

Wireless – beyond the myths

The myths and facts associated with wireless plant communications

Wireless technology makes it possible to incorporate new strategic measurements and other data to solutions that simply were either not practical or even possible to implement in a wired communications environment.

When wireless technology is used, solutions for process optimisation, device management, real-time equipment condition monitoring, energy management, personnel tracking, asset tracking, security, and enterprise asset management can all work in unison to address both industrial asset utilisation and availability.

There are some limitations to a wired infrastructure, especially in the plant environment. New applications often require upgraded cabling and expansion to existing applications may require additional cabling.

Along with the cabling itself, there are many associated costs with this kind of infrastructure. In order to expand cabling within a plant, costly engineering studies need to be performed so that the most appropriate wiring locations and paths can be determined.

Also, depending on the age and condition of the existing environment, some issues may need to be remediated when cabling is added. For example, asbestos may exist behind walls that are used to house the cabling. Trenching may be required to run new cabling. The environment inherently raises issues that need to be taken into consideration, such as excessive heat, magnetic fields, and other characteristics of a plant environment. Wireless networking can be used to eliminate these problems.

Wireless networks provide the connectivity required by the existing and new applications, but also allow for some additional benefits. Deploying a wireless network for a particular application allows access even in places where it is impossible to run cables. A wireless network can be designed to be self-healing and redundant so that single points of failure in the network are virtually eliminated. Roaming can be configured so that a mobile worker can traverse the entire plant and never lose connectivity to a centrally managed application.

Strategic site review

As in the case of wired networking deployments, an engineering, or site, survey will need to be performed in order to determine the most efficient placement of wireless networking devices. Typically these studies are considerably less expensive than studies executed for wired networks.

A properly designed and deployed wireless network is fully expandable and has a very short-term return on investment (ROI).

For this reason, IPS uses a team approach to developing wireless solutions. This begins with a strategic review that includes representatives from various functional units to ascertain current, near-term and future needs. It also involves working closely with the facility/corporate IT department to address connectivity and security needs and requirements. Crucial, too, is the RF site survey that not only ascertains current wireless activity at a particular facility, but also RF signal measurements and coverage.

When this has been carried out, IPS engineers are able to generate a low-impact, highly-coordinated, non-disruptive, comprehensive report that includes both strategic alternatives and a recommended action plan.

For example, the report is vendor agnostic, being driven by best practices rather than particular suppliers. It takes a holistic systems approach to security, uses a common wireless infrastructure, and integrates third-party solutions into the total offering. The re-

sult is a proposal for fully engineered solutions aimed at: process optimisation; safety and security; asset performance maintenance; asset management material tracking; condition monitoring; and IT communications.

In addition, IPS experts continually audit technology evolution, vendor strategies, standards bodies, and government regulation and compliance issues. Working with wireless partners such as Aprion, Alvarion and 3eTI ensures that potential customers have the very latest on ION, WiMax and Wi-Fi technologies respectively.

Myths and facts

The catch-all term 'wi-fi' refers to the protocols contained in the 802.11a, b, and g standards, which represent wireless technologies typically deployed in the home, office, and plant environment. Beware of sales hype: it is a myth that the a and g standards operate at 54Mbps but on different frequencies. 802.11b and 802.11g utilise the same wireless frequency range (2.4GHz), but offer different speeds. 802.11g is significantly faster, providing a data rate of 54 Mbps, while 802.11b provides 11 Mbps.

From a distance perspective, wi-fi can be classified into indoor and fixed outdoor wireless. Distances of up to 25 km can be achieved with fixed outdoor wireless using either 2.4 or 5-GHz frequency by choosing a high-gain antenna (provided there is line of sight). In indoor applications, fixed outdoor wireless offers a distance up to 100 metres; however, interior building materials reduce the signal work efficiency from 30-50 metres between devices.

Another drawback for these tech-

nologies is that a number of other devices, such as cordless telephones and microwave ovens, also utilise the 2.4-GHz band. A properly conducted site survey will determine these points of contention and will assure that they are alleviated in the final design and deployment.

802.11a, on the other hand, utilises the 5-GHz band, providing speeds up to 54 Mbps. The advantage of using this protocol is that, since few devices utilise the 5-GHz band, interference or signal contention is virtually non-existent. Also, while 802.11b and 802.11g are compatible with each other, 802.11a is not compatible with either, so once again, there are few devices competing for this frequency. Note that 802.11n, the multi-in multi-out standard, has yet to be ratified. Finally there is the 802.11y standard, but this is only in use in the US at the moment.

Security issue

Wireless security is another hotbed for myths. For example, it is a myth that wireless networks are easily hacked. If implemented properly they are also very secure against jamming, too. It is a fact that wireless networks could be insecure, but an attack would require in-depth knowledge and some very expensive equipment. It is also a fact that security measures do slow down wireless speeds.

Now let us look at the security standards. Wireless equivalent privacy (WEP) is intended to provide confidentiality. However, it has several serious weaknesses, not least that it can be cracked within minutes using readily-available software. WEP2 is a stop-gap enhancement designed

to overcome this, and has the added advantage of being implementable on equipment that is not able to handle wi-fi protected access (WPA) or WPA2.

For its part, WPA was established as an intermediate measure during the preparation of 802.11i. Its password or pass phrase must be great than 6-8 characters to ensure full security. WPA2 goes to the next level, implementing the now mandatory requirements of 802.11i. Importantly, WPA2 also introduces AES-based 'counter mode with cipher block chaining message authentication code' (CCMP) algorithm. CCMP is now mandatory for all new devices.

Then there is WPA2 PSK, or pre-shared key mode. This ideal for homes and small offices and requires each user to enter a pass phrase before access is possible. Such phrases can use 8-63 printable ASCII characters or 64 Hex. Bear in mind, however, that a weak pass phrase equals weak security.

Finally there is the extensible authentication protocol (EAP) under WPA and WPA2. This is a universal authentication framework that employs a number of authentication protocols and also implements a four-way handshake. Here, the AP sends a nonce-value to the client who now has all the attributes to construct the pairwise master key (PMK). The client sends its own nonce-value to the AP, together with a message identity code (MIC). The AP sends the group temporal key (GTK) and a sequence number with a MIC. The client then sends confirmation and as soon as the

PTK is obtained, it is divided into five separate keys.

In real life

One IPS client needed to constantly monitor the temperature profile on a steam pipe in order to reduce condensation and prevent damage that could have run into millions of Dollars. A wired solution proved to be logistically unfeasible, so a wireless solution was successfully implemented.

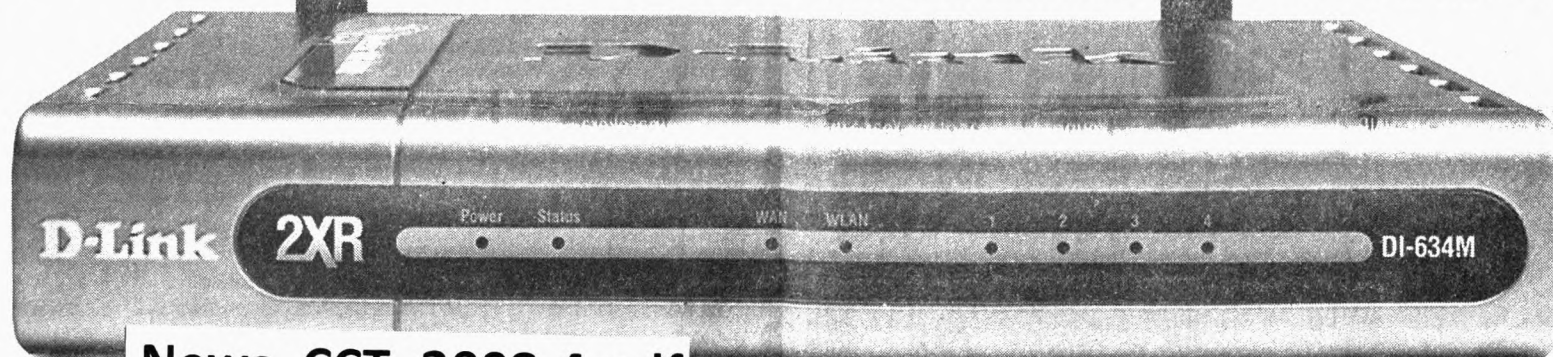
Another client was keen to boost perimeter security with the addition of motion detection, video and other sensors. Because of the terrain around the site and the prohibitive cost of a wired solution, a wireless network was implemented.

In another project, IPS helped a client meet Occupational Safety and Health Administration (OSHA) recommendations that there should be activation notification whenever a safety shower is in use. The task of installing activation sensors on over 1000 showers and integrating them with emergency services proved an ideal use of wireless technology.

Although many myths still surround the use of wireless technology, it is becoming increasingly accepted by many industries around the world. As a result, IPS has already successfully implemented wireless projects for a diverse range of companies, including: Ontario Power, Petro Canada, Husky Energy, PPG, Tate & Lyle, Bowater, Texas Utilities, Florida Power, 3M, Huntsman and Orlando Utilities - to name but a few.

Today potential applications of wireless technology include such broad-ranging applications as personnel tracking/locating, field operator efficiency, field maintenance efficiency and plant security. Add to this a host of others - including process management, safety event monitoring, leak detection, key performance measurements and disaster recovery - and it's not hard to see why wireless is becoming the technology of choice for an increasing number of companies.

Gary Williams is Principal Consultant Wireless EMEA Enterprise Networks & Security Services with Invensys Process Systems (IPS).



News_CCT_2008-4.pdf

National Digitization Project

National Science Foundation

Institute : INSTITUTION OF ENGINEERS, SRI LANKA (IESL)

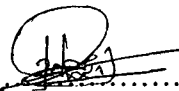
1. Place of Scanning : INSTITUTION OF ENGINEERS, SRI LANKA (IESL)

2. Date Scanned : 2017 / 09 / 26

3. Name of Digitizing Company : Sanje (Private) Ltd, No 435/16, Kottawa Rd,
Hokandara North, Arangala, Hokandara

4. Scanning Officer

Name : D. P. N. Senaviratna

Signature : 

Certification of Scanning

I hereby certify that the scanning of this document was carried out under my supervision, according to the norms and standards of digital scanning accurately, also keeping with the originality of the original document to be accepted in a court of law.

Certifying Officer

Designation : LIBRARY STAFF

Name : MR. NISHANTHA HETTIARACHCHI

Signature : 

Date : 26 / 09 / 2017

"This document/publication was digitized under National Digitization Project of the National Science Foundation, Sri Lanka"