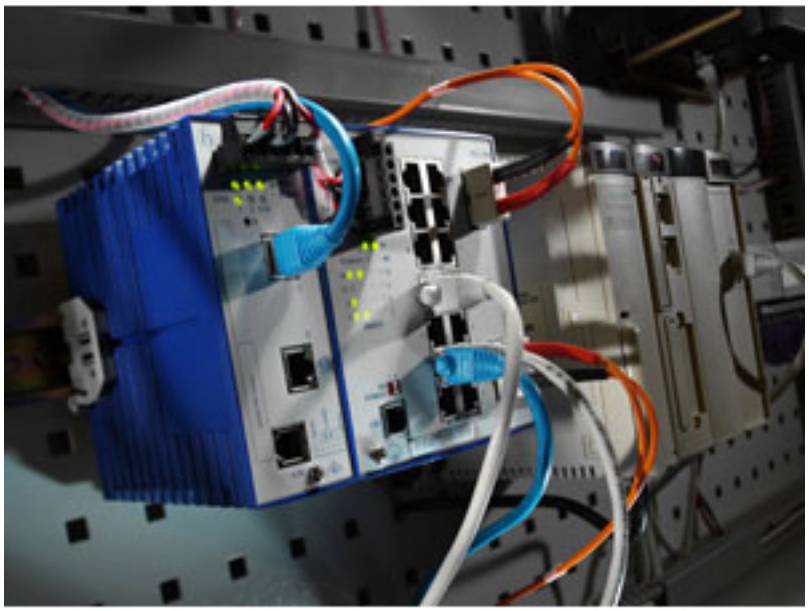
Risky Business



By MIKE MICLOT & JEFF CODY, Belden

Over the past few years, industrial Ethernet (i.e., standardized Ethernet communications over a hardened networking infrastructure) has advanced and is fast becoming the communications protocol of choice for manufacturing and production operations, automation and control. Although industrial Ethernet offers significant benefits, it is not without challenges and risks, especially in terms of security.

Security today is an essential part of every manufacturing operation. But protecting data and information flow in industrial environments can be a challenge. While standard Ethernet in an office environment may be unharmed by occasional signal transmission faults, in the industrial world, it is a different story.

The industrial Ethernet must carry signals between devices on a precise, exacting schedule and with 24/7 reliability. Plant floor networks 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 from an inadvertent or unintentional error or from a deliberate cyber attack -- is always expensive and can put assets at risk. As production equipment -- and the systems that connect and control it -- become increasingly complex and sophisticated, the measures needed to protect them become more critical as well.

Ethernet Advantages & Challenges

Using common protocols to interconnect a standards-based networking system has many advantages on both sides of the enterprise. It enables seamless interoperability between the two, and makes multi-network connectivity, anytime and anywhere, a reality. Corporations having multiple geographical locations can be united as if in a single building. Multifaceted organizations can more easily collaborate, simplifying intersystem relationships. Yet these advantages are often the very cause of the vulnerabilities and weaknesses that expose industrial networks to many of the same security woes of enterprise networks -- and, in some cases, even more.

Manufacturing Data Requires Special Protection

The security mechanisms and controls typically used to protect enterprise networks are, quite simply, insufficient or ineffective for industrial networks, even though both use the same types of networking equipment and protocols. While enterprise networks can withstand periodic network outages ranging from a few minutes to a few hours, firewalls, operating system patches, anti-virus software, and proxy servers effectively protect them from internal and external threats.

Industrial networks are inherently different. They have a more specialized nature, with environments ranging from climate controlled clean rooms to hazardous plant floor settings. In addition, the job of monitoring and maintaining the industrial network typically falls to plant, production, or control engineers who are already responsible for maintaining high-production rates on lean budgets within stringent timelines.

Furthermore, deterministic control networks usually operate within strict timing constraints, and support sustained rather than intermittent traffic. In this environment, any outage is intolerable. Any disruption is too long and can lead to waste or contamination of raw or in-process materials or goods. Unplanned disruptions can pose risks to manufacturing assets and might also require an entire batch to be scrapped or a process to be restarted. Also, production machines rarely can be secured with a software patch, anti-virus system, or intrusion detection mechanism, but rather must be updated by the vendor at significant cost in time and money.

In addition, industrial networks vary widely in how they are linked to corporate networks. This adds yet another layer of complexity. 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 specific 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.

Building Protection into the Network

The overall goal of industrial network protection should be to protect all sensitive areas of the production process, while supporting the long-term integration of the office and plant in the company-wide environment. A variety of security techniques and technologies are available in today's marketplace to help provide this protection. These include, but are not limited to, industrial networking firewalls and routers; security appliances; and VPN, authentication, and encryption devices.

When properly applied and installed, these mechanisms can provide industrial networks with the security required 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.

Here is a brief description of some of these protective devices and techniques:

Firewalls & Firewall/Routers. Firewalls come in many types, including plug-and-play devices which can be installed anywhere on the network without the need to configure or re-configure end devices. No changes to the network settings are required and networks do not have to be divided into separate IP subnets. Firewall/routers usually are combination devices, consisting either of routers with some built-in firewall functionalities, or firewalls with routing functionalities built in. These devices excel at protecting the industrial network edge: the points of vulnerability where the industrial network meets the corporate network or Internet. They 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.

Security Appliances. Security appliances are another type of in-line hardware designed to provide a device or small group of devices real-time protection from unwanted and undesirable traffic. The newest types offer zone level security, including deep packet inspection for groups PLCs, DCSs, RTUs, and HMIs -- and their industry specific communication protocols. The devices are usually simpler to install than other security products, and can be installed and implemented on a live network with no special training, pre-configuration, or system downtime.

VPNs, Authentication & 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.

Choosing devices and techniques to secure the industrial communications network, however, is only part of the challenge. Installing the equipment properly also plays a significant role, with the volume of components and number of variables involved making for a complex task, far beyond the scope of this article.

Key Evaluation Takeaways

In evaluating industrial network protection, it's important to note that one size or approach does not fit all, or even most. However, some general concepts and guidelines do apply. For example, the security components or system selected should:

Provide scalable functionality. Be easy to integrate into the existing network architecture. Be relatively easy to install, operate and maintain. Include comprehensive diagnostics, such as Web-based management and status LEDs. Support network redundancy. Consist of hardened components designed specifically to withstand the rigors of harsh industrial environments.

Finally, no network security system should be installed and forgotten. Security is an ongoing, dynamic process that demands constant vigilance, periodic evaluation and updates, and regular maintenance and improvements. Education is a smart first step, and help is available from numerous sources, including technology and communications systems vendors, to government agencies, to industry standards associations.

The important thing is to start now -- if you have not already -- to take the steps necessary to protect your Ethernet network's manufacturing data and production processes from unwanted disruptions and intrusion. To do otherwise, is just risky business.

Mike Miclot is VP of Marketing for Belden's Industrial Solutions Division, and Jeff Cody is Industrial Ethernet Technical Support Engineer for Hirschmann, a Belden Brand. For more information, please visit www.belden.com *[1].*

Links:
[1] http://www.belden.com/