Wireless Technology Heightens Manufacturer Security Risk

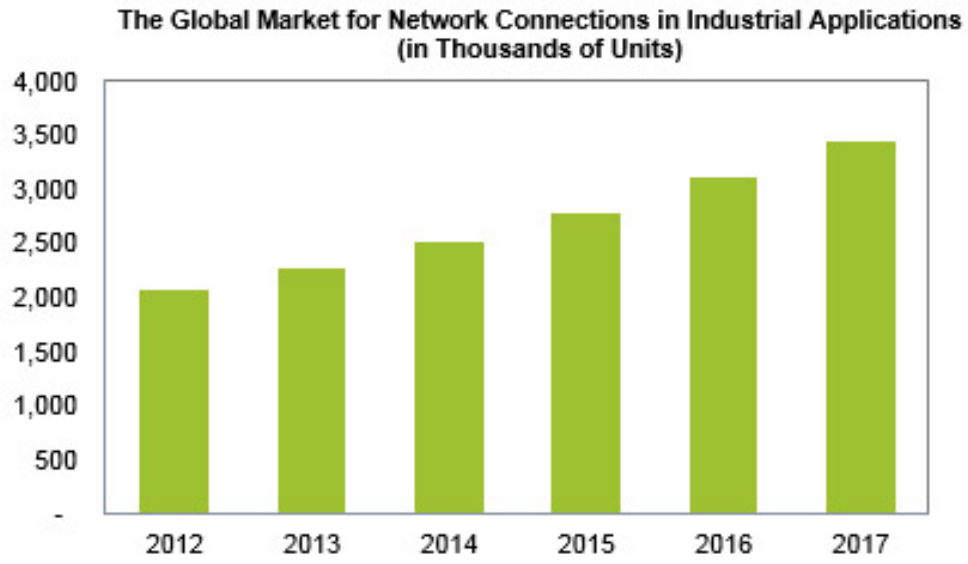
IHS Technology

Increasing networking of manufacturing equipment is opening up factories to the benefits of flexible production and wireless mobile communications. However, the rising use of connected devices is also exposing production sites to security breaches and cyber-attacks, compelling companies to seek ways to protect their networks.

Wireless network connections in industrial automation components in global factories will rise from 2.1 million in 2012 to 3.4 million by 2017. This increase magnifies risk factors to manufacturing environments.

	2012	2013	2014	2015	2016	2017
Thousands of Units	2,067	2,265	2,509	2,784	3,103	3,445

Source: IHS Technology February 2014



Source: IHS Technology February 2014

Do the worm

The issue of security in manufacturing networks became front-page news in 2010, when the Stuxnet computer worm afflicted industrial control systems in Iran. Stuxnet was designed to both subvert and engage in the surveillance of supervisory control and data acquisition systems made by Siemens.

While Stuxnet is thought be an intelligence tool, other types of malware are designed simply to infect and cause damage to manufacturing systems. In some cases, hackers have engaged in blackmailing the manufacturing operations of companies, demanding a ransom in order to lift the malware from their systems.

Mobile malady and catching flies

The rising use of wireless networks and industrial Ethernet is leading to a growing trend in the so-called bring-your-own-device (BYOD [1]) movement in the manufacturing business, with workers utilizing their own smartphones and tablets to monitor and control industrial equipment. However, such devices may lack adequate security, offering hackers easy access to confidential data—or allowing them to spread malware through factory automation systems.

To counter this threat, manufacturing operations are taking cyber-security measures. Among these is the “honeypot,” a site that masquerades as a manufacturing network but is actually an isolated system designed to divert and gather information about hackers.

Wireless technology proliferates

Manufacturing networks continue to adopt a wide variety of wireless technologies.

For instance, wireless LAN (WLAN) was the most widely adopted protocol in the industrial space. The technology is highly suitable for many applications because of its advances in the enterprise and consumer sectors, allowing knowledge and technology to filter into industrial applications.

Bluetooth is another protocol extensively used in the consumer space that is also popular for industrial automation networking. Bluetooth’s advantage lies in its capability to pair devices, providing greater security and reducing the potential for opportunistic hacking attacks.

WirelessHART and ISA 100.11a are the two major “true” industrial wireless technologies. They compete directly and are more prevalent in process industries compared to WLAN and Bluetooth, which are more commonly used in discrete industries.

Industry goes wireless

The current level of adoption of wireless in factory and process environments is low.

Nonetheless, the technology's presence is expanding, bringing both benefits—as well as increased risks from hackers—to the manufacturing market.

Mark Watson, associate director of the industrial automation group at IHS Technology [2], manages a team of analysts producing highly detailed annual market statistics on industrial PCs, operator terminals, machine vision, embedded computer boards and modules, discrete machine safety components and all types of industrial communication (Fieldbus, Industrial Ethernet and Wireless).

Links:
[1] http://www.chem.info/articles/2013/10/risks-and-benefits-bring-your-own-device-part-1#.UvUx-PldUVw
[2] https://technology.ihs.com/