

Wireless IP

Surveillance for the masses

Roy Alves, country manager,
Axis Communications SA

From Bluetooth, to Wi-Fi, to WiMax, wireless technologies have become everyone's preferred means of transmitting data. When it comes to monitoring and surveillance, though, the best way to harness the power of wireless connectivity is with wireless IP surveillance systems.

Unlike most wireless technologies that traditionally come at a premium price, wireless IP surveillance systems are highly flexible and scalable, allowing users the freedom to design a system that is perfect for their needs and budget. This makes wireless surveillance suitable for a wide array of environments, including, but not limited to, small businesses, factory plants, university campuses, or even mining sites.

HOW IT WORKS

IP surveillance cameras (network cameras) convert images into data packets that can be easily transmitted over the Internet. The wireless cameras positioned at the different locations are then connected to wireless bridges or subscriber units, which send the data back to the wireless Base Station Unit, which is located at an organisation's command and control centre.

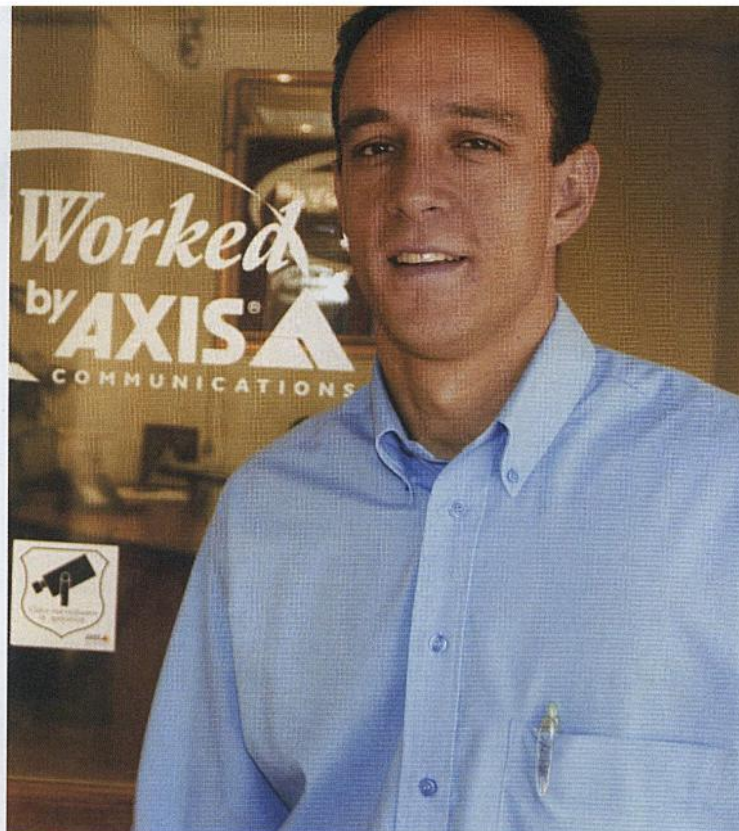
With high-performance point-to-point solutions, the range between the camera and the command centre could be up to 60 kilometres, which is almost ten times the maximum length to which Ethernet cables can be laid. With wireless network cameras all that is needed at the camera level is a power source.

WHY USE WIRELESS IP SURVEILLANCE?

Wireless IP surveillance systems are fast and easy to deploy. They do not require any disruptive and time-consuming excavations. Furthermore, they are well suited to cover large surveillance areas, because the cameras can be placed at a considerable distance from the control centre, without the need for a lot of cabling that can cost a company tens of thousands of rands.

The wireless environment also makes it very easy to up-scale the system. Additional wireless IP cameras can be added, without the need to run any Ethernet cables at all. To optimise the system, cameras can also be moved around with ease to ensure that the best possible coverage is received.

Over and above these, wireless IP systems come with the other advantages that are inherent in IP surveillance systems, like remote monitoring from anywhere where there is Internet connectivity, intelligent cameras and superior image quality.



Roy Alves... with wireless network cameras all that is needed at the camera level is a power source.

IS IT SAFE?

The idea of transmitting classified information over the Internet has always had its sceptics, and the same applies to wireless IP surveillance. Questions have been asked about how safe it is to run an entire surveillance network on the Internet.

The Internet has on many occasions proved itself to be a very reliable medium for transmitting even the most sensitive of information. Proof of this is the popularity of applications such as Internet banking and trading. Companies involved in these industries apply the most stringent security policies to ensure that they and their customers do not fall victim to Internet fraud.

To ensure that the wireless IP surveillance system is also protected from criminals or any other unsolicited visitors, there are several solutions that are available to system administrators. The most basic of these are firewalls and password protection.

Firewalls are either software- or hardware-based. They act as electronic gates to prevent unauthorised entry into a network. In addition to firewalls, administrators can also introduce password protection into the system. This ensures that the system is not only protected from external threats, but also from users who have legitimate access to the network, but are restricted from accessing certain files.

There is also encryption, a technique that requires that the same make of equipment be used on both the sender's and the receiver's sides, in order to decode the data. Data coding is another security feature that can be introduced into wireless IP surveillance systems. This means that potential intruders would have to obtain a unique transmission code set by the system administrator in order to decode the data.

In stark contrast, analogue systems do not allow for any data encryption whatsoever, making it very easy for anyone to tap into the system and view what is supposed to be secure, privileged, video data. ■