Over the last several years, the use of wireless networks in control systems has yielded a number of benefits to critical infrastructure while revolutionizing operations in key areas of industry, such as energy and transportation. Apart from the benefits of eliminating signal and power wiring, wireless sensor networks can enable measurement applications in sites that are hard to access, or where the wiring cost cannot be justified. They are also invaluable for modernizing existing legacy facilities, for temporary installations, or for locations where a power source is not available. However, the practical implementation of wireless technology in industrial settings has faced a number of challenges, not least of which is the adoption of industry security standards.

The increased transmission of plant data through networks has given rise to ominous cyber attacks that threaten networks, businesses, and end-user devices alike. Wireless sensor networks (WSN) are currently receiving the most industry attention focused on such areas as condition monitoring, process control, wireless instrumentation, and measurements. One of the greatest inhibitors to the adoption of WSN in the private sector is the concern for security in critical industrial applications. While significant advances have been made in topology management, routing algorithms, and sensor data management, lingering concerns remain that WSNs are inherently untrustworthy.

Integrating wireless into legacy networks designed for and deployed in enterprise environments provides increased flexibility and ease of use, but the need for security on the physical and network levels—and even the protocols built atop it (i.e., ISA100, WirelessHART, and 6LowPAN) — reflects the heightened stakes when these networks are deployed for critical operations in industrial settings.

Today, most general-purpose operational systems incorporate ISA-adopted security concepts. However, there is no guarantee that a supplier selling commercial-off-the-shelf Fast Forward

- Industrial control systems are increasingly under attack
- Basic wireless security is inadequate
- Proven government solutions increase

Government-validated technologies can be used to achieve greater cybersecurity

Leveraging DoD wireless security standards for automation and control

By Thurston Brooks

Wireless advantages in industrial applications.
Forty percent of those attacks were deemed serious. Systems were hit with 198 "documented" threats, 60% of which were cyber attacks. 40% of these attacks were on critical infrastructure regarding the true nature of security lies in how it is implemented. 15% of the 80 threat vectors were cyber threats.

Industrial control systems: under attack

Although recent cyber-attacks on The New York Times, Twitter, and major U.S. banks have received disproportionate media attention, industrial control systems have increasingly become a target of choice for attackers, who have specifically sought to disrupt and damage industrial control systems and their integrated wired and wireless networks. "Alarms of possible risks to critical infrastructure operations released by the Industrial Control Systems (ICS) and Cyber Emergency Response Team (CERT) are up 50 percent from a year ago," said Earl Perkins, research vice president in systems, security, and risk at Garnter. In fact, a Department of Homeland Security (DHS) report released in January revealed that industrial control systems were hit with 198 "documented" cyber attacks in 2012 and that many of these attacks were deemed serious. Forty percent of those attacks were on energy firms, according to ISC-CERT, which reviewed every incident. Water utilities came in second, with 15 percent.

The meteoric rise in successful cyber attacks demonstrates that attackers can not only disrupt, compromise, and control networks but also the automation and control systems that are linked to them. Defense Secretary Leon Panetta pointed to cyber attacks in a recent policy announcement, noting that they mark "a significant escalation" in cyber warfare. Many of these threats can be effectively counteracted by private industry through the use of military-grade, COTS security processes in their industrial control systems.

ISA100 security by design

In the industrial automation and control world, insecure devices, such as access points and user stations, can seriously compromise both wireless networks and wired networks. Hackers deliberately target insecure devices, and the challenges of securing such devices are magnified by the fact that they need to operate 24 hours a day, without interruption, for long periods of time. Systems are designed to operate at multiple layers, and even if control computers backed up by local controllers that are, in turn, backed up by safety shutdown systems.

A major step in adopting good security lies in how it is implemented. ISA100 incorporates basic "security by design," a concept that incorporates security at every stage of network design, construction, and operations. Successful security by design results in a "more robust" security infrastructure that minimizes insider access to materials and opportunities for risks (i.e., people) associated with malicious acts (i.e., processes) and their potential to manipulate the system in unanticipated ways.

The national cybersecurity strategy sets forth for federal organizations by the National Institute of Standards and Technology (NIST). Once tested and certified, products can then be listed in the DoD Portfolio. This list can be used by government agencies to identify and purchase secure and certified products. Today’s DoD standards can act as an important role model to encourage industry to develop and implement solutions that are independently tested and certified for compliance.

Today’s DoD standards can act as an important role model to encourage industry to develop and implement solutions that are independently tested and certified for compliance.
quick to recognize the cost and time benefits of integrating advanced wireless solutions into its existing network infrastructure. For example, wireless integration could accommodate a variety of topologies and meet the needs of specific applications while increasing productivity and providing a path toward lower operational costs. However, the DoD’s stringent security requirements limited the Navy to those solutions that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption and Common Criteria certifications that offered FIPS 140-2 validated encryption. The AirGuard iMesh wireless network technology, that are ISA100-compliant for industrial sensor networking based on security that is independently validated, approved, and deployed by the U.S. military. Designed for lower power and flexible integration, these devices form a cyber-secure bridge linking ISA100 sensors nodes with 802.11 Wi-Fi and Ethernet networks for sensor applications, including oil refineries, utilities, factories, electrical power substations, and processing plants to interface a variety of sensors (pressure, temperature, vibration, etc.) to remote network locations. The resulting wireless mesh network enables system operators to improve regulatory compliance while achieving greater visibility over system operations with configurable sensor sampling and reporting. The Navy is now deploying two systems, which utilize wired and secure wireless mesh technology. The first system is the Enterprise Industrial Controls System (EICS) – an advanced, cyber-secure, wired and wireless sensor networking system that integrates disparate industrial control systems across several Navy bases into a centralized facility operations center. The second system, the Virtual Perimeter Monitoring System (VPMS), is a wired and secure wireless critical infrastructure protection and perimeter monitoring solution. Leveraging a robust, integrated network enabled through the use of secure wireless technology, the Navy is moving to control energy to achieve cost savings and efficiencies, secure critical infrastructure operations, and enhance situational awareness. More than 5,000 secure wireless devices are being installed to network sensor systems on DoD installations. They will measure energy usage and energy allocation while enabling real-time energy resource management to reduce energy consumption at the building level while complying with the Energy Policy Act of 2005 and the Energy Independence and Security Act of 2007.

Summary

The military is realizing the benefits of deploying integrated systems that leverage secure wireless technology. These benefits range from obvious cost reductions brought about by the elimination of wiring to better plant productivity, improved asset management, and strong data reporting. The success achieved while complying with the DoD’s restrictive security requirements demonstrates that secure wireless technology can be adopted by operators of critical systems looking to implement more robust, secure, reliable, cost-effective systems. In the absence of any commercial or federal cybersecurity standards or requirements, the industrial sector has looked to the military for an example of best practices and security requirements. Although integrated networks provide undeniable benefits, some critical infrastructure operators are still in denial about cyber threats targeting, disrupting and/or damaging industrial control systems. Recent threats such as Stuxnet and Flame have powerfully demonstrated that once-theoretical threats have now become a reality; cyber attacks that threaten to penetrate and sabotage critical control and monitoring systems continue to generate serious consequences.

Many of these threats can be effectively countered and defended against with changes to key security processes and organization. Cyber warfare is not just a threat for the future – it is a very real threat today, forcing an increased need for robust security to ensure the continued operation and protection of critical control and monitoring systems worldwide. The time to future-proof plant control systems is now, and the DoD approaches described in this article should pave the way for broader industrial adoption of secure wireless networks.

ABOUT THE AUTHOR

Thurston Brooks, vice president of product marketing, Ultra Electronics, 3eTI, is focused on developing new technologies and solutions for industrial and commercial applications for the protection of critical infrastructure. He has more than 30 years of professional experience in developing and managing a wide variety of solutions for military and industrial applications and holds engineering degrees from the University of Florida (B.S.), the Massachusetts Institute of Technology (M.S.), with a thesis in human-machine systems and controls, and the University of Chicago (M.B.A.). He contributed as a key member of the IEEENIST Committee on Smart Sensors (IEEE 1451). Brooks has authored more than 45 publications in referred journals, symposiums, and conferences, and holds two patents. One patented product won the 1993 Star Tech Award for Best New Product in Washington Technology magazine.

View the online version at www.isa.org/intech/20130401