



Frequency Hopping & Unwanted Intruders

By Randy Klassen & Åke Severinson, OMNEX Control Systems Inc.



All types of data transfer offer the opportunity for both data interception and injection. In wired systems, it usually takes some direct physical connection to gain access, with tampering being possible anywhere along the transmission wires. Radio systems, on the other hand, take the potential for data interception or injection out of the realm of actual physical contact and force tampering to occur in the radio frequency (RF) realm. Further to this, various radio systems and technologies set up different types of "road blocks" that must be overcome by the wireless intruder.

CONVENTIONAL SINGLE CHANNEL VHF/UHF RADIO

A single channel radio (where a listener finds the specific radio frequency and listens to the message being sent) has an added element of security over a wire because message is usually encoded and the listener can only make sense of it when he/she has the appropriate receiver. A person without the appropriate equipment to decode the message is thus forced to find the frequency used and acquire knowledge of the protocol before he/she can decode the signal. Likewise, injection of data into the signal can only happen if the code is 'broken'. This differentiates radio signals from wired communications that are typically not encoded. Take, for example, standard industrial signals such as ON/OFF status and 4-20mA current. These signals are encoded when passed through a radio, but not usually encoded when passed by wire.

FREQUENCY-HOPPING SPREAD SPECTRUM RADIO

To further inhibit unwanted intrusions, the military developed Frequency Hopping (FH) radios that add an additional set of barriers for a would-be intruder to overcome. This technology has been available to commercial radio manufacturers since 1987 and the following list highlights a few of its detection avoidance features:

- ◆ Like the single channel VHF/UHF radios, each packet is encoded, thereby forcing the intruder to gain knowledge of the protocol, ID and decoding.
- ◆ Unlike single channel radio, the FH data is continually hopped across a wide range of frequencies in a pseudo random sequence. To listen to the data, the intruder must know (or establish) the hopping sequence and follow along as the bits and pieces of the message "jump around." As an example, the OMNEX HopLink system uses 252 different pseudo random hopping sequences.
- ◆ Data transmissions are tightly timed to make sure both ends of the system are on the same frequency at the same time. To make a FH system efficient, the time required to hop from one frequency to another must be made very short. The relevance of this from the intruder's point of view is that he/she cannot make use of "generic" radios normally designed to switch slowly to keep the cost of the equipment low. For all intents and purposes, the intruder needs to have an OMNEX radio set to stand much of a chance of intercepting an OMNEX HopLink transmission.

In conclusion, with an OMNEX HopLink system, the intruder needs to: a) be technically competent; b) have detailed knowledge of the inner workings of both the hardware (frequencies, bandwidths, hop and synchronization sequences and timing) and software (data packet construction, time tracking, synchronization strategy, etc.) in the HopLink equipment; and c) be very tenacious. And though the case can be made that nothing is really safe against a determined intruder, in the case of a Frequency Hopping HopLink, military-type equipment and experience are needed to "break into" this type of radio system.