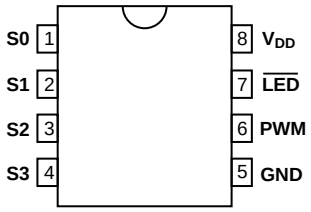
A SureLok™ Security Product
Rolling Code Encoder
Authentication Encoder, Decoder Coprocessor

FEATURES

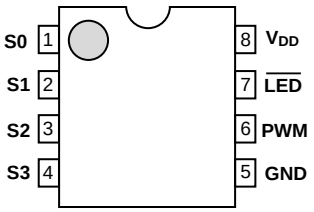
- **Rolling code encoder operation**
  - **Code encryption using 64-bit key**
  - **Unidirectional communication**
  - **56-bit transmission code**
    - **24-bit fixed**
    - **32-bit dynamic**
  - **Up to seven functions (buttons)**
    - **Secondary delay function option**
  - **Button inputs debounced/pulled down**
  - **Automatic power down**
  - **Low battery detect LED output**
  - **On chip oscillator**
- **Authentication encoder operation**
  - **Code encryption using 64-bit key**
  - **Bidirectional communication**
  - **32-bit challenge and response**
  - **Four selectable keys**
- **Decoder coprocessor**
  - **Code decryption using 64-bit keys**
  - **Secure eight key storage**
  - **High speed serial interface**

PIN CONFIGURATION

Plastic Dual-in-line
"P" Package



EIAJ Small Outline
"F" Package



D0020 ILL A01.2

PIN NAMES

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

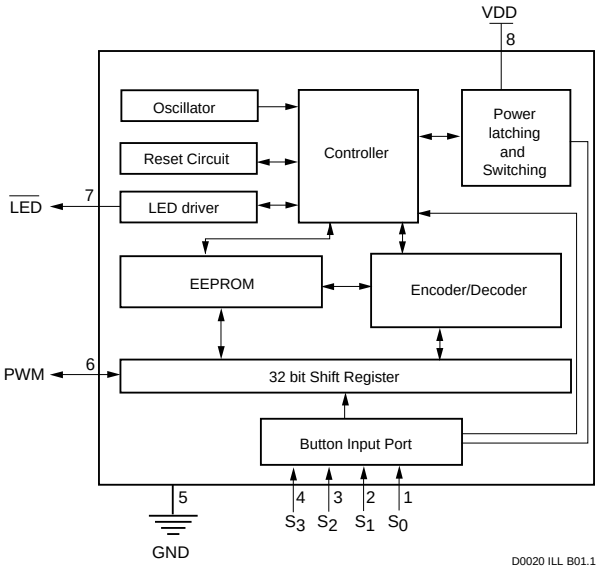
DESCRIPTION

The XL106 is a rolling code encoder, an authentication encoder, and a decoder coprocessor. As a rolling code encoder it is intended for use in secure remote control systems using infrared (IR), microwave and radio frequency (RF) transmitters. In this mode the XL106 utilizes a proprietary encoding technique that generates a 56-bit transmission format. The 56-bit data transmission is composed of a 24-bit fixed code that remains constant for all transmissions from the same transmitter while the 32-bit code is dynamic and is unique for each transmission. The combination of the 32 dynamic bits and the 24 fixed bits provides more than 70 million billion unique transmissions.

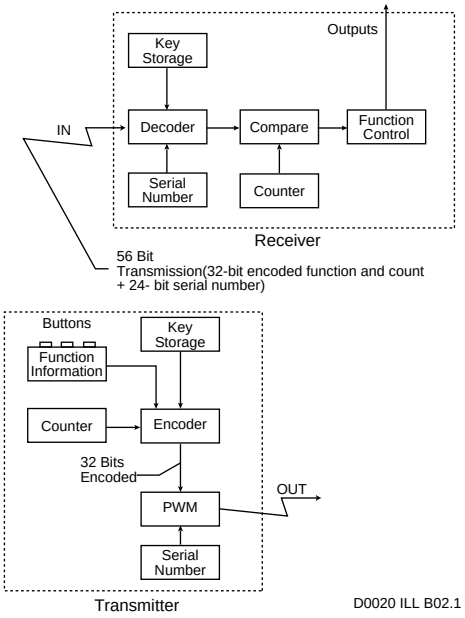
As an authentication encoder, the XL106 provides contact based access control using bidirectional communication. The XL106 receives a 32-bit challenge and returns an encrypted 32-bit response based on the challenge. This implementation provides for over 4000 million unique challenges and responses.

In coprocessor mode, the XL106 provides an encryption and decryption engine, secure E^2PROM storage and secure algorithm key generation using a high speed serial interface.

Functional Block Diagram



Rolling Code Transmitter and Receiver Implementation Block Diagram



Terminology

The following defines the terminology and conventions used in this data sheet.

Manufacturer Key - This is a unique 64-bit key that is selected by the original equipment manufacturer (OEM).

Serial Number - This is a 24-bit transmitter identifier, that is selected by the OEM and is different for each transmitter.

Secret Key - This is a 64-bit key that is used by the encryption and decryption algorithm. It is generated by combining the manufacturer key with the serial number.

Function - This 3-bit button ID is used to represent different transmitter button inputs.

Fixed Code - This is a 24-bit transmitter serial number that is transmitted as the fixed-code portion of the transmission data.

Rolling Code - This is the 32-bit dynamic portion of the transmission code. This code is the result of data encryption and changes after each transmission.

Token - This refers to an XL106 being used in the authentication mode.

Operational Overview

All rolling code systems have one thing in common; they generate a different code each time the transmitter is activated in such a way that an outsider is not able to predict the next code in the sequence. After a specific code has been accepted, the decoder will not accept the same code again.

The XL106 is based on a proprietary system which uses a encryption/decryption architecture. The XL106 is initially programmed by the OEM with a 24-bit serial number and a 64-bit manufacturer key. These are combined to generate the 64-bit secret key used by the XL106 in its encryption algorithm. A third component also stored in memory is a count number that is managed by the XL106; whenever the device is activated it will increment and restore the new count prior to transmission. This count is encrypted, along with the function selected. The XL106 will output the count and function within the 32-bit encoded portion of the transmission, along with the unencoded serial number. The receiver will decode the transmission and compare its stored count value with the received count value to verify it is not a repeated count (re transmission by a code grabber). The key is never transmitted, it is only used within the device to generate the rolling code that is then sent through as output.

PIN FUNCTIONS

Switch Inputs S0-S3

The XL106 has four switch inputs: S0 thru S3. These inputs are used to select a variety of XL106 operations. All four inputs are fully debounced and each input is internally pulled down. When all four inputs are open (internally at GND) the XL106 will be placed in the low power reset state. Any switch closure (raising any input to VIH min.) will cause the XL106 to "wake-up" and configure itself to perform the selected operation. Table 1 illustrates the possible actions with all switch closure combinations.

$\overline{\text{LED}}$

The $\overline{\text{LED}}$ output is designed to directly drive a light emitting diode (LED). During a normal operation the output is driven low when a low battery condition is detected. When a low battery condition is detected, the LED output will pulse low every other eight codes.

PWM

The PWM I/O can be directly connected to the transmitter circuit. This I/O is internally tied to ground through a pulled-down resistor. When used in the authentication mode the PWM is used as both an input and output.

Device Operation

Depending upon the end application and the programmed options of the XL106, the combination of switch closures on S0 through S3 will result in various actions as illustrated in Table 1.

OPERATING MODES

Reset Mode [0000]

The Reset Mode occurs when all four XL106 switches are open.

Dependent Modes [0001 - 0111]

The Dependent Mode is an operation whereby a transmitter uses a single key but can transmit multiple coded functions. The XL106 is capable of transmitting seven individual functions on a single key. An example is a remote keyless entry application where multiple functions are transmitted to a single controller in an automobile that unlocks the driver's door and trunk, and lowers the windows.

Programming Mode [1000]

The operating mode enables programming of the XL106.

Switch Input Activation Table

S3	S2	S1	S0	Mode/Function
0	0	0	0	Reset State
0	0	0	1	Tx 1A: Key1 Function 1
0	0	1	0	Tx 1B: Key1 Function 2
0	0	1	1	Tx 1C: Key1 Function 3
0	1	0	0	Tx 1D: Key1 Function 4
0	1	0	1	Tx 1E: Key1 Function 5
0	1	1	0	Tx 1F: Key1 Function 6
0	1	1	1	Tx 1G: Key1 Function 7
1	0	0	0	Programming Mode
1	0	0	1	Tx Fixed Code
1	0	1	0	Tx 6: Key 6
1	0	1	1	Tx 7: Key 7
1	1	0	0	Tx 4: Key 4
1	1	0	1	Tx 5: Key 5
1	1	1	0	Authentication Mode
1	1	1	1	No Operation

D0020 PGM T01.1

Table 1

Transmit Fixed Code Mode [1001]

The Transmit Fixed Code Mode allows the XL106 to operate with existing fixed code systems. While the security of the rolling code transmitter is not available in these applications, the XL106 in most instances can provide E^2 configurability at significant cost savings.

Independent Mode [1010 - 1110]

The Independent Mode allows programming of a single transmitter with multiple keys (up to 5), allowing the transmitter access to multiple receivers. An example of where this might be useful is in the home environment where five buttons (switch inputs) on a remote control access a vehicle door lock, a garage door opener, home security lighting, or a security gate. Each receiver is independent from the other but each is accessible to a single control unit with multiple input selections.

Authentication Mode [1110]

The Authentication Mode is an interactive method of passing and verifying authenticity. The processor generates a challenge (32-bit word) and sends this to the encoder. The encoder then performs an encoding operation based on its key and then retransmits the encoded data back to the controller for verification.

No Operation Mode [1111]

As the name implies, no action will be taken by the device but the overall current consumption will be increased through the pull down resistor path to ground.

DETAILED DESCRIPTION

Encoder Operation

Delay to Action

The Delay to Action function is based on the XL106 sensing a switch closure and starting an internal timer. After the timer has timed out without a reset, a new encoded function will be transmitted. This delay to action will force the user to take a positive action to enable critical functions such as activation of a panic function by the receiver. This function is optional and can be programmed into the XL106.

Automatic Power Down

In battery powered applications power conservation is critical. The XL106 contains a sense circuit that automatically shuts down operation if it detects that a switch has been closed continuously for an extended period. The XL106 will automatically reset after the switch is released and all switch inputs return to ground.

2-Button/3-Function Operation

Although the XL106 will decode multiple switch closure combinations, the S0 and S1 inputs have a special relationship that simplifies the implementation of a 2-button/3-function transmitter. With multiple button transmitters, single buttons can control multiple switch inputs on the XL106. For example, if S0 is closed and the XL106 begins outputting Tx1A during the middle of this transmission, S1 also closes. The Tx1A transmission will be completed and the XL106 will automatically begin transmitting Tx1C.

PWM Output Data Rate

The XL106 has a on-board oscillator that controls the programmable output data rate. The basic fast data rate clock division is 212µs and the slow data rate clock division is 424µs. A normal transmission consist of a guard pulse (32 clocks), a preamble (32 clocks), a header (20 clocks) and the 56 bits of data (168 clocks).

Duty Cycle Reduction

To reduce the average transmission duty cycle, an alternate code word blanking option may be configured. When this option is selected, a standard transmission output (guard pulse, preamble, header and data) will be followed by a transmission of all zeroes for a period of 252 clocks.

Coprocessor Operation

As an encoder transmitter the XL106 is a standalone device that need only be interfaced to a RF circuit. The receiving unit may be implemented in three basic configurations. The simplest form is interfacing an EXEL decoder and the XL106 as a coprocessor. There are three decoders/controllers available from EXEL: the XL109 in conjunction with the XL106 will take the RF input information and provide seven discrete output functions; the XL110 in conjunction with the XL106 will take the RF input information and provide a serial data output that can be further processed by a system's controller. The XL138 is used in conjunction with the XL106 to provide the front end operation in the authentication mode of operation. Refer to figures on pages 10, 11 and 12, for schematic representations of these implementations.

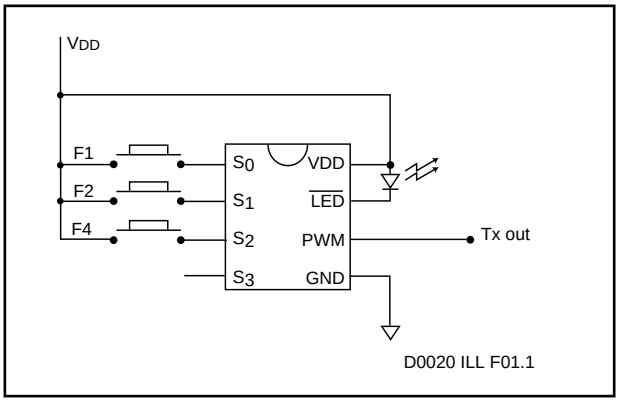
An alternative receiver option is to receive and control transmissions in a system microcontroller, and EXEL provides the routines necessary for interfacing to the XL106. The XL106 is able to provide the necessary decoding of the received data and storage of count information and keys in its secure nonvolatile memory. A third alternative is for EXEL to provide reception and encryption routines to the OEM, and in turn, the OEM can provide their own controller and external nonvolatile memory; this implementation provides lower security because keys are stored in standard E^2PROM.

Detailed information on implementations and applications support is available from EXEL. Refer to the list of design aids shown with the ordering information.

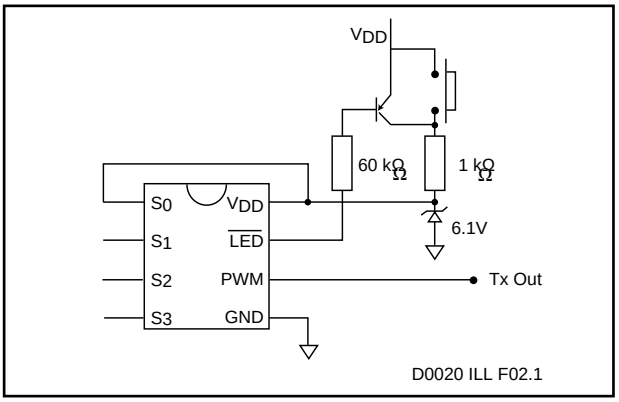
OEM Programming

The XL106 has 1024 bits of E^2PROM that is used for serial number and key storage. The memory array is divided into areas that can be programmed by the OEM. Key storage is done in secure locations. Production programming information is available directly from EXEL.

Application Circuits

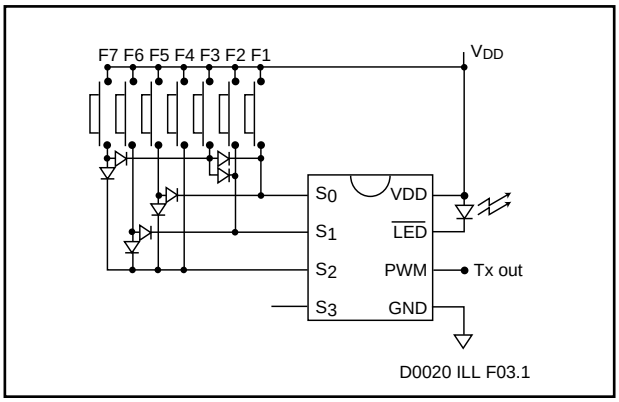


3-Button Remote Control Transmitter



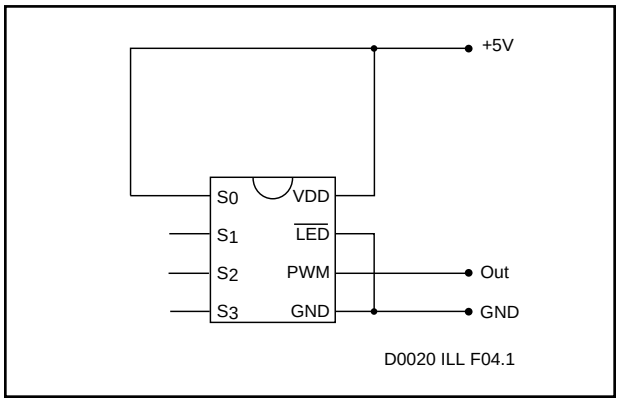
12-Volt Transmitter with Automatic Code Word Completion

Note: Circuit as shown will continue to transmit until power-down. To terminate transmission at the end of the current code word, a double pole pushbutton should be used to isolate S0.

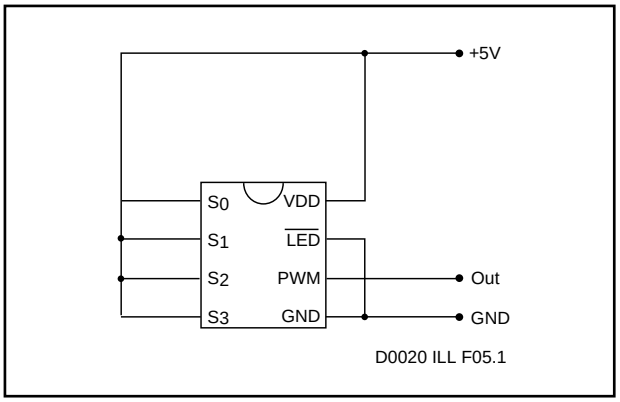


7-Button Remote Control Transmitter

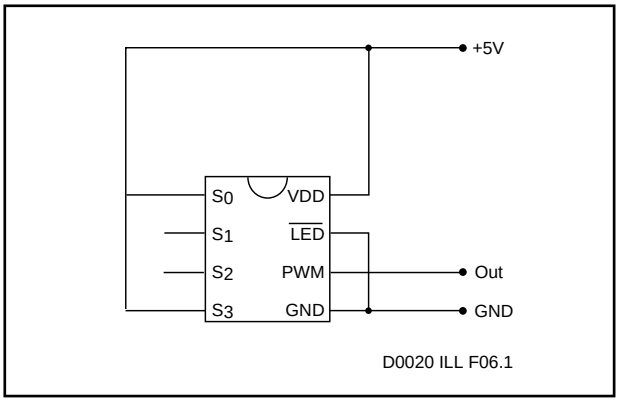
Note: Any simpler transmitter is a subset of the circuit shown.



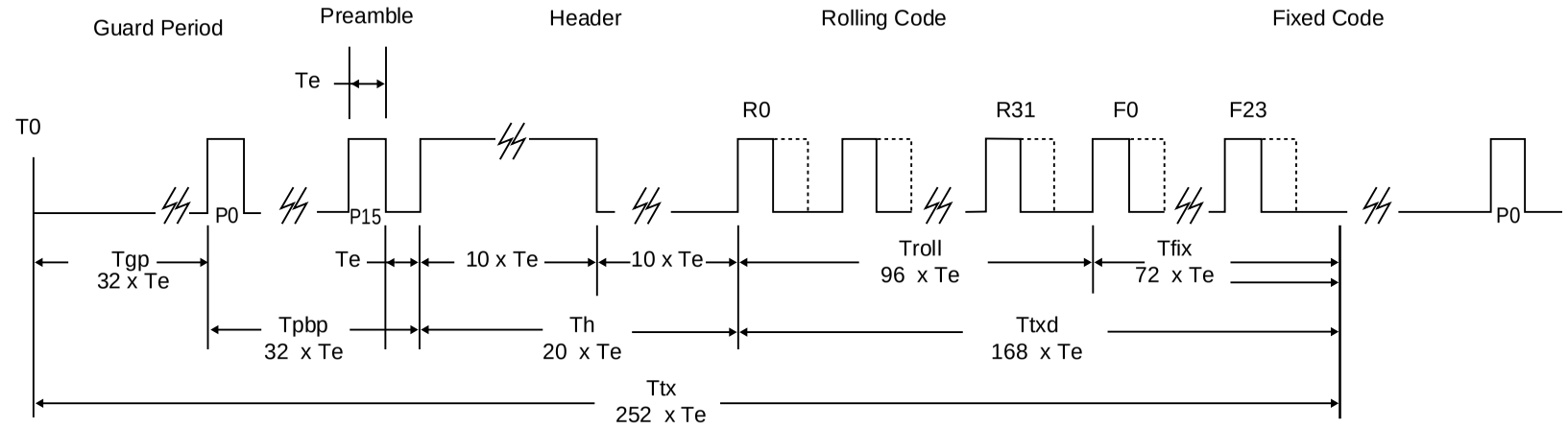
Token Operation (Rolling Code)



Token Operation Authentication Mode

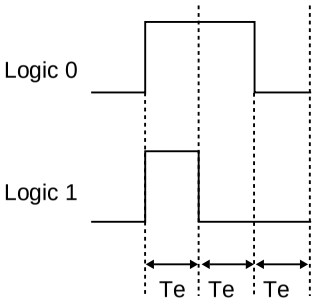


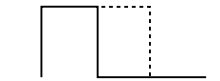
Token Operation (Fixed Code)



Rolling Code Transmission Format

D0020 ILL F07.1





Timing Diagram Format

Pulse Width Modulation Data Format

ABSOLUTE MAXIMUM RATINGS

Temperature Under Bias . . . . . -40°C to +85°C
Storage Temperature . . . . . -65°C to +125°C
Lead Soldering Temperature
(less than 10 Seconds) . . . . . 300°C
Supply Voltage . . . . . -0.3V to 6.5V
Voltage on Any Pin . . . . . -0.3V to V_{DD}+0.3V
ESD Voltage 2000V

Note:
These are STRESS ratings only. Stresses beyond those absolute maximum ratings may permanently damage the part. Prolonged exposure to these conditions may affect device reliability.

ELECTRICAL CHARACTERISTICS

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		25	1000	nA
I_{CC2}	Auto shutdown current			20	µA
V_{IH}	Input H voltage	0.6 V_{DD}			V
V_{IL}	Input L voltage			0.15 V_{DD}	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		2.0		mA
R_{S0-3}	Pull down resistance; S0-3 Pins		50		kΩ
R_{PWM}	Pull down resistance; PWM Pin		100		kΩ

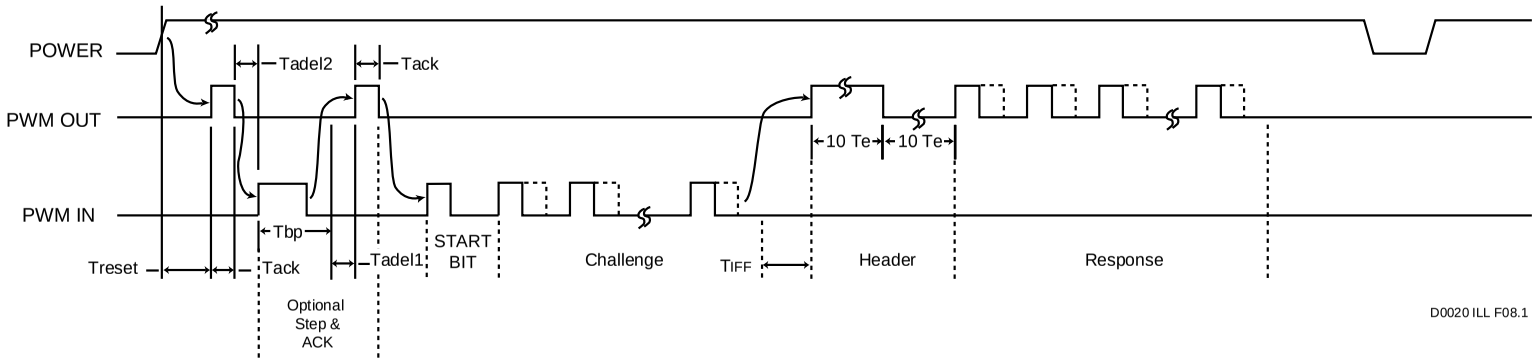
D0020 PGM T02.1

AC ELECTRICAL CHARACTERISTICS, PWM OUTPUT

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

Symbol	Parameter	Te Multiple	Min	Typical	Max	Unit
FOSC	Operating Frequency Stability		-30		+30	%
TTPWR	Transmit Delay From Power On (or Switch Closure)			28		ms
Te	Basic Timing Division - Slow - Fast			424 212		ms
Tbp	Bit Period	3				Te
Tgp	Guard Period	32				Te
Tpb	Preamble Bit Period	32				Te
Th	Header (synchronization) Period	20				Te
Troll	Rolling Code Duration	96				Te
Tfix	Fixed Code Duration	72				Te
Ttx	Total Transmission Period	252				Te

D0020 PGM T03.1



XL106 Authentication Mode Sequences

Note: 1. Authentication mode is initiated by applying power to the token. After Treset the XL106 will output an acknowledgment (ACK) to the controller.

2. The controller will respond in one of two ways.

a. If the system is designed to use Key1, the controller will output a start bit immediately followed by a 32-bit challenge.

b. If the system is set to operate with multiple keys, it must indicate to the XL106 which key address to use. This is done by issuing step commands. Each step command increments the address, and in response to each step command, the XL106 will issue an ACK. After the key address has been set, the controller will then issue a start bit immediately followed by the 32-bit challenge.

3. The 32-bit challenge will also be issued to an XL106 that is interfaced to the controller.

4. Both XL106 devices will encode the challenge and send the result back to the controller for verification.

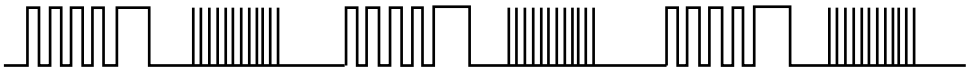
AC ELECTRICAL CHARACTERISTICS, AUTHENTICATION MODE

Symbol	Parameter	Te Multiple	Min	Typical	Max	Unit
Treset	Power-on to ACK Response			14		ms
Te	Basic Timing Element			212		µs
Tack	ACK Duration	1				
Tadel1	Delay to ACK	1				
Tadel2	Delay from ACK to Next Command		20			µs
Tstep	Address Stepping Period			2.1		ms
T_{IFF}	Response to Challenge Delay			525		µs

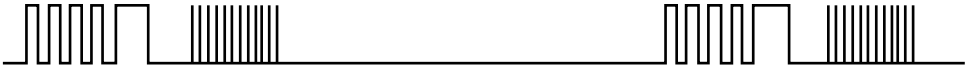
D0020 PGM T04.1

Notes: 1. XL106 timing parameters are specified at V_{DD}=5.0V.
Typical variations with supply voltages at 3.5V=+3.5% and at 6.0V=-3%.
2. I_{FF} Challenges (PWM IN) timing must meet the XL106 internal clock rate ±15%.
3. Te can be calculated by measuring Treset and divide by 65. (Te=Treset/65).

Transmitter Power/Duty Cycle Calculations



Standard Code Transmission



Optional alternate code word suppression, effectively halves the duty cycle, and allows 2x the peak envelope power.

D0020 ILL F09.1

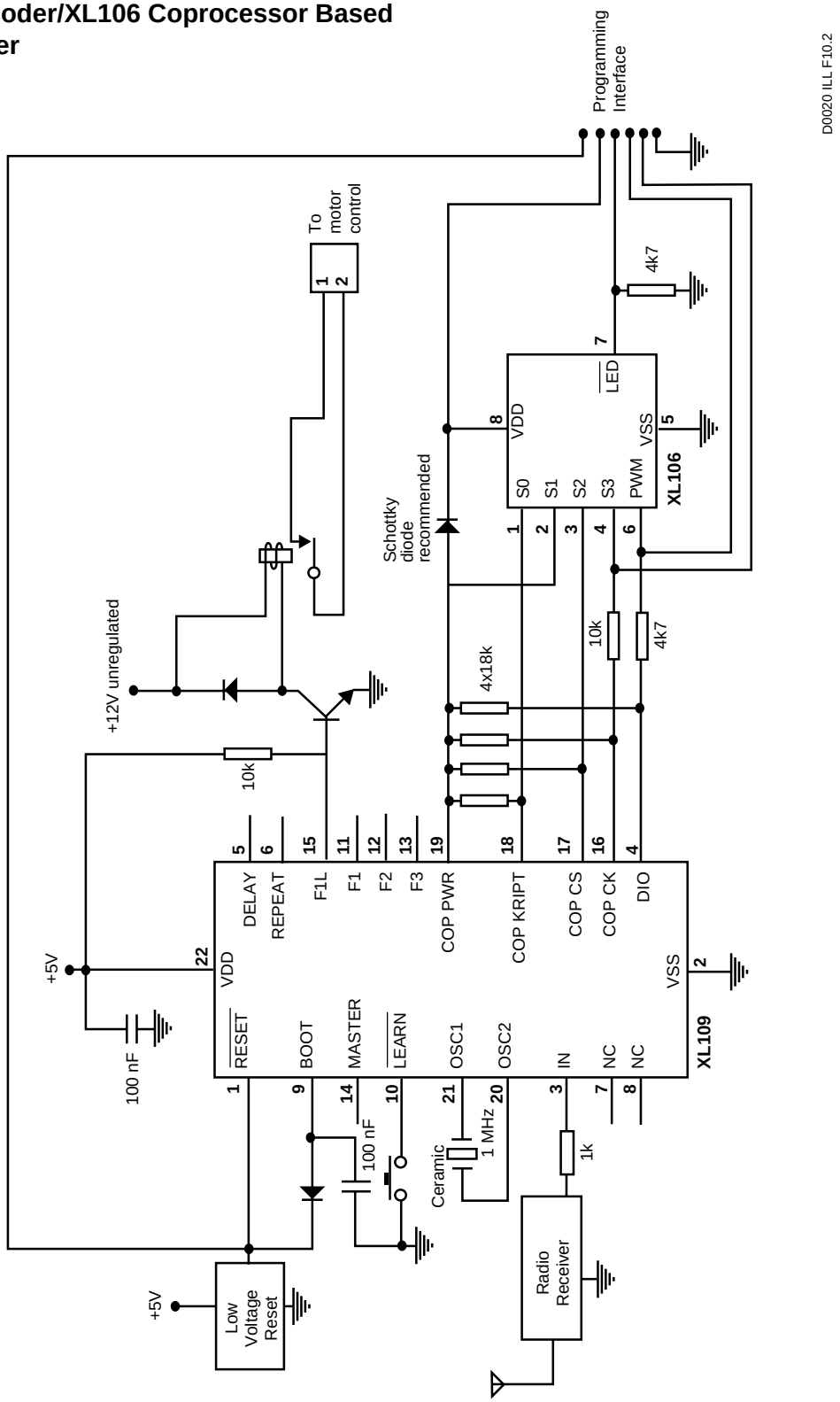
Assuming the total transmission time (Ttx) for each code word transmitted is 252 basic timing elements (Te) then the duty cycle calculations would be as follows:

	Te Count	Duty Cycle	Best Case		Worst Case		Nominal	
			Te Low	Te High	Te Low	Te High	Te Low	Te High
Header	32	0	32	0	32	0	32	0
Preamble	32	50%	16	16	16	16	16	16
Header	20	50%	10	10	10	10	10	10
Rolling & Fixed Code	168	66.7%	112	56	56	112	84	84
Standard Transmission Duty Cycle			32.5%		54.7%		43.6%	
Suppressed Code Word Duty Cycle			16.26%		27.4%		21.8%	

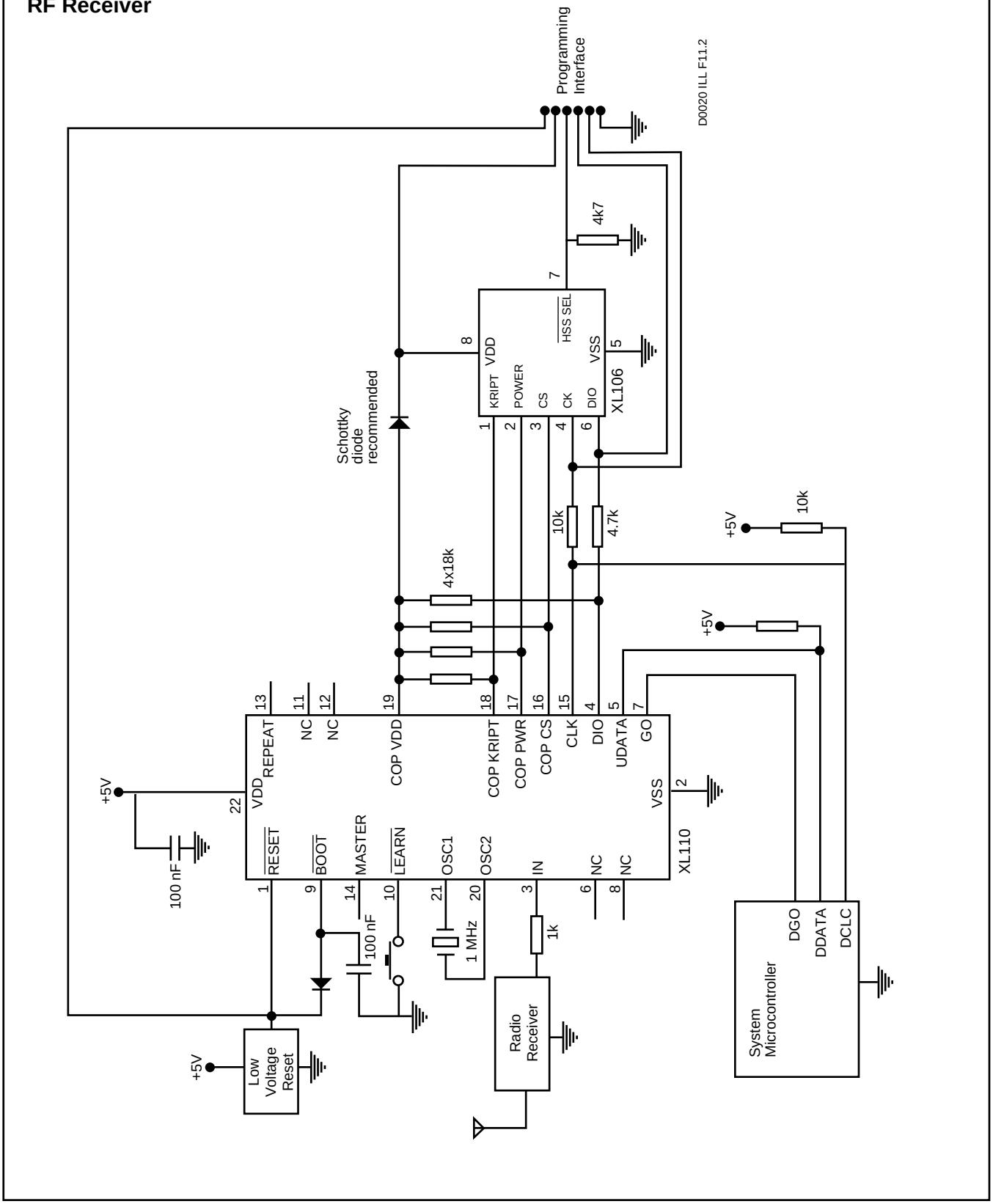
D0020 PGM T05.1

The following schematics represent interfaces with the XL109, the XL110, and XL138.

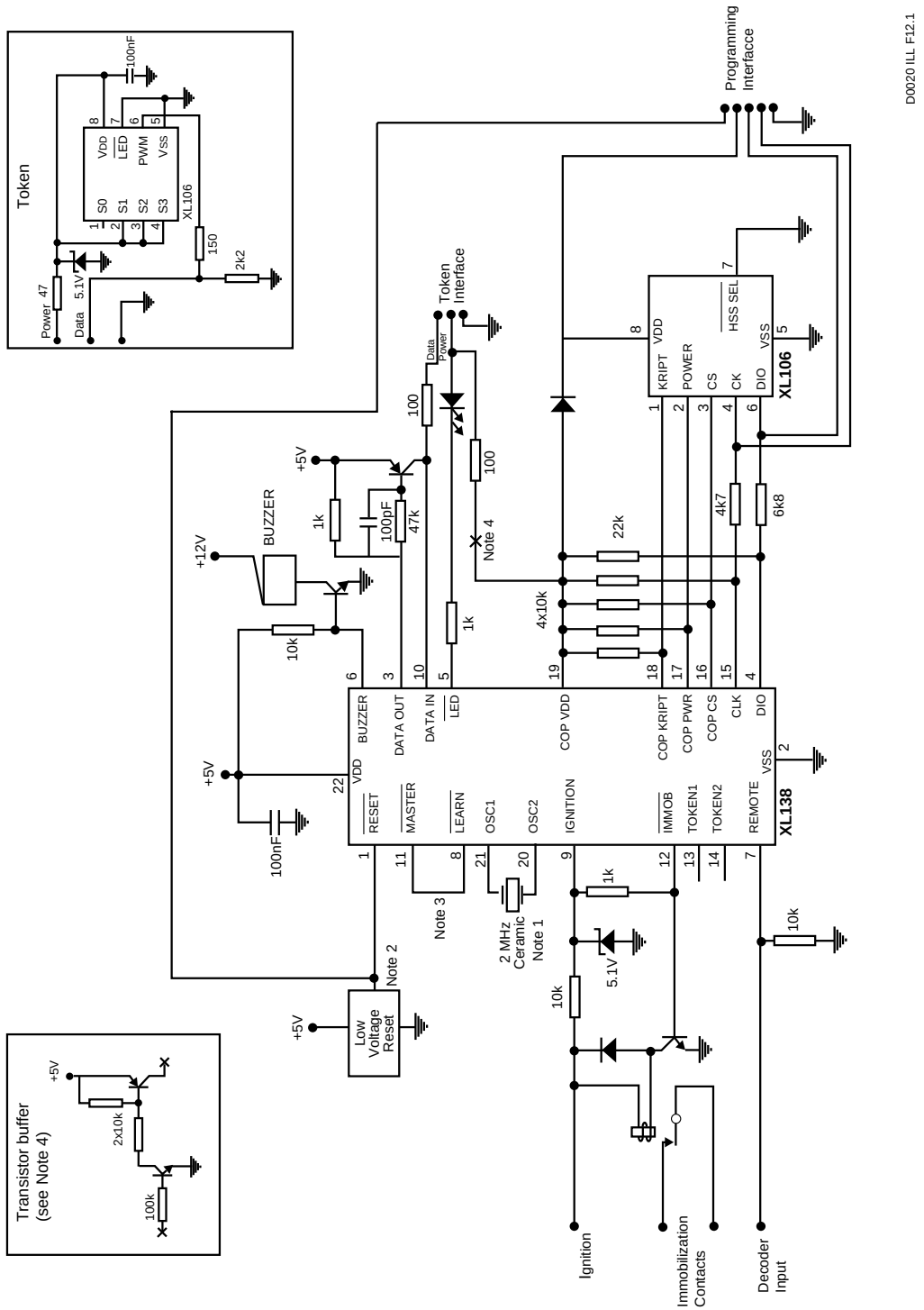
XL109 Decoder/XL106 Coprocessor Based RF Receiver



XL110 Decoder/XL106 Coprocessor Based RF Receiver



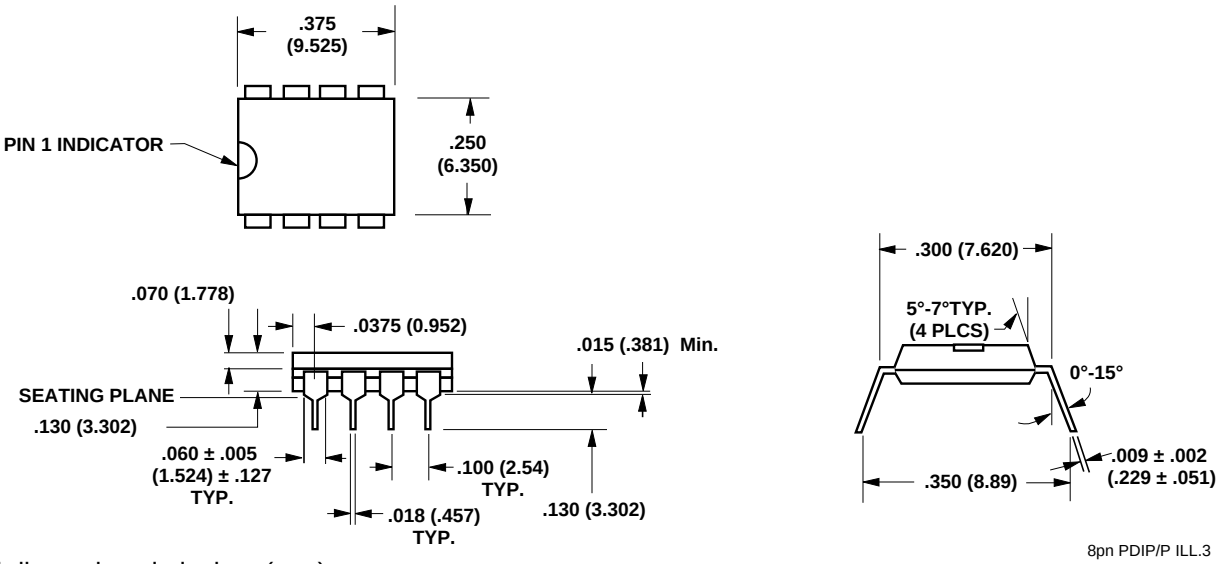
XL138 Controller/XL106 Coprocessor Based Token Authenticator



Notes:
1. Earlier versions required a 1 MHz resonator.
2. Low voltage reset circuit must ground $\overline{\text{RESET}}$ at $V_{DD} \leq 4.5V$.
3. $\overline{\text{LEARN}}$ must be protected from induced noise.
4. The transistor buffer must be inserted if XL105 tokens or connectors producing momentary short circuits are used.

PACKAGE DIAGRAMS

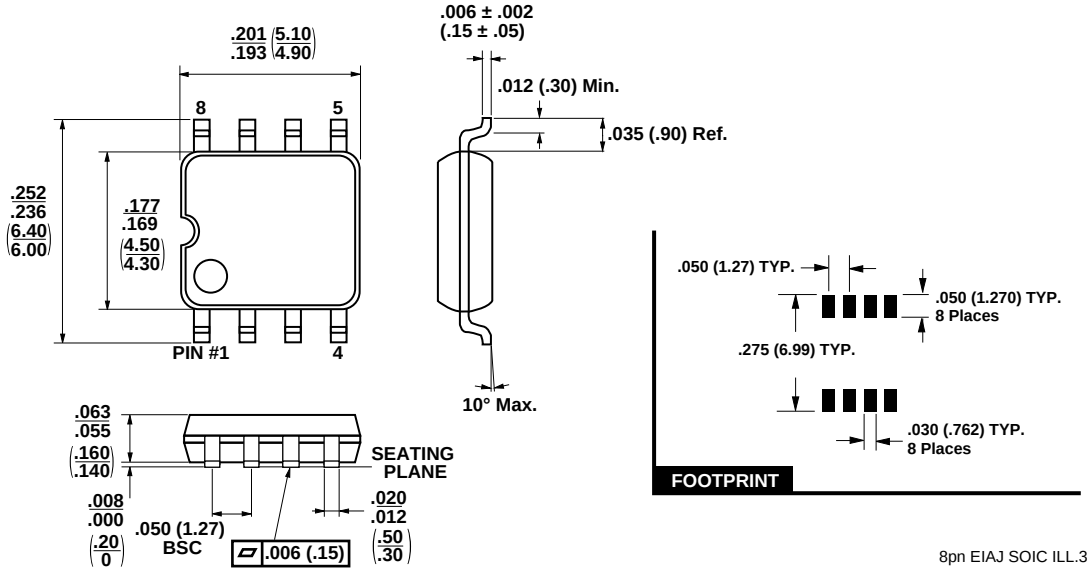
Plastic Dual-in-line (Type "P") Package (PDIP)



8pn PDIP/P ILL.3

All dimensions in inches (mm).

8 pin SOIC (Type "F") Package (EIAJ 175 mil. body width)



8pn EIAJ SOIC ILL.3

All dimensions in inches (mm).

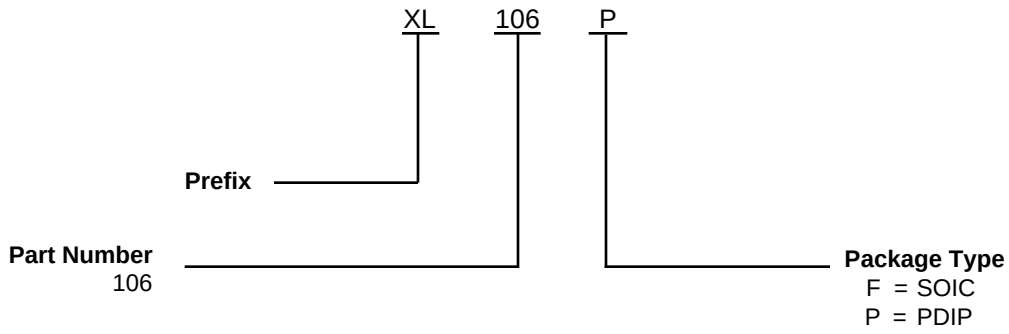
ORDERING INFORMATION

Standard Configurations

Prefix Type	Part Type	Package Type
XL	106	P, F

D0020 PGM T06.1

Part Numbers:



Application Notes

Family Overview

A complete discussion of the EXEL's rolling code Surelok Security Products, features and applications.

Remote Keyless Entry/Immobilizer System

An application note describing a complete remote keyless entry and immobilizer system based on EXEL's Surelok Security Products.

Remote Control Garage Door System

An application note describing a garage door receiver and transmitter system based on EXEL's Surelok Security Products.

Communicating with the XL110

An application note describing details on the XL110 serial interface.

Support Systems

XL CHD EVA Customer Evaluation Kit

This is a fully equipped evaluation kit that will allow testing and evaluation of all the components in the rolling code family. It is accompanied by the EV106 Evaluation Kit User's Manual (also available separately).

XL CHD FPK Factory Programming Kit

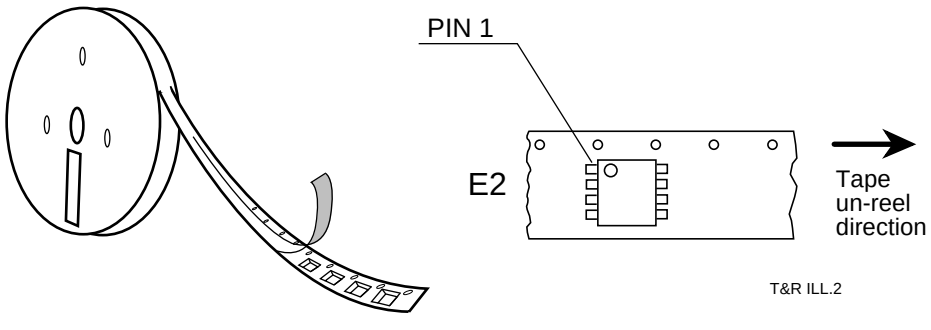
This is a complete system for production programming of rolling code devices. The kit includes a PC card and cables, software, documentation and a smartcard reader.

Applications Hot Line
Dial (408) 432-0500
Ask for Applications Engineering

MARKING INFORMATION

TAPE AND REEL (EMBOSSED) INFORMATION

Surface mount devices, which are normally shipped in antistatic plastic tubes, are also available mounted on embossed tape for customers using automatic placement systems. The following diagram provides general information regarding the direction of the IC's. Tape "E2" shall be designated with PIN 1 at the trail direction.



Quantity per reel: 2,500 parts

NOTICE

EXEL Microelectronics, Inc. reserves the right to make changes to the products contained in this publication in order to improve design, performance or reliability. EXEL Microelectronics, Inc. assumes no responsibility for the use of any circuits described herein, conveys no license under any patent or other right, and makes no representation that the circuits are free of patent infringement. Charts and schedules contained herein reflect representative operating parameters, and may vary depending upon a user's specific application. While the information in this publication has been carefully checked, EXEL Microelectronics, Inc. shall not be liable for any damages arising as a result of any error or omission.

EXEL Microelectronics, Inc. does not recommend the use of any of its products in life support applications where the failure or malfunction of the product can reasonably be expected to cause failure of the life support system or to significantly affect its safety or effectiveness. Products are not authorized for use in such applications unless EXEL Microelectronics, Inc. receives written assurances, to its satisfaction, that: (a) the risk of injury or damage has been minimized; (b) the user assumes all such risks; and (c) potential liability of EXEL Microelectronics, Inc. is adequately protected under the circumstances.

Surelok™ is a trademark of EXEL Microelectronics, Inc.

D0020 4/96
DVPTD 6931-05