EXEL Excellence in E² EXEL Microelectronics, Inc.

XL138 SureLok

Rolling Code Token Authentication Controller
A SureLok™ Security Product

FEATURES

- **64 Bit Key (1.8 X 10^{19} Possible Keys)**
- **Any Number of Tokens Per System**
- **Up to Two Keys Per Token**
- **Secure Learning Operation**
- **Vehicle Immobilizer Capability**
- **32 Bit Variable Code Ensures Over 4000 Million Combinations**
- **Programming and Reprogramming of the Coprocessor Done Through a Serial Communications Port, Dispensing with DIP Switches**
- **22-pin SOIC and PDIP**

OVERVIEW

The XL138 is a low cost token controller for use in vehicle security, access control and other security systems. An IFF (challenge and response) architecture is used.

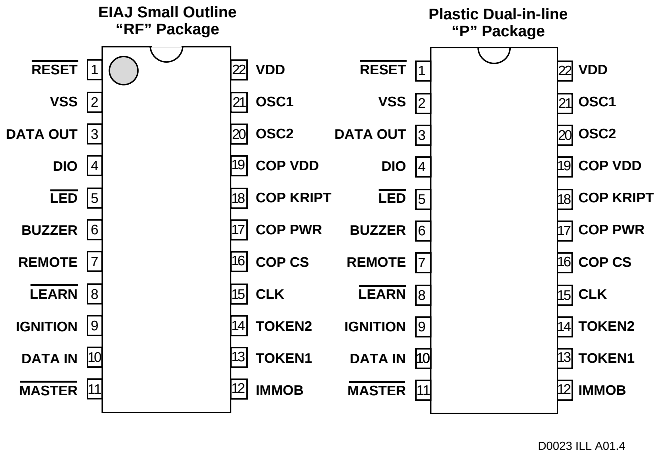
The controller is designed for use with XL106 based security tokens. Up to six groups of tokens, each with a unique key, can be used with a specific decoder. A group can contain any number of individual tokens.

The XL138 can "learn" the identity of new tokens, making it unnecessary to solicit dealer assistance when tokens are to be replaced or added to the system. A new token or group of tokens can be purchased off the shelf. A master token authorized learning system can be implemented, giving the owner exclusive control of the self-learning process. The master token for each system is unique, providing immunity even against breaches of security at service stations and installation centers.

The XL 106 coprocessor is used as a nonvolatile storage and decryption device. It is possible for an external microcontroller to use the coprocessor directly as nonvolatile storage, and for the user to program the coprocessor on the PC board.

More than one IFF key can be programmed into each security token. Two key locations can be detected by the XL138. Separate outputs exist for indicating the presence of a valid first or second key. The user can allocate different access privileges to different users by supplying each user with a unique key in either of the key locations.

PIN CONFIGURATION



PIN NAMES

$\overline{\text{RESET}}$	Hardware Reset Input
VSS	Ground Reference
IN	Decoder Input
DATA OUT	Data to Token
DIO	Data To/From Coprocessor
$\overline{\text{LED}}$	LED Driver
BUZZER	Buzzer Driver
REMOTE	Input From Remote Control Decoder
$\overline{\text{LEARN}}$	Self-Learning Select
IGNITION	Vehicle Ignition In
DATA IN	Data From Token
MASTER	Master Transmitter
IMMOB.	Immobilize output
TOKEN1	Token Key 1 Valid
TOKEN2	Token Key 2 Valid
CLK	Coprocessor Clock
COP CS	Coprocessor Select
COP PWR	Coprocessor Power
COP KRIPT	Coprocessor Control
COP VDD	Token/Coprocessor Power
OSC1-2	Oscillator Timing
VDD	Supply Voltage

APPLICATIONS

The controller can be used in various applications, including the following:

Vehicle Immobilizer

The controller monitors the vehicle's ignition line, and provides an output that allows or disallows starting and engine operation as required. Provision for short shutdowns without cut-out (to allow restarts) is included.

Access Controller

The TOKEN1 or TOKEN2 output is activated whenever a valid token is present in the socket. Separate indications are provided for the presence of a master token. The master token can be used to authorize learning, or for other special control operations.

GENERAL DESCRIPTION

The XL138 is designed to function with XL106 based tokens and uses an external XL106 coprocessor for decoding and nonvolatile storage. Typical applications include vehicle security and access control systems.

The rolling code system comprises an encoding and decoding algorithm with excellent resistance to key cloning, code interception and even sophisticated analytical attacks. A different challenge is used every time a token is inserted, making it impossible to construct a simple code interceptor for unauthorized access.

Direct access to the XL106 coprocessor can be arranged, making it possible to use the coprocessor as storage device for an external microcontroller. Keys and synchronization information can also be programmed directly into the coprocessor without removing it from the PC board.

The EXEL family provides unparalleled flexibility and use, and requires an absolute minimum of peripheral circuitry. Remote control and token systems can be implemented easily and economically using EXEL's devices. Considerable savings can be realized in most circuits, as circuit board space requirements and assembly costs are significantly reduced from the levels currently required. The XL138 controller provides the designer with considerable system flexibility while retaining the economic advantages of the low parts count. Programmable tokens and controller coprocessors make the process of configuring matching systems extremely fast and simple, while maintaining the highest possible level of security.

EXEL supplies evaluation kits, containing documentation, software, a programming probe and samples of the integrated circuits as well as tokens, transmitters and receivers. These kits can be used to assess the operational aspects of the devices. The probes and software can also be used for production runs.

FUNCTIONAL DESCRIPTION

The XL138 is a token controller for use in high security system. Vehicle security, access control and alarm activation are suitable applications for token based system.

The XL138 accommodates any number of tokens. Up to two keys per token can be used, making it possible to implement systems where different users have different users have different priority levels.

A group of tokens, sharing a single key, can be added to the decoder during a programming session. Up to five groups of tokens can be accommodated. A separate master key is used to authorize learning.

Token learning capability is built in, making it possible for the master to add new tokens to an existing system without dealer intervention.

The XL138 operates in one of two modes, depending on the application desired.

Vehicle Immobilizer Mode

The controller monitors the vehicle's ignition line, and makes available direct outputs for immobilizer control.

The user disarms the system by simply inserting a token into the receptacle, and then removing it.

Time-outs are included to enable the user to restart a vehicle without having to use the token again. Safeguards are included to ensure that, even if the controller fails during use, the vehicle will not be shut off while already moving.

Direct support for an LED and a buzzer are included. The REMOTE input makes it possible to use the vehicle security capabilities with an external remote control decoder.

Access Controller

Each token can contain two keys. Two separate outputs (TOKEN1 and TOKEN2) are provided. Each of these outputs is associated with a particular key position in the token. If a valid key is found in location 1, TOKEN1 will be asserted. By monitoring both of these outputs, two different levels of priority can be allocated to each user. The TOKEN outputs are asserted for as long as the token remains in the receptacle.

User Storage

The XL106 coprocessor is accessible through a three wire interface. A user's microcontroller can use the coprocessor EEPROM directly for nonvolatile storage. Any form of operational information stored in the coprocessor will be held through power interruptions.

Keys can be programmed directly into the 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

The XL138 token controller is an authentication system, implementing an IFF protocol in conjunction with XL106 based tokens.

The IFF protocol requires bidirectional communications between the controller and the tokens, rendering it unsuitable for simple remote control systems. However, the XL138 is ideal for the implementation of low cost vehicle security and access control systems. Tokens can be implemented in smart cards, custom plastic housings and jack plugs.

The IFF (Identification Friend or Foe) protocol is based on the token's ability too calculate and return a response, based on a challenge and an internal key. In the case of EXEL's IFF system, a 32 bit challenge is supplied to the token. The response is calculated from the challenge and a 64 bit key. The response length is also 32 bits.

The 64 bit key is stored in EEPROM, and will be retained for more than a decade, even if power is never applied to the token. In addition, the key is read protected, making it impossible to inspect the key from outside.

To attack an IFF system, the assailant would compile a large lookup table of challenges and their associated responses. A device containing this lookup table is then presented in lieu of the legitimate token. When the controller presents its challenge, the correct response is looked up in the table and returned to the controller.

However, due to the large number of possible challenges in the XL138 system (around 4300 million), constructing such a lookup table is not feasible.

Also, the relationship between the challenge, the key and the response is dependent on a nonlinear function, and even with a large number of samples, the relationship cannot readily be determined. Analytical attacks are therefore also not feasible in EXEL IFF systems.

Tokens cannot be copied, because of the impossibility of reading the keys from an existing token. While it is possible to manufacture any number of tokens with the same key if required, an existing token can in no way be cloned.

The XL138 features a learning system, where users can add new tokens or replace existing ones without dealer intervention; range, learning has been implemented without compromising the system's security. A master token can be used to authorize all learning operations, making it impossible even for service personnel with unrestricted access to the vehicle to add their own tokens to the system without the owner's consent.

In addition to the security of the coding system, the XL138 provides an immobilizer protocol, including ignition monitoring and automatic restart time-out. When the ignition is turned off, the driver has 30 seconds to restart his vehicle without having to disarm the immobilizer again.

Also, the XL138 stores its state in EEPROM, and even removing the power from the unit will not cause it to lose track of its state and grant access to an unauthorized user.

ABSOLUTE MAXIMUM RATINGS

Supply Voltage	-0.3 to 6.5V
Voltage on any Pin	-0.3 to V_{DD} +0.3V
Storage Temperature	-55 to +125°C
Soldering Temperature (less than 10 seconds)	300°C
ESD Voltage (JEDEC method)	2000V

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
	Oscillator Stability	±1	%

D0023 PGM T01.1

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		4		mA
V_{IH}	Input H voltage	2.25			V
V_{IL}	Input L voltage			0.75	V
I_{OL}	Output sink current*			10	mA

*Open collector outputs

D0023 PGM T02.1

AC ELECTRICAL CHARACTERISTICS

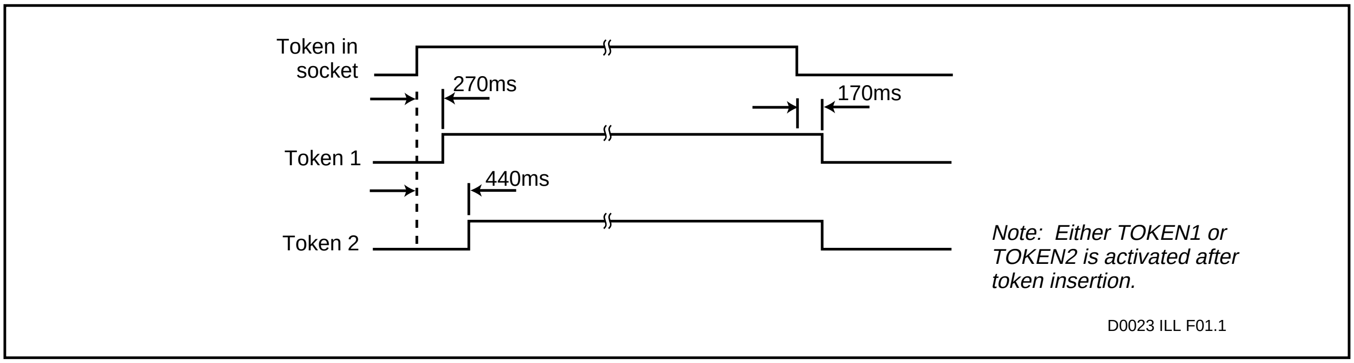
Ta = -40°C to 85°C, V_{DD} = 5V ± 10% unless otherwise specified

Symbol	Parameter	Min	Typ	Max	Unit
T_{RESET}	Reset time	50			µs
T_{DPWR}	Delay from power on		100		ms
T_{PWM}	Input bit period	160		540	µs
F_{IDR}	Input data rate		1500		bps
T_{TT1}	Token in to Token1 output		270		ms
T_{TT2}	Token in to Token2 output		440		ms
F_{LEDA}	LED flash rate armed		1		Hz
F_{LEDD}	LED flash rate disarmed		3		Hz
D_{LEDA}	LED duty cycle armed		15		%
D_{LEDD}	LED duty cycle disarmed		50		%
T_{IMMOB}	Immobilize time from ignition off		30		s
T_{LEARN}	Learn activation time	10			ms

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

D0023 PGM T03.1

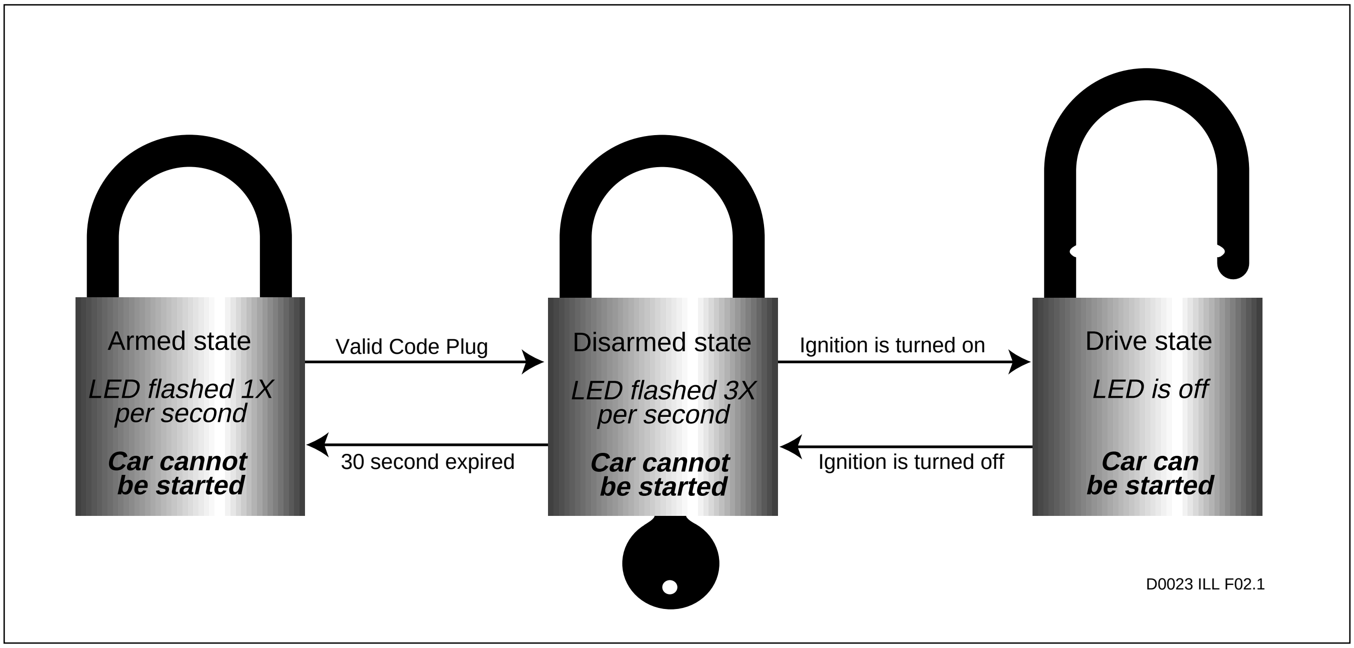
ACCESS CONTROL TIMING



Note: Either TOKEN1 or TOKEN2 is activated after token insertion.

D0023 ILL F01.1

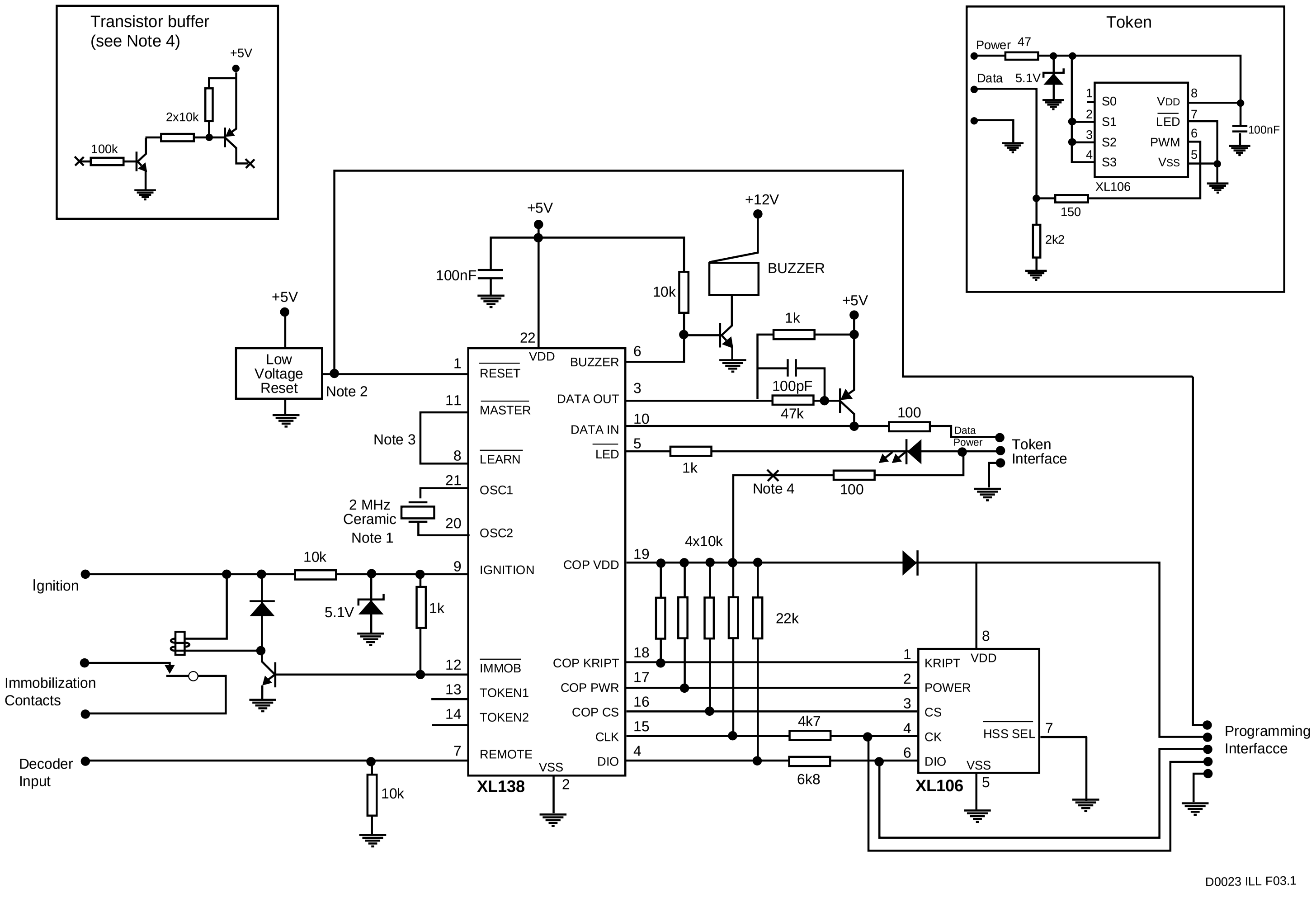
IMMOBILIZER STATE DIAGRAM



D0023 ILL F02.1

APPLICATION EXAMPLE

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.

Pin Functions

Pin	Name	Description	Type
1	$\overline{\text{RESET}}$	Hardware reset input	I1
2	V_{SS}	Ground reference	—
3	DATA OUT	Data to token	B2
4	DIO	Data to/from coprocessor	B2
5	$\overline{\text{LED}}$	LED driver	B2
6	BUZZER	Buzzer driver	B2
7	REMOTE	Input from remote control decoder	I2
8	$\overline{\text{LEARN}}$	Learn mode select	I2
9	IGNITION	Vehicle ignition in	I2
10	DATA IN	Data from token	I2
11	$\overline{\text{MASTER}}$	Master output	O3
12	$\overline{\text{IMMOB}}$	Immobilize output	O3
13	TOKEN1	Token key 1 valid	O3
14	TOKEN2	Token key 2 valid	O3
15	CLK	Coprocessor clock	O3
16	COP CS	Coprocessor select	O3
17	COP PWR	Coprocessor power	O3
18	COP KRIPT	Coprocessor control	O3
19	COP VDD	Token/coprocessor power	C
20	OSC2	Oscillator timing	—
21	OSC1	Oscillator timing	—
22	V_{DD}	Supply voltage	—

D0023 PGM T04.1

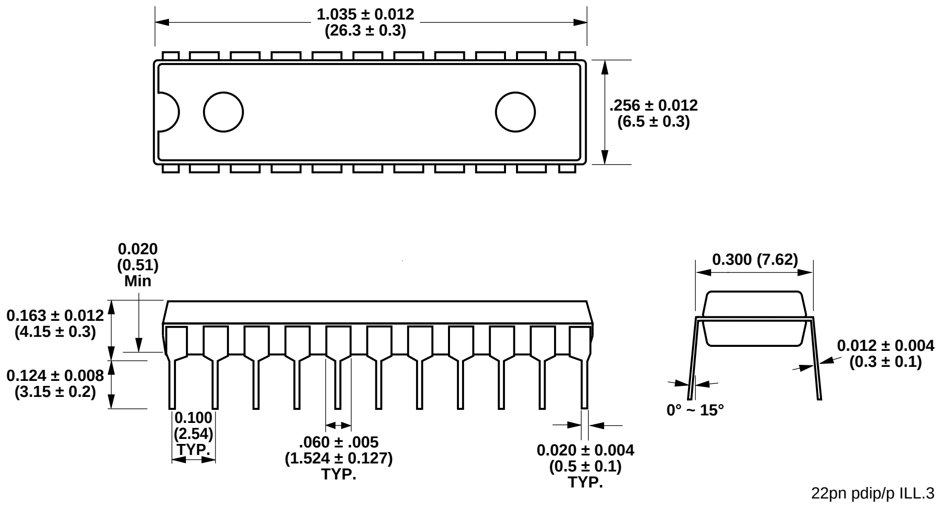
Key to I/O types

I = Input
B = Bidirectional (open drain output)
O = Open drain output
C = CMOS output
1 = 500 kΩ pullup resistor
2 = 70μA pullup. Approximately equivalent to 70 kΩ pullup resistor
3 = Protection diode to V_{DD} Reverse biased for normal operation

Specified currents and resistances are nominal, and are subject to -50% and +100% variation.

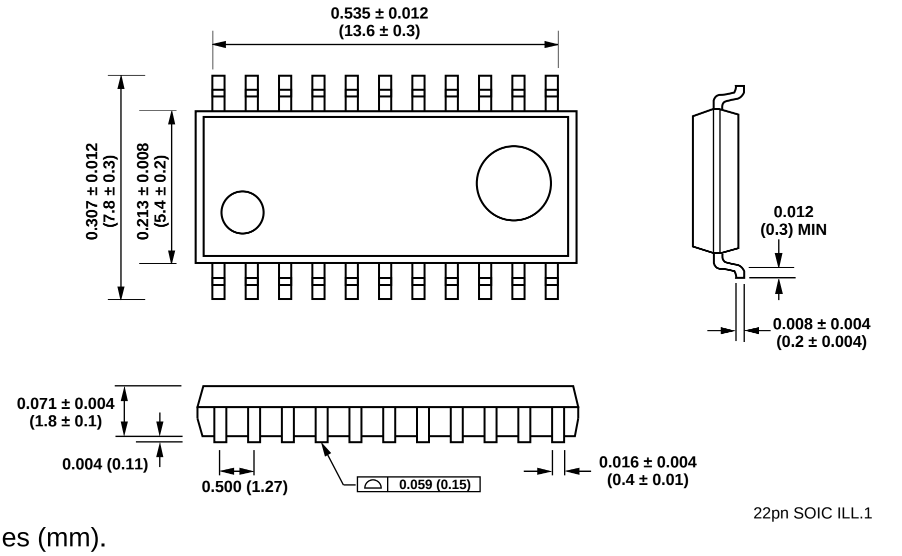
PACKAGE DIAGRAMS

Plastic Dual-in-line (Type “P”) Package (PDIP)



All dimensions in inches (mm).

EIAJ Small Outline (Type “F”) Package (SOIC)



All dimensions in inches (mm).

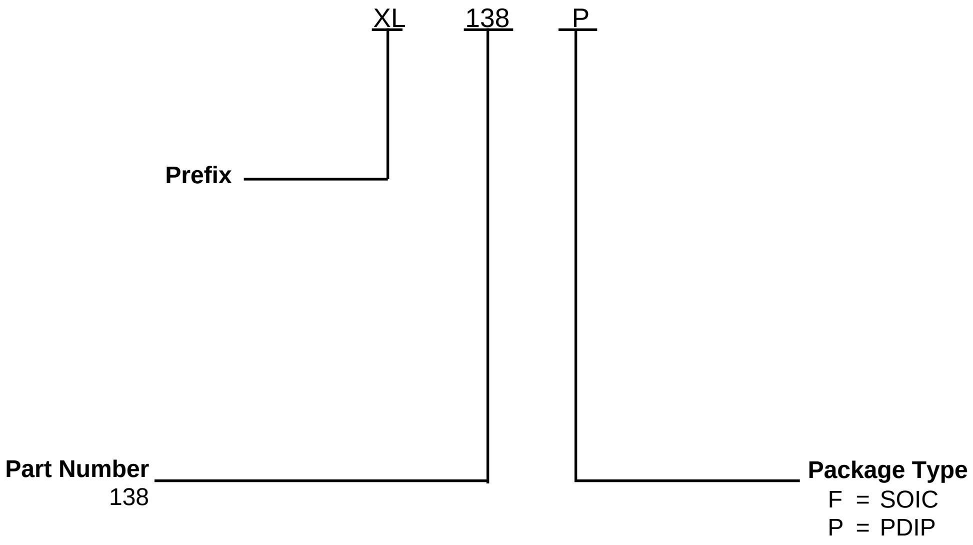
ORDERING INFORMATION

Standard Configurations

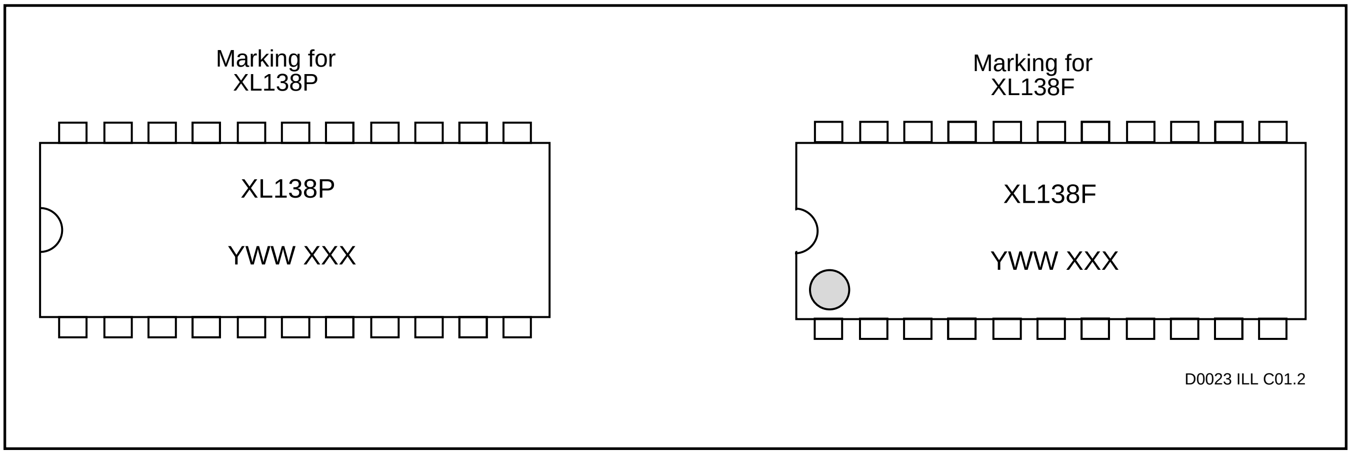
Prefix Type	Part Type	Package Type
XL	138	P, F

D0023 PGM T05.1

Part Numbers:

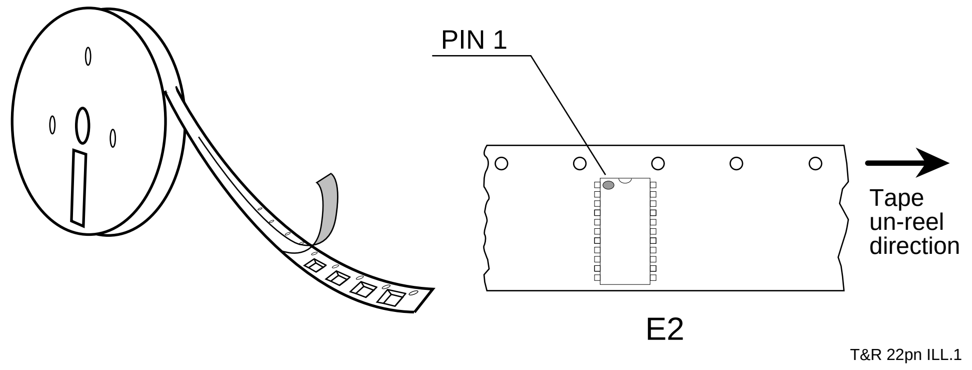


MARKING INFORMATION



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: 1,000 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.