HIGH SECURITY

HS SERIES

DECODER

HS SERIES DECODER DATA GUIDE

DESCRIPTION

HS Series encoders and decoders are designed for maximum security remote control applications. Together, they allow the status of up to eight buttons or contacts to be transferred via a highly secure encrypted transmission intended for wireless links. The HS Series uses CipherLinx™ technology, which is based on the Skipjack algorithm developed by the U.S. National Security Agency (NSA) and has been independently evaluated by ISE. CipherLinx™ never sends or accepts the same data twice, never loses sync, and changes codes on every packet, not just every button press. In addition to state-of-the-art security, the tiny 20-pin SSOP packaged parts also offer innovative features, including up to 8 data lines, multiple baud rates, individual “button level” permissions, keypad user PIN, encoder identity output at the decoder, low power consumption, and easy setup.

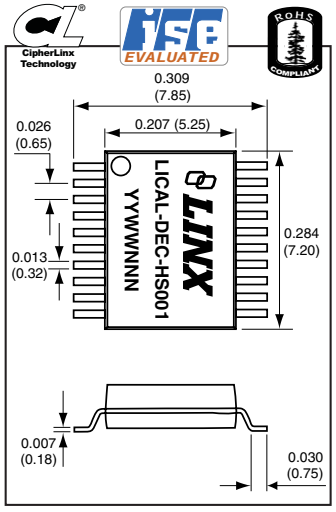

Figure 1: Package Dimensions

FEATURES

- CipherLinx™ security technology
- ISE evaluated
- Never sends the same packet twice
- Never loses sync
- PIN-protected encoder access
- 8 selectable data lines
- “Button level” permissions
- Encoder ID available at decoder
- Wide 2.0 to 5.5V operating voltage
- Low supply current (370µA @ 3V)
- Ultra-low 0.1µA sleep current
- Selectable baud rates
- No programmer required
- Small SMD package

APPLICATIONS INCLUDE

- Keyless Entry / Access Control
- Door and Gate Openers
- Security Systems
- Remote Device Control
- Car Alarms / Starters
- Home / Industrial Automation
- Remote Status Monitoring

ORDERING INFORMATION

PART #	DESCRIPTION
LICAL-ENC-HS001	HS Encoder
LICAL-DEC-HS001	HS Decoder
MDEV-LICAL-HS	HS Master Development System
HS encoders are shipped on reels of 1,600	

Patents Pending

Revised 1/28/08

ELECTRICAL SPECIFICATIONS

Parameter	Designation	Min.	Typical	Max.	Units	Notes
POWER SUPPLY						
Operating Voltage	V_{CC}	2.0	–	5.5	VDC	–
Supply Current:	I_{CC}					
At 2.0V V_{CC}		–	240	300	µA	1
At 3.0V V_{CC}		–	370	470	µA	1
At 5.0V V_{CC}		–	670	780	µA	1
Power-Down Current:	I_{PDN}					
At 2.0V V_{CC}		–	0.10	0.80	µA	–
At 3.0V V_{CC}		–	0.10	0.85	µA	–
At 5.0V V_{CC}		–	0.20	0.95	µA	–
DECODER SECTION						
Input Low	V_{IL}	0.0	–	0.15 x V_{CC}	V	2
Input High	V_{IH}	0.8 x V_{CC}	–	V_{CC}	V	3
Output Low	V_{OL}	–	–	0.6	V	–
Output High	V_{OH}	V_{CC} - 0.7	–	–	V	–
Output Sink Current	–	–	–	25	mA	–
Output Drive Current	–	–	–	25	mA	–
ENVIRONMENTAL						
Operating Temperature Range	–	-40	–	+125	°C	–

Table 1: Electrical Specifications

Notes

1. Current consumption with no active loads.
2. For 3V supply, (0.15 x 3.0) = 0.45V max.
3. For 3V supply, (0.8 x 3.0) = 2.4V min.

ABSOLUTE MAXIMUM RATINGS

Supply Voltage V_{CC}	-0.3	to	+6.5	VDC
Any Input or Output Pin	-0.3	to	V_{CC} + 0.3	VDC
Max. Current Sourced By Output Pins			25	mA
Max. Current Sunk By Output Pins			25	mA
Max. Current Into V_{CC}			250	mA
Max. Current Out Of GND			300	mA
Operating Temperature	-40	to	+125	°C
Storage Temperature	-65	to	+150	°C

***NOTE* Exceeding any of the limits of this section may lead to permanent damage to the device. Furthermore, extended operation at these maximum ratings may reduce the life of this device.**

Baud Rate	Decoder Activation Time
4,800	67
28,800	36

Table 2: Encoder SEND to Decoder Activation Times (mS)

RECOMMENDED PAD LAYOUT

HS Series encoders and decoders are implemented in an industry standard 20-pin Shrink Small Outline Package (20-SSOP). The recommended layout dimensions are shown below.

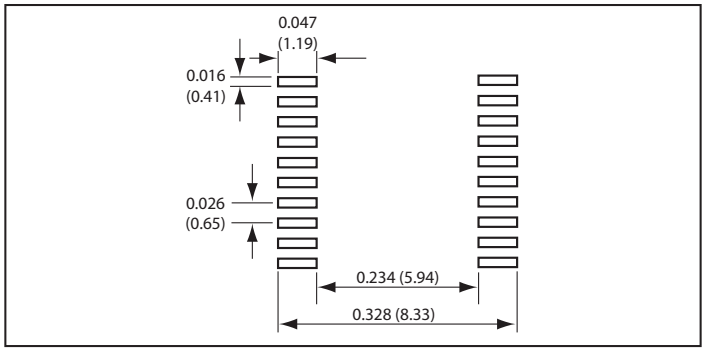

Figure 2: HS Series Decoder PCB Layout Dimensions

PRODUCTION CONSIDERATIONS

These surface-mount components are designed to comply with standard reflow production methods. The recommended reflow profile is shown below and should not be exceeded, as permanent damage to the part may result.

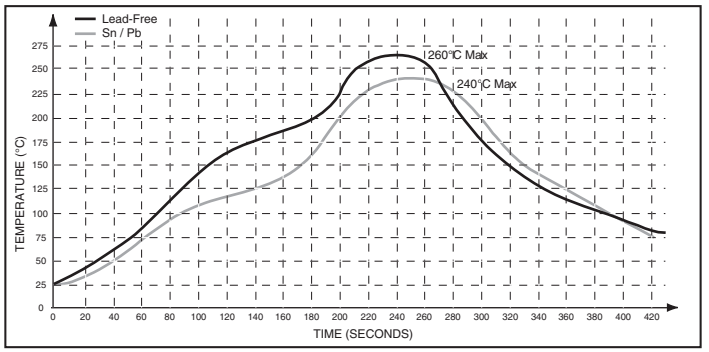

Figure 3: HS Series Reflow Profile

CAUTION

This product is a static-sensitive component. Always wear an ESD wrist strap and observe proper ESD handling procedures when working with this device. Failure to observe this precaution may result in device damage or failure.

PIN ASSIGNMENTS

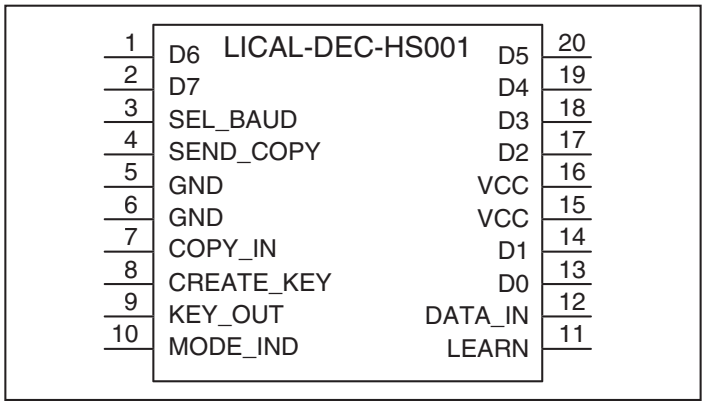

Figure 4: HS Series Decoder Pin Assignments

Pin Name	Pin Number	I/O	Description
D0-D7	1, 2, 13, 14, 17-20	O	Data Output Lines
SEL_BAUD	3	I	Baud Rate Selection Line
SEND_COPY	4	I	Send Copy Activation Line
GND	5, 6	--	Ground
COPY_IN	7	I	Copy Input Line
CREATE_KEY	8	I	Create Key Activation Line
KEY_OUT	9	O	Key and Transmitter ID Output Line
MODE_IND	10	O	Mode Indicator Output
LEARN	11	I	Learn Mode Activation Line
DATA_IN	12	I	Data Input Line
V_{CC}	15, 16	--	Positive Power Supply

Table 3: HS Series Decoder Pin Assignments

NOTE:

None of the input lines have internal pull-up or pull-down resistors. The input lines must be in a known state (either GND or V_{CC}) at all times or the operation may not be predictable. The designer must ensure that the input lines are never floating, either by using external resistors, by tying the lines directly to GND or V_{CC}, or by use of other circuits to control the line state.

PIN DESCRIPTIONS

Data Lines

The decoder has eight data lines, D0 through D7. These lines will reproduce the state of the encoder's data lines upon reception of a valid packet.

SEL_BAUD

This line is used to select the baud rate of the serial data stream. The state of the line allows the selection of one of two possible baud rates, as shown in the adjacent table.

SEL_BAUD	Baud Rate (bps)
0	4,800
1	28,800

Table 4: Baud Rate Selection Table

The baud rate must be set before power-up. The decoder will not recognize any change in the baud rate setting after it is on.

SEND_COPY

When this line is taken high along with the LEARN line, the decoder will enter Send Copy Mode and output the User Data on the KEY_OUT line. When taken high with the CREATE_KEY line at power-up, Send Copy Mode will be disabled.

GND

These lines are connected to ground.

COPY_IN

This line is used to input the User Data from another decoder.

CREATE_KEY

When this line is taken high along with the LEARN line, the decoder will enter Create Mode and create a key and encoder ID. It will then send these to the encoder through the KEY_OUT line. When taken high with the SEND_COPY line at power-up, Send Copy Mode will be disabled.

KEY_OUT

When the SEND_COPY and LEARN lines are taken high at the same time, the decoder will output the User Data on this line. This line will also output the transmitter identity upon reception of the first valid packet of each session.

MODE_IND

This line will activate when a valid transmission is received, when the decoder enters Learn Mode, Get Key Mode, Create Key Mode, or Send Copy Mode, and when the memory is cleared. This allows for the connection of a LED to indicate to the user that these events have taken or are taking place.

LEARN

When this line goes high and is then pulled low, the decoder will enter Learn Mode to accept permissions from an encoder and store it in memory. If it is held high for ten seconds, the decoder will clear all User Data from memory. If it goes high with SEND_COPY or CREATE_KEY, then the decoder will enter Send Copy Mode or Create Key Mode, respectively.

DATA_IN

This line accepts serial data from the encoder, usually via a wireless link.

V_{CC}

These lines are connected to the positive power supply.

REMOTE CONTROL OVERVIEW

Wireless remote control is growing in popularity and finding its way into more unique applications. Remote Keyless Entry (RKE) systems for unlocking cars or opening garage doors quickly come to mind, but how about a trash container that signals the maintenance office when it needs to be emptied? The idea behind remote control is simple: a button press or contact closure on one end causes some action to be taken at the other. Implementation of the wireless RF stage has traditionally been complicated, but with the advent of simpler discrete solutions and modular products, such as those from Linx, implementation has become significantly easier.

Encoder and decoder ICs are generally employed to maintain the security and uniqueness of a wireless RF or IR link. These devices encode the status of inputs, usually button or contact closures, into a data stream suitable for wireless transmission. Upon successful recovery and validation, the decoder's outputs are set to replicate the states of the encoder's inputs. These outputs can then be used to control the circuitry required by the application.

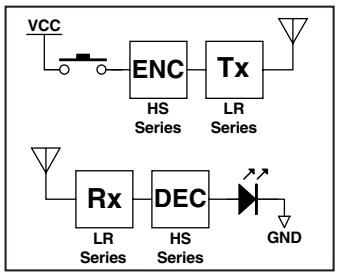

Figure 5: Remote Control Block Diagram

Prior to the arrival of the Linx HS Series, encoders and decoders typically fell into one of two categories. First were older generation, low-security devices that transmitted a fixed address code, usually set manually with a DIP switch. These products were easy to use, but had significant security vulnerabilities. Since they sent the same code in every transmission, they were subject to code grabbing. This is where an attacker records the transmission from an authorized transmitter and then replays the transmission to gain access to the system. Since the same code was transmitted every time, the decoder had no way to validate the transmission.

These concerns resulted in the development of a second type of encoder and decoder that focused on security and utilized a changing code to guard against code grabbing. Typically, the contents of each transmission changes based on complex mathematical algorithms to prevent someone from reusing a transmission. These devices gained rapid popularity due to their security and the elimination of manual switches; however, they imposed some limitations of their own. Such devices typically offer a limited number of inputs, the transmitter and receiver can become desynchronized, and creating relationships and associations among groups of transmitters and receivers is difficult.

The HS Series offers the best of all worlds. The HS Series uses an advanced high security encryption algorithm called CipherLinx™ that will never become desynchronized or send the same packet twice. It is easily configured without production programming and allows for "button level" permissions and unique encoder and decoder relationships. Eight inputs are available, allowing a large number of buttons or contacts to be connected.

To learn more about different encoder and decoder methodologies please refer to Application Note AN-00310.

HS SERIES OVERVIEW

The HS Series encoder encodes the status of up to eight buttons or contacts into highly secure encrypted serial data stream intended for wireless transmission via an RF or infrared link. The series uses CipherLinx™ technology, which is based on the Skipjack algorithm developed by the United States National Security Agency (NSA). The CipherLinx™ protocol in the HS Series has been independently evaluated by Independent Security Evaluators (ISE). A full evaluation white paper is available at www.linxtechnologies.com/cipherlinx.

The encoder combines eight bits representing the state of the eight data lines with counter bits and integrity bits to form a 128-bit message. To prevent unauthorized access this message is encrypted with CipherLinx™ in a mode of operation that provides data integrity as well as secrecy. CipherLinx™ never sends or accepts the same data twice, never loses sync, and changes codes on every packet, not just every button press.

Decoding of the received data signal is accomplished by the HS Series decoder. When the decoder receives a valid command from an encoder, it will activate its logic-level outputs, which can be used to activate external circuitry. The encoder will send data continuously as long as the SEND line is held high. Each time the algorithm is executed, the counter is decremented, causing the code to be changed with the transmission of each packet. This, combined with the large counter value and the timing associated with the protocol, ensures that the same transmission is never sent twice.

An 80-bit key used to encrypt the data is created in the decoder by the user. The decoder is placed into Create Key Mode, and a line is toggled 10 times, usually by a button. This is required to gather entropy to ensure that the key is random and chosen from all 2^{80} possible keys. A high-speed timer is triggered by each rise and fall of voltage, recording the time that the line is high and low. The 80-bit key is generated by combining the low-order bits of the twenty timer values. To create an association, the key, a 40-bit counter, and a decoder-generated ID are sent to the encoder via a wire, contacts, IR, or other secure serial connection.

The HS Series allows the end user or manufacturer to create associations between the encoder and decoder. If the encoder and decoder have been associated through a successful key exchange, then the decoder will respond to the encoder's commands based on its permissions. If an encoder has not been associated with a decoder, its commands will not be recognized.

The user or manufacturer may also set "button level" permissions. Permission settings control how the decoder will respond to the reception of a valid command, either allowing the activation of an individual data line or not. The decoder is programmed with the permission settings during set-up, and those permissions are retained in the decoder's non-volatile memory.

The HS decoder has the ability to identify and output a decoder-assigned identification number for a specific encoder. An encoder's key, a 40-bit counter, and permissions are stored in one of fifteen memory locations within the decoder. The decoder is able to output an 8-bit binary number that corresponds to the memory location of the encoder's information. This provides the ability to identify the specific encoder from which a signal originated. This identification can be used in various ways, including systems that record access attempts or in applications where the originating user needs to be known.

HS SERIES SECURITY OVERVIEW

Encryption algorithms are complex mathematical equations that use a number, called a key, to encrypt data before transmission. This is done so that unauthorized persons who may intercept the transmission cannot access the data. In order to decrypt the transmission, the decoder must use the same key that was used to encrypt it. The decoder will perform the same calculations as the encoder and, if the key is the same, the data will be recovered.

The HS Series uses the CipherLinx™ algorithm, which is based on Skipjack, a cipher designed by the U.S. National Security Agency (NSA). At the time of this writing, there are no known cryptographic attacks on the full Skipjack algorithm. Skipjack uses 80-bit keys to encipher 64-bit data blocks. The CipherLinx™ algorithm uses Skipjack in a provably secure authenticated encryption mode both to protect the secrecy of the data and ensure that it is not modified by an adversary. 8 bits of data are combined with a 40-bit counter and 80 bits of integrity protection before being encrypted to produce each 128-bit packet.

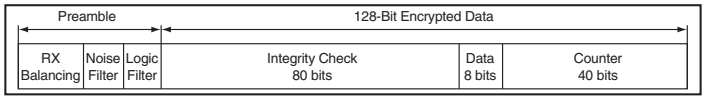

Figure 6: HS Series Data Structure

There are several methods an attacker may use to try to gain access to the data or the secured area. Because a key is used to interpret an encrypted message, trying to find the key is one way to attack the protected message. The attacker would either try using random numbers or go through all possible numbers sequentially to try to get the key and access the data. Because of this, it is sometimes believed that a larger key size will determine the strength of the encryption. This is not entirely true. Although it is a factor in the equation, there are many other factors that need to be included to maintain secure encryption.

One factor is the way that the underlying cipher (in the case of the CipherLinx™ algorithm, Skipjack) is used to encrypt the data. This is referred to as the cipher's "mode of operation." If a highly secure cipher is used in an insecure mode, the resulting encryption will be insecure. For example, some encryption modes allow an adversary to combine parts of legitimate encrypted messages together to create a new (and possibly malicious) encrypted message. This is known as a "cut-and-paste" attack. The mode of operation used by the CipherLinx™ algorithm is proven to prevent this type of attack.

Another critical factor is how often the message changes. To prevent code grabbing, most high-security systems send different data with each transmission. Some remote control applications will encrypt the message once per activation and repeat the same message over again until it is deactivated. This gives an attacker the opportunity to copy the message and retransmit it to maintain the state of the protected device and "hold the door open", or worse yet, have the option to come back later and gain access. The HS Series goes a step further and sends different data with EACH PACKET, so the data will change continuously during each transmission. This means that at 28,800bps, there will be a completely new 128-bit message sent every 25.5mS.

HS SERIES SECURITY OVERVIEW (CONT.)

Another factor is how often the message will be repeated and the intervals between repeats. Some applications use a counter to change the appearance of the message. This is good, but at some point, the counter will roll over and the message will be repeated. For example, if attackers were to copy an encrypted message and save it, they could potentially gain access to the protected device at a later time. Depending on the size of the counter, this vulnerability could occur frequently. The HS Series uses a 40-bit decrementing counter to keep this from ever happening. If the SEND line was held high continuously at the high baud rate (28,800bps), it would take 889 years before the counter would reach zero, at which point the key would be erased and the encoder would have to get a new key. The math used is: $[(2^{40} * 25.5ms) / (1000mS*60s*60m*24h*365d)] =$ 889 years. This large counter prevents a packet from ever being sent twice and prevents the encoder from ever losing sync with the decoder.

The key is generated with the decoder by the user through multiple button presses. This is ensures that the key is random and chosen from all 2^{80} possible keys. Since all of the keys are created by the user and are internal to the part, there is no list of numbers anywhere that could be accessed to compromise the system.

Encryption of the transmitted data is only one factor in the security of a system. With most systems, once an encoder is authorized to access a decoder, it can activate all of the decoder data lines. With the HS Series, each encoder can be set to only activate certain lines. This means that the same hardware can be set up with multiple levels of control, all at the press of a button.

Another factor in system security is the control of the encoder. If attackers gain control of the encoder, typically they would be able to access the system. The HS offers the option of adding a Personal Identification Number (PIN) to the encoder that must be entered before the encoder will activate. Furthermore, since each encoder has its own key and the Control Permissions are stored in the decoder, all the attackers would be able to do is duplicate the device that they have already taken. They will not be able to grant themselves greater authority, create a new controller, or replicate another encoder.

Before the encoder sends a packet, it will calculate the Hamming Weight (the number of '1's in the string) of the packet to determine the duty cycle. If the duty cycle is greater than 50% (more '1's than '0's), the encoder will logically invert all of the bits. This ensures that every packet will always contain 50% or less '1's. Since the FCC allows transmitter output power to be averaged over 100mS, this allows a legal improvement in link range and performance for many devices using an ASK / OOK transmitter. A 50% duty cycle is generally the best compromise between data volume and output power.

Some other manufacturers may use a Pulse Width Modulation (PWM) scheme or Manchester Encoding scheme to maintain a 50% duty cycle. Both of these methods work, but are inefficient and do not make use of the full link budget. The HS Series uses true serial data while maintaining a 50% duty cycle. Application Note AN-00310 covers these issues in detail.

DECODER POWER-UP

When the decoder first powers up, it will set the baud rate and go to sleep until: 1) the LEARN line is taken high, placing the decoder into Learn Mode, 2) a rising edge (low to high transition) on the COPY_IN line puts it into Get Copy Mode, or 3) a rising edge on the DATA_IN line puts it into Receive Mode.

DECODER RECEIVE MODE

When a rising edge is seen on the DATA_IN line, the decoder enters Receive Mode. It will begin by looking for a valid packet (meaning one that can be decrypted with the saved key) that has no errors. If the packet is valid, then the decoder will replicate the Data byte on its data lines and pull the MODE_IND line high. It will also output a number that represents the ID of the encoder. It will output this number once when the first valid packet is received. The decoder will then look for the next valid packet. If an error is detected at any time, or if the transmission cannot be decrypted with the saved key, then the decoder will ignore the packet and look for the next one.

If no valid packet is detected within 262mS, the decoder will go back to sleep.

DECODER CREATE KEY MODE

Create Key Mode is entered when the LEARN and CREATE_KEY lines on the decoder are taken high at the same time. When this happens, the MODE_IND line will go high as an indication that the decoder is ready to create the key. The CREATE_KEY line will need to go high ten times to set the key. Each edge on the line starts a timer that is used to populate a part of the key. This method is used to gather entropy so that the key will be truly random and will choose from among all 2^{80} possible keys.

Following the tenth press, the decoder will begin to send the key to the encoder on the KEY_OUT line. This will be output as a serial data stream, so it can be sent to the encoder by any method suitable for serial data transfer. This can include the use of a wire, contact points on an enclosure, or infrared. The HS Series Master Development System demonstrates wire and infrared transfer methods. You may wish to refer to the development system User's Guide for circuit schematics and further details.

Once the encoder receives the key on its KEY_IN line, it will send a confirmation to the decoder through its DATA_OUT line. This means that the standard mode of communication, whether a wire, RF, or infrared, must be active. When the decoder receives this confirmation, it will send a final confirmation through the KEY_OUT line. The MODE_IND LED lines on the encoder and the decoder will turn on for one second. This indicates that the encoder and decoder are now ready to be used. The decoder will output the key information for seventeen seconds or until it receives a valid confirmation from the encoder. If Control Permissions are going to be used, they may now be set as described in the Decoder Learn Mode section.

Note that the CREATE_KEY line should be connected to a button or another contact that will give random times between presses. Connecting this line to a deterministic source, such as a microprocessor clock, will not produce a secure key and could compromise the system.

DECODER LEARN MODE

Learn Mode serves several functions in the HS decoder. First, it provides the access point for other modes, such as Send Copy, Create Key, and Clear Memory. It also enables the decoder to learn the Control Permissions for an encoder. One of the most innovative features of the MS and HS Series is their ability to establish a unique user identity and profile for the device containing the encoder. In other products, all encoded transmissions are either recognized or denied based on the address. In cases where encoder and decoder addresses match, the state of all data lines is recognized and output. The HS Series uniquely allows a user or manufacturer to define which encoder inputs will be acknowledged by each decoder.

Consider this practical example: a three door garage houses Dad's Corvette, Mom's Mercedes, and Son's Yugo. With most competitive products, any user's keyfob could open any garage door as long as the addresses match. In a Linx HS-based system, the keyfobs could easily be configured to open only certain doors (guess which one Son gets to open!)

The decoder is placed into Learn Mode by pulling the LEARN line high and then taking it low within ten seconds. The decoder will begin toggling the MODE_IND line to indicate that the decoder is ready to learn the Control Permissions for a specific encoder. On the encoder end, simply activate each data line that it will be allowed to access and the decoder will record the lines that were activated as the Control Permissions. Pull the LEARN line high again or let the decoder time-out after 17 seconds, after which it will automatically exit Learn Mode and return to sleep.

The decoder can store up to 15 encoder IDs in memory. If a new encoder is learned while the memory is full, then the decoder will wrap around and write the new User Data over the first User Data in memory. The decoder will flash the MODE_IND line five times as an indication that the memory is full and the next code learned will overwrite the first. This must be clearly conveyed to the end user, since system users' access would be affected by the overwrites.

If the LEARN line is held high for ten seconds, the decoder will erase all of the saved User Data from memory. The MODE_IND line will be high for as long as the LEARN line is high, but after ten seconds, it will go low. Once the LEARN line is pulled low again, the MODE_IND line will go high for two seconds to indicate that the memory has been cleared.

If the LEARN line is held high at the same time as the SEND_COPY line, the decoder will enter Send Copy Mode. Once in this mode, the state of the LEARN line is not checked again, so it can be held high or pulled to ground, whichever is more convenient for the application.

If the LEARN line is held high at the same time as the CREATE_KEY line, the decoder will enter Create Key Mode.

DECODER TX ID

Upon receipt of the first valid packet, the decoder will output a binary number on the KEY_OUT line that corresponds to one of the learned transmitters. It will output the number only once, as soon as the first packet is accepted. An encoder's key, a 40-bit counter, and permissions are stored in one of 15 memory locations within the decoder. The decoder is able to output an 8-bit binary number that corresponds to the memory location of the encoder's information. The first encoder that is learned will be assigned 1, the second will be assigned 2 and so on. Once assigned, it is an easy task for a software program to read that number and associate it with a particular encoder. This makes applications such as logging access attempts simple.

The ID will be asynchronously output as an eight-bit binary number at the baud rate selected by the SEL_BAUD line. For example, if the SEL_BAUD line is grounded and the first encoder that the decoder learned sends a signal, then once the first packet is received, the decoder will output '0000 0001' (binary 1) at 2,400bps on the KEY_OUT line.

Application Note AN-00156 shows an example program that will read this number and display it on an LCD screen. The code is written in C and is well documented so that it can be easily modified for a specific application. The code and include files can be downloaded as a .zip file from the Linx website.

SEND COPY MODE

The HS Series decoder has the ability to send a copy of all of the learned encoders to another decoder. This makes it possible to use the same transmitter, encoder, and Control Permissions in multiple locations. Send Copy Mode is entered when the SEND_COPY line and the LEARN line are taken high at the same time. Once in this mode, the decoder will output all of its User Data on the KEY_OUT line for asynchronous transfer to another HS Series decoder. The decoder that receives the User Data becomes a copy and will lose the ability to create a key and send a copy. It can only set Control Permissions until its memory is erased, at which point it will regain full functionality.

The two decoders will need to be connected together with some method of transferring asynchronous serial data, such as a wire or short-range infrared. RF is not recommended for this transfer because it can represent a security risk, since RF will broadcast in all directions. A wire is the most secure method of transfer. Simply connect the KEY_OUT of the originating decoder to the COPY_IN line of the receiving decoder and connect the COPY_IN of the originating decoder to the KEY_OUT of the receiving decoder. Then connect the ground lines together and send the data (refer to Figure 11).

The Send Copy feature can be disabled by setting the SEND_COPY and CREATE_KEY lines high when the decoder is powered on. The MODE_IND line will blink three times to indicate that this has taken place. The decoder will not be able to send a copy of its User Data again until its memory is cleared.

GET COPY MODE

Get Copy Mode is entered when valid data is present on the COPY_IN line. The decoder will read the User Data from another decoder and save it in non-volatile memory. If the decoder is made into a copy of another decoder, it will not have the ability to send the copy or to create new keys. All of the User Data will need to be erased before the decoder can create new keys. This is done by holding the LEARN line high for ten seconds.

DECODER MODE_IND DEFINITIONS

The MODE_IND line is the primary means of indicating the state of the decoder to the user. The table below gives the definitions of the MODE_IND signals.

Receive Mode	ON for as long as the decoder is receiving valid data.
Create Key Mode	ON during the key generation process and OFF when created. Then ON for 1 second after the key has been successfully transferred and the user profile is saved. After the 15th user profile has been saved, it will blink* 5 times. The next user profile will overwrite the first.
Learn Mode	ON while the LEARN line is HIGH until taken LOW to enter Learn Mode, then it flashes* for 15 seconds until time-out or until the LEARN line goes HIGH again.
Erase Mode	ON while the LEARN line is held HIGH for 10 seconds and Erase Mode is entered, then it turns OFF. It turns back ON again for 2 seconds when erase is completed.
Send Copy Mode	ON for the duration of this mode.
Get Copy Mode	Blinks* each time a user profile has been successfully transferred and saved. If all user profiles have been successfully received, it will blink* twice.
Disable Send Copy	Blinks* three times when Send Copy is disabled.
*Blink = ON for 1sec and OFF 1/2sec *Flash = ON for 200ms and OFF for 200ms	

Table 5: HS Series Decoder MODE_IND Definitions

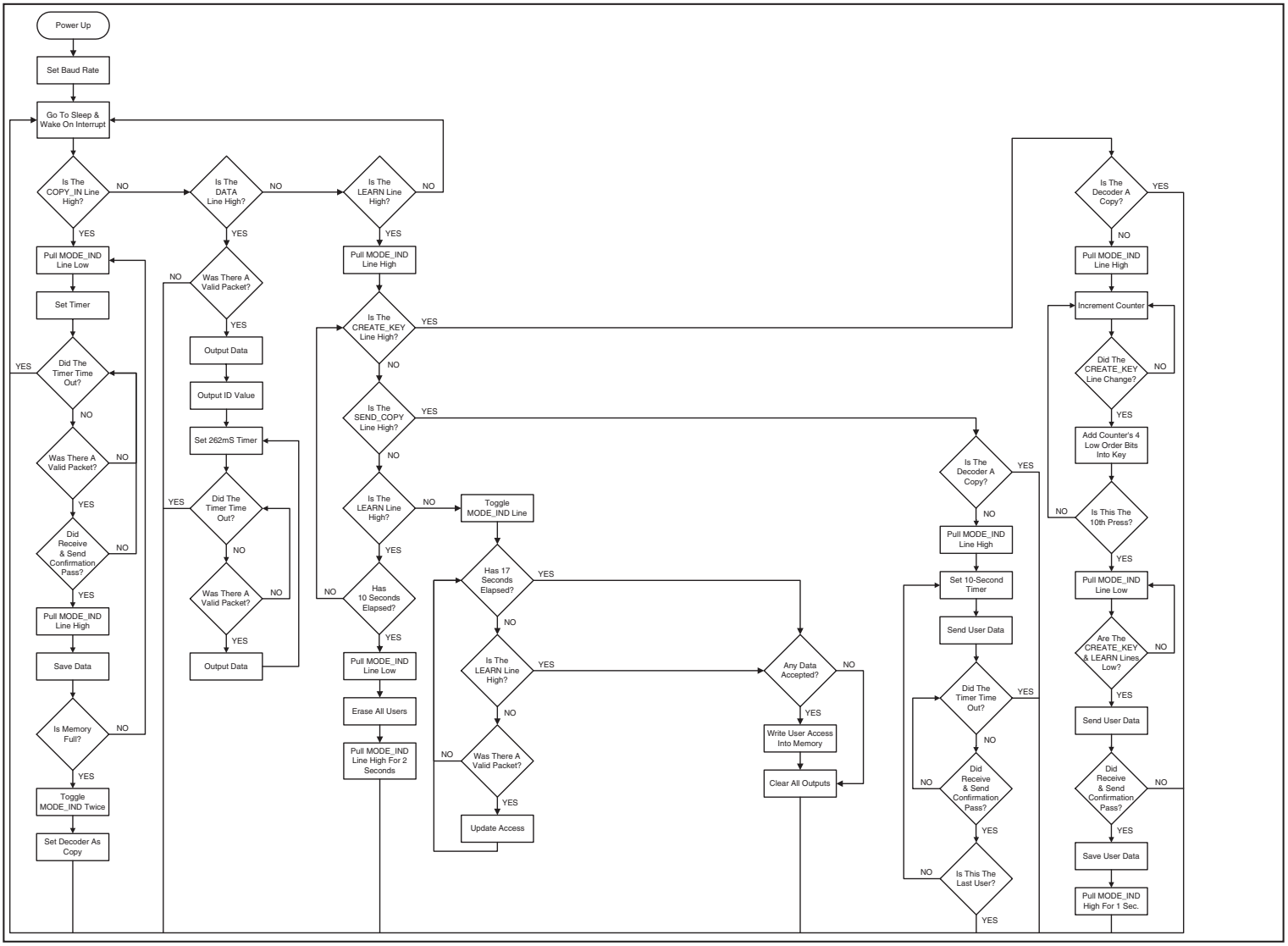

Figure 7: HS Series Decoder Flowchart

TYPICAL APPLICATIONS

The HS Series is ideal for registering button presses in secure remote control applications. An example application circuit of the decoder side is shown below.

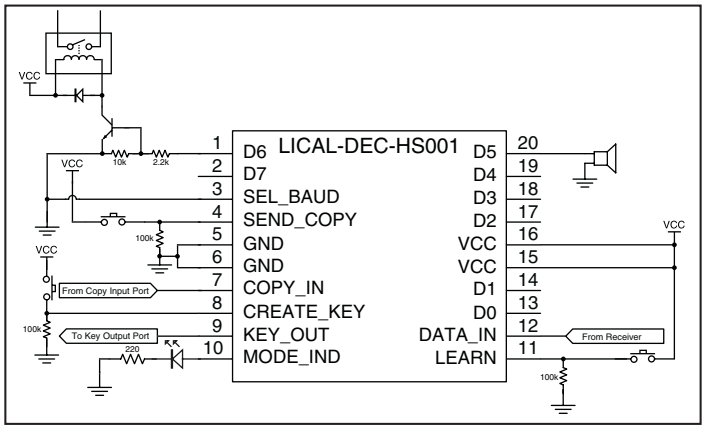

Figure 8: HS Series Decoder Application Circuit

In this circuit, the baud has been set for 2,400bps by pulling the SEL_BAUD line to ground.

SEND_COPY, CREATE_KEY, and LEARN are all connected to buttons that will pull the line high when pressed. Since the lines do not have internal resistors, 100kΩ resistors are used to pull the lines to ground when not in use.

COPY_IN is connected to a port that allows the transfer of the User Data from another decoder. This port can be a simple wire, an infrared receiver, or any other device that allows the transmission of asynchronous serial data.

The KEY_OUT line is connected to a port that allows the transfer of the key to an encoder or another decoder. This port can be a simple wire, an infrared diode, or any other device that allows the transmission of asynchronous serial data.

The KEY_OUT line can also be connected to a microprocessor or a PC to record the transmitter identity. Application Note AN-00156 has sample C code that will read the transmitter ID and display the ID number on an LCD screen.

A LED indicator is attached to the MODE_IND line to provide visual feedback that an operation is taking place. This line will source a maximum of 25mA, so the limiting resistor may not be needed, depending on the LED chosen.

The DATA_IN line is connected directly to the data output of the receiver.

Data Lines D0 through D7 can be connected directly to the external circuitry that is to be activated remotely. In this example, D5 is connected directly to a piezoelectric buzzer, which will cause the buzzer to sound when the D5 line on the encoder goes high. Line D6 will activate a relay through a transistor buffer when it goes high. A buffer like this may be needed if the decoder cannot source enough current or voltage to energize the relay coil. The decoder will turn on the transistor, which will provide the appropriate drive levels to the relay.

TYPICAL SYSTEM SETUP

The HS Series offers an unmatched combination of features and security, yet is easy for system designers and end users to operate. To demonstrate this, let's take a brief look at a typical user setup followed by more detailed design information. The Typical Applications sections of the encoder and decoder data guides show the circuit schematics on which these examples are based.

1. Create and exchange a key from a decoder to an encoder

The high security key is created and exchanged by placing the decoder in the Create Key Mode. The decoder's MODE_IND line LED will light to indicate that the decoder has entered Create Key Mode. The decoder's CREATE_KEY button is then pressed ten times to create the key. After the tenth press, the MODE_IND LED will turn off and the decoder will send the key out of the KEY_OUT line. The MODE_IND LED on the encoder will light to indicate that the key has been successfully transferred.

2. Establish Control Permissions

The user establishes what buttons on the encoder will be recognized by pressing the decoder LEARN button. The decoder's MODE_IND LED will start flashing and the user presses the buttons that will be allowed access. Control Permissions are stored when the LEARN button is pressed again or automatically after 17 seconds.

There are other powerful options such as programming a user PIN or copying a decoder but these simple steps are all that is required for a typical setup. It is really that simple for a manufacturer or end user to setup the product!

DESIGN STEPS TO USING THE HS SERIES

Key creation and exchange from a decoder to an encoder

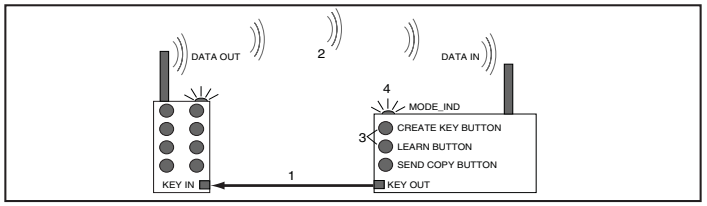

Figure 9: Steps to Exchange a Key

1. Provide a serial data connection from the decoder's KEY_OUT line to the encoder's KEY_IN line. Typically this would be a wire, contact, or infrared.
2. Provide a serial data connection from the encoder's DATA_OUT line to the decoder's DATA_IN line. Typically, this would be a wireless connection using a transmitter and receiver combination.
3. On the decoder, set the LEARN line high and then the CREATE_KEY line high to enter Create Key Mode. Take the LEARN line low, and toggle the CREATE_KEY line high and low ten times to generate the key.
4. The encoder and decoder will automatically exchange the key using the DATA_OUT / DATA_IN and KEY_OUT / KEY_IN lines. If the key exchange is successful, the decoder and encoder MODE_IND lines will go high for 1 second.

DESIGN STEPS TO USING THE HS SERIES (CONT.)

Creation of Control Permissions

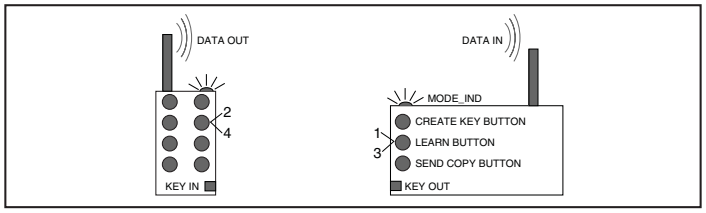

Figure 10: Steps to Create Control Permissions

1. On the decoder, set the LEARN line high, then take it low to enter Learn Mode.
2. While the decoder's MODE_IND line is toggling high / low, set a data line on the encoder high, then low. Repeat for each line to which permission will be granted.
3. After all the desired data lines have been selected, set the LEARN line high, then low again, or wait until the 15-second time-out occurs. The permissions will now be saved in the decoder.
4. Select the data lines during an actual transmission to confirm that the learn process was successful.

Send a copy of decoder A User Data to decoder B

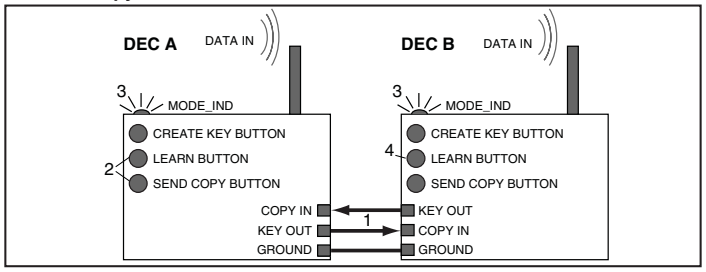

Figure 11: Steps to Send a Copy

1. Provide a serial data connection from decoder A's KEY_OUT line to decoder B's COPY_IN line, and decoder B's KEY_OUT line to decoder A's COPY_IN line.
2. On decoder A, set the LEARN line high and then set the SEND_COPY line high to enter Send Copy Mode. Next, clear both the LEARN line and the SEND_COPY line low.
3. The MODE_IND line on decoder A will be set high while data is being exchanged. The MODE_IND line on decoder B will toggle as each user profile is being received from decoder A. If a successful copy has been made, the MODE_IND on decoder B will blink twice.
4. The copied decoder B will only be allowed to learn new permissions from the copied set of users and activate data lines accordingly. All other features will be removed from decoder B until its memory has been successfully erased.

SYSTEM EXPANSION

A system based on the HS Series can be expanded in several ways. One of the simplest is to add users by adding more decoders to the receiver output. With each decoder added to the chain, another 15 encoders can be used within the system. The associated decoder data line outputs can be connected together so that any decoder will activate the circuit. So, if Data Line D1 is being used to activate a relay, then the D1 lines of Decoders A, B, and C can all be connected to the input of the relay. Diodes will be needed to isolate the active line from the inactive lines, thus preventing a short circuit.

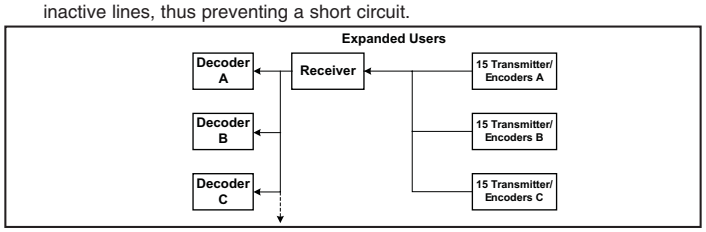

Figure 12: Expanding Users with the HS Series

The ability of the HS Series decoder to create copies of itself allows for the expansion of access points within a system. This means that the same encoder can access multiple locations without any hardware changes. An example of this would be a single keyfob transmitter that can open the front door of a building and the supply room. A master decoder is first set up with all of the users for the system. It is then connected to other HS Series decoders to transfer its User Data. These copies are then deployed in other locations and will respond to an encoder the same way the master system will. For greater security, these copies cannot make other copies or add new users, just change Control Permissions. Because of this, it is recommended that only copies are used in the system while the original is stored in a secure location. This is particularly useful in settings where access to the decoder cannot be strictly limited.

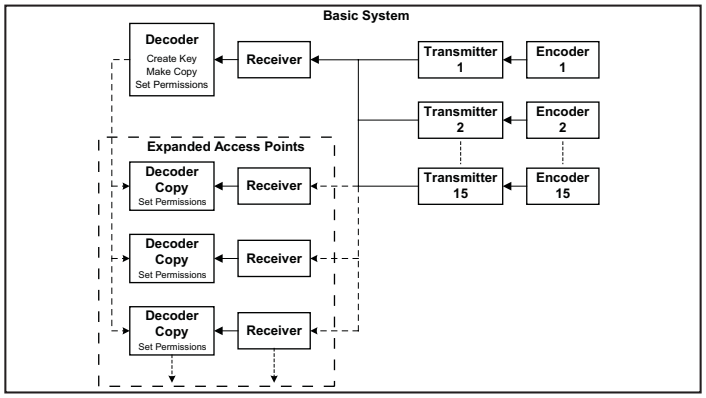

Figure 13: Expanding Access Points with the HS Series

U.S. CORPORATE HEADQUARTERS

LINX TECHNOLOGIES, INC.
159 ORT LANE
MERLIN, OR 97532

PHONE: (541) 471-6256
FAX: (541) 471-6251
www.linxtechnologies.com

Disclaimer

Linx Technologies is continually striving to improve the quality and function of its products. For this reason, we reserve the right to make changes to our products without notice. The information contained in this Overview Guide is believed to be accurate as of the time of publication. Specifications are based on representative lot samples. Values may vary from lot-to-lot and are not guaranteed. "Typical" parameters can and do vary over lots and application. Linx Technologies makes no guarantee, warranty, or representation regarding the suitability of any product for use in any specific application. It is the customer's responsibility to verify the suitability of the part for the intended application. NO LINX PRODUCT IS INTENDED FOR USE IN ANY APPLICATION WHERE THE SAFETY OF LIFE OR PROPERTY IS AT RISK.

Linx Technologies DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL LINX TECHNOLOGIES BE LIABLE FOR ANY OF CUSTOMER'S INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING IN ANY WAY FROM ANY DEFECTIVE OR NON-CONFORMING PRODUCTS OR FOR ANY OTHER BREACH OF CONTRACT BY LINX TECHNOLOGIES. The limitations on Linx Technologies' liability are applicable to any and all claims or theories of recovery asserted by Customer, including, without limitation, breach of contract, breach of warranty, strict liability, or negligence. Customer assumes all liability (including, without limitation, liability for injury to person or property, economic loss, or business interruption) for all claims, including claims from third parties, arising from the use of the Products. The Customer will indemnify, defend, protect, and hold harmless Linx Technologies and its officers, employees, subsidiaries, affiliates, distributors, and representatives from and against all claims, damages, actions, suits, proceedings, demands, assessments, adjustments, costs, and expenses incurred by Linx Technologies as a result of or arising from any Products sold by Linx Technologies to Customer. Under no conditions will Linx Technologies be responsible for losses arising from the use or failure of the device in any application, other than the repair, replacement, or refund limited to the original product purchase price. Devices described in this publication may contain proprietary, patented, or copyrighted techniques, components, or materials. Under no circumstances shall any user be conveyed any license or right to the use or ownership of such items.

Certain products and methods presented in this Data Guide are protected by one or more patents pending.