Rise of Wireless Technology Poses Security Risks for Manufacturers

Release Date:
Monday, February 3, 2014 9:00 am EST

Terms:
Design & Supply Chain Media  Product Design  Supply Chain  Technology

Dateline City:
EL SEGUNDO, Calif.

Contacts:
IHS Media Relations

Rise of Wireless Technology Poses Security Risks for Manufacturers

EL SEGUNDO, Calif. (Feb. 3, 2014)—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, according to a new white paper from IHS Technology (NYSE: IHS).

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

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) movement in the manufacturing business, with workers utilizing their own smartphones and tablets to monitor and control industrial equipment,” said Mark Watson, associate director, industrial automation group at IHS. “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.

Learn more about this topic with the new IHS white paper, entitled: “Industrial Automation Sector Trends in 2014.”

---

**About IHS** ([www.ihs.com](http://www.ihs.com))

IHS (NYSE: IHS) is the leading source of information, insight and analytics in critical areas that shape today's business landscape. Businesses and governments in more than 165 countries around the globe rely on the comprehensive content, expert independent analysis and flexible delivery methods of IHS to make high-impact decisions and develop strategies with speed and confidence. IHS has been in business since 1959 and became a publicly traded company on the New York Stock Exchange in 2005. Headquartered in Englewood, Colorado, USA, IHS is committed to sustainable, profitable growth and employs approximately 8,000 people in 31 countries around the world.

*IHS is a registered trademark of IHS Inc. All other company and product names may be trademarks of their respective owners. Copyright © 2014 IHS Inc. All rights reserved.*

---

**Language:**

English