The Basics of Remote Control and Remote Keyless Entry

Application Note AN-00320

Introduction

As wireless systems have become more integrated and lower in cost, more and more products are seeking a competitive edge through the addition of remote control features. Despite this wireless explosion, there is still some trepidation among product designers at the thought of undertaking a wireless design. This application note discusses the basics of remote control systems including legal and technical considerations.

Remote control is the act of controlling something from a distance. Remote Keyless Entry (RKE) is a form of remote control in which the device being controlled provides access to a secure location. A common example of this type of system is an automotive door lock. The lock on the car door is remotely controlled by a transmitter in a fob. Most systems are unidirectional (one-way or simplex); however, new generation technologies are now available for bidirectional (two-way or duplex) communication.

System Configuration

A simple remote control system consists of an encoder, RF transmitter, RF receiver and a decoder.

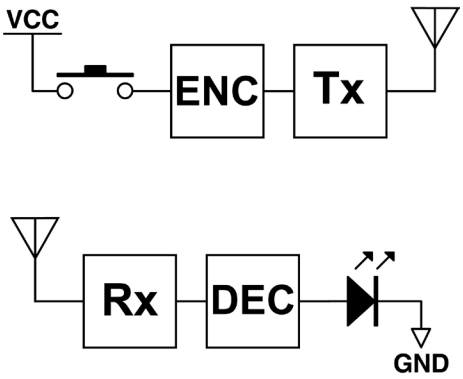

Figure 1: A Basic Remote Control System

The encoder is generally connected to one or more buttons, switches or contacts. The encoder detects the closure of one of the switches and converts that into a digital data stream. This data is then sent to an RF transmitter that conveys this data into free space. An RF receiver receives the data and sends it to a decoder. The decoder analyzes the data and, if it is valid, replicates the switch closure on an output. This output is then connected to whatever circuitry is to be controlled. With that basic overview of the system, a more detailed look at the system components can be undertaken.

Radio Considerations

When considering a radio for the system, legal considerations are just as important as technical considerations. Various governments regulate the radio spectrum within their countries and specify what can and cannot be done at a particular frequency. Understanding the legal requirements in the countries in which the end product will be sold is the first place to start when choosing a radio.

Fortunately, many governments have recognized the advantages of globally consistent regulations, so the requirements for remote control systems tend to fall into two camps. The United States Federal Communications Commission (FCC) has specified the 260MHz to 470MHz band to be used for the transmission of command and control data. There are a number of requirements and restrictions in this band that are intended to keep it clear of interference. Linx Application Note AN-00125 goes into the regulations in this band in detail. Canada and Brazil have adopted regulations that are very close to the US regulations. 315MHz and 433.92MHz are the most common frequencies for RKE in those countries.

The European Union has adopted a different set of regulations, but these regulations are followed by all member countries and several Pacific and Asian countries. Europe has allocated the 433.05MHz to 434.79MHz band for remote control and command applications. Since this band is so narrow, the center of the band (433.92MHz) is typically chosen so that products still fall within the band over temperature and component variations.

This frequency overlaps the FCC band, meaning a single 433.92MHz radio design can be used in the U.S. and Europe. This makes hardware design and manufacturing efficient, but it also makes the band crowded with devices. It is up to the designer to understand the regulations and determine the best frequency of operation for their product.

Once the radio's frequency is chosen based on the legal regulations, the radio type and modulation method can be chosen. The two most common types of modulation for RKE devices are On-Off-Key (OOK) and Frequency Shift Key (FSK) modulation.

OOK modulation represents a logic '1' by turning the RF carrier on and a logic '0' by turning the RF carrier off.

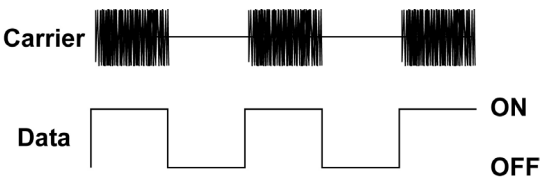

Figure 2: OOK Modulation

This method of modulation requires few components and is inexpensive to implement, but it is highly prone to interference from external sources. However, one of the key advantages of OOK arises in countries like the United States that average output power over time. Since the carrier is turned off for a '0', the average power over the test time is decreased proportionally to the number of '0's in the data stream. This means that the power allowed for the '1's can be proportionally higher, extending the system range. As an example, if the data stream contains 50% '0's, then the system will be allowed 6dB more output power than if the carrier were on all the time like in an FSK system. This represents a doubling of the range of the system. Higher power is allowed for systems with lower duty cycles, down to a 10% lower limit.

FSK modulation is a type of modulation in which a logic '1' is represented by a carrier at one frequency and a logic '0' is represented by a carrier at another frequency.

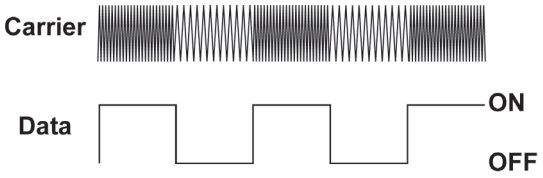

Figure 3: FSK Modulation

The advantage of FSK is that since the carrier is never turned off, the receiver can lock onto the transmitted signal, making the system more immune to external interference. The disadvantage is that it is more complicated and more expensive to implement and will not offer the range improvement in countries that average output power.

Since most remote control/RKE transmissions are not highly critical and are cost-sensitive, most products use an OOK radio.

The Encoder and Decoder

The encoder and decoder are the brains of the system. The encoder detects the button presses or switch closures then formats them into a digital data stream and sends the data to the transmitter. The decoder takes the data stream from the receiver, checks to make sure that it is valid, and if it is, replicates the switch closures on its outputs. These outputs are then connected to the application circuitry that is being controlled. This system makes it appear as though the switches are connected directly to the application circuitry.

The encoders and decoders can come in a variety of flavors and there are several considerations in choosing the best technology for an application. First, some different levels of technology are presented.

Basic

These systems have no addressing or security features, but are very easy to use and set up. Typically every encoder will activate every decoder without any setup beyond connecting power.

Unique

These systems offer simple addressing capabilities that give each system a unique identity. This prevents unintentional activation of the system by someone else with the same system. The more addresses offered by the system, the more unique the system can be and the less likely that a neighbor will activate the system. However, more addresses generally means a more complicated set-up.

Low end systems generally use DIP switches or jumpers to set the address. The user must set the switches the same on the transmitter and receiver to have the system communicate. Between 4 and 10 switches are common in these systems, giving 16 to 1024 unique addresses.

Higher end systems use digital numbers as an address. These numbers are typically between 24 and 80 bits long, giving millions of unique addresses. However, creating the addresses is more complicated, typically involving external programmers to program the address into both ends or a learning system in which one end creates the address and the other end is placed into a special mode to learn the address.

Regardless of the length of the address, these systems transmit the same data stream repeatedly while the button is pressed with no encryption or security features. These systems are less expensive and easier to use than the systems with encryption and are suitable for many applications that do not require security. It is not a major problem if your neighbor activates your mosquito misting system, but it is not desirable for securing a garage or automobile.

Secure

Secure systems encrypt a portion of the digital data stream before sending it to the transmitter. There are several encryption algorithms used, but the best systems use algorithms that are well-documented and publicly available. These include AES, DES and Skipjack, among others. The encryption makes the transmitted data look completely random to someone on the outside unless they have the encryption key. This prevents an attacker from guessing the next transmission or recording a transmission and playing it back to gain access to the system. These types of encoders and decoders are typically used for access control and RKE where security is paramount.

The high security comes at a higher price and a more complicated set-up. Many devices require a programmer or PC interface in production to program the encryption keys into the encoder and decoder. Other

systems use a sequence of button presses to create the key, then a learning system to exchange the key with the other end. The learning system may require additional circuitry to enable or facilitate the key transfer.

A significant challenge to selecting a secure system is evaluating the true security of the available products on the market. While such a comparison is beyond the scope of this note, it is suggested that the system designer stick with an industry accepted encryption scheme and follow the manufacturer's implementation recommendations. Homemade encryption techniques are rarely as secure as the designers want to believe, so it is always best to use one that is already proven.

Transcoder

A new generation of devices called transcoders are now available that combine aspects of encoders and decoders into one device. These enable bidirectional command and control as well as confirmation that the command was received by the remote end. The transcoders can range from encoders and decoders with confirmation, to transcoders with a set number of inputs and outputs, to devices that are completely dynamic and configurable by the manufacturer or end user. These devices can be used in applications such as a car paging the keyfob to indicate that the car alarm has activated.

Ultimately the designer is responsible for balancing the security, ease of use, and cost when selecting a technology that will be used in a remote control or RKE system. The advantages and disadvantages of each must be weighed against the needs of the product.

Solutions

Linx Technologies offers complete solutions to meet the requirements of many remote control/RKE systems.

Radios

The LR Series transmitter and receiver are low cost, high performance OOK radios. They are capable of over 2,000 feet of line-of-sight range.

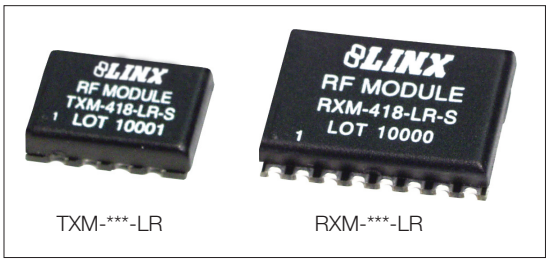

Figure 4: LR Series RF Modules

The LT Series transceiver is a combination of the LR Series transmitter and receiver in a package that is smaller than the receiver. It is suitable for the bidirectional transfer of digital data and is capable of up to 3,000 feet of line-of-sight range.

Figure 5: LT Series Transceiver

Other modules are available for FM modulation and transmission of data and analog information such as audio.

Encoders, Decoders and Transcoders

In non-secure applications where many transmitters and receivers are required to use the same address, the DS Series can be used. This part uses 10 address inputs that are typically set by DIP switches. It offers 2^{10} (1,022) combinations of addresses where all GND and all V_{CC} are not allowed.

Figure 6: DS Series Encoder / Decoder Combo

The MS Series is a step up in technology from the DS parts. A single line on the encoder is used to randomize a 24-bit address, giving over 16.77 million unique addresses. A single line on the decoder places it into a Learn Mode to complete the association. Advanced features include control permissions, adjustable baud rate, and a transmitter ID.

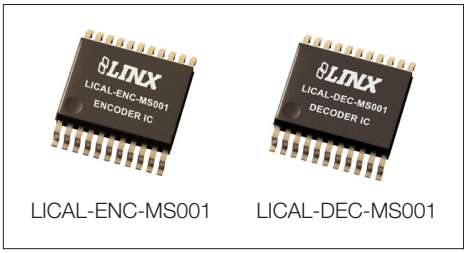

Figure 7: MS Series Encoder and Decoder

For the ultimate in secure remote control, Linx recommends the HS Series. Built on an NSA encryption algorithm called Skipjack, the HS Series offers a wealth of additional patent pending features. These include control permissions, optional encoder PIN, encoder ID and a method for never sending the same data twice and never losing sync, among others. The encryption protocol was analyzed by the Independent Security Evaluators, a well-respected company in the industry, and was given a strong review. The review and additional information on the technology are available on the Web at www.cipherlinx.com.

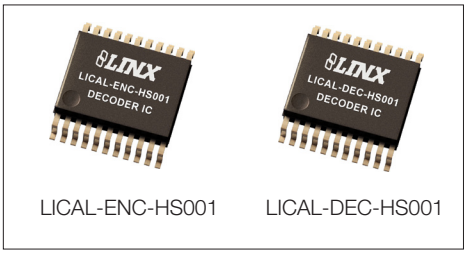

Figure 8: HS Series Encoder and Decoder

The MT Series transcoder is designed for bidirectional command and control. Offering eight lines that can dynamically be set as button inputs or control outputs, the MT is filled with features. While the MT can be configured manually with a few button presses, a serial interface engine offers the ability to use a PC application for configuration. Because it is a standard serial interface, no special programmer is required. The MT Series is also completely compatible with the MS Series, offering the option for mixed-mode systems. Other unique features include control permissions, transmitter ID, open access mode, custom data byte transmission and targeting.

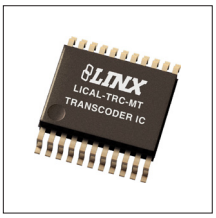

Figure 9: MT Series Transcoder

Since the transmitter side of many remote control or RKE systems is commonly a handheld or keyfob design, Linx manufactures a complete line of OEM transmitters. These transmitters are pre-certified for use in the United States, Canada and Europe. The transmitters are available in several styles and can be easily customized with logos or unique artwork.

Figure 10: Handheld Transmitters

For more information on these or any Linx products, please see www.linxtechnologies.com or call +1 800 736 6677 (+1 541 471 6256 if outside the United States) and speak to an application engineer.

159 Ort Lane, Merlin, OR, US 97532
Phone: +1 541 471 6256
Fax: +1 541 471 6251
www.linxtechnologies.com