

Defense in cyberspace

Beating cyber threats that target mesh networks

By Trent Nelson and Jeff Becker

Wireless technology has aroused as much interest as it has skepticism in the industrial control systems industry.

While many recognize the easier installation and reduced costs, others question the reliability and security of wireless networks.

The principle requirement of industrial wireless technology is clear: It must be robust, reliable, cost-effective, and completely secure.

Despite the benefits, the adoption of wireless networks has been gradual in the industry due in part to security concerns.

For industrial facilities, the increased vulnerability of the enterprise resulting from open wireless architectures, coupled with a rise in cyber attacks, has made electronic security a major concern.

We can no longer take for granted the integrity of vital assets, including operational processes, network architectures, and business applications.

The Control Systems Security Program (CSSP) cyber researchers regularly evaluate new and introduced solutions. Their reviews suggest wireless solutions can be as secure as wired solutions, alleviating industry concerns.

Surpassing wired systems

Today, cyber security threats against a site can take different forms and shake out into four categories:

1. Indiscriminant and potentially destructive: This is the most publicized category, malware, which includes viruses, Trojans, and worms attacks.
2. Performance impacts and potential safety issues: Network spoofing and “denial of service” threats have performance implications. For example, a denial-of-service attack can clog a network with spurious requests, keeping an operator from receiving a legitimate alarm, which can result in degraded performance and/or safety issues.
3. Confidentiality: With eavesdropping and password cracking, protecting data from unauthorized use becomes a concern along with safety.
4. Integrity: This includes data tampering, impersonation, and packet modification and is especially hazardous if the intruder has malicious intent.

The idea that a hacker could access data while it is airborne and stop certain operations at the plant causes great concern in the industry. Indeed, industrial manufacturers are becoming

increasingly aware of the threats of industrial espionage and cyber terrorism. However, strong policies and procedures, proven encryption and authentication strategies, and proper wireless system design can guarantee a level of security at least equaling, or even surpassing, wired systems.

Beating the hackers back

Industrial control systems employing wireless technology are subject to increasing cyber attacks from inside and outside the network infrastructure. Automation suppliers must recognize the risk to wireless network security and understand how attackers can use wireless vulnerabilities to their advantage.

Cyber threats to an industrial control system can come from within an organization by trusted users or from remote locations by unknown persons using the Internet. Attacks also can come from hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber barrier around the system infrastructure.

Since the radio frequency medium is susceptible to eavesdropping and spoofing, care is paramount to ensure the wireless network is no less secure than traditional wired networks. To combat these inherent vulnerabilities, wireless networks must have strong encryption and authentication technology, coupled with robust implementations and management. Security must be integral to the system design, and not an afterthought.

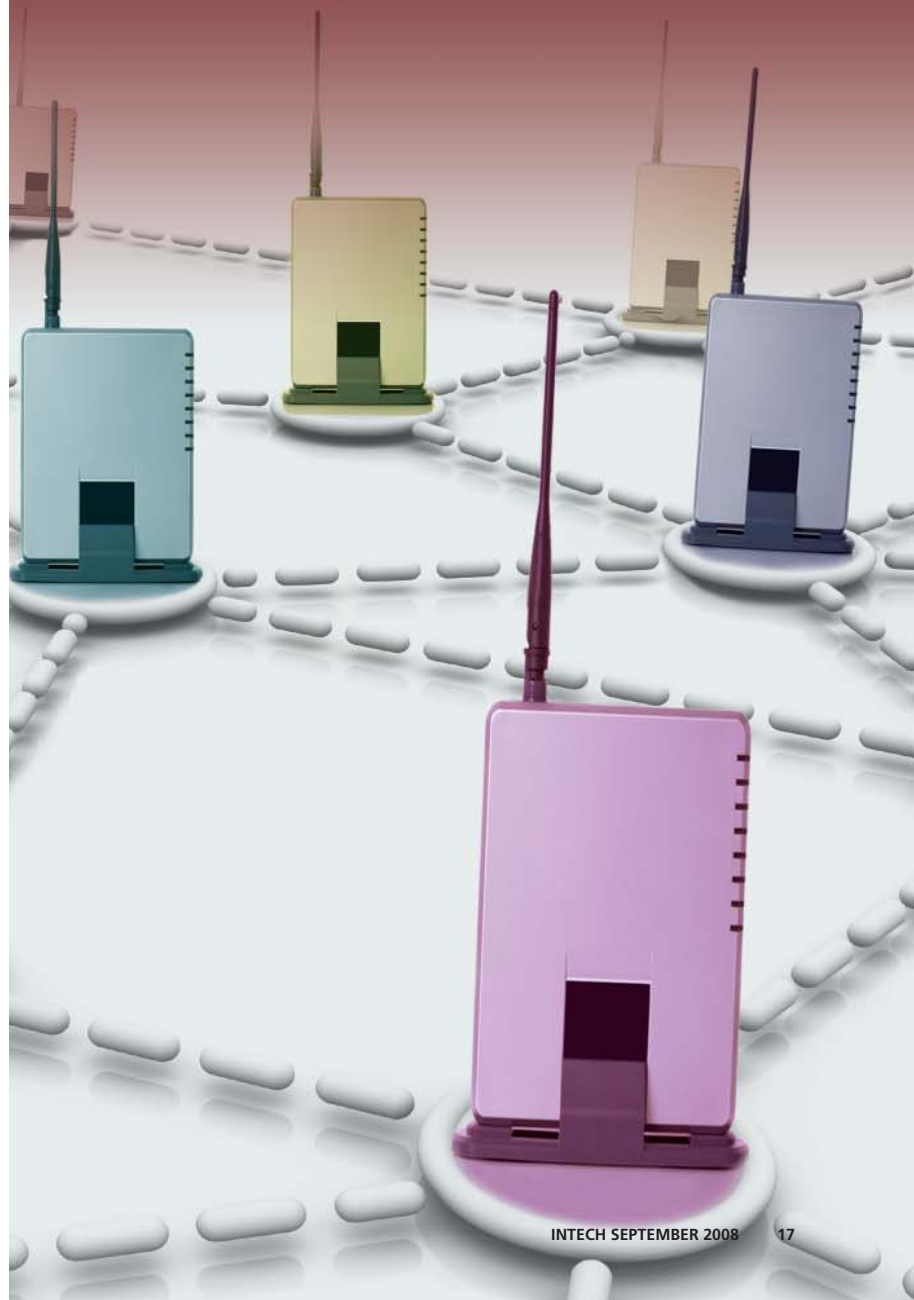
For example, the security layer design must accommodate multiple security levels to satisfy various industry requirements. An application that requires a more stringent security necessitates more capable systems, including nodes of potentially higher cost or installation inconvenience.

The security layer must be general enough to meet the needs of multiple applications and the underlying network layers. It must support both sensor-to-control system and node-to-node communications, directly or through intermediaries. For industrial control systems, all of the communications paradigms of common field I/O protocols should also be supportable.

The best security is in layers, with protection that ensures a single security breach does not compromise the entire system through cascading attacks. The integrity of the security layer should not require that individual nodes will not go down, but should ensure the compromise of

FAST FORWARD

- The idea that a hacker could access data while it is airborne is troublesome.
- Automation suppliers must recognize the risk to wireless network security.
- Automation suppliers and government cyber security specialists are making strides in industrial control system security.



a single node does not compromise the data confidentiality or message integrity of communications sessions of which the compromised node is not a part.

Specific requirements for the network security layer are here.

Data confidentiality Application information exchanged through the network may be sensitive, and the network must protect that information against eavesdropping. To insure a compromise of a network element does not compromise confidentiality, end-to-end encryption is a necessity. The encryptions algorithms should be well known and tested, of appropriate key length, and have the ability to accept re-keying as necessary. The current

It is important the authentication mechanism be cryptographically secure, using unique and time-sensitive keys.

recommended practice is to use 128-bit AES encryption for all over-the-air communications.

Entity authentication (device trust establishment): Before one node communicates with another, the devices need to authenticate themselves to each other. Entity authentication is the process by which one entity is certain of the identity of a second entity. This prevents unauthorized devices from entering the network. It is important the authentication mechanism be cryptographically secure, using unique and time-sensitive keys. The current recommended practice is to pass unique, time-sensitive, one-time-use cryptographically secure keys through an out-of-band mechanism (such as Infrared transmission) in a manner that does not expose the key to human operations.

Message integrity and sender authentication: Data integrity establishes fault processes, such as noise or random error, have not altered a message between transmission and reception. Message

Mesh is reliable, redundant, algorithm driven

A wireless mesh network is a communications system that uses radio nodes organized in a mesh topology.

The coverage area of the radio nodes is akin to a mesh cloud that operates as a single network. The radio nodes in this cloud work together to create a radio network.

A mesh network is reliable, and it has redundancy. When one node does not work, the rest of the nodes can still communicate with each other either directly or through one and or more intermediate nodes.

Mesh networks are good solutions for diverse communication needs and difficult environments, such as emergency situations, tunnels, oilrigs, battlefield surveillance, high-speed mobile video applications on board public transport, real-time racing car telemetry, and in industrial automation applications.

The principle of a mesh network is similar to the way packets travel around the wired Internet. Data hops from one device to another until it reaches its destination.

Dynamic routing algorithms in each device allow this to happen. To implement such dynamic routing protocols, each device needs to communicate routing information to other devices in the network.

Each device then determines what to do with the data it receives whether it is to pass it on to the next device or hold onto it.

The routing algorithm makes sure the data takes the most efficacious path to keep the process stable and productive. There are numerous competing schemes for routing packets across mesh networks.

The ISA100 standard, Wireless Systems for Industrial Automation, is at work establishing standards for implementing wireless systems in the automation and control environment with focus on the field level.

The IEEE is developing a set of standards under the title 802.11s to define an architecture and protocol for ESS (Extended Service Set) Mesh Networking.

authentication establishes an attacker has not maliciously fabricated or altered a message. Sender authentication establishes a message originated from a limited set of authorized senders. Together, these features substantiate that received messages are not corrupt and are from an authorized sender. This is essential, as compromised data could lead to invalid computation. Moreover, bandwidth and radio transmit energy should be minimized by not reacting to forged messages or denial of service attacks from unauthorized sources.

Fault tolerance over the lossy channel: The low-rate wireless network used by sensors is lossy, as there is a likelihood of interference. The security layer must adapt to loss of packets, detect loss of

synchronization, and provide a mechanism for re-synchronizing the session endpoints.

Data freshness: General data freshness is not a security layer goal. However, the security layer must protect against replay attacks.

Low packet overhead: For efficient use of bandwidth and battery power, the amount of "overhead" data the security layer adds to the focal transmitted/received data should be as little as possible.

Key escrow: Long-term key escrow may be required to satisfy regulatory requirements or because of customer corporate policy. Using the key escrow mechanism for backup of keying material to support failure recovery is



We're the government; we're here to help

The goal of the Department of Homeland Security National Cyber Security Division's Control System Security Program (CSSP) is to reduce control system risks within and across all critical infrastructure sectors by coordinating efforts among federal, state, local, and tribal governments, as well as control systems owners, operators, and vendors.

The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

These risk-mitigation activities have resulted in these tools:

- Catalog of Control Systems Security: Recommendations for Standards Developers
- Control System Cyber Security Self-Assessment Tool (CS2SAT)
- CSSP Documents
- Critical Infrastructure and Control Systems Security Curriculum
- Cyber Security Procurement Language for Control Systems
- Recommended Practices
- Training

The ISA Automation Standards Compliance Institute is a licensed distributor of the CS2SAT.

This application, created by the CSSP for the Department of Homeland Security National Cyber Security Division, assists SCADA and Process Control System users in improving the cyber security posture of their control systems.



possible. Supporting remote key escrow is necessary.

Firmware updates: Nodes may require firmware updates to repair software flaws or to add new features. Protecting nodes so they do not accept corrupted firmware or firmware from an unauthorized source is necessary.

FIPS 140-2 compliance: Cryptographic modules should be FIPS 140-2 compliant during operation. Nodes should be of such design that we may classify them as "single chip cryptographic modules." Achieving this rating requires, among other things, keys are encrypted whenever off-chip—in other words, keys are never exposed "in the clear" off-chip. There must also be no easy way to read out the chip's data (e.g., disable debugging ports).

Availability: Availability means ensuring the services offered by the secured nodes will be available to legitimate users when expected. Attacks on availability are Denial of Service (DoS) attacks. The security protocol should attempt to ensure the wireless network is not a force multiplier for the adversary,

meaning the magnitude of the attack does not become greater by retransmission through the network. The security layer design should also include features to mitigate battery exhaustion

In response to growing cyber security threats, the U.S. Department of Homeland Security, National Cyber Security Division, created CSSP.

(sleep deprivation) attacks and flash memory wear-out attacks.

Protection against traffic analysis: Traffic analysis is a method of inferring node identities, node functions, and probable system states from observation of the timing, lengths, and unencrypted portions of messages.

This is only a test

In response to growing cyber security threats, the U.S. Department of Homeland Security (DHS), National Cyber Security Division, created CSSP. The goal of the CSSP is to reduce the risks to control systems within and across all critical infrastructure and key resources

by coordinating efforts among federal, state, local, and tribal governments.

National laboratories, such as the Idaho National Laboratory, support the CSSP through providing technology expertise, data analysis, and research and testing capabilities. A key objective of the CSSP is to help reduce the likelihood of success, and severity of impact, of a cyber attack against critical infrastructure control systems through risk-mitigation activities including red teaming scenarios.

These activities platform on a clear understanding of cyber threats, control systems vulnerabilities and attack paths, and control systems engineering. The CSSP works closely with the control systems community to ensure industry subject-matter experts have vetted recommended best practices before they are publicly available.

DHS CSSP regularly assesses vendors' development of product updates and enhancements so as to improve their products' security posture and to provide DHS with greater awareness of related security issues.

An assessment may take as many as 1,200 hours. One of the targets of evaluation (TOE) is the sensor-to-multinode communications. The cyber security researchers (hackers) were able to con-

firm the cyber security enhancements for the defined TOE.

A recent test of a Honeywell technology demonstrated strong key encryption on all sensor-to-server data transfers. For additional protection, data was encrypted again when transferred over the mesh network (double encryption), making it extremely difficult to capture and modify data.

Additional testing took place to evaluate disruption and manipulation of gateway-to-control network communications. This work proved to be challenging for the cyber engineers, since it required reverse engineering of communications protocols.

They had to use the Control Data Access protocol in clear text format and limited it to Level 1 and 2 networks. Additionally, the limited protocol structure did not provide the information needed to manipulate or conduct a successful attack. Correlation of data had to take place with an additional component of the control system in order to identify the data points, making it inherently harder to perform.

A CSSC assessment of the OneWireless technology solution did identify additional findings. Honeywell and the CSSC are currently addressing these findings in a proactive manner by developing and mitigating the vulnerabilities. Under the worst-case scenario, cyber test engineers could only degrade throughput in the system, but not stop it. Under these conditions, no data corruption occurred, and the system remained functional throughout the evaluation.

Working together, automation suppliers and government cyber security specialists are making strides in recognizing potential risks in industrial control system security, and understanding how attackers can use cyber vulnerabilities to threaten the security to critical infrastructure and key resources.

Protecting your plant

Process engineers and operations management professionals often wonder if the IT group is not already handling the cyber security concerns.

One of the best ways to determine this is to do a self-assessment at your plant. Usually there are some definite differences between the requirements of the corporate network and the control network.

There are:

- Differences in goals between the two network organizations
- Differences in assumptions of what needs to be protected
- Understanding of what “real-time performance and continuous operation” really means
- The nature of control systems and how some well-intentioned software-based security solutions can interfere with operations

No matter which department ad-

resses cyber security within the plant, it is crucial there be protection against both deliberate attack and human error. When it comes to security, the “best in class” perspective is not a choice, it is a necessity.

Wireless technology has proven it can deliver security as well as wired solutions. As more and more plants start implementing wireless technology, it is vital to be aware of how the system is able to protect against malicious intent and to protect your intellectual property, your bottom line, and your people.

ABOUT THE AUTHORS

Trent Nelson (Trent.Nelson@inl.gov) is cyber security assessment lead at the Idaho National Laboratory in Idaho Falls, Idaho.

Jeff Becker (jeffrey.becker@honeywell.com) is global wireless director at Honeywell Process Solutions in Phoenix.

View the online version at www.isa.org/intech/20080901.

TERMINOLOGY

Lossy is a term describing a data compression algorithm, which actually reduces the amount of information in the data, rather than just the number of bits used to represent that information. One is usually able to remove some information because it is subjectively less important to the quality of the data (usually an image or sound) or because we can recover it by interpolation from the remaining data. MPEG and JPEG are examples of lossy compression techniques.

FIPS 140-2: The Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2, is a U.S. government computer security standard used to accredit cryptographic modules.

RESOURCES

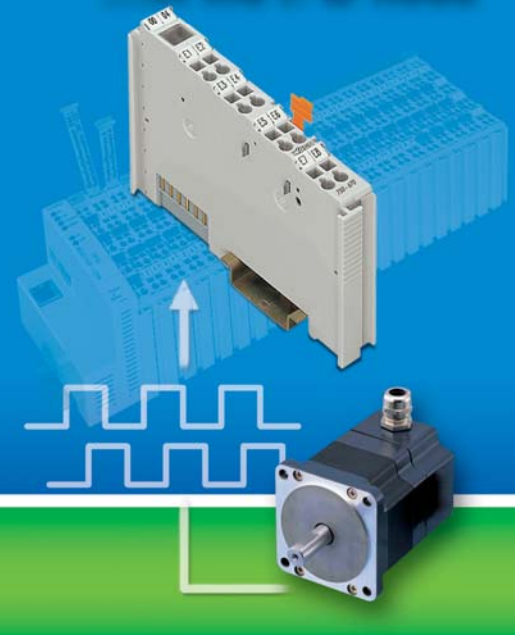
U.S. Department of Homeland Security: Control Systems Security Program
http://www.us-cert.gov/control_systems/

CS2SAT - Control System Cyber Security Self-Assessment Tool
www.isa.org/link/CS2SAtool

ZigBee short on power by design
www.isa.org/link/Zig200405

Stepper Motor Control...

...in the I/O node



Need to integrate stepper motor control on multiple industrial networks and with a variety of signal types? Then integrate your next stepper application in the I/O node with the WAGO-I/O-SYSTEM.

The WAGO-I/O-SYSTEM

- Support for 16+ industrial networks (incl. Ethernet, DeviceNet, Profibus, etc.)
- Choice of bus-coupler, programmable controller, or IPC hardware
- Over 300 digital, analog, and special function I/O modules

Stepper Motor Control Modules

- Control of 2-phase stepper motors or stepper drives
- 12mm wide modules for convenient mounting in stand-alone or distributed I/O nodes
- Supports common stepper operating modes, as well as special functions
- Quick implementation of stepper functions via Function Blocks

Contact WAGO to integrate your next stepper application in the I/O node:

1-800-DIN-RAIL (346-7245) or

info.us@wago.com

www.wago.us/stepper.htm

