T-46-13-27

CATALYST SEMICONDUCTOR
2231 CALLE DE LUNA, SANTA CLARA, CA 95054 Telephone: (408) 748-7700

CAT35C704, CAT35C704I [Industrial Temperature]
4K-bit SECURE ACCESS Serial E^2PROM

Preliminary

DESCRIPTION

The CAT35C704 is a 4K-bit Serial E^2PROM that offers a unique ***on-chip capability to safeguard stored data from unauthorized users***. Onboard E^2PROM "Access Registers" store a "password" which, once set, is used for authentication purposes prior to device operation. Two operating modes are provided: an unprotected and a password protected (secure) mode. In the unprotected mode, the CAT35C704 is a simple-to-use 4K-bit serial E^2PROM that features software memory partitioning and easy interfacing with standard microcontrollers.

In the password-protected mode, access to all or part of the device is prohibited until the correct access code has been entered. The boundary between the protected and unprotected area is user programmable. The protected area is only accessible via the correct access code, while the unprotected area allows any user READ-only access. The length of the access code is user selectable from one to eight bytes long (>$1.8x10^{19}$ combinations). With a maximum clock rate and 8 bytes of access code, it would take millions of years to attempt all the possible combinations.

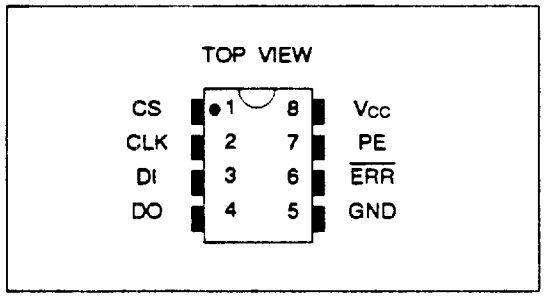
In the unprotected mode, with the use of the memory pointer, the device may be divided into read/write and read-only areas. The boundary is user programmable and can be changed without the use of an access code. This feature provides write-protection against inadvertent erasure or overwriting of data without invoking the password protection mechanism.

The CAT35C704 uses a unique ***Serial-byte*** synchronous communication protocol.

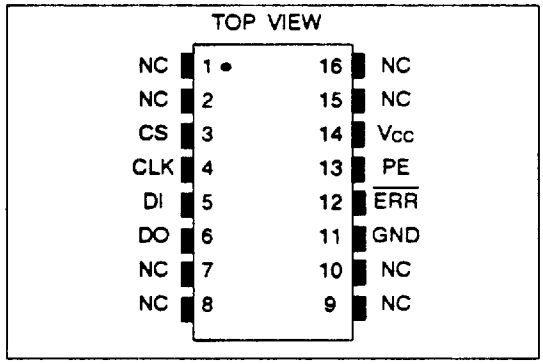
FEATURES

- Reliable 3V or 5V CMOS technology
- Password READ/WRITE - protect
- Non-password WRITE - protect
- Sequential data register READ
- User definable protected area
- Password length: 1 to 8 bytes
- Memory Array organization: x8 or x16
- High Speed synchronous protocol
- Low power consumption:
  - Active: 3mA
  - Standby: 200µA
- Operating frequency: DC-3MHz
- 10 year data retention
- 10,000 write/erase cycles
- Available in 3V version

PIN OUT **DIP**



PIN OUT **SO**



PIN FUNCTIONS

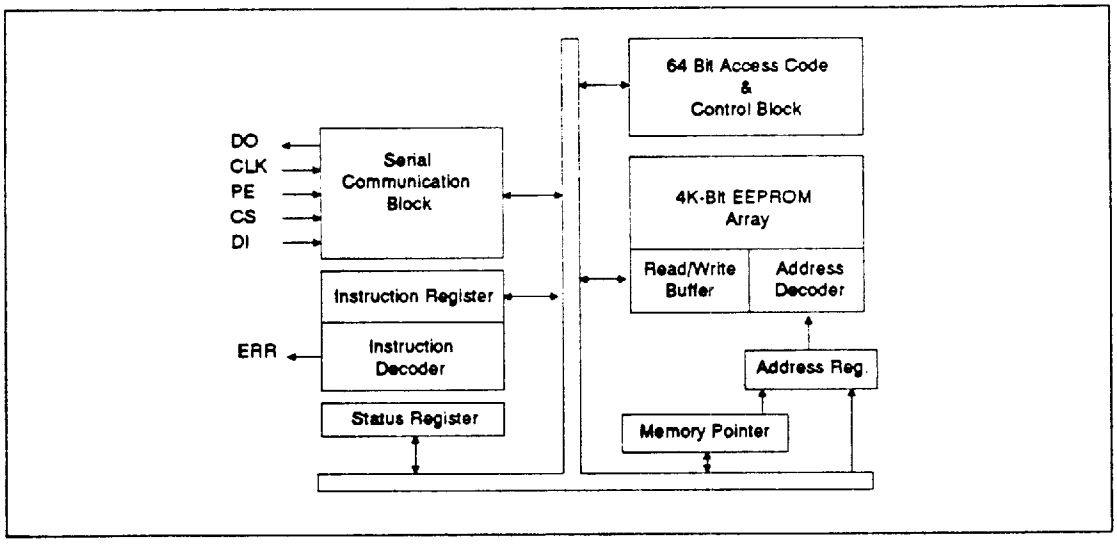
CS	Chip select	PE	Parity enable
DO *	Serial data output	ERR	Error indication pin
CLK	Clock input	Vcc	Positive power supply
DI *	Serial data input	GND	Ground

* DI,DO may be tied together to form a common I/O.

SECURE ACCESS SERIAL DEVICE FAMILY

DEVICE	OPERATING VOLTAGE	PROTOCOL	CLOCK FREQ	I/O SPEED
35C704	5V	SECS	3 MHz	3 MHz
33C704	3V	SECS	1 MHz	1 MHz
35C804-A	5V	UART	4.9152 MHz	9600 Baud
35C804-B	5V	UART	3.579545 MHz	9600 Baud
33C804-A	3V	UART	4.9152 MHz	9600 Baud
33C804-B	3V	UART	3.579545 MHz	9600 Baud

BLOCK DIAGRAM



ABSOLUTE MAXIMUM RATINGS *

Storage temperature	T_{stg}	-65°C to +150°C
Power supply	V_{CC}	+7 V
Voltage on any input pin		-0.3 to +7V
Voltage on any output pin		-0.3V to V_{CC} +0.3V

*Stresses above those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and the functional operation of the device at these or any other conditions above those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

DC CHARACTERISTICS

(V_{CC} = +5V ±10%, T_A = -40°C to +85°C Industrial, 0°C to +70°C Commercial. For I_{CC} DO is unloaded.)

Symbol	Parameter	Conditions	Limits			Unit
			Min.	Typ.	Max.	
I_{CC}	Programming Supply Current	V_{CC} =5.5V, CS = V_{CC}			3	mA
I_{SB}	Standby Supply Current	V_{CC} = 5.5V, CS = 0V DI = 0V, CLK = 0V			200	µA
V_{IL}	Input Voltage, LOW		-0.1		0.8	V
V_{IH}	Input Voltage, HIGH		2.0			V
V_{OL}	Output Voltage, LOW	I_{OL} = 2.1mA			0.4	V
V_{OH}	Output Voltage, HIGH	I_{OH} = -400µA	2.4			V
I_{LI}	Input Leakage Current	V_{IN} = 5.5V			10	µA
I_{LO}	Output Leakage Current	V_{OUT} = 5.5V CS = 0V			10	µA

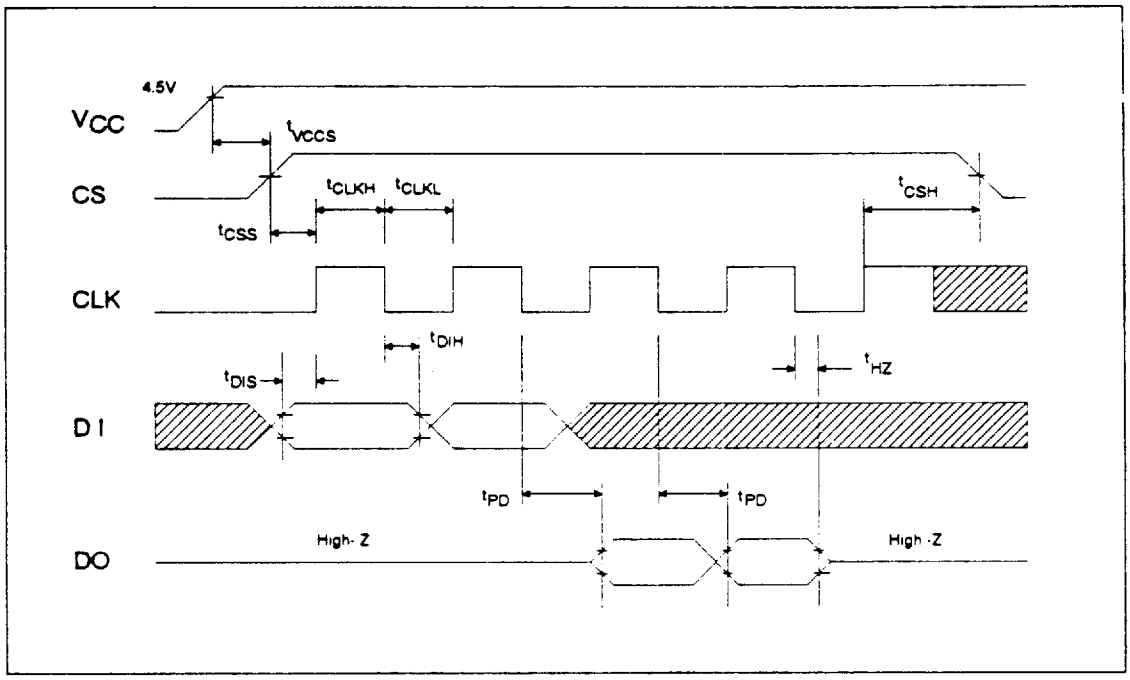
AC CHARACTERISTICS

(V_{CC} = +5V ±10%, T_A = -40°C to +85°C Industrial, 0° to +70° Commercial)

Symbol	Parameter	Conditions	Limits			Unit
			Min.	Typ.	Max.	
t_{CSS}	CS setup time	C_L = 100pF V_{IN} = V_{IH} or V_{IL} V_{OUT} = V_{OH} or V_{OL}	150			ns
t_{CSH}	CS hold time		0			ns
t_{DIS}	DI setup time		50			ns
t_{DIH}	DI hold time		0			ns
t_{PD}	CLK to DO delay				150	ns
t_{HZ} *	CLK to DO high-z delay				50	ns
t_{EW}	Erase/Write pulse width				10	ms
t_{CSL}	CS low pulse width		200			ns
t_{CLKH}	CLK high pulse width		165			ns
t_{CLKL}	Clock low pulse width		100			ns
t_{SV}	ERR output delay	C_L = 100pF			150	ns
t_{VCCS}	V_{CC} to CS setup time	C_L = 100pF	5			µs
t_{CSZ}	CS to DO high-z delay				50	ns
t_{CSD}	CS to DO busy delay				150	ns
f_{CLK}	Maximum clock frequency		DC		3	MHz

* t_{HZ} is measured from the falling edge of the clock to the time when the output is no longer driven.

AC TIMING



INTRODUCTION

The CAT35C704 is a 4K E^2PROM that features a password protection scheme to prevent unauthorized access to the information stored in the device. It contains an access code register which stores one to eight bytes of access code along with the length of that access code. Additionally, a memory pointer register stores the address that partitions the memory into protected and unprotected areas.

As shipped from the factory, the device is unprogrammed and unprotected. The length of the access code is equal to zero and the memory pointer register points to location zero. Every byte of the device is fully accessible without an access code. Setting a password and moving the memory pointer register to cover all or part of the memory secures the device. Once secured, the memory is divided into a read/write area and a read-only area with the entry of a valid access code. If no access code is entered, the memory is divided into a read-only area and a non-access area. Figure 1 illlustrates this partitioning of the memory array.

Another feature of the CAT35C704 is WRITE-protection without the use of an access code. If the memory pointer register is set to cover all or part of the memory, without setting the access code register, the device may be divided into an area which allows full access, and an area which allows READ-only access. To write into the READ-only area the user can override the memory pointer register for every WRITE instruction or he can simply move the address in the memory pointer register to uncover this area, and then WRITE into the memory. This mechanism prevents inadvertent overwriting of important data in the memory without the use of an access code. Figure 2 illustrates this partitioning of the memory array.

To allow for convenient reading of blocks of contiguous data, the device has a READ SEQUENTIAL instruction which accepts a starting address of the block and continuously outputs data of subsequent addresses until the end of memory, or until CHIP SELECT goes LOW.

The CAT35C704 communicates with external devices via a synchronous serial communication protocol (SECS) that has a maximum transmission rate of 3 MHz. The data transmission may be a continuous stream of data or it can be packed by pulsing CHIP SELECT LOW in between each packet of information. (Except for the SEQUENTIAL READ instruction where CHIP SELECT must be held high)

FIGURE 1

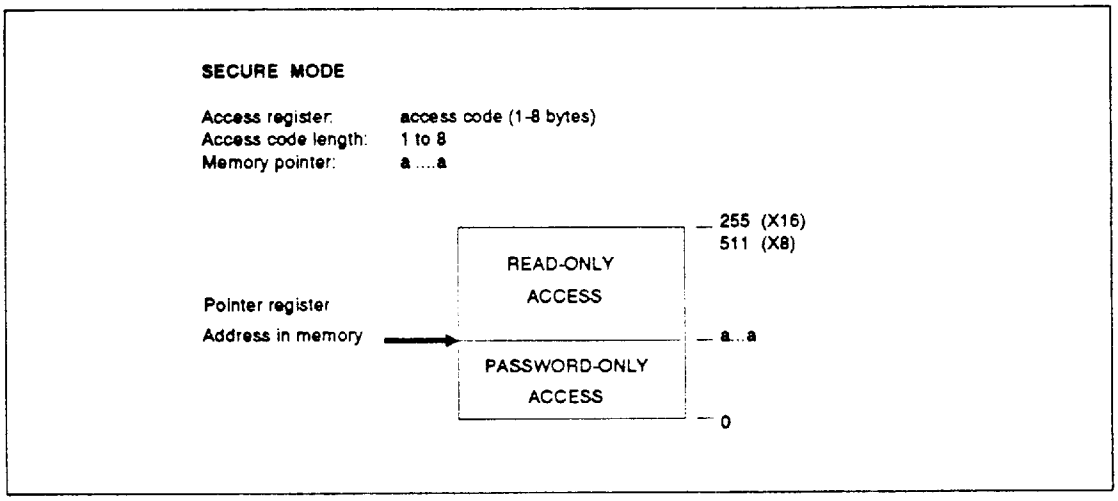
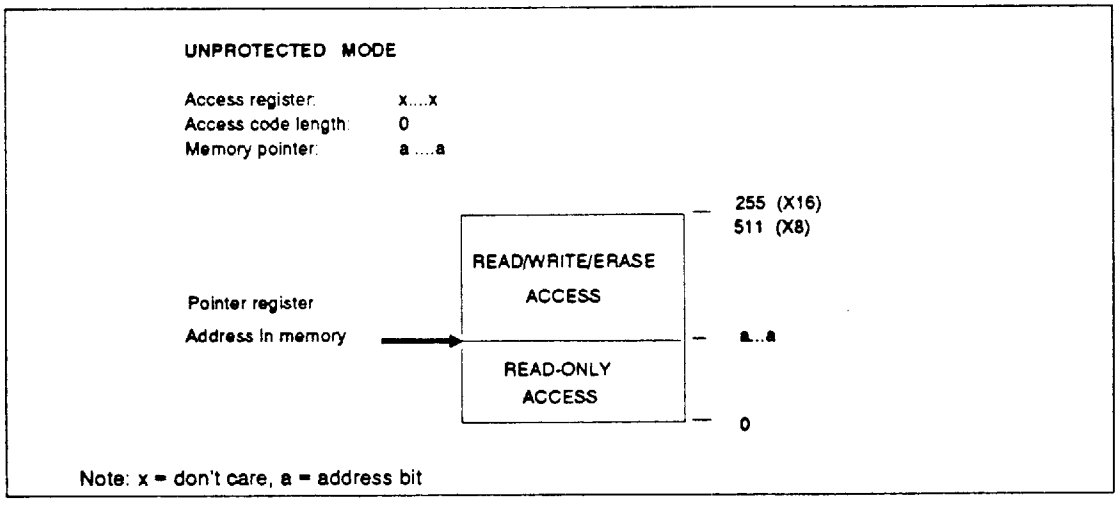


FIGURE 2



PIN DESCRIPTION

CS

Chip Select is a TTL compatible input which, when set HIGH, allows normal operation of the device. Any time Chip Select is set LOW, it resets the device, terminating all I/O communication, and puts the output in a high impedance state. CS is used to reset the device if an error condition exists or to put the device in a power-down mode to minimize power consumption. It may also be used to frame data transmission in applications where the clock and data input have to be ignored from time to time. Although CS resets the device, it does not change the write/erase or the access-enable status, nor does it terminate a programming cycle once it has started. The write/erase and access-enable functions, once enabled, will remain enabled until specific disabling instructions are sent or until power is removed.

CLK

The System Clock is a TTL compatible input pin that allows operation of the device over a frequency range of DC to 3 MHz (1 MHz for the CAT33C704).

DI

The Data Input pin is TTL compatible and accepts data and instructions in a serial format. Each instruction must begin with "1" as a start bit. The device will accept as many bytes as an instruction requires, including both data and address bytes. With the SECS protocol, extra bits will be disregarded if they are "0's", and misinterpreted as the next instruction if they are "1's". An instruction error will cause the device to abort operation and all I/O communication will be terminated until a reset is received.

DO

The Data Output pin is a tri-state TTL compatible output. It is normally in a high impedance state unless a READ or an ENABLE BUSY instruction is executed. Following the completion of a 16-bit or 8-bit data stream, the output will return to the high impedance state. During a WRITE/ERASE cycle, if the ENABLE BUSY instruction has been previously executed, the output will stay LOW while the device is BUSY, and it will be set HIGH when the WRITE/ERASE cycle is completed. DO will stay HIGH until the completion of the next instruction's op-code and, if the next instruction is a READ, DO will output the appropriate data at the end of the instruction. If ENABLE BUSY has not been previously executed, DO will stay in a high impedance state. DO will also go to the high impedance state if an error condition is detected. If ENABLE BUSY has not been executed, to determine whether the device is in a WRITE/ERASE cycle or in an error condition, a READ STATUS instruction may be entered. When the device is in a WRITE/ERASE cycle it will output an 8-bit status word. If it does not, it is in an error condition.

PE

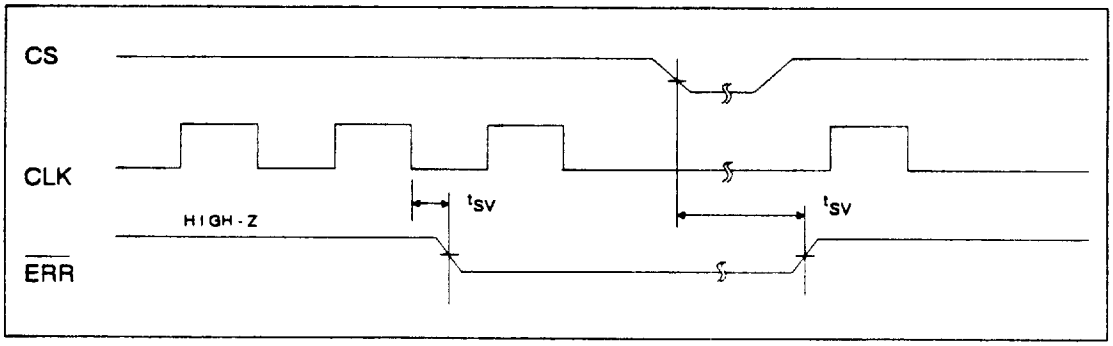
The Parity Enable pin is a TTL compatible input. If the PE pin is set HIGH, the device will be configured to communicate using even parity, and if the pin is set LOW, it will use no parity. In this case, instructions or data that include parity bits will not be interpreted correctly.

Note: The PE input is internally pulled down to GND (i.e. default = no parity). As with all CMOS devices, CS, CLK and DI inputs must be connected to either HIGH or LOW, and not left floating.

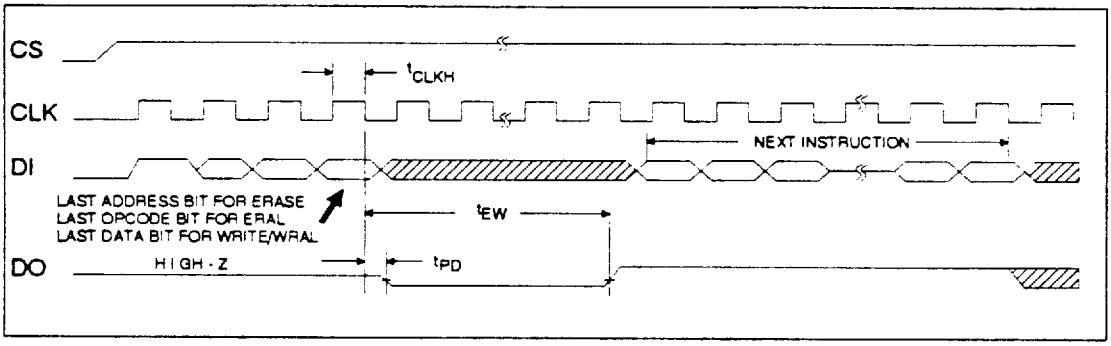
$\overline{\text{ERR}}$

The Error indication pin is an open drain output. If either an instruction or parity error exists, the ERR pin will output a "0" until the device is reset. This can be done by pulsing CS LOW.

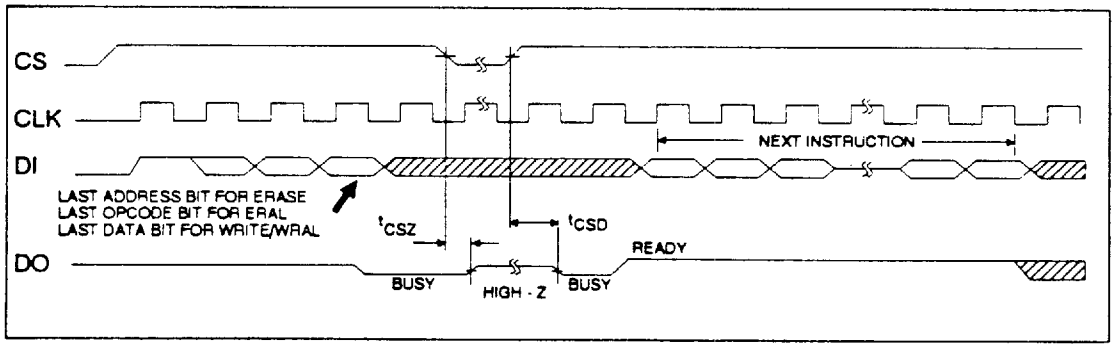
AC TIMING <$\overline{ERR}$ PIN TIMING>



AC TIMING



AC TIMING <CS = 0>



DEVICE OPERATION

INSTRUCTIONS

The CAT35C704 instruction set includes 19 instructions.
Six instructions are related to security or write protection:

DISAC Disable Access
ENAC Enable Access
MACC Modify Access Code
OVMPR Override Memory Pointer Register
RMPR Read Memory Pointer Register
WMPR Write Memory Pointer Register

Six instructions are READ/WRITE/ERASE instructions:

ERAL Erase All
ERASE ERASE memory
READ READ memory
RSEQ Read Sequentially
WRAL Write All
WRITE WRITE memory

Note: All write instructions will automatically perform an erase before writing data.

Seven instructions are used as control and status functions:

DISBSY Disable Busy
ENBSY Enable Busy
EWEN Erase/Write Enable
EWDS Erase/Write Disable
NOP No Operations
ORG Select Memory Organization
RSR Read Status Register

UNPROTECTED MODE

As shipped from the factory, the CAT35C704 is in the unprotected mode. The access code length is set to 0, and the memory pointer is at address 00 hex. While in this mode, any portion of the E^2PROM array can be read or written to without an access code. A portion of the memory may be protected from any write or erase operation by setting the memory pointer to the appropriate address via the WMPR (Write Memory Pointer Register) instruction:

WMPR [address]

As shown previously in Figure 2, memory locations below the address set in the memory pointer will be write/erase protected. Thus, unintentional erasure or overwriting of data in this area will be prevented, while memory locations at or above the protected area still allow full access. This protection does not apply to the ERAL and WRAL commands which are not blocked by the memory pointer.

SECURE MODE

As shown previously in Figure 1, in the secure mode, memory locations at or above the address set in the memory pointer allow READ-only access. Memory locations below that address will require an access code before they can be accessed. The secure mode is activated with an MACC (Modify Access Code) instruction followed by a user access code which can be one to eight bytes in length.

EWEN
MACC [old code][new code][new code]

The EWEN instruction enables the device to perform WRITE/ERASE operations. The new access code must be entered twice for verification. If the device already has an access code, the old access code must be entered before the new access code can be accepted. The length of the password is incorporated into the MACC portion of the instruction.

Once the secure mode is activated, access to memory locations is under software control. Access (read, write, and erase operations) to the memory locations below the address in the memory pointer is allowed only if the ENAC (Enable Access) instruction followed by the correct access code has been previously executed.

ENAC [access code]
EWEN
WRITE [address][data]

The ENAC instruction, along with the access code, enables access to the protected area of the device.

The EWEN instruction enables execution of the ERASE/WRITE operations. This portion of the memory is otherwise inaccessible for any operation. Read-only access is allowed without the access code for memory locations at or above the address in the memory pointer.

The access code can be changed by the following instruction :

ENAC [old access code]
EWEN
MACC [old code][new code][new code]

A two-tier protection scheme is implemented to protect data against inadvertent overwriting or erasure. To write to the memory, an EWEN (Erase/Write Enable) must first be issued. The CAT35C704 will now allow write/erase operations to be performed only on memory locations at or above the address set in the memory pointer. The remaining portion of the memory is still protected. To override this protection, an OVMPR (Override Memory Pointer Register -- see Memory Pointer Register) must be issued for every write/erase instruction which accesses the protected area :

ENAC [access code]
EWEN
OVMPR
WRITE [address][data]

As an alternative to the OVMPR instruction, the WMPR (Write Memory Pointer Register) instruction may be used to move the memory pointer address to uncover the area where writing is to be performed:

ENAC [access code]
EWEN
WMPR [address]
WRITE [address][data]

As shipped from the factory, the device is in the unprotected mode. The length of the access code is user selectable from a minimum of one byte to a maximum of eight bytes (> 1.84×10^{19} combinations). Loading a zero-length access code will disable protection.

MEMORY POINTER REGISTER

The memory pointer enables the user to segment the E^2PROM array into two sections. In the unprotected mode, the array can be segmented between read-only and full access, while in the secure mode, the memory may be segmented between read-only access and password-only access. Three instructions are dedicated to the memory pointer operations. The first one is WMPR (Write Memory Pointer Register). This instruction, followed by an address, will load the memory pointer register with a new address. This address will be stored in the E^2PROM and can be modified only by another WMPR instruction. The second instruction is OVMPR (Override Memory Pointer Register) which allows a single write/erase to be performed to memory locations below the address set in the memory pointer. This instruction allows the user to modify data in a segmented array without having to move the memory pointer. Once the operation is complete, the device returns to the protected mode. If the device is in the secure mode both of these instructions require the ENAC instruction and a valid access code prior to their execution. The third instruction is the RMPR (Read Memory Pointer Register) which will place the current contents of the register in the serial output buffer.

SECS PROTOCOL

The CAT35C704 implements the SECS communication protocol which uses an 8-bit transmission format. As shown in Figures 3-9, all instructions are 8-bits long with the first bit being the start bit and the following 7 bits being the op-code. Data can be one or two bytes long depending on the instruction and the memory array organization. By the same token each address is one or two bytes long depending on the organization of the memory array. In this protocol, the transmission of the MSB is always first and the LSB last. The CS (Chip Select) of the CAT35C704 may be used to frame the data transmission packet or it may be set HIGH for the entire duration of operation. If an error in op-code or parity (if enabled) has been detected, the ERR output will be set LOW and the CAT35C704 will stop receiving and sending data until CS is toggled from HIGH to LOW to HIGH again. Alternatively, an error condition may be detected by interrogating the device for

a status word. If an error condition has been detected, DO (Data Output) will not respond. DO may be programmed to become tri-stated or to output a READY/BUSY status flag during write/erase cycles (see ENBSY instruction).

STATUS REGISTER

An eight bit status register is provided to allow the user to determine the status of the CAT35C704. The contents of the first three bits of the register are 101 which allows the user to quickly determine the condition of the device. The next three bits indicate the status of the device; they are instruction error, parity error and ready/busy status. The last two bits are reserved for future use.

ERASE ALL AND WRITE ALL

As a precaution, the ERAL instruction has to be entered twice before it is executed. This measure is required as a redundancy check on the incoming instruction for possible transmission errors. The WRAL instruction requires sending an ERAL first (this sets a flag only) and then the WRAL instruction. The CAT35C704 will accept the following commands:

ERAL	**ERAL**	An ERAL will be executed
ERAL	**WRAL**	A WRAL will be executed

Both the ERAL and WRAL commands will erase or write to the entire array and will not be blocked by the memory pointer.

THE PARITY BIT

The SECS protocol supports an even parity bit if the PE pin of the device is set HIGH, otherwise, there is no parity. If PE is set LOW and the incoming instruction contains a parity bit, it may be interpreted as the start bit of the next instruction. When PE is HIGH, the CAT35C704 expects a parity bit at the end of every incoming instruction packet. For example, the RSEQ instruction will look like this :

1100 1011
A15.....A8
A7.....A0 P

The device then outputs data continuously until it reaches the end of the memory. The last byte of data contains 9 bits. The ninth bit is the parity bit calculated over the entire transmitted data packet. The RSEQ instruction may be terminated at any time by bringing CS low; the output will then go to high impedance.

SYSTEM ERRORS

Whenever an error occurs, be it an instruction error (unknown instruction), or parity error (perhaps caused by transmission error), the device will stop its operation. To return to normal operation, the device must be reset by pulsing CS LOW and then set back to HIGH. Resetting the device will not affect the ENAC, EWEN and ENBSY status. The error may be determined by entering the READ STATUS REGISTER (RSR) instruction immediatly following the reset. The status output is an 8-bit word with the first three bits being 101. This three bit pattern indicates that the device is functioning normally. The fourth bit is "1" if an instruction error occurred. The fifth bit is a "1" if a parity error occurred. The sixth bit is a "1" if the device is in a WRITE/ERASE cycle. The last two bits are reserved for future use.

The reason for the "101" pattern is to distinguish between an error conditon (DO tri-stated) and a device busy status. If an error condition exists, it will not respond to any input instruction from DI. However, if the device is in a WRITE/ERASE cycle, it responds to the RSR instruction by outputting "101 00100". If RSR is executed at the end of a WRITE/ERASE cycle, the output will be "101000 00".

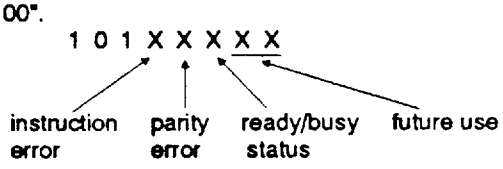


Figure 3 <READ TIMING>

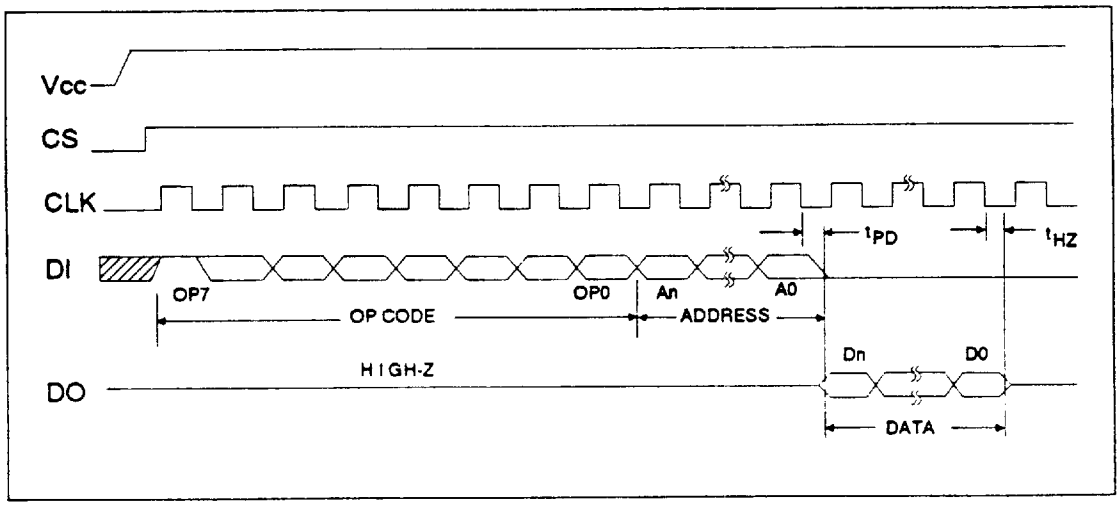


Figure 4 <WRITE TIMING>

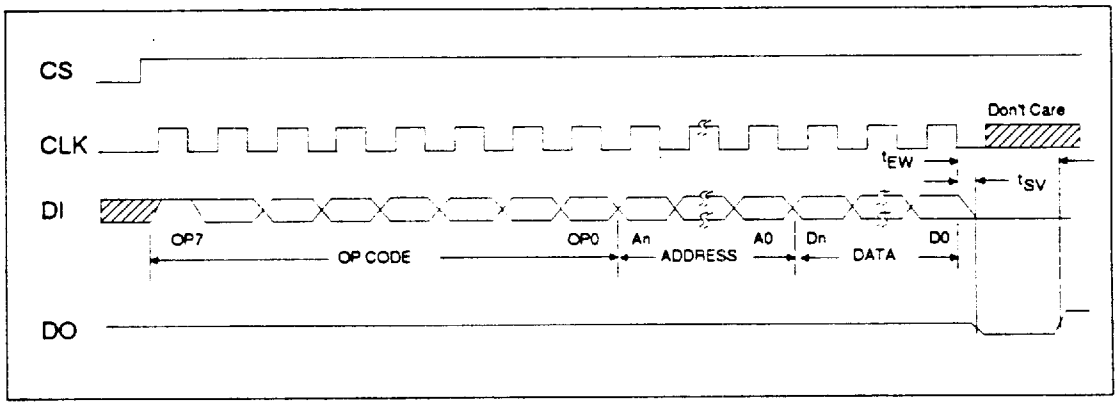


Figure 5 <EWEN/EWDS TIMING>

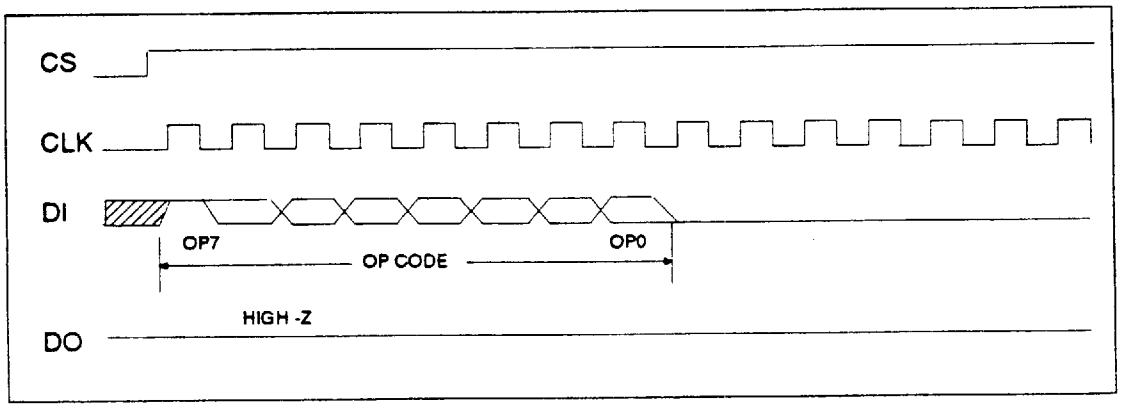


Figure 6 <ERASE TIMING>

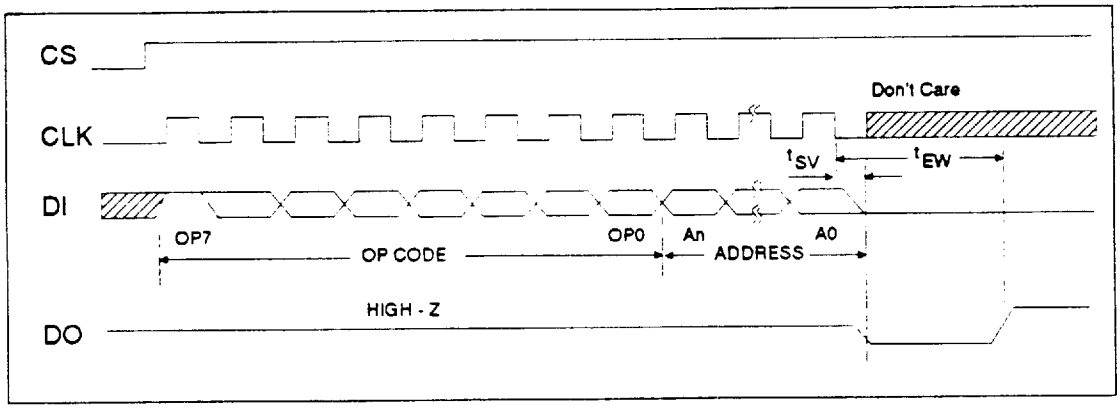


Figure 7 <ERAL TIMING>

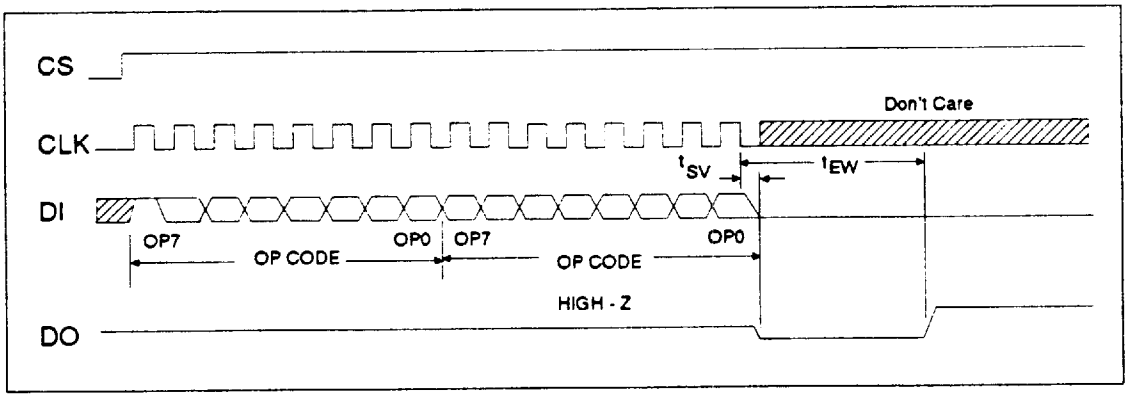


Figure 8 <WRAL TIMING>

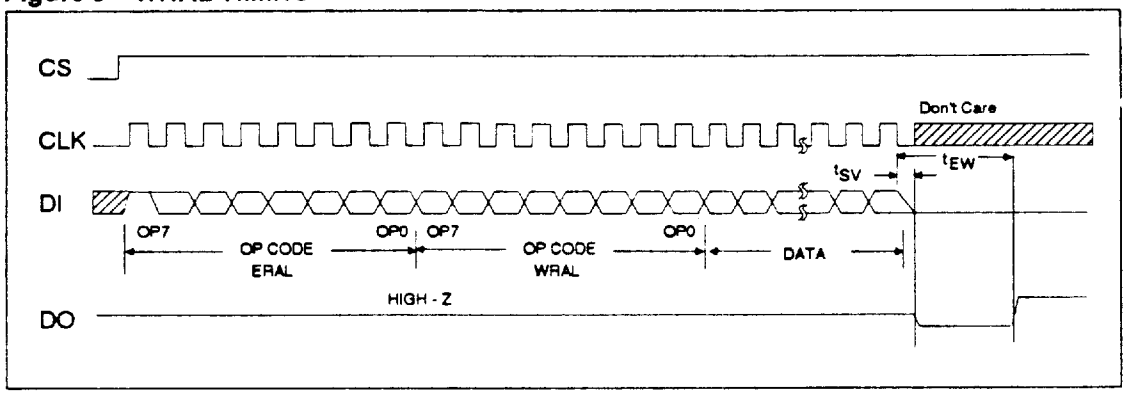
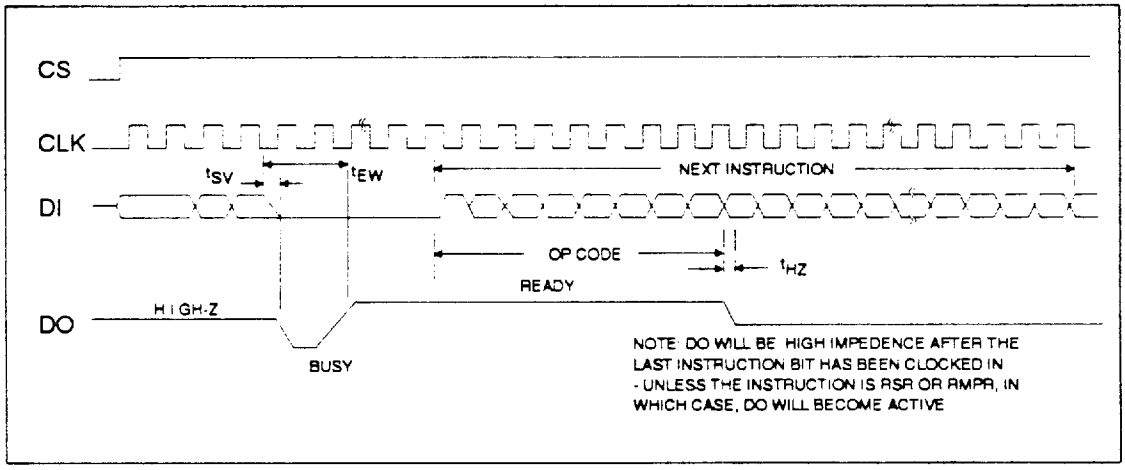


Figure 9 <WRITE TIMING>



INSTRUCTION SET:

DISAC Disable Access

1000	1000

In the protected mode this instruction inhibits all write/erase operations, and reads below memory pointer, regardless of the contents of the memory pointer. A write is accomplished by entering the ENAC instruction and a valid access code. In the unprotected mode this is the same as executing a NOP instruction.

ENAC Enable Access

1100	0101	[Access Code]

In the protected mode, this instruction, followed by a valid access code, unlocks the device for read/write/erase access.

WMPR Write Memory Pointer Register

1100	0100	[A15-A8] [A7-A0] *(x8)*

The WMPR instruction followed by 8 or 16 bits of address (depending on organization) will move the pointer to the newly specified address.

MACC Modify Access Code

1101	length	[Old code][New code] [New code]

This instruction requires the user to enter the length of the password in bytes, the old access code, if one was set previously, followed by the new access code and a re-entry of the new access code for verification. The length may be specified as follows:

[0] = No access code. Set device to unprotected mode.
[1-8] = Length of access code is 1 to 8 bytes.
[>8] = Illegal number of bytes. This causes an instruction error.

RMPR Read Memory Pointer Register

1100	1010

Output the content of the memory pointer register to the serial output port.

OVMPR Override Memory Pointer Register

1000	0011

Override the memory protection for the next multi-byte instruction. This allows the user to uncover memory protected area for a one-time write operation.

READ Read Memory

1100	1001	[A15-A8] [A7-A0] *(x8)*

Output the contents of the addressed memory location to the serial port.

WRITE Write Memory

1100	0001	[A15-A8] [A7-A0] [D7-D0] *(x8)*

This instruction writes the 8 or 16 bit data to the addressed memory location. After the instruction, address, and data have been entered, the self-timed WRITE sequence will start. The addressed memory location will be erased before data is written. The DO pin may be used to output the RDY/BUSY status by having previously entered the ENBSY instruction. During the write cycle, DO will output a LOW for BUSY, and once the cycle is completed a HIGH for READY.

ERASE Erase Memory

1100	0000	[A15-A8] [A7-A0] *(x8)*

Erase data in the specified memory location (set memory to "1"). After the instruction and the address have been entered, the self-timed erase sequence will start. The DO pin may be used to

output the READY/BUSY status by having previously entered the ENSBY instruction. During the erase cycle, DO will output a LOW for BUSY, and once the cycle has been completed, a HIGH for READY.

ERAL Erase All

1000	1001	1000	1001

Erase the data of all memory locations (all cells can be set to "1"). For protection against inadvertent chip erase, the ERAL instruction is required to be entered twice.

WRAL Write All

1000	1001	1100	0011

[D15-D7] [D7-D0] *(x16)*

Write one or two bytes of data to all memory locations. An ERAL will be automatically performed before the WRAL is executed. For protection from inadvertent overwriting of data, the ERAL instruction is required to be entered preceding the WRAL instruction.

RSEQ Read Sequential

1100	1011

[A15-A8] [A7-A0] *(x8)*

Read memory starting from the specified address sequentially to the highest address or until CS goes LOW. The instruction is terminated when CS goes LOW.

ENBSY Enable Busy

1000	0100

Enable the status indicator on DO during write/erase cycle. DO goes LOW then HIGH once the write cycle is complete. DO will go to HIGH-Z at the end of the next op code transmission. The device powers up in the disable busy state.

DISBSY Disable Busy

1000	0101

Disable the status indicator on DO during write/erase cycle.

EWEN Erase/Write Enable

1000	0001

Enable write/erase to be performed on non-protected portion of memory. This instruction must be entered before any write/erase instruction will be carried out. Once entered, it remains valid until power-down or an EWDS is executed.

EWDS Erase/Write disable

1000	0010

Disable all erase and write functions.

ORG Select Memory Organization

1000	011R

[R = 0 or 1]

Set memory organization to 512 x 8 if R = 0, and to 256 x 16 if R = 1.

RSR Read Status Register

1100	1000

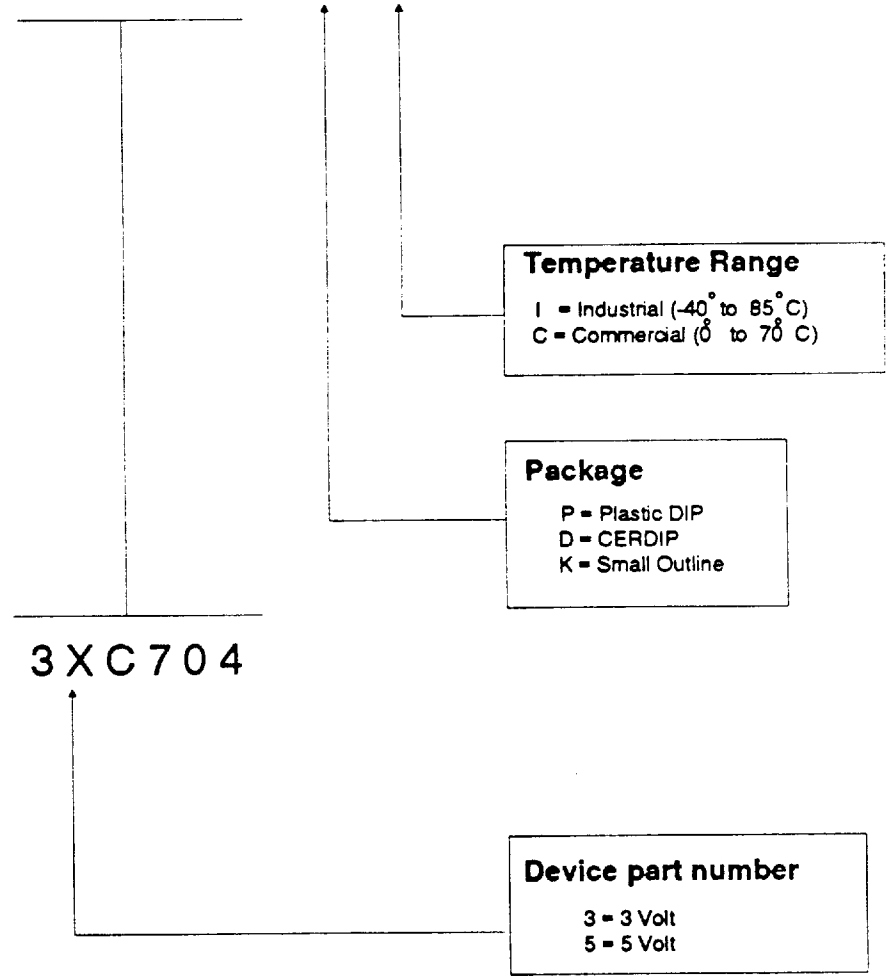
Outputs the contents of the 8-bit status register. The first three bits of the register are 101 allowing the user to quickly determine if the device is functioning properly. The next three bits indicate instruction error, parity error and ready/busy status.

NOP No Operation

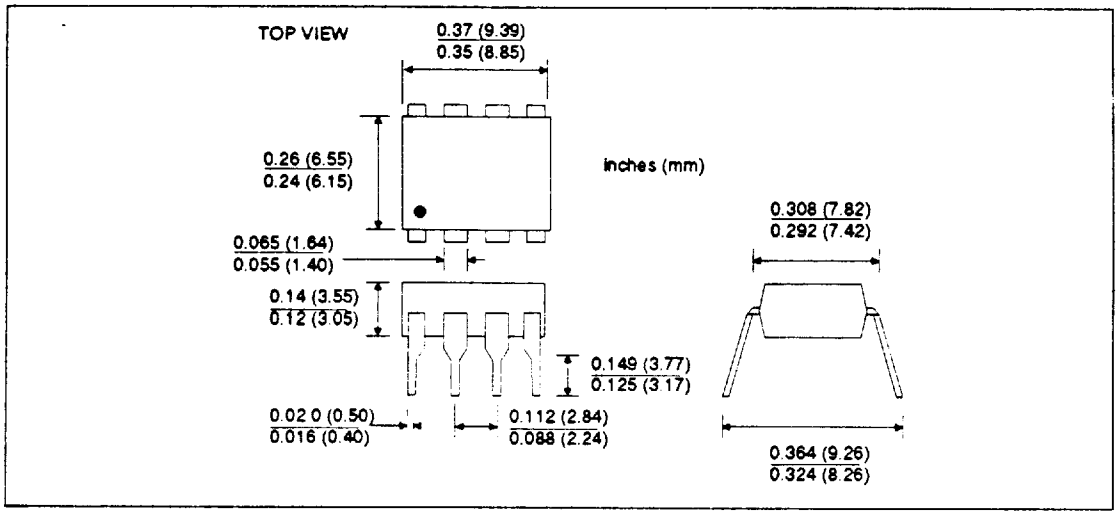
1000	0000

ORDERING INFORMATION

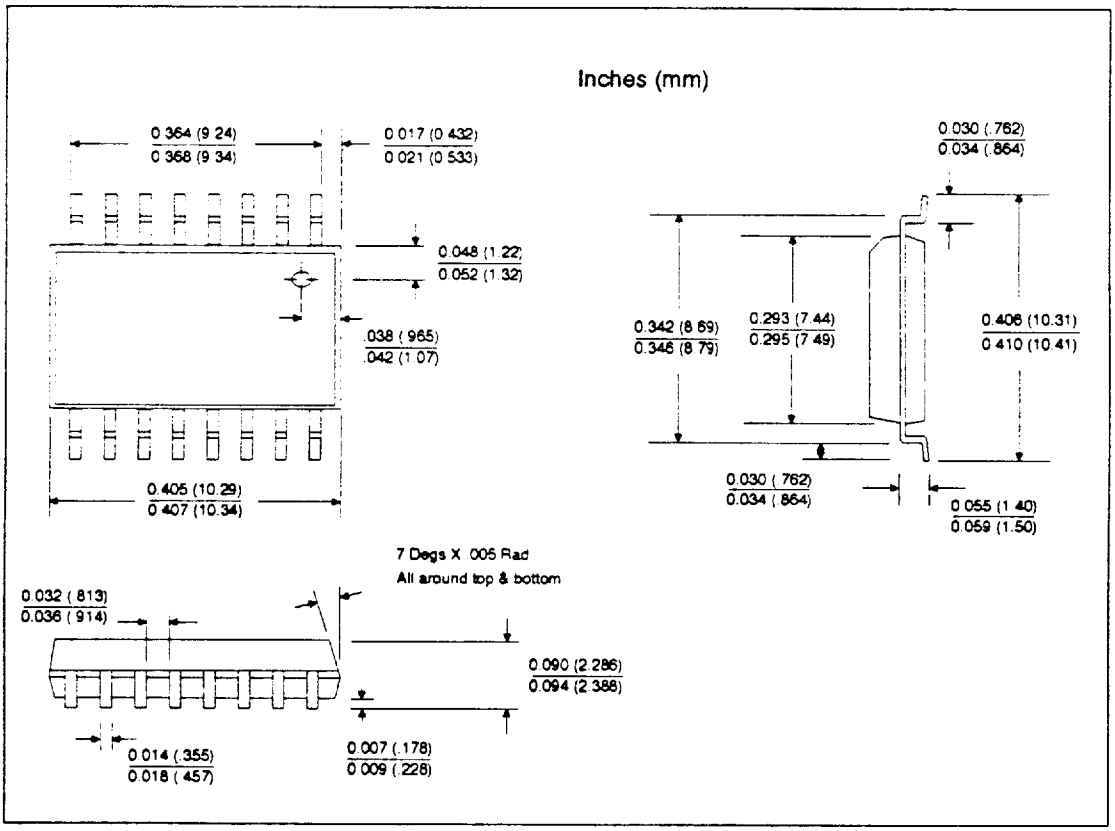
Prefix	Device #	Suffix
CAT	35C704	P I



8-PIN DIP



16-PIN SO



LIMITED WARRANTY

Devices sold by Catalyst Semiconductor, Inc. are covered by the warranty and patent indemnification provisions appearing in its Terms of Sale only. Catalyst Semiconductor, Inc. makes no warranty, express, statutory, implied, or by description, regarding the information set forth herein or regarding the freedom of the described devices from patent infringement. Catalyst Semiconductor, Inc. makes no warranty of merchantability or fitness for any purpose. Catalyst Semiconductor, Inc. reserves the right to discontinue production and change specifications and prices at any time and without notice. Catalyst Semiconductor, Inc. assumes no responsibility for the use of any circuitry other than circuitry embodied in a Catalyst Semiconductor, Inc. product. No other circuits, patents, licenses are implied.

LIFE RELATED POLICY

In situations where semiconductor component failure may endanger life, system designers using this product should design the system with appropriate error detection and correction, redundancy and back-up features to prevent such an occurrence.

Catalyst Semiconductor's products are not authorized for use as critical components in life support devices or systems.

Stock No. 100-066 8/91 TLY