By Thurston Brooks

Leveraging DoD wireless security standards for automation and control

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

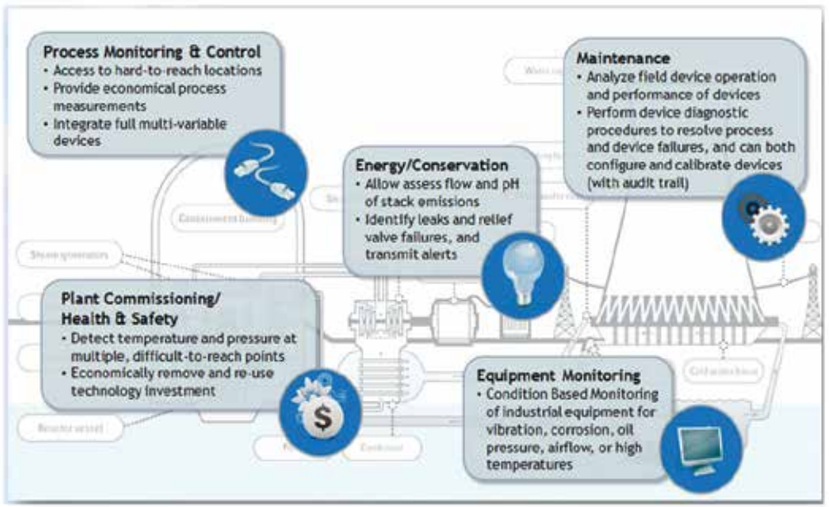
Government-validated technologies can be used to achieve greater cybersecurity

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

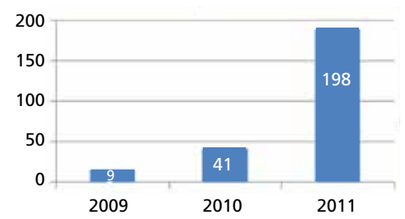


Wireless advantages in industrial applications.

(COTS) products has implemented security correctly. To overcome lingering security concerns about the use of wireless networks in critical industrial operations, facility managers are increasingly looking to the government for guidance on deploying secure networks more effectively. Government agencies require a minimum level of assurance that a product's stated security claim for protecting sensitive data is valid. Today, the government develops and implements networks using proven security standards, such as independently tested and certified-for-compliance solutions to ensure industrial applications and critical data are sufficiently protected.

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 wireless networks. "Alerts of possible risks to critical infrastructure operations released by the Industrial Control Systems (ICS) and Cyber Emergency Response Team (CERT) are up



ICS-CERT incident response trend data.

50 percent from a year ago," said Earl Perkins, research vice president in systems, security, and risk at Gartner.

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 of the attacks focused on them.

The meteoric rise in successful cyber attacks demonstrates that attackers can not only disrupt communication 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, using specialized tools to break encryption and authentication. Since most wireless networks connect back to a wired network at some point, hackers can use any unsecure wireless station as a launch pad to breach a network.

ISA99 is the Industrial Automation and Control System Security Committee of the International Society of Automation (ISA). The purpose of the ISA99 committee is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices.

Today, many plant operation systems have adopted ISA99 security protocols, although it is not mandatory. Unfortunately, Gartner's Earl Perkins has found that, "there is denial in some portions of industries with critical infrastructure regarding the true threat," referencing "cyber threats" damaging and disrupting industrial control systems in the recent ICS-CERT report. The first step in embracing the ISA99 protocols is simple recognition that cybersecurity is not an irrelevance or distraction, but rather must become an integral component of planning and acquisition from the outset.

ISA99 provides additional focus to improve the confidentiality, integrity, and availability of components or systems used for industrial automation and control and to provide criteria for procuring and implementing secure control systems. They endeavor to improve system security and help identify vulnerabilities to address them, thereby reducing the risk of compromising confidential information or causing degradation (or failure) of the equipment or process under control. These three concepts (confidentiality, integrity, and availability) form the basis of businesses' IT security. For enterprise systems, the first priority is confidentiality. Logically, for real-time operational systems used in industrial settings, the priorities are reversed, with availability shifted to top priority – the control system needs to operate 24 hours a day, without interruption, for long periods of time. Systems are designed to operate at multiple levels, with redundant 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 into all aspects 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 risk(s) associated with malicious acts (i.e., sabotage, diversion, etc.), while providing flexibility to respond to a changing threat environment.

Wireless networks created under the ISA-100.11a-2011 standard feature authentication and encryption controlled by a flexible security policy, which can be varied under ISA-100.11a's two-layered security methodology. First, "link layer" security is associated with hop-to-hop authentication and encryption. ISA-100.11a wireless subnets feature multi-hop, mesh-enabled subnets with packets of data being routed over multiple devices to the subnet extraction point. Each router used in this apparatus authenticates and encrypts/decrypts the packet that it routes.

The second layer, or "transport layer," security, is associated with end-to-end authentication and encryption of data messages. Here, the originating device authenticates and encrypts the packet at the transport layer, and only the destination authenticates and decrypts the packet. This is accomplished through sessions that are established between pairs of devices that communicate at the transport layer.

Various levels of authentication and encryption can be enabled for both layers of security, and these levels are inherited from the security policies supported by IEEE 802.15.4 – the underlying wireless technology on which ISA-100.11a is based.

Although ISA100 has security built in by design within the standard, it still needs to be implemented correctly. In effect, improperly implemented security is equivalent to no security at all. Many vendors claim product functionality and/or offer security without any validation or oversight. Knowledge gained from DHS CSSP assessments and ICS-CERT documented daily on their ICS-CERT vulnerability disclosure policy web page proves that the number of product vulnerabilities found in the industrial control sector continues to rise.

Demystifying government-validated solutions

The federal government and Department of Defense (DoD) facilities require resilient networks that assure delivery of critical assets to support our armed forces at home and abroad. Current mandates provide significant incentive for these agencies to build more efficient and resilient systems that consume less energy *and* are protected from disasters, accidents, and attacks.

Government agencies require a minimum level of assurance that a product's stated security claim for protecting sensitive data is valid. Today, federal policy requires government agencies to develop interconnection agreements for federal systems that share or exchange information with external networks. For wireless networks, government agencies require FIPS 140-2 validated encryption to ensure the protection of data in transit. Considered a benchmark for security in government, FIPS validation assures users that a given technology has passed rigorous testing under either the CAVP (cryptographic algorithm validation program) or CMVP (cryptographic module validation program).

Private sector vendors who want to have their products certified for use in government departments (and regulated industries) must complete a rigorous government-validation process in order to meet the security requirements set forth for federal organizations by the National Institute of Standards and Technology (NIST). Once tested and certified, private sector vendors can assure government agencies that all data downloaded to wireless devices is in full compliance with U.S. federal government guidance and policy.

Core components of the ISA99 Security Standards are built from the defense-in-depth (DID) strategy, which was conceived by the National Security Agency (NSA). The DID strategy, largely employed by the U.S. government, is based on implementing multiple layers of security controls (defense) throughout a system. Its intent is to provide redundancy in the event that a security control fails or vulnerability becomes exploited, as a single countermeasure cannot be depended on to mitigate all security issues.

There are also legislative restrictions regarding certain types of technology, such as cryptography, that require federal agencies to use only tested and validated 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. Without independent validation, there is no guarantee that the supplier has subjected their product to sufficiently rigorous testing. Independent validation allows buyers to obtain that assurance and perform necessary product security comparisons.

NSA basic tenets of cyber defense

National Security Agency (NSA) basic tenets of cyber defense-in-depth include:

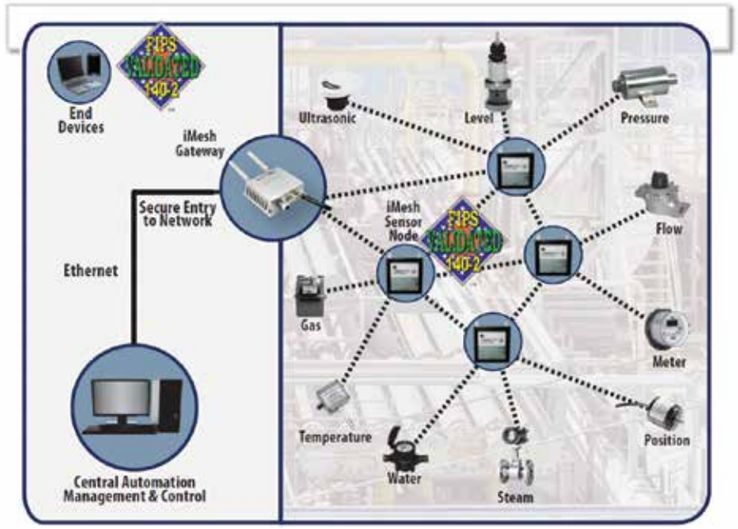
- Know the security risks that an organization faces
- Quantify and qualify risks
- Use key resources to mitigate security risks
- Define each resource's core competency and identify any overlapping areas
- Abide by existing or emerging security standards for specific controls
- Create and customize specific controls that are unique to an organization

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.

Implementing standards-based secure wireless (case study)

In October 2009, the Secretary of the Navy laid out five aggressive energy goals to improve energy security and efficiency, increase energy independence, and help lead the nation toward a clean energy economy. In 2010 the Navy initiated a SmartGrid pilot program comprised of interconnected technologies that could securely, collectively, and intelligently monitor, predict, control, and respond to building and utility management systems.

The need to deploy sensors anywhere in distributed environments requires a tremendous effort, and the DoD was



Implementing a secure wireless infrastructure using validated solutions.

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 certified levels of security.

Although many companies offer wireless solutions, none had robust products that met the DoD's information technology security requirements while providing battery-powered wireless sensor interfaces. The solution had to fully comply with DoD information security requirements, including directives for information assurance (IA) during activities involving data and information interchange. Meeting all these requirements was critical to enabling a successful integration and program rollout. There is a new breed of solutions, such as 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 industrial wireless mesh network enables system operators to improve regulatory compliance while achieving greater visibility over system operations with configurable sensor sampling and reporting.

Secure gateway connects sensors using high-level encryption.

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, ensure 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.

Cyber warfare is not just a threat for the future – it is a very real threat today, forcing an increased need for robust security.

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 IEEE/NIST 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