HIGH SECURITY

HS SERIES

ENCODER

HS SERIES ENCODER DATA GUIDE

DESCRIPTION

HS Series encoders and decoders are designed for maximum security remote control applications. The HS encoder encodes the status of up to eight buttons or contacts into a highly secure encrypted output intended for wireless transmission via a RF or infrared link. 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, low power consumption, and easy setup.

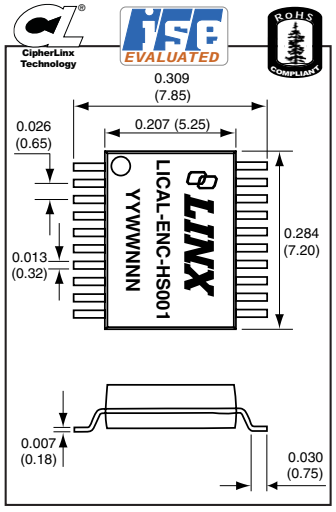

Figure 1: Package Dimensions

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	–
ENCODER 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	–
SEND High to DATA_OUT	–	–	3.3	–	mS	–
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.

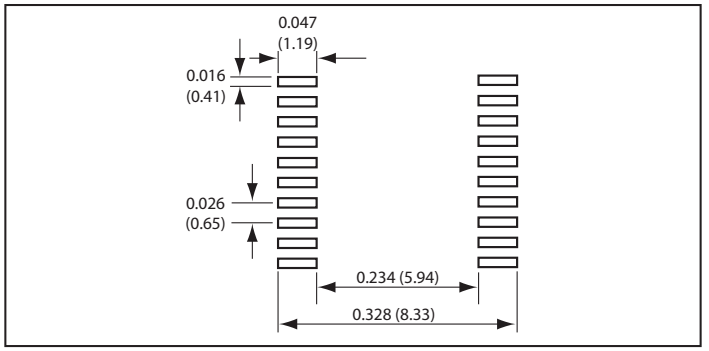

Figure 2: HS Series Encoder PCB Layout Dimensions

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.

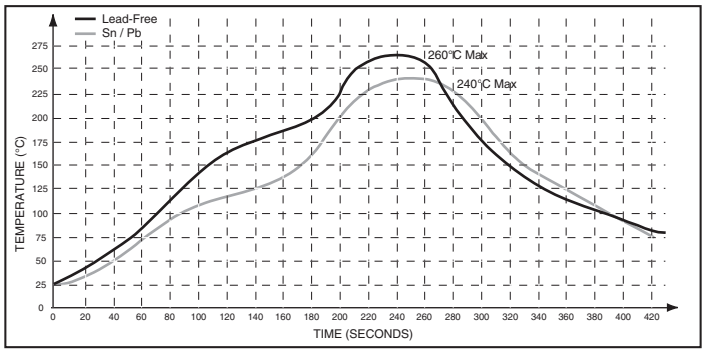

Figure 3: HS Series Reflow Profile

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

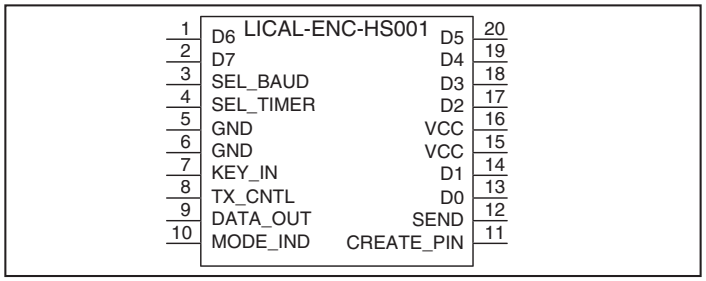

Figure 4: HS Series Encoder Pin Assignments

Pin Name	Pin Number	I/O	Description
D0-D7	1, 2, 13, 14, 17-20	I	Data Input Lines
SEL_BAUD	3	I	Baud Rate Selection Line
SEL_TIMER	4	I	PIN Time-Out Timer Select Line
GND	5, 6	—	Ground
KEY_IN	7	I	Key Input Pin
TX_CNTL	8	O	External Transmitter Control Line
DATA_OUT	9	O	Serial Data Output
MODE_IND	10	O	Mode Indicator Output
CREATE_PIN	11	I	Create PIN Mode Selection Line
SEND	12	I	Encoder Send Data Line
V_{CC}	15, 16	—	Positive Power Supply

Table 3: HS Series Encoder Pin Assignments

NOTE:

None of the input lines have internal pull-up or pull-down resistors. The input lines must always 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.

ENCODER MODE_IND INDICATION TABLE

The MODE_IND line is the primary means of indicating the state of the encoder to the user. The table below provides definitions for the MODE_IND signals.

Get Key Mode	ON for 1 second after a successful key transfer.
Create PIN Mode	Flashes* for 15 seconds while waiting for user to enter a PIN. It stops flashing when the fourth number is entered or when it times out.
Enter PIN Mode	ON when each PIN is entered.
*Flash = ON for 200ms and OFF for 200ms	

Table 4: HS Series Encoder MODE_IND Definitions

PIN DESCRIPTIONS

Data Lines

The encoder has eight data lines, D0 through D7. when the SEND line goes high, the states of these lines are recorded, encrypted for transmission, then reproduced on the outputs of the decoder.

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 5: Baud Rate Selection Table

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

SEL_TIMER

This line is used to set the length of inactive time before PIN reentry is required.

GND

These lines are connected to ground.

KEY_IN

This line is used to input the key from the decoder.

TX_CNTL

This line goes high when the SEND line goes high and low when the SEND line goes low. This can be used to power up external devices, such as a transmitter, when the encoder is sending data, and power it down when the encoder is asleep. It can also be used to drive a LED for visual indication of transmission.

DATA_OUT

The encoder will output an encrypted serial data stream on this line. This line can directly interface with all Linx RF transmitter modules or it can be used to modulate an IR diode.

MODE_IND

This line will be activated while the encoder is in Get Key Mode or Create Pin Mode. It allows the connection of a LED or other indicator for user feedback.

CREATE_PIN

When this line is taken high, the encoder will enter Create PIN Mode and allow the user to set a Personal Identification Number (PIN) to control encoder access.

SEND

When this line goes high, the encoder will record the states of the data lines, encrypt them for transmission, and send the packet as a serial bit stream through the DATA_OUT line at the baud rate selected by the state of the SEL_BAUD line.

V_{CC}

This is 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.

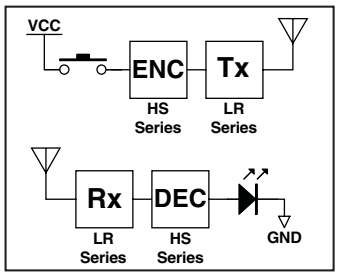

Figure 5: Remote Control Block Diagram

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 is transmitted every time, the decoder has 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 encrypts 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 with every packet, not just every button press.

Decoding of the received data signal is accomplished by a corresponding Linx 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 control 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.

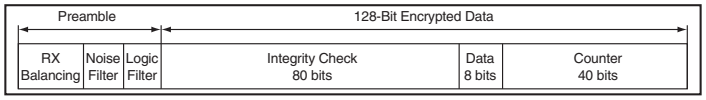

Figure 6: HS Series Data Structure

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.

ENCODER OPERATION

Upon power-up, the encoder sets the baud rate based on the state of the SEL_BAUD line, pulls the TX_CNTL line low, and goes into a low-power sleep mode. It will remain asleep until either the KEY_IN, SEND, or CREATE_PIN line goes high. These lines place the encoder in either Get Key Mode, Send Mode, or Create PIN Mode as described in the following sections.

ENCODER GET KEY MODE

When the encoder registers activity on the KEY_IN line, it will enter Get Key Mode. In this mode, the encoder will look for an encryption key and user ID from a decoder. When it receives this information, it will send a confirmation on the DATA_OUT line to the decoder. It will then look for a final confirmation from the decoder on the KEY_IN line. Once this confirmation is received, the encoder will take the MODE_IND line high for one second to indicate that the key has been successfully transferred and that the units may now work together.

ENCODER SEND MODE

When the SEND line goes high, the encoder will enter Send Mode. It will pull the TX_CNTL line high to activate the transmitter and record the state of the data lines. The encoder will then encrypt the data using the saved key and send it through the DATA_OUT line. It will continue doing this for as long as the SEND line is high, updating the state of the data lines with each transmission. Once SEND is pulled low, the encoder will finish the current transmission, pull TX_CNTL low to deactivate the transmitter, and go to sleep.

For simple applications that require only a single input, SEND can be tied directly to the data input line, allowing a single connection. If additional lines are used in this manner, diodes or dual contact switches will be necessary to prevent voltage on one data line from activating all of the data lines. The Typical Applications section of this data guide demonstrates the use of diodes for this purpose.

ENCODER CREATE PIN MODE

For higher security applications, the HS Series encoder has the option to set a Personal Identification Number (PIN) to control access to the encoder. This PIN is a four-digit combination of the eight data lines that must be entered before the encoder will transmit any commands to the decoder.

Create PIN Mode is entered by pressing the CREATE button on the encoder. The MODE_IND line will begin flashing to indicate that the encoder is ready for the PIN to be entered. The user will have 15 seconds to press any 4-button combination to set the PIN. After the fourth button press, the MODE_IND line will go low. If 4 buttons are not pressed or the CREATE line goes high within the 15 second window, no PIN will be set. Once created, the PIN can be erased only by learning a new key from the decoder.

Once the PIN has been set, the user must enter it correctly before the encoder will transmit any commands. When entered, the encoder will be active for a period of time set by the SEL_TIMER line. If this line is connected to ground, the PIN will need to be entered after 15 minutes of inactivity. If this line is high, the PIN will need to be entered after 30 seconds of inactivity. If no PIN is set, then the encoder will activate as soon as the SEND line goes high.

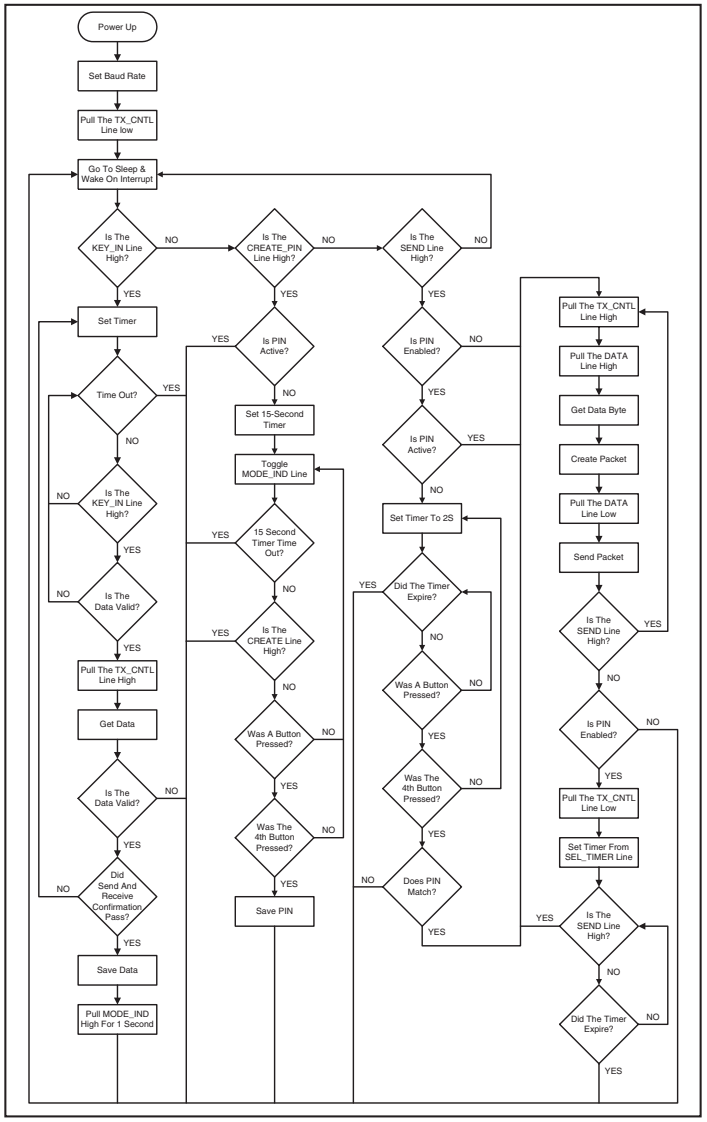

Figure 7: HS Series Encoder Flowchart

TYPICAL APPLICATION

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

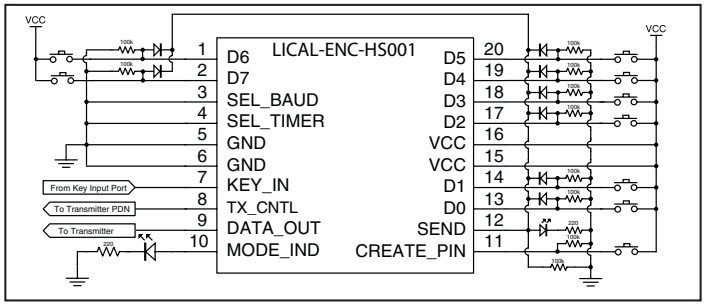

Figure 8: HS Series Encoder Application Circuit

In this example, the data lines are connected to buttons, and when any button is pressed, the SEND line is pulled high and causes the encoder to transmit. Diodes are used to prevent the voltage on one data line from affecting another.

The KEY_IN line is attached to a port that allows the key to be transferred from the decoder during setup. To ensure security, this would normally be a wire, contact, or short range IR link, although any connection capable of transferring asynchronous serial data may be utilized.

None of the inputs have pull-up or pull-down resistors internally, so 100kΩ pull-down resistors are used on the data, SEND, and CREATE_PIN lines. These resistors are used to pull the lines to ground when the buttons are not being pressed, which ensures that the pins are always in a known state and not floating. Without these resistors, the state of the lines cannot be guaranteed and encoder operation may not be predictable.

A LED is attached to the MODE_IND line to provide visual feedback to the user 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 and the brightness desired. A LED can also be connected to the TX_CNTL line to provide visual indication that the encoder is sending data.

Outgoing encrypted data will be sent via the DATA_OUT line at the baud rate determined by the state of the SEL_BAUD line. In the circuit above, the baud has been set for 4,800bps by pulling it to ground. The DATA_OUT line can be connected directly to the DATA_IN line of a Linx transmitter or other wireless device.

The TX_CNTL line may be connected to the PDN line of a Linx transmitter so that the module will enter a low power state when not in use.

In this example, the data lines are pulled high by simple pushbutton switches, but many other methods may be employed. Contacts, reed switches, or microcontrollers are just some examples of other ways to pull the data lines high. The flexibility of the encoder, combined with the associative options of the matching decoder, opens a new world of options for creative product designers.

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

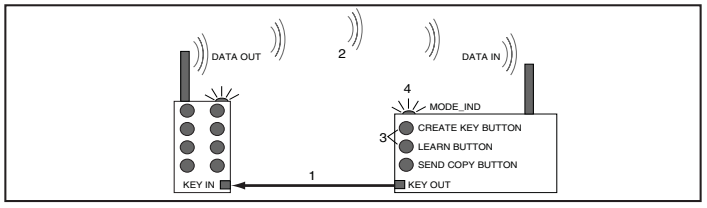

Figure 9: Steps to Exchange a Key

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

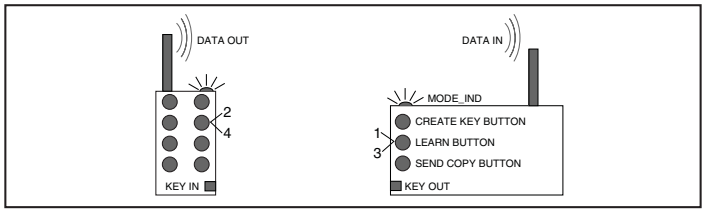

Figure 10: Steps to Create Control Permissions

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 17-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 permissions have been successfully created.

USING THE OPTIONAL ENCODER PIN

Creation of an encoder PIN

1. Set the CREATE line high, then low to enter Create PIN Mode. The MODE_IND line will begin toggling high / low until either a PIN is successfully entered or 15 seconds has passed.
2. To enter the PIN, set high then low a sequence of any four data lines. The MODE_IND will stop toggling and the PIN will be created.
3. To cancel the Create PIN Mode prior to the fourth entry, either wait for the 15 second timeout to pass or set and clear the CREATE line. The MODE_IND will stop toggling and no PIN will be created.
4. If a new KEY is created, the PIN will be automatically erased.

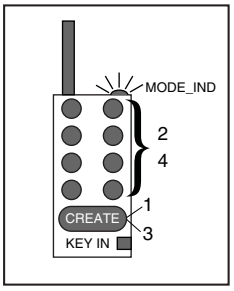

Figure 11: Encoder PIN Setup

Using the PIN

1. The PIN is entered by setting each data line high, then taking it low until all four entries have been made. There is a maximum 2-second time limit between entries after which the PIN must be reentered in its entirety.
2. Once the PIN is successfully entered, the encoder will be operational unless it is inactive for a period longer than what is chosen by the SEL_TIMER line, in which case PIN reentry would be necessary.

ONLINE RESOURCES

LINX® TECHNOLOGIES

www.linxtechnologies.com

- **Latest News**
- **Data Guides**
- **Application Notes**
- **Knowledgebase**
- **Software Updates**

If you have questions regarding any Linx product and have Internet access, make www.linxtechnologies.com your first stop. Our website is organized in an intuitive format to immediately give you the answers you need. Day or night, the Linx website gives you instant access to the latest information regarding the products and services of Linx. It's all here: manual and software updates, application notes, a comprehensive knowledgebase, FCC information, and much more. Be sure to visit often!

ANTENNA FACTOR

www.antennafactor.com

The Antenna Factor division of Linx offers a diverse array of antenna styles, many of which are optimized for use with our RF modules. From innovative embeddable antennas to low-cost whips, domes to Yagis, and even GPS, Antenna Factor likely has an antenna for you, or can design one to meet your requirements.

CONNECTOR CITY
THE VALUE OF CONNECTIONS

www.connectorcity.com

Through its Connector City division, Linx offers a wide selection of high-quality RF connectors, including FCC compliant types such as RP-SMAs that are an ideal match for our modules and antennas. Connector City focuses on volume OEM requirements, which allows standard and custom RF connectors and cable assemblies to be offered at a low cost.

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.