

## Honeywell Process Solutions



## **Defense in Cyber Space** ***Beating Cyber Threats that Target Mesh Networks***

Trent Nelson, Cyber Security Assessment Lead, Idaho National Laboratory  
Jeff Becker, Global Wireless Business Director, Honeywell Process Solutions

## Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>Introduction .....</b>	<b>3</b>
<b>The Situation.....</b>	<b>3</b>
<b>Beating the Hackers .....</b>	<b>3</b>
<b>This is Only a Test.....</b>	<b>5</b>
<b>Protecting Your Plant.....</b>	<b>6</b>

## Introduction

Wireless technology has aroused as much interest as it has skepticism within 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. The integrity of vital assets, including operational processes, network architectures and business applications, can no longer be taken for granted.

## The Situation

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

- **Indiscriminant and potentially destructive** – This is the most publicized category, malware; which includes viruses, Trojans and worms attacks.
- **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.
- **Confidentiality** – With eavesdropping and password cracking, protecting data from unauthorized use becomes a concern along with safety.
- **Integrity**– This area 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’s being transmitted 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

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 be directed 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 (RF) medium is susceptible to eavesdropping and spoofing, care must be taken 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 after-thought.

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 that a single security breach does not compromise the entire system through cascading attacks. The integrity of the security layer should not require individual nodes will not be suborned, but should ensure the compromise of 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 include:

**Data confidentiality:** Application information exchanged through the network may be sensitive and must be protected against eavesdropping. To insure that 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 be re-keyed as necessary. The current 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 be authenticated to each other. Entity authentication is the process by which one entity is assured of the identity of a second entity. This prevents unauthorized devices from entering the network. It is important that 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 though 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 that fault processes, such as noise or random error, have not altered a message between transmission and reception. Message authentication establishes that an attacker has not maliciously fabricated or altered a message. Sender authentication establishes that a message originated from a limited set of authorized senders. Together, these features substantiate that received messages are not corrupted and have been sent by 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 minimized.

**Key escrow:** Long-term key escrow may be required to satisfy regulatory requirements or because of customer corporate policy. The key escrow mechanism may also be used for backup of keying material to support failure recovery. Remote key escrow must be supported.

**Firmware updates:** Nodes may require firmware updates to repair software flaws or to add new features. Nodes must be protected so they do not accept corrupted firmware or firmware from an unauthorized source.

**FIPS 140-2 compliance:** Cryptographic modules should be FIPS 140-2 compliant during operation. Nodes should be designed so they may be classified as “single chip cryptographic modules.” Achieving this rating requires, among other things, that 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., debugging ports must be disabled).

**Availability:** Availability means ensuring the services offered by the secured nodes will be available to legitimate users when expected. Attacks on availability are called Denial of Service (DoS) attacks. The security protocol should attempt to ensure that the wireless network is not a force multiplier for the adversary, meaning that the magnitude of the attack is not magnified by retransmission through the network. The security layer design should also include features to mitigate battery exhaustion (“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 the Control Systems Security Program (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 (INL), 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 are based 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 that industry subject-matter experts have vetted recommended best practices before they are made publicly available.

Recently, DHS CSSP sponsored cyber security specialists from the Control Systems Security Center (CSSC), located in Idaho Falls, Idaho to work with Honeywell to assess the security effectiveness of Honeywell’s OneWireless solution. The goal of the assessment was to support Honeywell’s development of product updates and enhancements improving its security posture, and to provide DHS with greater awareness of related security issues.

Assessment of the OneWireless mesh network solution was performed in May 2008, which took over 1200 hours with Honeywell participation. One of the targets of evaluation (TOE) for this evaluation was the sensor-to-multinode communications. The cyber security researchers (hackers) were able to confirm the cyber security enhancements for the defined TOE. The tests 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 was conducted 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. The Control Data Access (CDA) protocol had to be used in clear text format and was limited 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 be done with an additional component of the control system in order to identify the data points, making it inherently harder to perform.

The CSSC assessment of Honeywell’s OneWireless 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 most of the cyber security concerns aren't already handled by their company's IT group. 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, all the way from:

- 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 addresses cyber security within the plant, it is crucial to be protected against both deliberate attack and human error. When it comes to security, the "best in class" perspective isn't a choice – it's 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.

### For More Information

For more information about Honeywell's wireless solutions, visit our website at [www.honeywell.com/ps/wireless](http://www.honeywell.com/ps/wireless) or contact your Honeywell account manager.

### Automation & Control Solutions

Process Solutions  
Honeywell  
2500 W. Union Hills Dr.  
Phoenix, AZ 85027  
Tel: 877.466.3993 or 602.313.6665  
[www.honeywell.com/ps](http://www.honeywell.com/ps)

WP-08-28-ENG  
September 2008  
Printed in USA  
© 2008 Honeywell International Inc.

The Honeywell logo is displayed in a bold, red, sans-serif font.