Memex Automation Inc.
3425 Harvester Rd., Suite 200
Burlington, Ontario L7N 3N1 Canada,
www.memex.ca

TECHNOTE: Wireless Ethernet Communications

Memex has been asked for deployment of our Ax9150 or Mx1053 machine interface using wireless technology. In response to such requests Memex cautions such deployment given the following trends in the wireless industry and fundamental deficiencies based on environmental issues.

Wireless Deployment and Security Issues:

One issue with corporate wireless networks in general, and WLANs in particular, involves the need for security. Many early access points could not discern whether or not a particular user had authorization to access the network. Although this problem reflects issues that have long troubled many types of wired networks (it has been possible in the past for individuals to plug computers into randomly available Ethernet jacks and get access to a local network), this did not usually pose a significant problem, since many organizations had reasonably good physical security. However, the fact that radio signals bleed outside of buildings and across property lines makes physical security largely irrelevant to Piggybackers (reference: http://en.wikipedia.org/wiki/Wireless_LAN_security)
There are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge. (http://en.wikipedia.org/wiki/Wireless_security)

(http://www.networkcomputing.com/data-networking-management/gartner-misconfigured-aps-cause-most-wlan-breaches.php)

Today all (or almost all) access points incorporate Wired Equivalent Privacy (WEP) encryption and most wireless routers are sold with WEP turned on. However, security analysts have criticized WEP's inadequacies, and the U.S. FBI has demonstrated the ability to break WEP protection in only three minutes using tools available to the general public. Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. (see aircrack http://www.aircrack-ng.org/).

Growing Environmental Concerns over the use of Wireless Technology:

A wireless local area network (WLAN) links two or more devices using a wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.
Over the last few years there has been a growing concern as to potential health issues around the deployment and use of wireless technology. Citing the possibility of health risks associated with the usage of WiFi networks, Lakehead University President Fred Gilbert refuses to sign off on their campus-wide installation. Noting a California Public Utilities Commission study which said that the possible risk of tumors and other diseases due to exposure to electromagnetic fields (EMFs) needs to be further investigated, Gilbert says he's going to hold off on the installation of a campus-wide WiFi network.(http://arstechnica.com/old/content/2006/02/6235.ars other published information: http://www.wireless-center.net/Mobile-and-Wireless/1673.html , http://www.emfsolutions.ca/?gclid=CJT_54nAoaYCFUdrKgodTma9oA)

Environmental Barriers to WLAN Deployment:

WLAN deployment and use are susceptible to environmental conditions within the plant. All steel construction, metal ductwork, high voltage lighting or high ceilings can cause exposed node problems (http://en.wikipedia.org/wiki/Exposed_terminal_problem) and access point over attenuation.
In some instances electrostatic noise from machine tools and EDM machines can render segments of a WLAN inoperative or intermittently error prone in data transmission.

Conclusion:

Even though the deployment of a wireless topology may be inviting by providing a fast method of Ethernet connectivity, the potential risks must be weighed against the perceived benefits. Wireless technology is a rapidly evolving technology where protocols are changing and being obsoleted. Investment in a wireless topology may in fact be a detriment to a facility given security issues, exposure to health issues and their potential for litigation and the outright unreliability of such a topology under certain conditions. The deployment of wireless technology in an office building may be acceptable; however, a factory environment deployment should be approached cautiously.