Keeloq™ Code Hopping Decoder

FEATURES

- **Unique Master Transmitter for Each System**
- **Up to Five (5) Learnable Other Transmitters Per Decoder**
- **Each Transmitter with a Unique Key**
- **Secure Transmitter Self-Learning**
- **Separate Transmitter Synchronization**
- **Automatic Compensation for Differences in Component Timing**
- **Master Transmitter Applications:**
  - **— Authorize self-learning**
  - **— Higher user priority**
  - **— Privileged Access**
- **Outputs Permanently Available:**
  - **— Up to 3 pulsed outputs**
  - **— 1 latched output**
  - **— Valid signal indicator (REPEAT)**
  - **— Delayed function indicator (DELAY)**
  - **— Master transmitter indicator**
- **22-pin SOIC and PDIP**

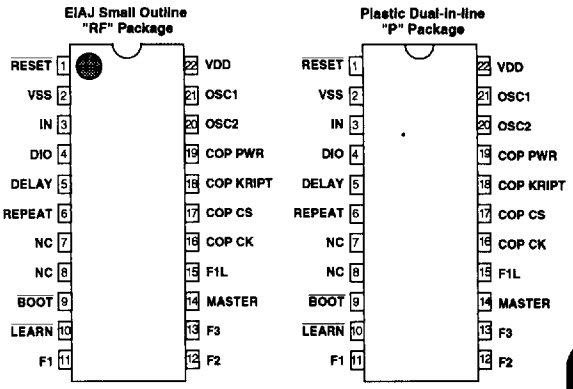
OVERVIEW

The XL109 is a low cost remote control decoder for use in security systems. It makes use of revolutionary code hopping technology, offering an unprecedented level of security in remote control systems. Typical applications include vehicle security and access control systems.

The decoder is designed to be used with XL105 based transmitters and uses the XL105 as a coprocessor. The XL105 is used as a non-volatile storage and decoding device. Direct access to the XL105 coprocessor can be arranged from outside, making it possible for an external microcontroller to use the coprocessor as non-volatile storage, and for the user to program the coprocessor on the PC board.

The XL109 decoder contains sophisticated error checking algorithms to ensure that only valid transmissions are decoded. Sophisticated synchronization checking ensures that the user can remain totally unconcerned with synchronization issues. Extensive history evaluation provides maximum protection against "code grabbing" and other unauthorized code generation technologies. Automatic baud rate compensation ensures that the system will remain operational despite variations in timing component values.

PIN CONFIGURATION



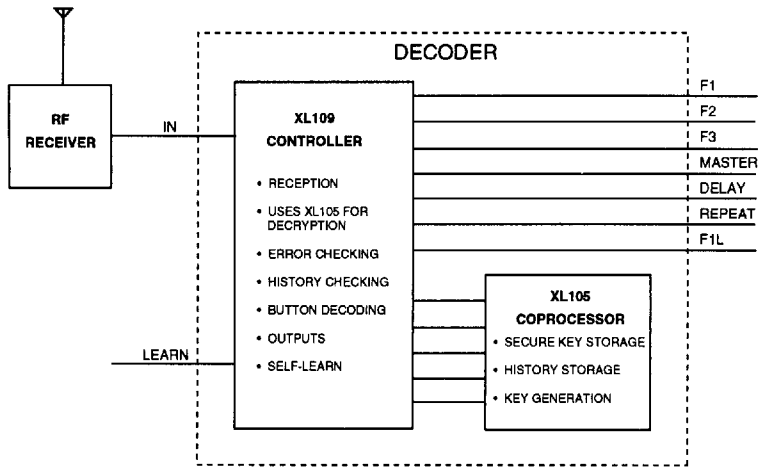
PIN NAMES

$\overline{\text{RESET}}$	Hardware Reset Output
VSS	Ground Reference
IN	Decoder Input
DIO	Data To/From Coprocessor
DELAY	Delayed Function Output
REPEAT	Valid Signal Indicator
NC	No Connect
$\overline{\text{BOOT}}$	Cold Reset Input
$\overline{\text{LEARN}}$	Self-Learning Select
F1-F3	Pulsed Output
VDD	Supply Voltage
OSC1-2	Oscillator Timing
COP PWR	Coprocessor Power
COP KRIPT	Coprocessor Control
COP CS	Coprocessor Select
COP CK	Coprocessor Clock
F1L	F1 Latched Output
MASTER	Master Transmitted

5

EXEL Microelectronics
A Division of ROHM Corporation
2150 Commerce Drive • P.O. Box 49038 • San Jose, CA 95161-9038
PHONE 408 432-0500 • FAX 408 432-8710

BLOCK DIAGRAM OF XL109 CONTROLLER AND XL105 COPROCESSOR



APPLICATIONS

Applications of the XL109 include: vehicle security systems, gate and garage door openers, burglar alarm systems, remote control units, and central locking systems.

GENERAL DESCRIPTION

The XL109 integrated circuit is a remote control decoder for use in high security remote control applications such as vehicle security and access control systems.

In remote control operation, a high degree of security is provided by 56 bit non-repetitive codes. The XL109 is designed to function with transmitters based on XL105. An external XL105 is used with the XL109 as coprocessor for decoding and non-volatile storage.

The Keeloq™ code hopping system provides greatly enhanced security by being immune to attacks by code scanners and code grabbers and even against more sophisticated analytical attacks.

By isolating the XL105 coprocessor from the XL109 with resistors, it is possible to use the coprocessor as a storage device for an external microcontroller. Keys and system information can also be programmed directly into the XL105 coprocessor without removing it from the PC board.Programming and reprogramming of the XL105 coprocessor can be done through serial communications port, totally dispensing with DIP switches.

The Keeloq™ encoders provide flexibility and ease of use, and require an absolute minimum of peripheral circuitry. Considerable savings can be realized in most circuits, as circuit board space requirements and labor costs are significantly reduced. This decoder provides the designer with system flexibility while retaining the economic advantages of the Keeloq™ system. Programmable decoders, tokens and transmitters make the process of configuring matching systems extremely fast and simple, while maintaining the highest possible level of security.

EXEL supplies Keeloq™ evaluation and demonstration kits, containing documentation, software, a programming probe and samples of the integrated circuits as well as transmitters and receivers. These kits can be used to assess the operational aspects of the devices. EXEL also supplies production hardware and software.

FUNCTIONAL DESCRIPTION

The XL109 offers a variety of options, allowing the system designer full flexibility with very modest external component requirements.

Function Outputs

Three function outputs (F1 to F3) are permanently available. A delayed output (activated when the user depresses a transmitter button for more than about 3.5 seconds) is also available. The three function outputs can be used where a single receiver is used to control several functions. A typical example is a single controller controlling a security gate, an alarm system and garage door.

One of the function outputs is available in latched and pulsed format. The latched output dispenses with the need for an expensive latching relay in cases where a continuous output is required to activate a system. Switching transistors or standard relays can be used instead.

DELAY — Delayed function indicator:
This output is activated only when a transmitter button has been pressed for an extended period. This output is ideal for the implementation of panic buttons, where inadvertent output activation is undesirable.

REPEAT — Valid signal indicator:
50 ms pulses will appear at regular intervals on this output as long as a valid code is being received. The valid signal indicator can be used to implement systems where the duration of the transmitter activation is important — a car window winder is a good example. The user would depress the transmitter button until the desired position is reached, and then release the button.

MASTER output:
One of the transmitters acts as a master transmitter. When this transmitter is activated, the outputs are activated in the normal way. However, in addition, the MASTER output is activated to indicate that the special transmitter has been used. This output may be used to authorize self-learning, or to provide special levels of privilege to a single user. To facilitate the use of this transmitter for self-learning, its key is stored in a special location, where it will never be written over by the learning process. For this reason, the master transmitter cannot be replaced through self-learning — its keys and synchronization information are programmed directly onto the coprocessor.

Self-Learn:
XL109 enters the learn mode when $\overline{\text{LEARN}}$ is brought low momentarily. Learning can be done in either of the following ways: 1) Pull $\overline{\text{RESET}}$ and $\overline{\text{LEARN}}$ low, release $\overline{\text{LEARN}}$ at least 20 ms after $\overline{\text{RESET}}$. 2) Hold $\overline{\text{LEARN}}$ low until REPEAT is high for more than 50 ms while all function outputs (F1-F3, DELAY) are low. The device stays in learn mode until it receives two valid transmissions. However, it automatically exits learn mode upon receiving two invalid transmissions.

5

Decoder Operation

The decoder operates in independent mode — each transmitter uses a unique key. Separate history information is also maintained for each transmitter. Button decoding is used — the decoder decides which outputs to activate, based on the button that has been used for transmitter activation.

The XL109 decoder and its XL105 coprocessor can act, without any external processing, as a simple controller for vehicle security systems, gate openers and other remote control systems. With a simple microcontroller, the decoder can become part of a more sophisticated system. The added security of code hopping remote controls can be added to existing fixed code systems with a minimum of expense and effort.

In addition, direct XL105 coprocessor access is made possible by isolating the coprocessor from the decoder with resistors. A microcontroller can use the XL105 EEPROM directly for non-volatile storage. Any form of operational information stored in the XL105 coprocessor will be retained even through power interruptions.

Keys can be programmed directly into the XL105 coprocessor while it is installed on the board. During the same operation, additional manufacturing information including date codes, batch numbers and even serial numbers can be programmed into the coprocessor EEPROM.

SECURITY CONSIDERATIONS

Remote control via RF or IR is popular for many applications, including the control of automatic garage doors and vehicle security systems. Conventional remote control systems are based on unidirectional transmission and offer very limited security. More sophisticated devices based on bidirectional transmission are also available. However because of their high cost and certain practical disadvantages, especially the requirement for two receivers, they are not widely used in commercial remote control devices.

Most popular unidirectional transmission systems currently have two very important security shortcomings. The codes they transmit are usually fixed and the number of possible code combinations is relatively small. Either of these shortcomings can lead to unauthorized access. Such unauthorized access can be obtained by scanning through all the combinations or by a code grabber. A code grabber records a transmission for retransmission at a later stage to gain access. Because frequencies are usually fixed in a specific country and the ease of making a code grabber the code grabbing principle is widely recognized as a very serious threat to current remote control systems.

Greatly improved security without cost increases (or possibly even with cost reductions) can be realized by using the Keeloq series of code hopping devices. The encoders feature a complex code hopping algorithm that uses a 64 bit key to scramble a 32 bit transmission word. The code hopping mechanism prevents code capturing, since a different code will be used with every transmission. A nonlinear scrambling process is used, making it impossible to calculate the key, even if numerous transmissions are captured and analyzed. This provides the highest possible level of security.

The 32 bit random portion of the transmission code provides for more than 4,000,000,000 combinations and thus prevents scanning (a complete scan would require around 12 years!)

It is impossible for someone without the 64 bit key to predict the next word in the sequence of transmission words. The 64 bit keys can be pre-programmed but cannot be read out of the EEPROM. This read protection ensures that codes will remain secret to anyone but the programmer. This system is far superior to current DIP systems, where the code being used is freely visible and can be easily duplicated onto another transmitter.

Once a code has been transmitted, it will not be used again for more than 65,000 transmissions. This means that every key will result in a unique sequence of over 65,000 values in the set of 232 (over 4,000 million) possible sequences of the transmission word (32 bit random portion). Likewise, a matching Keeloq decoder will never accept any previous codes again over several lifetimes of a typical system.

The risk of accidentally activating a decoder with another key is practically nonexistent (less than one in billions of operations).

This high level of security is becoming available at prices comparable to fixed code systems through special hardware and algorithm design techniques along with full custom integrated circuit implementation on state of the art silicon processes.

ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Unit
V_{DD}	Supply voltage	-0.3 to 6.5	V
V_{IN}	Input voltage	-0.3 to VDD +0.3	V
V_{OUT}	Output voltage	-0.3 to VDD +0.3	V
T_{STG}	Storage temperature	-55 to +125	°C
T_{LSOL}	Lead soldering temp	300	°C
V_{ESD}	ESD rating	2000	V

Note: Stresses above those listed under "ABSOLUTE MAXIMUM RATINGS" may cause permanent damage to the device.

RECOMMENDED OPERATING CONDITIONS

Symbol	Item	Rating	Unit
V_{DD}	Supply voltage	4.5 to 5.5	V
T_{AMB}	Operating temperature	-40 to 85	°C

5

DC ELECTRICAL CHARACTERISTICS

Ta = -40°C to 85°C, V_{DD} = 5V ± 10% unless otherwise specified

Symbol	Parameter	Min	Typ	Max	Unit
I_{CC}	Operating current		2.8		mA
V_{IH}	Input H voltage	2.25			V
V_{IL}	Input L voltage			0.75	V
I_{OL}	Output sink current*			10	mA
I_{OH}	Output source current*	N/A		N/A	

*Open collector outputs

AC ELECTRICAL CHARACTERISTICS

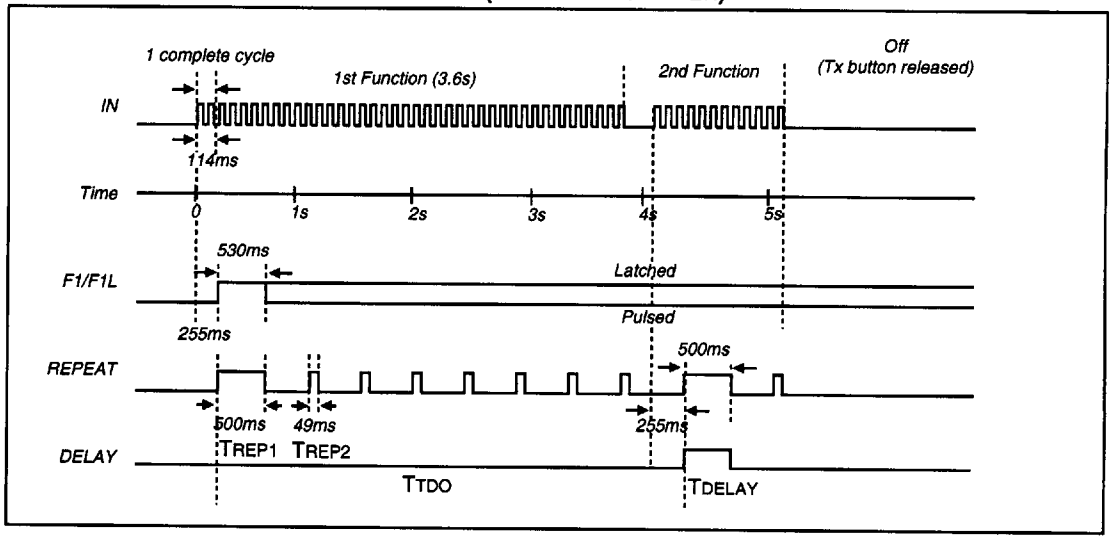
Ta = -40°C to 85°C, V_{DD} = 5V ± 10% unless otherwise specified

Symbol	Parameter	Min	Typ	Max	Unit
F_{OSC}	Operating frequency		1		MHz
T_{RESET}	Reset time	50			µs
T_{DPWR}	Delay from power on		100		ms
T_{PWM}	Input bit period - Code hopping	0.4		3.6	ms
F_{PWM}	PWM data rate	280		2500	bps
T_{TOS}	Transmission complete to output	122		160	ms
$T_{F1,2,3}$	Function outputs duration		530		ms
T_{REP1}	REPEAT output duration 1		500		ms
T_{REP2}	REPEAT output duration 2		49		ms
T_{DELAY}	DELAY output duration		500		ms
T_{LEARN}	Learn activation	1			s

* Learning can also be entered reliability with either of the following procedures:
1. Pull RESET and LEARN low. Release LEARN at least 20ms after RESET.
2. LEARN must be held low until REPEAT is high for more than 50ms while fuction outputs are low.

Note: All typical values are dependent on the operating frequency.

TIMING INFORMATION OUTPUT ACTIVATION (SLOW TRANSMITTER)



Notes:
1) F1L changes state every time F1 is activated.

2) When F1L is in the high state, low periods up to 50 µs may occur every 50 ms or greater. In some applications, a smoothing capacitor may be required on the F1L output, along with a 1KΩ series resistor between the output and the capacitor. Up to 350 nF of capacitance may be required for high impedance loads.

3) When REPEAT and DELAY are low, high periods of up to 20 µs may occur every 50 ms or greater. In some applications, smoothing capacitance may be required. The value will depend on the load impedance. For high impedance, 10 nF is required.

4) The spacing between pulses on the REPEAT output is influenced by the transmission rate of the transmitter. Typical spacing is around 260 ms. For high rate transmissions, the spacing may reduce to 160 ms, and for low rate transmissions, the pulse spacing may increase to 610 ms.

APPLICATION EXAMPLE

Remote Control Gate Opener