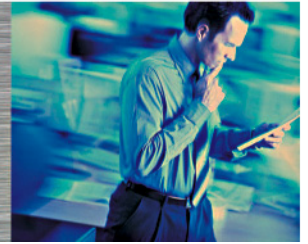


## Honeywell Process Solutions



# **Interference and Security Considerations for Wireless Communications in an Industrial Environment**

Stephen Muenstermann  
Honeywell Process Solutions

## Introduction

From traditional narrow-band to more complex spread-spectrum technologies, a variety of radio frequency (RF) communication techniques are available for deployment in industrial environments. Presented and evaluated here, in terms of their relative security and integrity performance, are the most common narrow-band and spread-spectrum alternatives.

### Narrow Band vs. Spread Spectrum Radio Operation

Conventional radio signals are referred to as narrow-band, which means that their power is concentrated within a very narrow portion of RF bandwidth. The Federal Communications Commission (FCC) has traditionally favored these radios for this very reason.

On the negative side, however, narrow-band radio signals are more vulnerable to interference by signals of identical or neighboring frequencies. Simple sidebands or more powerful continuous signals can completely jam narrow-band communications. Also, because they are localized in frequency, narrow-band signals can be relatively readily detected and intercepted.

Spread spectrum radio (SSR) signals, in contrast, are spread over a broader portion of the radio frequency band and are typically much more resistant to interference—by other co-existent signals or by intentional jamming.

Indeed, the same signal characteristics that make SSR less subject to interference also make it harder to detect and intercept. As such, SSR techniques have long been used for military communications, and some have been declassified as recently as the 1980s. It's important to note, however, that some SSR technologies, such as frequency shift keying (FSK), can rely on a relatively narrow frequency band and are still subject to complications due to sidebands and saturation.

### Frequency-Hopping Spread Spectrum (FHSS)

FHSS (frequency-hopping spread spectrum) is a highly secure type of spread spectrum radio. FHSS is used in a variety of communication transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies (Figure 1).

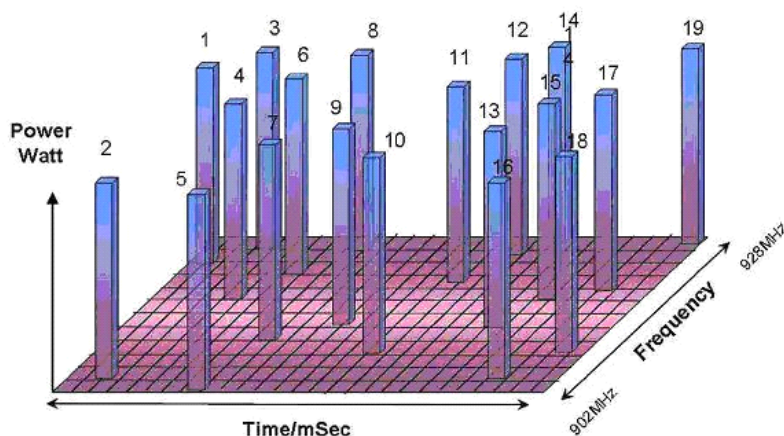


Figure 1: Frequency-hopping spread spectrum (FHSS) technology "hops" the signal in a predetermined pattern within the frequency band.

This technique has high noise immunity because competing narrow-band signals will only affect the spread spectrum signal if both are transmitting at exactly the same frequency at exactly the same time. If a particular signal does encounter interference, the data will simply be resent on the next hop.

The transmission frequencies are determined by a spreading, or hopping, sequence. The field device and base station must be precisely synchronized, transmitting and listening at the same frequencies at the same time. Because any unauthorized listening device will not know the spreading sequence, interception is extremely difficult. With FHSS, security and noise immunity are at a peak. FHSS is also the most forgiving in an environment that has co-existing radios. Even with a large number of radios, the probability of interference is remote, since each transmission is measured in milliseconds and is very low-powered. And, if on the remote chance two hops interfere, the data will simply be resent on the next hop. Most of Honeywell's systems in industrial use today use the 900MHz ISM (Industrial, Scientific and Mobile) band, and we've recorded no cases of interruption interference by other 900-MHz wireless devices.

### **Direct-Sequence Spread Spectrum**

DSSS (direct-sequence spread spectrum) is another type of SSR most commonly used for wide-band communications such as wireless Ethernet, including increasingly common 802.11 wireless networks.

The DSSS data signal is spread over the band/channel according to a spreading ratio. The code includes a redundant bit pattern for each bit that is transmitted, increasing the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data is resent. Most commonly operating in the 2.4-GHz range, DSSS spreads across the band and searches for interfering data as it sends its signals. If a packet of data is interrupted or interfered with, the packet is resent. DSSS technology also is used in more powerful microwave-based wide area networks (WANs).

### **Wireless Alternatives Compared**

In most industrial applications, FHSS is the best choice for co-existence without interference. DSSS, on the other hand, is highly capable of co-existing and will not typically interfere with existing signals. And while DSSS may be the first to fail in a given environment, an expertly designed wireless system can be made to work reliably and securely even in many tough industrial environments.

Finally, because every industrial environment is different, and may offer a unique set of obstacles to effective RF communication, a site survey is a recommended first step in determining which technology is most appropriate for any given application.

Technology	Noise Immunity	Non-interference w/ other RF technologies	Ability to send large packets of data	Susceptibility to jamming & interference	Inherent security & signal intercept protection
Narrow Band Analog Radio (Handheld Radio)	1	1	1	1	1
Narrow Band Digital Radio (Handheld Radio)	1	1	3	1	2
Cell Phones	3	1	4	1	2
Spread Spectrum	3	3	5	3	3
DSSS 2.4GHz	3	5	5	4	4
FHSS 900MHz	5	5	4	5	5

Table 1: Wireless transmission alternatives ranked on a scale of 1 to 5 (lowest to highest).

### More Information

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

### Automation & Control Solutions

Process Solutions

Honeywell

2500 W. Union Hills Dr.

Phoenix, AZ 85027

Tel: +1-602-313-6665 or 877-466-3993

[www.honeywell.com/ps](http://www.honeywell.com/ps)

WP-07-05-ENG  
June 2007  
© 2007 Honeywell International Inc.

