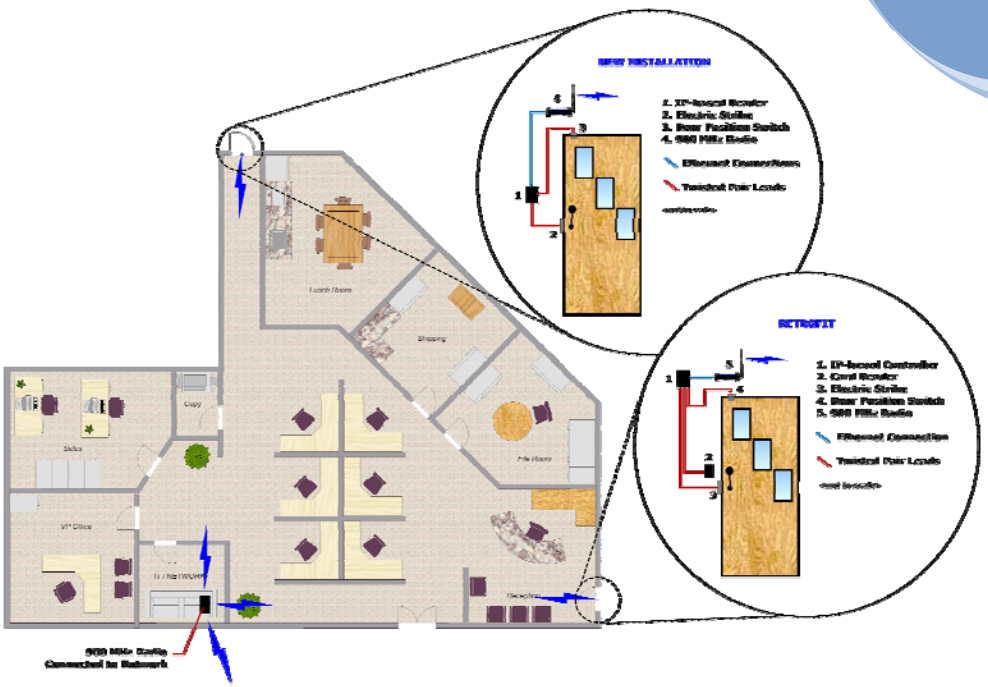
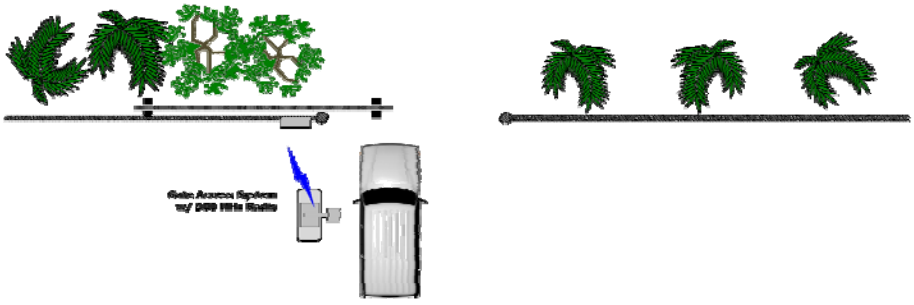




Wireless Access Control

Security Products

This whitepaper seeks to educate and explain the benefits of a wireless IP based access control system.

By AvaLAN Wireless Systems
www.avalanwireless.com

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Introduction

Over the past several years, much attention has been paid to the development and deployment of IP-based video surveillance systems. However, the rate of adoption of these exciting new technologies has been slowed in part by the heavy bandwidth consumption of video streams, and their resulting adverse impact on the network.

Meanwhile, unhindered by these restraints, manufacturers of (relatively low data-rate) access control systems have been gradually introducing network-based offerings of their own. The idea of course is to take advantage of the powerful and ubiquitous TCP/IP communication platform, without the drawback of negotiating to convince the IT department to allow you to consume large quantities of their most precious commodity: bandwidth.

Furthermore, the IP network is relatively affordable to deploy and universally understood; IT professionals from any nation of the world all work within the same framework and rule set, therefore installation and configuration challenges associated with proprietary technologies are all but eliminated.

However, in many cases, a wire-line network connection is not readily available at all of the locations where access control points may be required in the facility. Very few buildings – even those constructed in the modern era – include network connections (RJ-45 ports) at their doors and gates. As a result, wireless technologies are increasingly being considered to deploy these Ethernet-based edge devices.

This three-part series explores the factors to consider when designing and deploying a wireless Ethernet-based access control system.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Part 1) Technology Overview & The Business Case for Wireless Ethernet Solutions:

- **Why Select Ethernet vs. Other Transport Protocols?**
- **Why Choose Wireless for Ethernet Transmission?**

Traditional (non-Ethernet) Protocols

With its introduction several decades ago, electronic access control has solved many of the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

In most access control solutions in use today, the system using a simple challenge-response system to allow a visitor access to a door or gate. When a credential is presented to a reader, the reader sends the credential's information, in the form of an encrypted bit-string, to a control panel. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that, in turn, unlocks the door.

Therefore communication is typically taking place between the access control hardware at the door and a panel containing the system intelligence and database of authorized personnel. This communication traditionally has taken place along standard low voltage cabling creating a dedicated loop between the two devices. The advantage of this dedicated design is that it allows the systems designer complete end-to-end control of the system's cabling, without concern for impact from other devices running on the same wire. The principal disadvantage is that the reader devices must be hard wired to the central panel to facilitate the communication, and therefore costly cable runs are required to every access-enabled door, and the system cannot be easily accessed from other geographical locations.

Why Ethernet for Access Control Systems?

Before we can examine the case for wireless technology, we must first convince ourselves that an Ethernet-based solution is preferred over a traditional closed loop proprietary protocol. Here are the most compelling reasons to deploy an IP-based system:

<u>Ubiquitous Existing Infrastructure</u>

Billions of linear feet of CAT-3, CAT-5(e) and CAT-6 copper cabling and optical glass fiber are already installed worldwide. TCP/IP networks are everywhere, and are now being used to support data transmission in almost every vertical market application in existence.

Ethernet (IP) technologies are also widely understood by many types of IT and business process professionals; therefore it is easier to conduct discussions among disparate groups within a company to reach consensus and share network resources among users.

Finally, since TCP/IP networks are standards based, manufacturers can develop and bring to market products that are more cost effective and readily upgraded.

Thus, with all of this infrastructure already in place, access control companies are wisely now providing their customers with the ability to leverage the existing network, and not requiring them to home run new dedicated low voltage cabling from every door controller and/or card reader to a centralized database server.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Cost

Since so much of this TCP/IP network infrastructure already exists – and in many cases is underutilized and contains spare capacity - it behooves the systems designer to consider using existing network cabling prior to specifying a solution that requires new low voltage (dedicated) cabling to be installed. Fortunately, data rates required for access control are very low, therefore the systems designer as a rule can easily obtain permission from the IT department head to allow the system to use the current TCP/IP network.

Scalability

Access control systems are by their very nature spread out across fairly large areas. This is usually because the points of access / egress are at the edge or perimeter of the building or facility. Therefore, it makes perfect sense that the ideal technology to communicate between these devices is one tuned to fit these large areas.

As a result, when discussing which platform to standardize upon - whether we are referring to a few doors on a floor of a small office building, or gates spread across a 15 square-mile major international airport - integrators need a solution that will readily scale from very small to very large.

It is now generally accepted that Ethernet communication technologies provide the most robust, cost effective and easy-to-install solutions to deploy edge devices across a wide variety of geographic conditions. Ethernet networks are by design modular and highly scalable. Adding network subnets can be as simple as installing a managed switch or network bridge and laying additional cable. Using internal IP addressing, the number of network-based devices that can be installed to communicate with each other is very large.

Accessibility

Finally, and perhaps most importantly, the power of an IP-addressable system is most evident when examining its accessibility or visibility from other geographical locations. Inside the router – i.e. on the same subnet on the LAN – simply calling the internal IP address will provide instant access to the device. This is useful no doubt, however even more valuable is the ability to use network address translation (NAT) and port forwarding. By this means, any IP devices can be configured for easy access for external communication requirements from *outside* of the router serving the local area network. This means that, unlike closed loop dedicated point-to-point low voltage cabling, the IP-based system can be accessed from an Internet connection anywhere in the world.

Why Go Wireless?

It is not always the case that a wireless transmission solution is preferred. In fact, there is nothing more secure and reliable than a dedicated point-to-point cabled system. However, when transmission distances increase, and the bidding on the project becomes more and more competitive, it makes sense for the systems integrator to consider going wireless. Let's examine a few of the principal factors:

Cost

Price is always an important consideration for any job, and in the case of government projects *the* most significant factor. Therefore, when designing a new network-based access control system, the choice must now be made between the price of the materials and labor associated with running dedicated cabling runs and conduit vs. the cost of the Ethernet based radio transceiver and power supply. Since long range wireless Ethernet radio transceivers are now below three hundred dollars, while the price of copper and conduit is rapidly increasing, it can often makes sense to examine the feasibility of a wireless solution for any distance over 50-75 feet in a building.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

In the case of an outdoor installation, for example connecting from a main building to a perimeter gate access system, the case is even more compelling. The cost of trenching conduit in place can range from $15 to $35+ per foot, therefore a radio transmission system is almost always more cost effective in these situations.

In part due to rising insurance and health care costs, labor rates have climbed briskly over the past two decades, making the labor component very significant in the overall cost of the project. Labor to pull cable can be difficult to estimate – especially in older buildings - but is very likely to be far greater than the few hundred dollar cost of the wireless radio equipment.

Taking the steps to minimize labor costs will very likely permit the integrator to submit a lower bid, win the job, get the job done faster and move their highly skilled personnel on to the next project.

Interruption in Service

On the job site, the use of wireless radio transmission means that the system can be installed during regular business hours, without as much concern for the interruption in service associated with pulling cable through the facility. Long cable runs inside a building or excavating trenches outdoors across the project site will very often cause an interruption in service of the company or agency. This interruption in service should be taken in to account when estimating the actual total cost of the cabled solution versus that of a wireless enabled system.

Appearance

Trenching cable outdoors will in most cases leave an undesirable scar on the landscape. In many cases this is hard to quantify from a cost standpoint, but certainly most professional facilities managers will agree they would prefer not have their parking lot cut through unless absolutely necessary.

Unforeseen Incidents

Negotiating in-ceiling cable runs under difficult conditions – for example in an older building that might be contaminated with asbestos - is a nightmare for all parties involved with the project. Furthermore, digging trenches on a job site to lay conduit for the network cable can be risky if the underground utilities in the area are poorly understood.

Better Products & Frequency Selection

New products from wireless manufacturers released in just the past year are much more compact, require less power than their immediate predecessors, and are very reasonably priced. Furthermore, several manufacturers have released products in the 900 MHz ISM band, providing a simple, unlicensed transport capable of transmitting access control data through long distances, including penetrating walls and foliage at the project site.

***

In Part 2) of this series “System Design Elements”, we will examine the specific types of wireless access control solutions on the market today, with a discussion of wireless in access control and video surveillance and how the technology translates into better systems tailored to the needs of security professionals. We will focus on how to leverage and successfully deploy wireless access control solutions and discuss how to design systems with open Layer 2 architecture.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Part 2) Designing the System:

- **Types of access control interface technologies**
- **Principal IP access control topologies**
- **State-of-the-art wireless IP-based access solutions**
- **Integrating video surveillance at the door or gate**

Types of Access Control Interface Technologies

There are five principal interfaces or technologies used to impart data from the candidate requesting entry to the access control system:

Magnetic Stripe Readers
Magnetic stripe technology, usually called mag-stripe, is so named because of the stripe of magnetic oxide tape that is laminated on a card. There are three tracks of data on the magnetic stripe. Typically the data on each of the tracks follows a specific encoding standard, but it is possible to encode any format on any track. A mag-stripe card is fairly cost effective in comparison to other card technologies and is often easier to program. However, because it is a contact-based technology, magnetic stripe systems can susceptible to misreads, card wear, and data corruption.

Wiegand Card Technology
Wiegand card technology is a patented technology using embedded ferromagnetic wires strategically positioned to create a unique pattern that generates the access code bit string. The communications protocol used on a Wiegand interface is known as the Wiegand protocol and is the leading standard worldwide for access control. An advantage of the Wiegand signaling format is that it allows very long cable runs. The disadvantage is that it is a closed loop proprietary protocol that can only be connected in cases where the reader is in physical proximity to the logical access processor.

Proximity Cards
The Wiegand effect was used in early access cards. This method was abandoned in favor of other technologies. The new technologies retained the Wiegand upstream data so that the new readers were compatible with old systems. Readers are still called Wiegand but no longer use the Wiegand effect. A Wiegand reader radiates a 1" to 5" electrical field around itself. Cards use a simple LC circuit. When a card is presented to the reader, the reader's electrical field excites a coil in the card. The coil charges a capacitor and in turn powers a integrated circuit. The integrated circuit outputs the card number to the coil which transmits it to the reader.

Smart Cards
There are two types of smart cards: contact and contactless. Both have an embedded microprocessor and memory. The smart card differs from the card typically called a proximity card in that the microchip in the proximity card has only one function: to provide the reader with the card's identification number. The processor on the smart card has an operating system and can handle multiple applications such as a cash card, a pre-paid membership card, and even an access control card. The difference between the two types of smart cards is found in the manner with which the microprocessor on the card communicates with the outside world. A contact smart card has eight contacts, which must physically touch contacts on the reader to convey information between them. A contactless smart card uses the same radio-based technology as the proximity card with the exception of the frequency band used. Smart cards allow the access control system to save user information on a credential carried by the user rather than requiring more memory on each controller.

Personal Identification Number (PIN)
A personal identification number (PIN) falls in the category of what you know rather than what you have. The PIN is usually a number consisting of four to eight digits. Less and the number is too easy to guess. More and the number is too difficult to remember. The advantage to using a PIN as an access credential is that once the number is memorized, the credential cannot be lost or left somewhere. The disadvantage is the difficulty some

people have in remembering numbers that are not frequently used and the ease with which a PIN can be observed and therefore used by unauthorized people. The PIN is generally considered less secure than a bar code or magnetic stripe card.

***

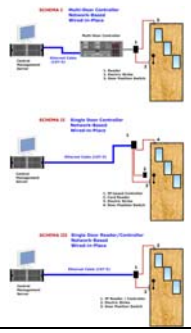
All of these data acquisition methods require that the interface element (in most cases a card reader) be immediately adjacent to the door or gate. Of course once the reader scans the card it must then have the ability to determine if the user credential is valid. If the intelligence to determine validity (ie. the database of valid contact ID's) is some distance away from the door, then the information from the card swipe request must be sent to the authentication server (or control board) to be approved or denied, and then the response must be sent back to the door unit to trigger the lock release.

By moving the database of acceptable credentials to the door - or to a multi-door control board adjacent to several doors - the round trip communication time is reduced to several milliseconds. In fact, the communication methodology becomes much less important since the connection is only used to *update* the remote database (from the central knowledgebase) and to send a log of the access events at the door or gate to the facility security officials.

It is for this reason that wireless technologies are now being considered for connectivity and transmission links. Wireless connections have higher latency and can be subject to RF interference and temporary interruption; and hence are rightfully considered less robust than hard wiring. Therefore, historically when a round trip authentication cycle from the remote door to the main database controller was *required to open the door,* then a wireless connection was not considered reliable enough. However, with new technologies that provide the intelligence at or near the door, a wireless transmission solution is now appropriate.

Principal Network-based Access Control Topologies

Before we examine *wireless* Ethernet solutions, let's quickly review several of the most common *wired* Ethernet technologies. While traditional Wiegand-based closed loop (proprietary) systems are still the norm, increasingly integrators are deploying one of the following three principal types of wired-in-place Ethernet-based access control design topologies:

<< Insert **Figure 1** Here **>>** 	Reader @ Door → Multi-Door Controller → Central Management Server
	Reader → Door Controller @ Door → Central Management Server
	Integrated Reader / Controller @ Door → Central Management Server

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Part 3) Installation tips, challenges, ROI and the future of the technology:

- **How to successfully deploy wireless access control solutions.**
- **Troubleshooting :: top five causes of wireless system failure**
- **ROI on wireless access control and when does wireless make sense**
- **Developing trends :: The future of wireless technologies**

Installation tips :: How to successfully deploy wireless IP-based access control solutions

Selecting the Right Products

The single most important factor in ensuring the successful deployment of a wireless Ethernet access control system is to select the right product and transmission frequency for your specific application. For example, if the installation includes short range indoor transmission to a few doors then there are numerous wireless Ethernet products available in the market that will accomplish this. However, if the access control system includes a long range connection to remote buildings or across larger distances to gates in the facility, then the choice of products is narrowed considerably. A few other factors to consider are the ease of installation and long-term maintenance and support of the product suite. Purchasing the lowest cost hardware may not always be the answer, especially if the product has a steep learning curve and/or the technical support offered by the manufacturer is below par.

[Note: A discussion of specific manufacturers and their products is beyond the scope of this article; however a wealth of information is available in previous issues of this publication, or by conducting a text search within the online Web portal of Security Products Magazine at this address: http://www.secprodonline.com/]

Antenna Selection

An often overlooked aspect of the wireless system is the antenna. For longer distances, or in crowded RF environments such as large cities or near communication facilities, it is imperative that *directional* antenna be used whenever possible. This increases the signal to noise ratio, and hence both the transmission and receive power of the radio, and allows the system to function well now and in years to come as the RF environment changes over time.

<< Insert **Figure 1** Here **>>**	Caption :: Typical panel-type and Yagi-type directional antenna

Tamper-proofing Your Installation

Radio transceivers are not by themselves a primary target for vandals, at least not any more so than any other piece of electronic equipment in an outdoor NEMA enclosure. However, when you add the presence of an antenna, they can become of interest to a would-be wrongdoer. Therefore, the best way to keep your investment safe is to put it out of reach of the public. This is usually accomplished by installing the equipment up a pole or on top of a building. Since this is generally more favorable from an RF transmission standpoint as well, it makes sense to do so. If you must install the antenna at ground level, consider using a stud-mount antenna which is bolted flush to the enclosure making it difficult to pry off the housing.

In-band Interference

The majority of Ethernet radios sold in North America today use one of three ISM bands: 900 MHz, 2.4 GHz and 5.8 GHz. These are unlicensed bands and hence you (and anyone else around you) are free to deploy FCC-certified products wherever you choose. This being the case, for larger projects it is important to conduct a site survey with a portable spectrum analyzer prior to implementation to assess the nature of the particular band you have chosen to use. If it turns out to be crowded then the in-band noise floor will be high, and your signal-to-noise ratio will be unfavorable, thereby adversely affecting your wireless range and performance. Alternatively, since spectrum analyzers are expensive, you can also select a radio transceiver product that has the ability to scan the ISM band in which it operates and assess the spectrum viability.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Near-band Interference

Another potential pitfall is RF noise interference from sources spectrally adjacent to the ISM band in which you have chosen to operate. For example, the FCC-reserved space for the 900 MHz band is 902 - 928 MHz. Unfortunately, several legacy paging systems use the space immediately above this in the 929 – 931 MHz range. While this frequency is not actually in the ISM band, the near-band interference can be significant since the output power from the paging tower is often several orders of magnitude higher than the lower power commercial off-the-shelf wireless Ethernet systems running in the ISM band itself. To address this, notch filters are available that preferentially discard all frequencies except the band in which you are operating. This allows the installer to add an inline component to neutralize the adverse effects of this interference.

Training

Many of the leading wireless Ethernet manufacturers offer free technical training for their products, either via online Webinars or in some cases on site in person in conjunction with their network of manufacturers' reps. It is highly recommended that you participate in this training before you attempt a large scale wireless access control system. This will go a long way toward ensuring your success on a project of this scope.

Technical Support

Installing a state-of-the-art wireless Ethernet system is as much an art as it is a science. Therefore, if you are new to the technology (and selected product suite) it is important to have access to the manufacturer's technical support team during the early stages of the job. Beginning the project late on a Friday afternoon, and planning to work through the weekend may not be in your best interest until you have installed a few projects and are fully comfortable with the process and potential issues.

Replacement / Spare Parts

As with any other mission-critical network technology, it is always a good idea to keep spare parts on hand. For example if you have deployed 25 radio transceivers, antennae and mounting hardware, it might make sense to purchase one or two extra kits to have on hand in the event of a failure.

Troubleshooting :: Top Five Causes of Wireless System Failure

1) The most likely cause of system failure is human error. Therefore, the most important thing to do prior to beginning an installation is to read the user manual. Many of the pitfalls awaiting the integrator have been addressed in this important documentation.
2) *Always* use high quality cabling and connector components. Skimping on these to save a few dollars now can cost you hundreds of dollars in labor costs and down time waiting for replacement parts down the road.
3) As with any networking device, be sure to check and double-check your connectors and cabling to make sure that they are seated properly and in good working condition.
4) RF signal to noise ratio. If you are experiencing a poor signal to noise ratio, and as a result, dropping Ethernet packets and unable to reliably send data, you should consider the following:
    a. Is there in-band or near-band interference in the area? Has your neighbor installed a high powered source of RF interference recently (ie after you conducted your site survey)?
    b. Are you attempting to transmit too far, or through obstacles with an RF spectrum not designed for this purpose? Consider swapping the radios for another frequency that may be better suited for your installation geometries and distances.
    c. Are you using directional antenna? Omni-directional antennae suffer a double whammy: not only do they have less transmission power, but they also pick up interference from *all* directions and not just from the direction you want it from (ie the other radio transceiver). If you are already using a directional antenna, try upgrading to a more powerful model with more RF gain.
5) Hardware failure. Because an Ethernet radio transceiver is a fairly complex system, they can and do fail from time to time. Typically, one out of every two or three hundred Ethernet radios shipped are simply defective or become defective during the shipping and handling process. While this is rare, it does happen so be sure to contact your manufacturer to discuss how to determine if you have an actual hardware failure.

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

Cost-Benefit Analysis :: ROI on wireless access control and when does wireless make sense

If we review the published cost-benefit analyses of *wired* IP-based access control systems, we see that using the existing network infrastructure - vs. installing dedicated cabling - to transmit access control data from doors and gates back to a central management server or off-site backup generally makes sense. It is for this reason that most industry experts believe that over time traditional proprietary access control systems will be replaced by open-standard Ethernet based systems.

Wired vs. Wireless
If we next examine a basic total cost of ownership formula:

TCO = [(Equipment + Installation Labor) + Disruption in Service] + Long-term Maintenance

And use this formula to compare and contrast wired vs. wireless access control solutions, it will reveal the following:

- Using wireless transmission technologies is not always indicated - when network cable is already in place at the door, or for short cable runs the additional cost of the radio and antenna at the control panel or door is not justified.
- If new cable has to be pulled, then the total cost of cable, labor and disruption of service (or overtime hours) must be compared to the cost of a radio transceiver and antenna at the panel or door.
- For long distances, such as out to a gate at the facility, wireless transmission is generally the preferred design topology.
- Cables rarely fail (unless tampered with by insects or small critters); whereas, over the long haul, the additional potential cost of failures of the radio equipment must be taken into account.

In summary, there are many compelling reasons to use open standards – such as Ethernet – to transmit access control data. Furthermore, in many cases, it makes sense to send that Ethernet packet via a low cost wireless radio transceiver rather than copper cable or glass fiber. In the end, this cost-benefit analysis must be performed for each project undertaken, which will in turn reveal the appropriate network architecture for the job.

Developing Trends :: The Future of Wireless Technologies

The ability to use a single radio platform to transmit both Ethernet and RS-232 / RS-485 serial data is compelling. Therefore, much work is currently being done in the area of integrated Ethernet / serial radio transceivers. Look for the continued release and refinement of this dual platform approach to add to the current generation of radios capable of handling specific proprietary access control protocols such as Wiegand.

The latest release in the class of 802.11 Ethernet transmission systems is the “N” specification. The 802.11N protocol uses MIMO multipath processing and channel bonding to offers some advantages in range and net throughput over traditional WiFi solutions. Several mainstream manufacturers have released products in this category with more to come over the next several years.

Over the past 5 years, mobile phone technology has evolved to include data transmission at moderate speeds and distances. Integrating this technology into fixed-in-place devices allows the system designer to install 2.5G and 3G network cards to send and receive data from a variety of platforms. These technologies are becoming more cost effective and faster every year, so look to see more solution providers using this wireless data backbone.

WiMax, a new technology which began its conceptual development in 2001, is based upon the 802.16 standard and uses fixed in place high-powered transmission equipment to send and receive high speed data. The WiMax forum, whom developed and manages the framework describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL”. Connecting to

AvaLAN Wireless Systems Inc.
125A Castle Drive
Madison, AL 35758
www.avalanwireless.com

a WiMax network will allow the end-user to send and receive moderate to high-speed data rates to and from the network to connect remote access control devices.

ZigBee is a new short-range (up to 10 meters) radio technology that does not likely have sufficient transmission power to make meaningful inroads into the wireless access control market application.

Closing

This series of articles has presented the factors to consider when designing and deploying a wireless Ethernet-based access control system. Since the data rates in question are orders of magnitude lower than in the case of IP video products, the challenges associated with bandwidth consumption are also minimized, and hence the rate of adoption of network-based access control systems will continue to grow over the coming years. The use of wireless transmission to support the remote deployment of these Ethernet devices is simply a natural extension of the technology and will only further accelerate the growth of IP-based access control solutions.

For Additional Information Please Contact AvaLAN Wireless
Phone: +1-650-384-0000
Website: www.avalanwireless.com
Email: sales5@avalanwireless.com