Security Enhancements through Industrial Wireless Networking

Prepared by
Microwave Data Systems
Rochester, New York
June 2002

industrial/wireless/performance

Introduction

Although physical security has long been a concern at utilities, private companies and large office buildings, last year's terrorist attacks have raised the issue to a new level. In response to these events, many organizations have re-assessed their security readiness, and are now installing new or upgraded security and/or surveillance systems. Facilities slated for improvement include power plants, power distribution stations, dams, reservoirs, refineries, open pipelines and places of public assembly.

Whether a security system is designed to detect intrusion, report smoke/fire, or perform video surveillance, the system is only as reliable as the communications link it is connected to. This paper discusses the benefits of using wireless communication over cable-based alternatives, with an emphasis on improving security, reliability and achieving a lower cost of operation.

It also includes a discussion on wireless video transmission, and shows how video cameras can be paired with recently developed transceivers from MDS to transmit video images over considerable distances. Video is receiving a great deal of attention today, because there is often no substitute for actually *seeing* what is happening at a remote site.

The type of video used depends on many factors, and requires careful consideration by system designers. In this paper, we discuss the implementation of one type of system that can serve the needs of many applications where true, full motion video is not required. The system described is capable of license-free transmission of video images up to 30 miles (48 km).

Why is Wireless Better?

Reliability, availability and cost are important considerations in any communications network. These factors become even more critical when the application involves monitoring alarms or surveillance devices, where a communications outage could render the system useless. 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. Security applications are not necessarily a leased line provider's highest priority.

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 public service and municipal agencies. 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.

Cost & Security Advantages

Once a wireless system is installed, the user owns the medium, and there are no ongoing charges for communications. The equipment costs for a wireless link are often recovered within a very short time. By contrast, the difficulty of installing and maintaining leased lines makes their cost very high. This is particularly true in high bandwidth applications, such as the transmission of video. The cost of video-capable lines can easily exceed $300 per month.

Network security is another concern with hardwired systems. 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, MDS wireless solutions offer an inherently more secure infrastructure, as there are no cables exposed to possible damage, sabotage or tapping by unauthorized persons. MDS Wireless systems replace the wired infrastructure with an over-the-air RF link, allowing immediate, reliable communication with remote sites at ranges up to 30 miles. More is said about cyber security in a white paper about the MDS iNET 900.

A New Player: Wireless Ethernet

One of the most exciting areas of growth in wireless communication today, involves the transmission of IP and industrial protocols over wireless Ethernet devices. This type of communication offers distinct advantages over serial transmission, including hardware and software platform interoperability, collision avoidance, high throughput efficiency, and the ability to add new devices to a network without disrupting traffic flow. The use of IP also opens up new possibilities for integrating an enterprise-wide Intranet, the World Wide Web and video into a network control scheme.

Until recently, most wireless Ethernet products were designed for office environments, and were not built to survive the harsh, external environments of industrial applications. Light duty transceivers of this type are suitable for carrying data short distances within a building, but are not intended for long haul, mission-critical applications.

Today, the MDS iNET 900™, an industrial-grade wireless device (Figure 1), can carry Ethernet and serial data considerable distances. It effectively eliminates the risks involved with running long spans of cable. Additionally, the iNET 900 is capable of handling multiple users and protocols in both new and legacy networks. In addition to traditional SCADA/Telemetry service, products of this type have huge potential for use in alarm and surveillance monitoring, including the transmission of video and other high bandwidth traffic.

Figure 1: The MDS iNET is a new wireless Ethernet transceiver by Microwave Data Systems. It is a license-free 900 MHz unit that supports both Ethernet and serial data transmission.

A growing number of peripheral devices are being manufactured today with direct Ethernet connections as standard features. This simplifies the connection of these devices to wireless equipment and makes the expansion of a network feasible from a cost standpoint. Software development at the host computer is also simplified, since multiple protocols can now be addressed by a common interface. The responsibility to integrate the different locations, protocols, interfaces and baud rates is delegated to the network itself.

Video over Wireless: A Practical Reality

In recent years, a number of IP-capable cameras have appeared on the market, driven chiefly by the interest in providing web cam services over the Internet. IP cameras can be connected directly to a personal computer (PC) and are typically supplied with software that provides all necessary setup and configuration tools. These cameras allow users to transmit near real-time video to a worldwide audience with minimal expense and plug-and-play installation.

While the history of IP cameras can be traced largely to the consumer market, several models have evolved into sophisticated industrial solutions worthy of consideration for the most demanding commercial applications. Indeed, some industry experts predict that IP solutions will eventually gain an edge over the currently dominant serial protocols used by many organizations.

Whether the need is to transmit serial or IP data, the MDS iNET 900 is the right choice, especially when range, reliability and total cost of ownership are the prime considerations. The iNET is especially well suited to applications where existing "legacy" systems are mixed with newer IP-based solutions.

IP Video meets Wireless

Because the MDS iNET 900 is an IP/Ethernet ready device, it possible to connect an IP camera directly to the transceiver and transmit video signals over a range of several miles. No special hardware, software or adapters are required between the camera and the radio. Instead of signals being carried over the Internet, they are transmitted over the radio channel to a second iNET 900 radio, where the images can be displayed on a connected PC. Figure 2 illustrates a basic setup of this type with two remote cameras reporting to a single Access Point. Many other variations are possible.

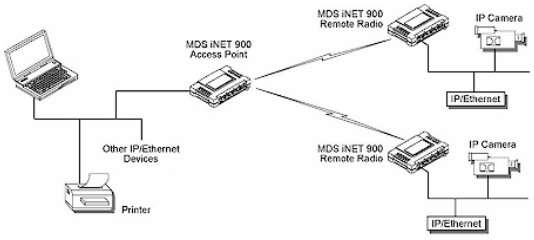


Figure 2. IP-capable cameras can be directly connected to an MDS iNET 900 Transceiver for the wireless transmission of video.

Setting Realistic Expectations

The wireless arrangement described above offers a simple, inexpensive and long-range wireless video solution. It is not intended to provide seamless, real-time video as with a closed circuit TV system, however, many applications do not require this level of operation, particularly when the need is simply to monitor a restricted area for unauthorized entry or tampering. Moreover, wireless systems are easier to install, and allow the network to be brought online in a much shorter time.

Consider for the moment an application where the entrance to a substation or control facility is to be monitored for intrusion. Using the basic arrangement described above, video images could be sent from the site to a central facility, where attempted entry could be detected. Armed with this information, personnel at the monitoring center can dispatch the appropriate authorities to investigate.

The decision on what type of video to use at a particular site depends on many factors and should be carefully considered by system designers. Wireless transmission offers several benefits that are difficult to achieve under hardwired schemes, and their reliability has been proven in real-world situations.

Today's Cameras: More than just a picture

Many IP surveillance cameras made today are equipped with software that can trigger an alert or email message if movement is detected at the installed site. This is a powerful tool that eliminates the need for an operator to continually watch the display for activity. The "sensitivity" of the camera can be set via the software to eliminate nuisance alarms that might occur from moving leaves, branches or other normal activity at the remote site.

Another useful feature included on some cameras is the ability to report contact closure or opening from external devices at the remote site (i.e., magnetic switches, other alarm sensors, etc.). When a change in status is sensed, a signal is sent over the RF link to inform personnel at the monitoring station.

Cameras with this capability are not intended to serve as full-featured alarm processors, but they do provide a convenient way to gather auxiliary information from the protected site and convey this data over the communication channel.

Typical Installation: What's Involved

The specific requirements for establishing a video link will vary widely depending on the conditions at the remote site and the monitoring location. There are, however, some common issues that should be considered for all installation sites. The following is an overview of these issues and provides some recommendations for achieving a successful installation. Instruction manuals provided with the wireless and video equipment provide further guidance on installation and setup.

Camera Selection & Placement

Almost any IP-capable video camera can be used with the iNET 900 Transceiver. Check with your MDS representative about other solutions that exist for both IP and Serial-based video equipment.

The camera equipment needs to be mounted in a location providing a good view of the area to be monitored. Most applications will employ a fixed mounted camera secured to a wall or pole, but there is nothing to prevent the user from setting up a temporary arrangement with a camera mounted on a tripod stand. This may be an ideal solution for monitoring work sites, special events or other temporary venues.

Environmental considerations must be taken into account to ensure that cameras are placed in a suitable location. A wide variety of cameras are available today to meet the needs of indoor or outdoor use, in temperatures ranges from “desert” to “arctic” conditions. The specifications of the camera should be reviewed before deciding on a final mounting location.

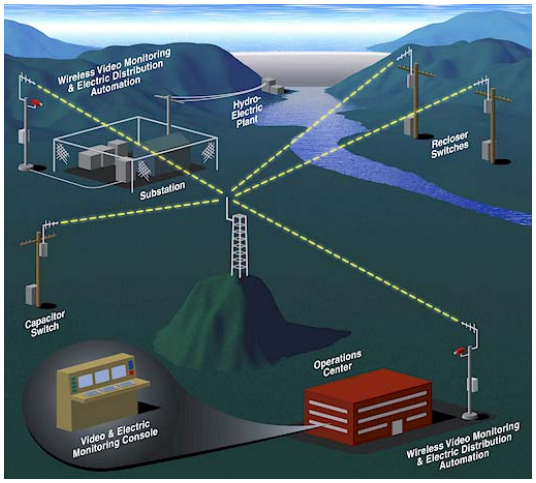
Power considerations

Most cameras come with a small power supply that furnishes low voltage DC (typically 9-12 Vdc) needed to operate the device. In some cases the installer may need to provide this power from a separate power supply. In any event, the camera specifications should be reviewed before applying power to ensure that the proper voltage and current ratings are observed.

Because of the low voltage and current requirements of the MDS transceiver and most cameras, alternative DC power arrangements are also possible, including the use of battery/solar power systems. The implementation of alternative power arrangements is beyond the intent of this paper, but is mentioned for those contemplating an installation in a remote area that lacks commercial power mains.

Frequency Range and Reliability

The operating frequency of a wireless transceiver deserves careful consideration. Many current designs (including office-grade wireless LANs) operate in the license-free 2.400-2.483 GHz band. By contrast, the 900 MHz band offers improved range, and reduced chance for interference with other Ethernet or consumer devices. (Many consumer devices operate in the 2.4 GHz band, including microwave ovens and many home audio and video systems.) 900 MHz is the preferred choice for range and reliability.



Wireless video has wide application in industrial and utility security systems. This illustration shows how video can be incorporated into the telemetry/SCADA network of an electric utility.

Spread Spectrum: A Proven Alternative

Wireless systems can be licensed or license-free. Traditionally, radio users have operated on fixed frequencies licensed to them by the FCC, Industry Canada, or other applicable licensing authority. This arrangement is intended to limit radio interference to or from other users within a geographic area, and for the most part it works very well.

In recent years however, overcrowding of frequencies has made it difficult, if not impossible, to obtain a radio license in certain areas—especially in or near large cities where the density of transmitting stations is much higher than average. Overcrowding of frequencies has forced users to explore other options for wireless data transmission.

In the U.S.A., Canada, and many other countries license-free operation is permitted under certain restrictions, and may offer a practical alternative to traditional (licensed) radio operation. License-free radios are limited to a maximum of 1-watt output, and must use a *spread spectrum* technique that distributes their RF energy over a wide swath of frequencies.

Despite their low power, spread spectrum radios often provide reliable coverage that rivals the range of licensed equipment. Well-designed radios also include a variety of interference-combating features that allow trouble-free operation even in heavily congested areas. More information on spread spectrum technology is available at **www.microwavedata.com**.

Conclusion

In this paper, we've given an overview of how industrial wireless can improve the reliability, efficiency and security of network communications. This technology is now a practical reality, and is being chosen by many organizations to replace older, less flexible systems.

With the added possibilities brought about by wireless video, many organizations are exploring how this technology can be employed in both new and existing security systems.

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**.