Wireless in the production plant

For various industries

www.ats-global.com
**Wireless in the production plant**

*How to avoid trouble when setting up a wireless network*

Are you considering to use wireless in your plant?

Do you know the most important differences between wireless for office applications and industrial wireless? Do you worry about security, unwanted access to your valuable plant data or your process control systems? Are you worried about network breaks?

If the answer to one or more of the above questions is yes, please continue to read and find out the answers. This White Paper takes a close look at the advantages and the pitfalls of wireless in an industrial manufacturing or processing environment. Explanation of the various considerations for wireless, security, the differences between office and industrial wireless as well as some examples of successful implementations will be discussed.

**The choice for wireless in manufacturing**

Typically, enterprises choose for a wireless network (either connected or not connected to the corporate LAN) in situations when a wired solution shows clear disadvantages. A wired solution may be the first thing that comes to mind, but in many industrial and processing applications it simply makes sense:

- Moving applications
- Hazardous locations
- Long distance communication
- Overcoming obstacles

**Important organizations to know**

Before starting to read, please find below an overview of the most important organizations involved in wireless communication:

- **ETSI**: European Telecommunications Standards Institute ([www.etsi.org](http://www.etsi.org)), a European official organization defining regulation for usage of radiofrequencies in Europe.
- **IEEE**: Institute of Electrical and Electronics Engineers. This organization is an authority on many domains involving electricity and electronics. It is at the origin of many standards such as the IEEE 802.3 set of standards, which specify the Ethernet support or IEEE 802.11, which specify the wireless Ethernet.
- **License-free 2.4 GHz band**: By convenience, everybody talks about the “2.4 GHz band”. This band goes from 2.400 000 GHz to 2.483 500 GHz. It is also known as the “ISM band” (Industry, Science and Medicine). It is a license-free band, which means that there is no need to ask for authorization or declaration for private applications. Note that the frequency limits might slightly change and that the power limitations might as well differ from one country to another. Emitted power is limited to 100 mW EIRP for indoor applications in most European countries, and to 100 or 10 mW for outdoor applications, depending on the frequency range inside the “2.4 GHz band”.

**Setting up a secure wireless network**

Wireless networks can consist of many different radio types based on radio frequency and modulation methods. Radios may be required to obtain a license to operate or be part of the FCC approved unlicensed ISM band. Radio technologies in the ISM band are most commonly available, supporting either “open” or proprietary standards. Most security issues are prevalent within “open” standards, such as 802.11.

Typical 802.11a/b/g (DSSS) wireless LAN architectures consist of wireless clients, wireless access points, wired computers and industrial...
PLC processors. Wireless clients typically are laptop computers but can also be industrial protocol/network gateways or PLC rack based modules. These clients communicate to other “wired” devices over LANs, typically through a wireless access point (AP) in “infrastructure” mode, or directly with each other peer-to-peer in “ad hoc” mode. An access point provides coverage to a particular area, known as a cell or a “hotspot”, and is usually connected to a wired network. Some access points are designed to act as a repeater, basically extending the range of the wireless connection, and allow for a “wireless” backbone, connecting several wireless hotspots.

The goal of wireless network implementations is to provide benefits that are identical to common wired networks. It should protect the network and its connected devices from security related issues. Depending on whether the connected devices are part of the corporate LAN and/or the industrial network, protection requires a sequence of events to occur:

1. **Authentication** is the verification process, where a user attempts to confirm identification to establish trust with the available resources.

   **Open authentication**
   The open system is the default setting, where any client can associate with the access point.

   **Shared authentication**
   The shared secret key is used to authenticate the client to the access point. Shared authentication uses a challenge-response protocol.

2. **Authorisation** protects computer / devices, only allowing those computers to be accessed by users who have been granted authority to do so.

3. **Encryption** obscures information, making it unreadable without special knowledge.

4. **Integrity** refers to the validity of data from malicious and accidental altering.

A wireless network missing any of these elements may expose known vulnerabilities to hackers and allow them to breach the confidentiality and integrity of the network resources.

---

### The top seven problems

There are seven primary wireless security problems confronting corporate LANs and industrial automation applications:

1. Easy access.
2. Rogue access points.
3. Unauthorised use of service.
5. MAC spoofing and session hijacking.
6. Traffic analyses and eavesdropping.

Each of these concerns can be grouped into two specific areas.

**Area A: Security concerns relating to issues when accessing corporate LANS through authentication and authorisation**

**Area B: Security concerns relating to issues about over-the-air wireless data packets**

Many industrial wireless applications are not subject to all of these security issues because not all wireless devices require connection to the corporate/industrial LAN and need only to be concerned with Area B security concerns. Grouping of these security concerns helps wireless site planners focus their attention to specific areas of security. Each of the above seven concerns are grouped and defined below with suggestions to help avoid getting into trouble when setting up a wireless network.

**Area A: accessing corporate LANS through authentication and authorisation.**

1. **Easy Access**

   Finding wireless LANs is not difficult. With open wireless specification and protocols, and with the correct tools, attackers can access networks, become authorised and authenticated to an internal LAN, and access corporate domain servers if left unprotected. To enable better protection, you can:

   - Turn on WEP or WPA security features and use 128-bit encryption.
   - Turn off beacon frames, when using 802.11 type access point radios. To hide your radio network from other 802.11 users, hide the network SSID by selecting not to broadcast the beacon frames. With the SSID hidden, your network does not show up when clients scan for an access point. You can still connect clients to the “hidden” network by typing the network SSID for client radios.
2. Rogue Access Points
Developing administrative security policies and monitoring for “rogue” access points are fundamental to reduce the risk of certain LAN access violations. You should:

- Place wireless access points outside the security perimeter (such as firewalls) and use VPN-IPsec protocol technology built-in to firewalls.
- Learn and identify where unauthorised networks have been deployed, and remove them before attackers exploit them. Laptop radio cards are available that can be used to locate wireless networks.
- Use low-gain directional and polarised antennas. Focus radio waves and energy to a confined area (hotspot).

TKIP provides three security improvements over standard WEP: fast-packet keying (key hashing per packet), real message integrity checking (to prevent forgery) and dynamic key management (re-keying).

3. Unauthorised use of service
The biggest defence against unauthorised use is to prevent unauthorised users from accessing the network.

- A precondition for authorisation is the use of strong cryptographically protected authentication where sensitive corporate LAN data is located. VPN solutions, deployed to protect traffic in transit across the radio link, provide strong authentication.
- Strong authentication schemes prevent unauthorised network access. Install a remote access dial-in server (Radius) for access point authentication. The 802.11i standard allows the use of a Radius server to manage encryption keys and control which radios are allowed to access the network. The radio first associates with the access point, and then is granted access only to the radius server. If the radio and server successfully authenticate each other, the Radius server sends a master key to the access point, which negotiates a session key with the radio. After authentication, the radio is connected to the network.
- Session hijacking can be prevented by using a strong cryptographic protocol, such as IPsec. Analysers can determine what security level is in use informing network administrators if the desired security protocols are in use.

4. Service and Performance Constraints
With the proliferation of wireless products, LANs can become crowded and overwhelmed with traffic. Wireless networks have limited transmission capacity.

For example, 802.11b/g have bit rates of 11 and 54 Mbps respectively, and the actual effective throughput amounts to about half of the nominal bit rate. With that in mind, it can be imagined how local applications might flood a network with limited capacity or how an attacker could launch a denial of service attack.

- Perform regular audits of wireless network access equipment to ensure that strong authentication mechanisms are in use and that network devices are properly configured. If an unauthorised station is found connected to the network, a handheld receiver can be used to track down its physical location. Analysers like the AirMagnet can also be used to verify the configuration of many access point parameters and raise alarms when access points expose security vulnerabilities.

5. MAC spoofing and Session Hijacking
Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions. By requiring authenticating potential users, unauthorised users can be kept from accessing the network. Attackers can use spoofed frames in active attacks as well. Attackers can pretend to be an access point.

- Use MAC address filtering. Each radio has a MAC address that can be placed on a list. The access point will only communicate with radios on the list.
- Adopt strong protocols and use them. Until the ratification of 802.11i, MAC spoofing will be a threat. Using IPsec and TLS protocols for LAN access points are important to proving identity.

6. Higher Level Attacks
Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell though is a soft, vulnerable centre. Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack.
Wireless in the production plant

ATS White Paper

• Using non-open standard radio types, such as 900 MHz and 2.4 GHz FHSS radio transceivers, offer a much higher degree of protection against would-be intruders. These radio types typically use proprietary type binary protocols and the hopping sequence is unknown.

The 802.1x standard is an authentication framework designed to provide controlled port access (and to deny access to the port when authentication fails) between wireless client devices, access points and servers that use the Extensible Authentication Protocol (EAP) and a Radius server. 802.1x further enhances security by enabling mutual authentication: the access point can validate the client, and the client can determine whether the access point is legitimate. Preinstalled digital certificates authenticate that their holders are who or what they claim to be. WPA includes both 802.1x and TKIP.

Area B: over-the-air wireless data packets.

Use encryption and proprietary binary protocols to prevent an eavesdropper or man-in-the-middle attack from understanding any intercepted transmission. 802.11 wireless packet frames can be visible to someone with a wireless network analyser. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker easy access to disrupt transmissions with spoofed frames. Earlier WEP implementations are vulnerable to cracking by tools such as AirSnort and WEPCrack, but the latest firmware releases from most vendors eliminate all known attacks.

There are products available on the marketplace that go one step further and use key management to change the WEP key often. So even the busiest wireless LAN could not generate enough data for attackers to recover the key in the interval of time allocated.

• Use non-open standard radio types, such as 900 MHz and 2.4 GHz FHSS Frequency Hopping Spread Spectrum.

• Use key management protocols for dynamic “key-rollover”. Changing the key prevents an eavesdropper from understanding what each packet of data consists of.

• Use low-gain directional antennas. Focus radio waves and energy to a confined area.

• The use of industrial (non-plain text based) binary based application protocols help drastically in prevention of hijacking and spoofing attacks. These binary protocols are often secret and therefore present a high degree of complexity to would-be trespassers. Suppliers do not publish their wireless protocol, and therefore it is proprietary in nature. Security tools and management software like AirMagnet can detect AP spoofing and can be configured by default to raise an alarm to alert administrators to investigate any such violations.

Additional wireless security guidelines

• Implement a robust networking and security architecture using standards such as PEAP and 802.11i authentication and authorisation methods.

• Use 802.11x EAP-TLS digital certificates and dynamic per-user/session WEP keys or IPsec VPNs.

• Deploy security tools and management software. Visit the websites of wireless security experts such as www.prosoft-technology.com to learn more.

• Use commercial or industrial type firewalls to separate wireless from wired LANs. A PLC with two unbridged network cards acts as a firewall but is not physically connected to each other acting as a data concentrator. The PLC data concentrator performs the communication with each network programmatically, controls the frequency of polled and/or change of state data and ultimately controls the channel bandwidth and overall network performance.

• Turn on WEP encryption and never deploy “open system”. Use 128-bit WEP keys. Change WEP keys often. Use products with dynamic key management features.

• Use MAC access control by using access points with MAC address filtering.

• Do not use default passwords and network names (SSID) and use difficult to crack bit WEP keys. Use 128-bit WEP keys. Change WEP keys often. Use products with dynamic key management features.

Some basic questions

Define your wireless network.
Is the network point-to-point, broadcast, point-to-multipoint, ad hoc or infrastructure? Interconnecting industrial networks and device applications may only require simple peer-to-peer communications. Some applications will connect devices and networks within a building, others will interconnect multiple buildings. Develop and control internal radiated hotspots and/or long-haul wireless connections.
Will I use open or proprietary standards?
It is virtually impossible for a would-be intruder to access raw or encrypted data from FHSS industrial wireless modems. Good radios provide three levels of security for wireless data networks: inherent security in FHSS technology, encryption at the hardware level and proprietary architecture.

What type of data will be transmitted and what type of protocols will I use?
Simple device-to-device communication provides over-the-air security all the way up to the application layer, using the PWP producer/consumer wireless protocol. These devices also provide encryption “key roll-over” management features and have built-in firewall (internal database) protection.

Will I need corporate LAN access to sensitive data or can I apply simple device to device communication?
Many industrial wireless applications provide simple communication between a PLC and a remote instrument or second PLC processor that is not connected to a physical LAN. Security concerns for this type of wireless network are outlined in Area B, # 6 - Traffic Analysis and Eavesdropping. Some wireless applications require short connection times, for example when programming a PLC over the air through a wireless in-chassis module.

Should I be using an ad-hoc (peer-to-peer) or infrastructure (access point) type network?
Ad hoc device to device communication of PLC to PLC backplane communications are isolated from corporate LAN sensitive data because, when using this type of device-to-device communication topology, a LAN access point may not be required (ad hoc). The PLC backplane becomes an additional firewall to industrial sensitive data, especially when in-rack based wireless modules are implemented.

Do I need open industry wireless standards?
There are many ISM radio product solutions available. These vary in types of RF modulation (FHSS and DSSS), physical interface types (serial, Ethernet, Ethernet to serial) and whether the products meet open industry standard specifications such as 802.11 or incorporate more secure specifications based on non-standard Frequency Hopping patterns and proprietary data protocol.

What application layer protocols will be used in transmission?
Are the transmission packets using ASCII text (plain-text) based or binary coded data frames? Many 802.3 protocols are ASCII-based and easily expose the data being transmitted. Binary protocols, plus encryption technology to scramble the data prior to transmission, offer a high degree of protection. The binary data (ones and zeros) are meshed with a WEP key like the ASCII protocols but do not expose the data in a plain text format that can be understood.

Separate protocol drivers communicate with each device network, then perform read and write functions to the database. This gateway technology acts as firewall for the connected networks. Another type of gateway technology used with ProSoft Technology is PLC In-Rack modules. Like the standalone gateway, it consists of an internal database. However, the other unexposed side of the database communicates directly with a processor backplane. This technology combined with RF site management creates a difficult challenge for someone to penetrate the remote network or compromise the integrity of the data.

Hans Damman is a Director of ATS International B.V. and an expert in wireless technologies and security issues. ATS operates globally and offers consulting, training, engineering, software development services and communication products to users of industrial-, process automation and IT.

**Commonly used acronyms:**

- **DSSS**: Direct Signal Spread Spectrum
- **FHSS**: Frequency Hopping Spread Spectrum
- **EIRP**: Effective Isotropic Radiated Power
- **RLAN**: Radio Local Area Network
- **WEP**: Wired Equivalent Privacy
- **LAN**: Local Area Network
- **WLAN**: Wireless Local Area Network
- **WPA**: Wi-Fi Protected Access
- **MAC**: Media Access Control
- **ISM**: Industrial, Scientific and Medical
- **IPsec**: Internet Protocol Security
- **TLS**: Transport Layer Security
- **TKIP**: Temporal Key Integrity Protocol
- **ARP**: Address Resolution Protocol
- **PEAP**: Protected Extensible Authentication Protocol
- **VPN**: Virtual Private Network
- **Wi-Fi**: Wireless Fidelity
About ATS

ATS is an Independent Solution Provider, with over 20 years experience and a wealth of experience undertaking Continuous Improvement initiatives and Manufacturing IT solution design, deployments and 24/7 support assignments.