Preliminary Information

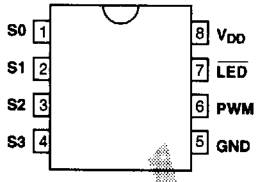
Keeloq™ Code Hopping Encoder

FEATURES

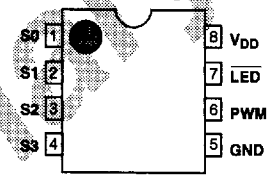
- Secret Keys Read Protected in All Modes
- Automatic Power Down
- Power "Low" Indication on LED
- Simple Programming Interface
- Hardware Error Correction on EEPROM
- EEPROM Low Voltage Write Protection
- Low External Component Count:
  - — On-chip 64x16 bit EEPROM
  - — On-chip oscillator
  - — On-chip oscillator timing components
  - — Complete on-chip reset circuit
  - — Current limiting on LED output
  - — Internally debounced inputs
  - — Inputs internally pulled low
  - — No DIP switches required
- Extended Voltage Operation (2.7 - 6.3V)
- Low Battery Warning Before Operation Stops
- Startup Delay Reduced to 15ms
- Automatic Transmission Completion
- Duty Cycle Reduction for FCC (Selectable)
- Combined Button Activation
- Preamble Transmission To Wake Up Receiver
- Transmission Time Extended to 23 Seconds
- Small 8-pin SOIC and PDIP

PIN CONFIGURATION

Plastic Dual-in-line
"P" Package



EIAJ Small Outline
"RF" Package



PIN NAMES

S0-S3	Configuration Inputs
GND	Ground Reference
PWM	PWM I/O Pin
$\overline{\text{LED}}$	LED Driver
V_{DD}	Supply Voltage

OVERVIEW

The XL106 is a code hopping encoder for contactless remote control systems using RF, microwave or IR transmitters and for contacted systems. It is intended for use with the Keeloq™ series decoders XL109, XL110, and XL138.

OPERATIONAL MODES

1) Code Hopping (CH) Contactless Remote Control Mode

- Each transmission is unique
- Programmable, read-protected keys
- Over $1.8x10^{19}$ different keys available
- For each XL106:
  - — Seven independent CH transmitters
  - — Seven 64 bit CH keys
  - — Five function buttons on one CH transmitter
- 56 bit transmission code length
- Delayed second functions
- Two selectable baud rates

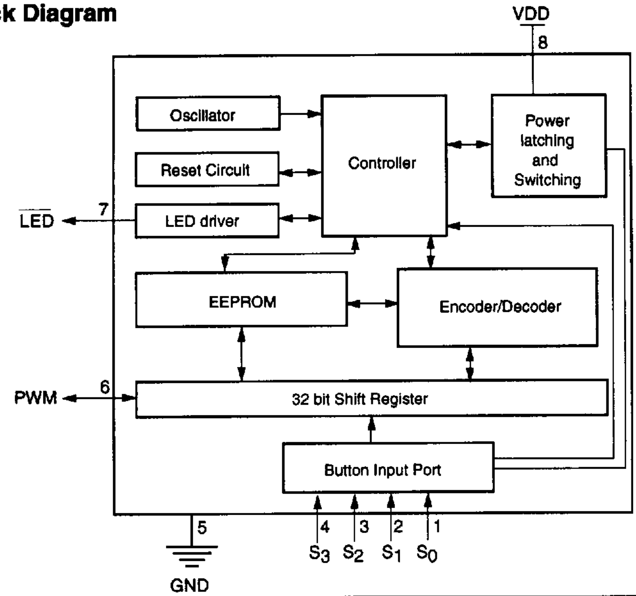
2) Identification Friend or Foe (IFF) - Contact Mode

- Bidirectional authentication
- Used for area access such as condominiums and apartments
- 32 bit challenge and response
- Four 64 bit IFF keys

3) Co-processor mode

- Protocol similar to Microwire™
- Five wire interface
- 32 bit encryption and decryption
- Secret key generation for self-learn
- User EEPROM storage
  - — Available (28-4*Tx) X16 bit words (Tx = Number of transmitters)

Functional Block Diagram



APPLICATIONS

Applications for the XL106 include: vehicle security systems, gate and garage door openers, vehicle immobilizers, burglar alarm systems, remote control units, central locking systems, electronic door locks, and identity tokens.

GENERAL DESCRIPTION

The Keeloq™ XL106 is a code hopping encoder intended for secure remote control systems. It is ideal for remote control applications using radio frequency (RF), microwave or infra-red (IR) transmitters.

The code hopping mechanism prevents unauthorized access through code capturing while the 56 bit code length prevents scanning.

The three main modes of operation and typical applications are:

- Code hopping encoder mode, used in remote transmitters in unidirectional transmission systems
- IFF mode, used in bidirectional systems such as code plugs in vehicle security
- Coprocessor mode used in receivers or controllers to interface the XL106 to a processor or decoder.

The mode of operation is selected according to the inputs and configuration of the device. An easy to use PWM (Pulse Width Modulation) serial interface is used to program the necessary keys, system parameters and user data into the system. The on board EEPROM is accessible via the PWM interface.

A powerful but easy to use capability to implement secure self-learn of transmitters to a receiver allows for simple procedures to add or replace transmitters in security and access control applications.

Low Voltage Warning
The XL106 encoder incorporates a low power warning mode - the LED warning will be activated well before operation is inhibited. The user is given ample warning to replace the batteries.

Improved Start-up Response
The start-up delay 15 ms. This delay will offer reduced response delays in security systems.

Automatic Transmission Completion
If the transmitter button is released during a transmission, the encoder will complete that transmission before turning itself off. This capability ensures that a complete code is transmitted, even if the user only taps the transmitter button. For this feature to operate, V_{DD} must be connected directly to the supply.

Duty Cycle Reduction Option
To reduce the average transmission duty cycle, a selectable alternate code word blanking capability has been introduced.

With the option selected, every other code word will be turned off, thereby reducing the duty cycle by a factor of two. This feature enables the designer to transmit higher peak power without increasing the average power in a 100 ms period.

Combined Button Activation
The XL106 user can access TX1C (the third function transmitter) by pressing the first two transmitter buttons simultaneously. This capability facilitates two button transmitters with three function capability.

Leading Pulses
Before each transmission, a series of 16 pulses is transmitted. The pulse repetition periods are now 600µs and 1.2 ms, for high and low data rates respectively. In both cases, the pulses have a duty cycle of 1/2.

The pulses are useful in receivers with variable decision thresholds, where the pulses will assist in setting the decision threshold correctly before the header and data arrive.

In the case of repeated transmissions (when the transmit button is being pressed for an extended period), each repetition of the code will be preceded by this group of 16 pulses.

Extended Transmission Time
The XL106 includes an automatic power down capability. The time after which this feature is activated, is being extended in the XL106. The maximum transmission length is now 23s. In the case where delayed function operation has been enabled, the first function will be transmitted for 3s, after which the delayed function will be transmitted for 20 s. Unlike the situation in the XL105, the 3s period is unaffected by the transmission baud rate.

LED Output Improvement
The LED output is now disabled when IFF Mode is selected. The output may be grounded or tied to the supply without increased current consumption, and without running the risk of inadvertently entering HSS mode.

IMPLEMENTATION

The application circuits clearly indicate the simplicity of implementations using Keeloq™ devices. No DIP switches, cutting of tracks or soldering is needed. In addition, the small footprint device and very limited external component requirements facilitate extremely small packaging. Also, the small printed circuit board size and low component count will realize significant savings in material and labor.

The personal computer based programming software is user friendly and efficient, making programming and reprogramming by authorized stations easy. A single probe is used to program a decoder and its matching encoders in a single session. Production line software for runs of single devices is also available. Transmitters can later be added or replaced using the self-learn mechanism.

SECURITY CONSIDERATIONS

Remote control via RF or IR is popular for the control of vehicle alarms, automatic garage doors and many other applications. 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.

The 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 XL106 features a complex nonlinear code hopping encoding 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. The scrambling process is nonlinear and prevents the calculation of the key, even if a large number of transmissions are captured and analyzed. This provides the highest possible level of security.

The 32 bit random portion of the transmission code provides for in excess of 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 XL106. This ensures that keys will remain secret to anyone but the programmer. In HSS mode, read-protected keys can be generated in secret and stored in EEPROM. The device cannot be forced to write keys to unprotected memory locations so that the EEPROM contents cannot be used by an unauthorized party to determine the keys.

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 more than 65,000 values in the set of 232 (over 4,000 million) possible sequences of the transmission word's 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.

Another important and very practical security feature is the inaccessibility of the keys. They cannot be read or otherwise accessed from outside the Keeloq device. This is far superior to DIP switch systems, where the code combination can easily be copied.

This high level of security at prices comparable to obsolete fixed code systems is made possible by special hardware and algorithm design techniques along with full

FCC POWER CALCULATION

Duty cycle of header .... (0.5) (50%)
Header time 4.3ms
Worst case duty cycle of data bits 0.667 (66.7%)
Data bits time 36.1ms
Total word time 50.0ms
Duty cycle of preamble .... (0.5) (50%)
Preamble Time 9.6ms
Average power without duty cycle reduction = (0.5*9.6 + 0.5*4.3 + 0.667*36.1)/50 = 0.62 (62%)
Average power with duty cycle reduction = (0.5*9.6 + 0.5*4.3 + 0.667*36.1)/100 = 0.31 (31%)
(37% worst case with clock variation)

PIN ACTIVATION

S3	S2	S1	S0	Function
0	0	0	0	Reset state
0	0	0	1	Tx1A: Key 1 fcn 1
0	0	1	0	Tx1B: Key 1 fcn 2
0	0	1	1	Tx1C: Key 1 fcn 3
0	1	0	0	Tx4: Key 4
0	1	0	1	Tx5: Key 5
0	1	1	0	Tx6: Key 6
0	1	1	1	Tx7: Key 7

S3	S2	S1	S0	Function
1	0	0	0	Programming mode
1	0	0	1	Tx: fixed code
1	0	1	0	Tx2: Key 2
1	0	1	1	Tx3: Key 3
1	1	0	0	Tx1D: Key 1 fcn 4
1	1	0	1	Tx1E: Key 1 fcn 5
1	1	1	0	IFF
1	1	1	1	No Operation

5

ELECTRICAL CHARACTERISTICS

ABSOLUTE MAXIMUM RATINGS

Symbol	Item	Rating	Units
V_{DD}	Supply Voltage	-0.3 to 6.5	V
V_{IN}	Input Voltage	-0.3 to V_{DD} + 0.3	V
V_{OUT}	Output Voltage	-0.3 to V_{DD} + 0.3	V
T_{STG}	Storage Temperature	-55 to +125	°C
T_{LSOL}	Lead soldering temperature	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	Units
V_{DD}	Supply Voltage	2.7 to 6.3	V
T_{AMB2}	Operating temperature	-40 to 85	°C

Notes:
1) S0-S3 are internally pulled low by 50k resistors.
2) PWM I/O pin is internally pulled by low 100k resistor.
3) LED driver (2 mA) and coprocessor select must be wired to VDD via a 10k resistor if no LED is used.

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

DC ELECTRICAL CHARACTERISTICS

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

Symbol	Parameter	Min	Typical	Max	Unit
I_{CC}	Operating current (average)		1.0		mA
I_{CC1}	Standby current			50	nA
I_{CC2}	Auto shutdown current			400	µA
V_{IH}	Input H voltage	0.7VDD			V
V_{IL}	Input L voltage			0.15VDD	V
V_{OH}	Output H voltage @ 2mA	2.4			V
V_{OL}	Output L voltage @ 2mA			0.4	V
I_{OL}	Output sink current			2.0	mA
I_{OH}	Output source current			2.0	mA
I_{OLED}	LED sink current	1.2	2.5	5.0	mA
R_{S0-3}	Pull down resistance; S0-3 Pins	30	50	85	kΩ
R_{PWM}	Pull down resistance; PWM Pin	60	100	170	kΩ

AC ELECTRICAL CHARACTERISTICS

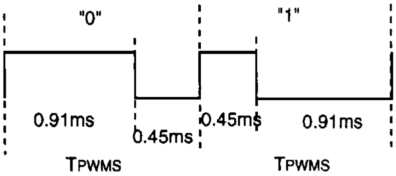
Ta=-40°C to 85°C, V_{DD}=5V ± 10% unless otherwise specified

Symbol	Parameter	Min	Typical	Max	Unit
F_{OSC}	Operating frequency stability	-30		30	%
T_{TPWR}	Transmit delay from power on		27		ms
T_{PWMS}	Bit period (slow mode)		1.36		ms
T_{PWMF}	Bit period (fast mode)		0.68		ms
T_{PWMP}	Bit period (IFF, program mode)		0.68		ms
T_{PPS}	Preamble Bit period (slow mode)		0.91		ms
T_{PPF}	Preamble Bit period (fast mode)		0.45		ms
T_{PTS}	Preamble time (slow mode)		14.53		ms
T_{PTF}	Preamble time (fast mode)		7.26		ms
T_{HS}	Header length (slow mode)		9.08		ms
T_{HF}	Header length (fast mode)		4.54		ms
T_{TXS}	Word duration (slow mode)		100		ms
T_{TXF}	Word duration (slow mode)		50		ms
T_{SDS1}	Shutdown with 2nd func (slow)		23		s
T_{SDS2}	Shutdown without 2nd func (slow)		3		s
T_{SDF1}	Shutdown with 2nd func (fast)		23		s
T_{SDF2}	Shutdown without 2nd func (fast)		3		s
T_{RESET}	Ready after power on			15	ms
T_{ACK}	Ready/Ack duration		30		µs
T_{DEL1}	Delay before Ack		300		µs
T_{DEL2}	Delay before next command	20			µs
T_{GEN}	Function generation time			5	ms

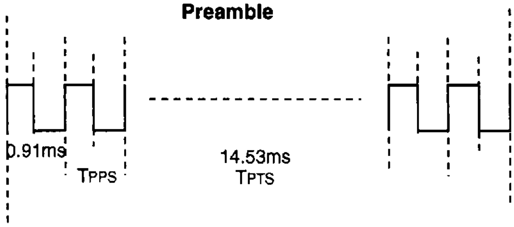
Note: All typical values are dependent on the internal oscillator frequency,

PULSE WIDTH MODULATION (PWM) FORMAT

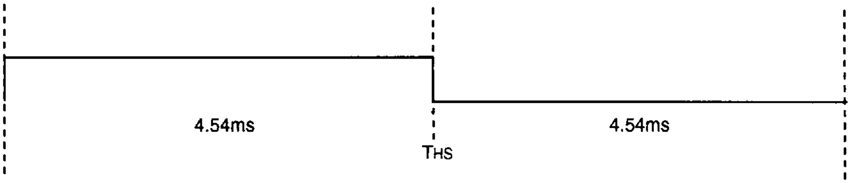
Bit format



Preamble



Header Format

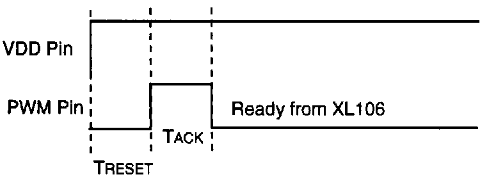


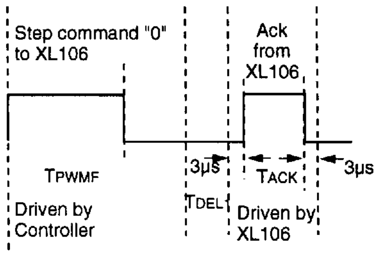
PWM word format

Preamble	Header	32 bit hop code	24 bit fixed code
14.53ms	9.08ms	43.58ms	32.69ms

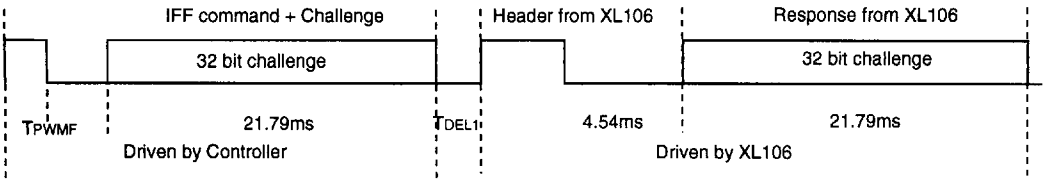
Note: Times Shown are for slow transmission

IFF CHALLENGE/RESPONSE

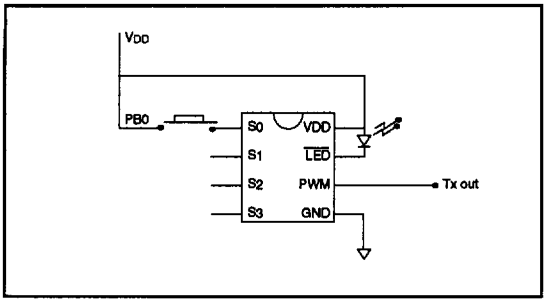




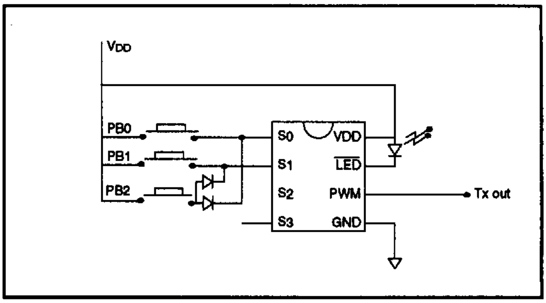
IFF command "1"



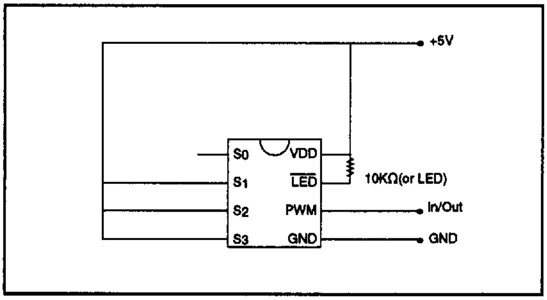
APPLICATION CIRCUITS



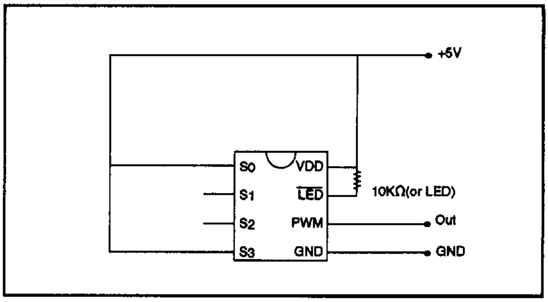
1 button remote control



3 button remote control



Code plug operation (IFF)



Code plug operation (Fixed Code)