Linx TECHNOLOGIES

HS Series
Remote Control Decoder
Data Guide

Wireless made simple®

Warning: Some customers may want Linx radio frequency ("RF") products to control machinery or devices remotely, including machinery or devices that can cause death, bodily injuries, and/or property damage if improperly or inadvertently triggered, particularly in industrial settings or other applications implicating life-safety concerns ("Life and Property Safety Situations").

NO OEM LINX REMOTE CONTROL OR FUNCTION MODULE SHOULD EVER BE USED IN LIFE AND PROPERTY SAFETY SITUATIONS. No OEM Linx Remote Control or Function Module should be modified for Life and Property Safety Situations. Such modification cannot provide sufficient safety and will void the product's regulatory certification and warranty.

Customers may use our (non-Function) Modules, Antenna and Connectors as part of other systems in Life Safety Situations, but only with necessary and industry appropriate redundancies and in compliance with applicable safety standards, including without limitation, ANSI and NFPA standards. It is solely the responsibility of any Linx customer who uses one or more of these products to incorporate appropriate redundancies and safety standards for the Life and Property Safety Situation application.

Do not use this or any Linx product to trigger an action directly from the data line or RSSI lines without a protocol or encoder/decoder to validate the data. Without validation, any signal from another unrelated transmitter in the environment received by the module could inadvertently trigger the action.

All RF products are susceptible to RF interference that can prevent communication. RF products without frequency agility or hopping implemented are more subject to interference. This module does not have a frequency hopping protocol built in.

Do not use any Linx product over the limits in this data guide. Excessive voltage or extended operation at the maximum voltage could cause product failure. Exceeding the reflow temperature profile could cause product failure which is not immediately evident.

Do not make any physical or electrical modifications to any Linx product. This will void the warranty and regulatory and UL certifications and may cause product failure which is not immediately evident.

Ordering Information

Ordering Information	
Part Number	**Description**
LICAL-ENC-HS001	HS Encoder
LICAL-DEC-HS001	HS Decoder
MDEV-LICAL-HS	HS Master Development System

HS decoders are shipped in reels of 1,600

Figure 2: Ordering Information

Absolute Maximum Ratings

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 Input Pins		25		mA
Max. Current Into V_{CC}		250		mA
Max. Current Out Of GND		300		mA
Operating Temperature	–40	to	+85	ºC
Storage Temperature	–65	to	+150	ºC

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.

Figure 3: Absolute Maximum Ratings

Timings

Encoder SEND to Decoder Activation Times (ms)	
Baud Rate	**Decoder Activation Time**
4,800	67
28,800	36

Figure 4: Encoder SEND to Decoder Activation Times (ms)

Pin Assignments

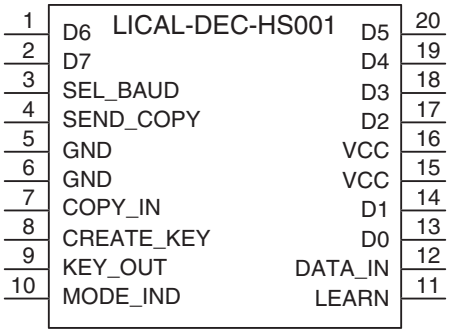

Figure 6: HS Series Decoder Pin Assignments

Pin Descriptions

Pin Number	Name	I/O	Description
1, 2, 13, 14, 17–20	D0–D7	O	Data Output Lines. These lines reproduce the state of the encoder's data lines upon reception of a valid packet.
3	SEL_BAUD	I	Baud Rate Selection Line. This line is used to select the baud rate of the serial data stream. If the line is high, the baud rate is 28,800bps, if it is low, the baud rate is 4,800bps. The baud rate must be set before power up. The transcoder will not recognize any change in the baud rate setting after it is on.
4	SEND_COPY	I	Send Copy Activation Line. When this line is taken high while the LEARN line is high, the decoder enters Send Copy Mode and outputs the User Data on the KEY_OUT line. When taken high while the CREATE_KEY line is high at power-up, Send Copy Mode is disabled.
5, 6	GND		Ground
7	COPY_IN	I	Copy Input Line. This line is used to input the User Data from another decoder.
8	CREATE_KEY	I	Create Key Activation Line. When this line is taken high while the LEARN line is high, the decoder enters Create Mode and creates a key and encoder ID. It then sends these to the encoder through the KEY_OUT line. When taken high while the SEND_COPY line is high at power-up, Send Copy Mode is disabled.
9	KEY_OUT	O	Key and Transmitter ID Output Line. When the SEND_COPY line is high when the LEARN line is taken high, the decoder outputs the User Data on this line. This line also outputs the transmitter identity upon reception of the first valid packet of each session.

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.

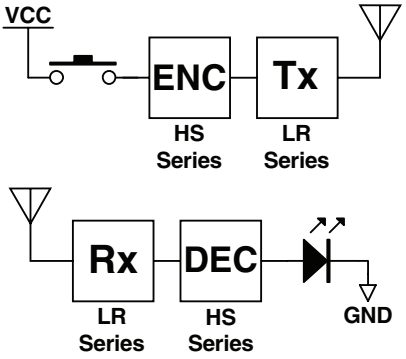

Figure 8: Remote Control Block Diagram

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,

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 states 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 activates its logic-level outputs, which can be used to control external circuitry. The encoder sends 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 for 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 responds to the encoder's commands based on its permissions. If an encoder has not been associated with a decoder, its commands are not recognized.

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 performs the same calculations as the encoder and, if the key is the same, the data is 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.

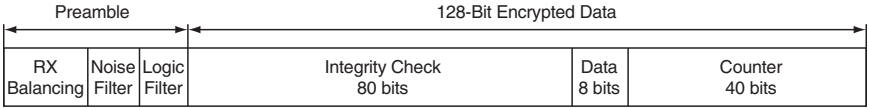

Figure 9: HS Series Data Structure

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 determines 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 is 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.

encoder that must be entered before the encoder activates. 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 calculates 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 logically inverts all of the bits. This ensures that every packet always contains 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 sets the baud rate and goes 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 begins 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 replicates the Data byte on its data lines and pulls the MODE_IND line high. It also outputs a number that represents the ID of the encoder once when the first valid packet is received. The decoder then looks 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 ignores the packet and looks for the next one.

If no valid packet is detected within 262ms, the decoder goes back to sleep.

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 HS Series is its 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 are 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 begins 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 should be allowed to access and the decoder records the lines that were activated as the Control Permissions. Pull the LEARN line high again or let the decoder timeout after 17 seconds, after which it automatically exits Learn Mode and returns to sleep.

The decoder can store up to 15 encoder IDs in memory. When the 15th encoder is learned, the decoder flashes the MODE_IND line five times as an indication that the memory is full. The next address learned overwrites the first address in memory. This must be clearly conveyed to the end user, since system users' access would be affected by the overwrites. The memory retains all of the learned encoders if power is removed.

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

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 is high when the LEARN line is taken high. Once in this mode, the decoder outputs 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 loses 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 regains full functionality.

The two decoders 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 is 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 15).

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 blinks three times to indicate that this has taken place. The decoder cannot 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 reads the User Data from another decoder and saves it in non-volatile memory. If the decoder is made into a copy of another decoder, it cannot send the copy or to create new keys. All of the User Data needs to be erased before the decoder can create new keys. This is done by holding the LEARN line high for ten seconds.

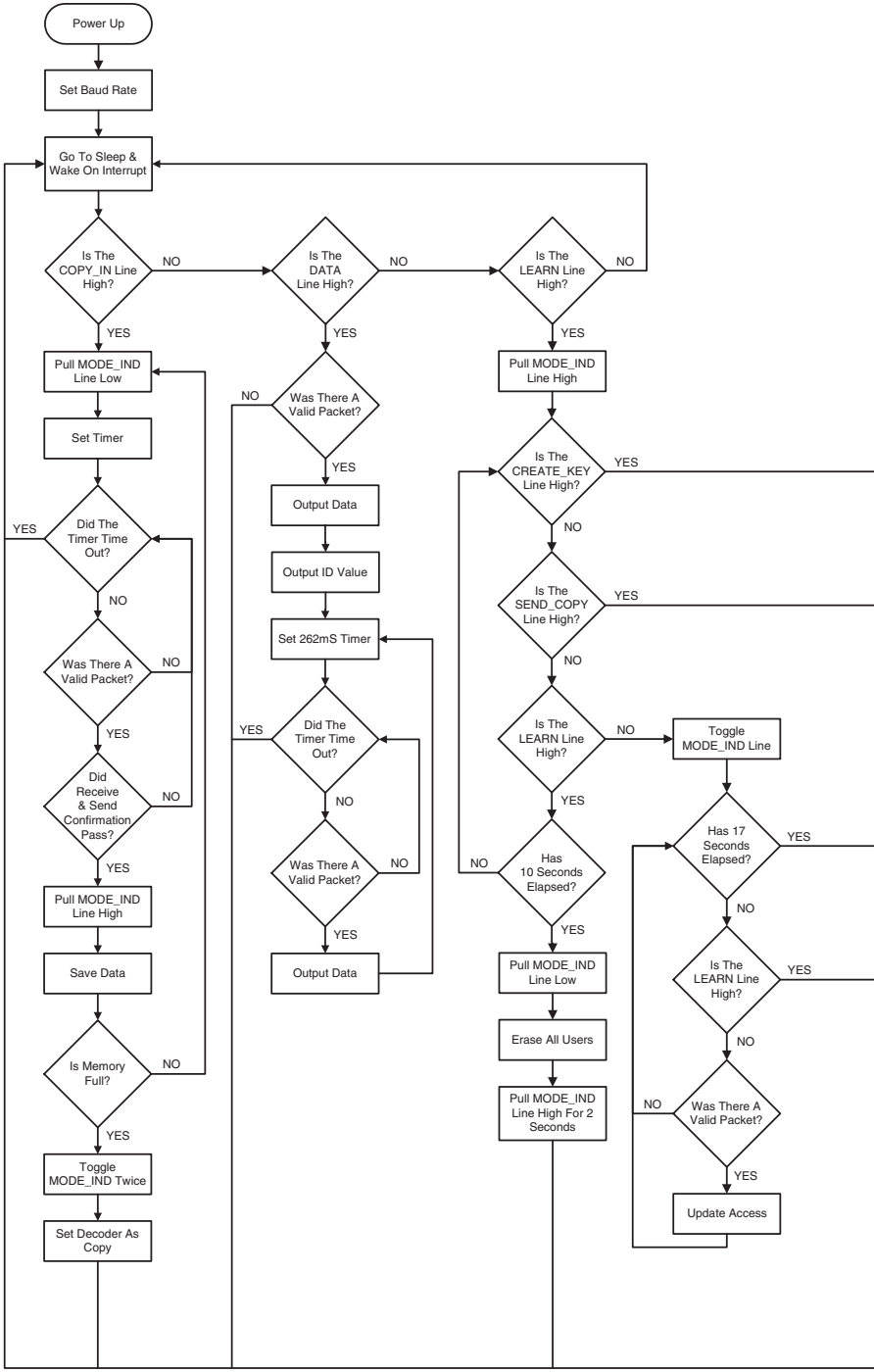

Figure 11: HS Series Decoder Flowchart

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 in Figure 12.

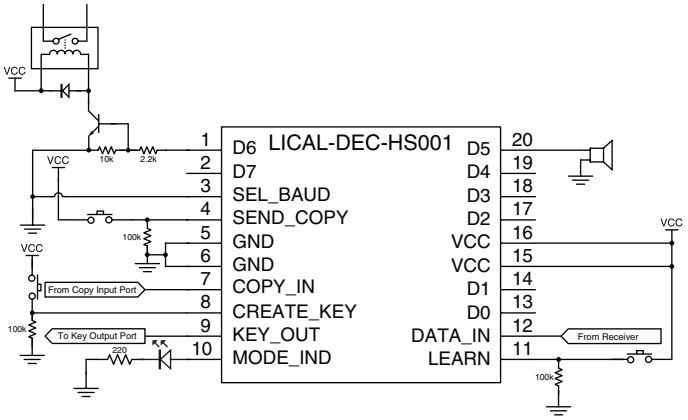

Figure 12: HS Series Decoder Application Circuit

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 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 the buttons are not pressed.

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 circuit that transfers 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 transfers 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 reads the transmitter ID and displays it on an LCD screen.

An LED indicator is attached to the MODE_IND line to provide visual feedback that an operation is taking place. This line sources a maximum of 25mA.

Design Steps to Using the HS Series

Key Creation and Exchange from a Decoder to an Encoder.

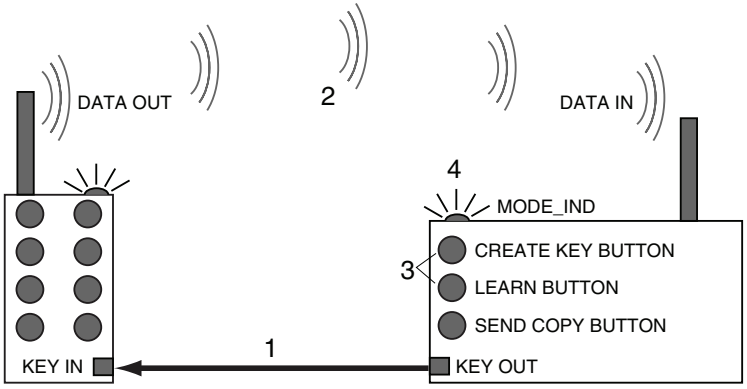

Figure 13: Steps to Exchange a Key

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 CREATE_KEY line high and then the LEARN 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 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 go high for 1 second.

Send a Copy of Decoder A User Data to Decoder B

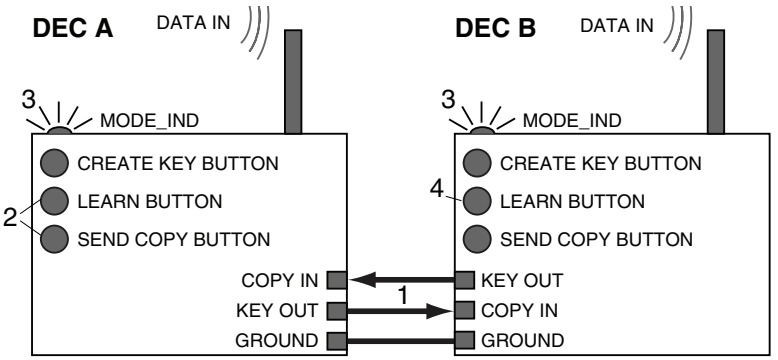

Figure 15: Steps to Send a Copy

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 SEND_COPY line high and then set the LEARN line high to enter Send Copy Mode. Next, take both lines low.

3. The MODE_IND line on decoder A is set high while data is being exchanged. The MODE_IND line on decoder B toggles as each user profile is being received from decoder A. If a successful copy has been made, the MODE_IND on decoder B blinks twice.

4. The copied decoder B is only allowed to learn new permissions from the copied set of users and activate data lines accordingly. All other features are removed from decoder B until its memory is successfully erased.

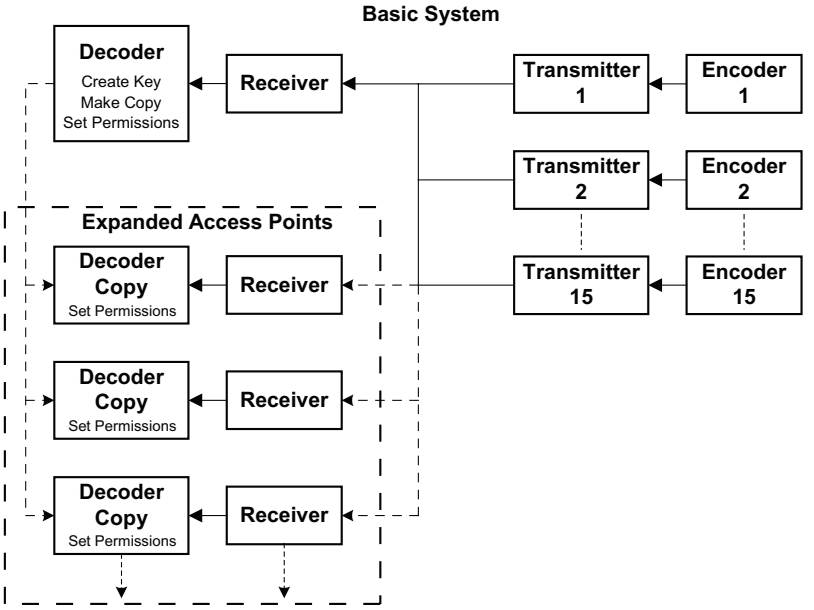

Figure 17: Expanding Access Points with the HS Series

Linx Technologies
159 Ort Lane
Merlin, OR, US 97532

Phone: +1 541 471 6256
Fax: +1 541 471 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 Data 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.

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Other Development Tools ***category:***

Click to view products by Linx Technologies ***manufacturer:***

Other Similar products are found below :

118777-HMC721LP3E ADL5391-EVALZ DS100BR410EVK-4/NOPB BK0004 BK0012 SN65MLVD2-3EVM TX517EVM DS80EP100-EVK 118777-HMC723LP3E MAX9979EVKIT MAX5432EVKIT+ MAX3397EEVKIT+ MAX14611EVKIT# MAX4951AEEVKIT+ MAX9647EVKIT# MAX9684EVKIT# MAX4952AEVKIT+ MAX13035EEVKIT+ DS1964SEVKIT# ESD-EVM-001 EVAL-CN0414-ARDZ K2-LTCC-WBZ+ K1-DBTC+ MAX14842EVKIT+ K2-DBTC+ EVAL01-HMC749LC3C TPD6F002-Q1EVM TS9002DB DS80PCI800EVK/NOPB HSC-ADC-FIFO5-INTZ EVAL-SDP-CH1Z 800-00360 EVAL-ADN469XEFDEBZ EVAL-ADN469XEHDEBZ MAXREFDES70# MAXREFDES67# MAXREFDES63# MAXREFDES64# BK0009 DS32EV100-EVK TS9001DB DK-RV-1.8-33 74AUP1Z04EVB DK-RV-1.8.TRK-33 800-00040 800-00060 800-00080 XRT5997ES AD633-EVALZ 118777-HMC722LC3C