

Industrial Wireless Network Security: The MDS Solution

Prepared by
Microwave Data Systems
Rochester, New York
February 14, 2003 (Revised)

industrial/wireless/performance



Introduction

As global corporations continue to grow their businesses, the ability to manage information flow from remote, geographically dispersed locations becomes increasingly important. Deregulation, mergers, competition, and increased customer demand for services, are forcing utilities to demand more from their information networks.

Merging industrial networks into corporate networks enables companies to experience new applications and services, and have access to information from anywhere at anytime. At the same time, increased use of the Internet is providing utilities with real-time access to business-critical information for competitive advantage and revenue generation.

A recent development in industrial networking is the ability to transmit serial and industrial protocols over Ethernet—in a wireless environment. Connecting disparate networks (the corporate network with the SCADA network), hardware and software platform interoperability, collision avoidance, high transmission efficiency, and the ability to add new devices to a network without disrupting traffic flow, are all benefits of this new practice. The use of IP over Ethernet also opens up new possibilities for integrating a utility-wide Intranet, the World Wide Web and/or video into a network control scheme.

While the above-noted benefits of an Ethernet-based industrial network are obvious, there are still some perceived risks associated with wireless networking. In this paper, we will look at the security issues, as well as what individual companies can do to increase network security with the help of their wireless partners.

Security in a Wireless World

While industrial networking has many advantages, security has moved to the

forefront as a critical element in data, voice, and video communications. In fact, wireless networks can actually offer security benefits that do not exist within a wired environment.

Cable-based systems that rely on telephone, fiber optics, or coaxial cable operate at a higher risk for breakage and damage from storms, motor vehicle accidents, construction work, or even sabotage. Signal quality can also suffer, especially in older wired systems that have become noisy due to poor connections. Cable troubles can be difficult to locate, and may take hours to repair depending on the priorities of maintenance crews. During a widespread event, such as a weather-related outage, repairs may have to wait for several days or even weeks while overloaded crews respond to other pressing incidents.

The availability of a wired network is also of concern, especially where the public-telephone system is involved. During periods of heavy telephone use, such as during a widespread emergency, it may not be possible to access the telephone network and get system data through. Unfortunately, this scenario will most likely occur at the very time a network is needed most by most organizations. It is important to note that cellular-based technologies, such as Cellular Digital Packet Data (CDPD), are also subject to these limitations. Consumer *voice traffic* is the first priority of cell providers, not data services.

Because cables are vulnerable to accidental or intentional damage, it is nearly impossible to ensure the integrity of the network. While no system can be 100% secure, wireless solutions offer an inherently more secure infrastructure, as there are no cables exposed to possible damage, sabotage or tapping by unauthorized persons. Wireless systems replace the wired infrastructure with an over-the-air RF link.

A wireless network can also provide an additional level of transmission security using a technique known as spread spectrum. Because the signal is spread over a range of frequencies, the communications link is more resilient to interference or jamming. Also, the spreading technique makes it more difficult for unwanted listeners to intercept network traffic.

The MDS Solution

Today, a utility's corporate communications network often incorporates public, private, physical, and wireless infrastructure. Assuming you have taken the appropriate steps to secure your network on an enterprise level, the next concern is incorporating wireless technology that enhances that security.

Using MDS' new iNET 900, customers can securely and easily integrate disparate communications standards and bring business-critical information over Ethernet and serial gateways onto corporate networks. This includes business-critical, revenue generating data from fixed assets such as oil and gas wells, compressor stations, pipelines, fluid storage tanks, and utility meters. It also enables portable network access for vehicle-based operation.

The iNET 900 offers several layers of security prohibiting unauthorized access and eavesdropping of data communications. It operates on the 902 - 928 MHz frequency band, unlike other wireless LANs using 802.11b solutions operating on the 2.400 - 2.483 GHz band.

Since 802.11b solutions are standard, anyone can purchase an 802.11b wireless card for their laptop. Hackers can use that card to monitor signals and determine the spreading sequence on which your information is transmitting.

MDS' transmission signal is unique in that it requires another MDS solution in order to receive it. It uses a modulation- type and frame structure combination, non-existent in other products.

The iNET 900 also uses Frequency Hopping Spread Spectrum. Originally designed to provide transmission security for military applications, the carrier frequency changes several times per second and requires another iNET radio to listen to any data being transmitted.

In the iNET 900, each pseudo-random sequence of hops is generated based upon a user-selected key that can result in tens of thousands of different combinations making it virtually impossible to reproduce.

Summary

While security of your network is paramount when conducting business, the advantages of an Ethernet/IP-based industrial network outweighs the risks involved. Security measures built into the equipment you use, as well as implementing basic network security techniques available to any organization, can keep your data and transactions secure.

Readers interested in more information about wireless applications for security monitoring can contact Microwave Data Systems, 175 Science Parkway, Rochester, NY 14620 (Tel. 585.242.9600). Additional information can also be found on the MDS website at www.microwavedata.com.

MDS products are manufactured under a quality system certified to ISO 9001. MDS reserves the right to make changes to specifications of products described in this document at any time without notice and without obligation to notify any person of such changes. Copyright 2003 MDS Inc.