POLITECNICO DI TORINO

ESAMI DI STATO PER L'ABILITAZIONE ALLA PROFESSIONE DI INGEGNERE
I SESSIONE – ANNO 1999

Ramo: Elettronica TEMA N. 2

Occorre realizzare un lettore di tessere elettroniche da utilizzarsi in punti di vendita e per servizi a pagamento. Le tessere date agli utenti contengono un microchip con memoria non volatile, in cui risiederanno i dati di identificazione, il conto in denaro a scalare ed i campi di protezione. Le caratteristiche del microchip della tessera sono in allegato.
Il sistema realizzato deve unicamente consentire operazioni di accredito e di spesa, mentre deve risultare sicuro e robusto contro tutte le altre possibili manovre.
Il lettore deve essere corredato di un display alfanumerico a cristalli liquidi, di una tastiera e di un avvisatore acustico. Il sistema viene attivato dalla semplice inserzione della tessera. Il sistema prevede un collegamento seriale con un calcolatore remoto per il trasferimento delle transazioni. Il lettore deve presentare consumi e costi contenuti.

Passi richiesti per il progetto:

1- Definire lo schema a blocchi dell'intero sistema, indicando per ciascun blocco le specifiche (funzionalità che deve svolgere, i segnali di interconnessione, il loro tipo, la codifica, l'eventuale dinamica, parallelismo ...).
2- Per ciascun blocco individuare il tipo di realizzazione ritenuta più conveniente, indicare i componenti idonei, quali processori, logiche programmabili, circuiti analogici, ... che si intendono impiegare.
3- Procedere alla progettazione (schemi elettrici), qualora si usino ASIC, FPGA, PLD riportare le loro funzionalità interne (o con schemi elettrici o con descrizioni VHDL), se il blocco è basato su microprocessore indicare le funzionalità software svolte mediante flow-chart delle procedure, riportando brani di codice in linguaggio C o equivalente.
4- Progettare il modulo per l'alimentazione della tessera. Il modulo deve prevedre un controllo dell'accensione/spegnimento del chip sulla tessera, la verifica dell'assorbimento, la protezione da cortocircuiti, e da extratensioni.
5- Svolgere una analisi del comportamento ai guasti del lettore progettato. In particolare prevedere circuiti o codice per sopperire alle seguenti situazioni:
   - mancanza di alimentazione totale o temporanea durante la transazione
   - tessera inserita erroneamente, o di altro fornitore, o falsa.
   - oggetto che pone in cortocircuito i contatti, ovvero inietta disturbi elettrici
   - estrazione della tessera durante la transazione
   - interruzione, disturbi, inserimenti sul canale seriale.

Preliminary

CAT35C704

4K-Bit Secure Access Serial E²PROM

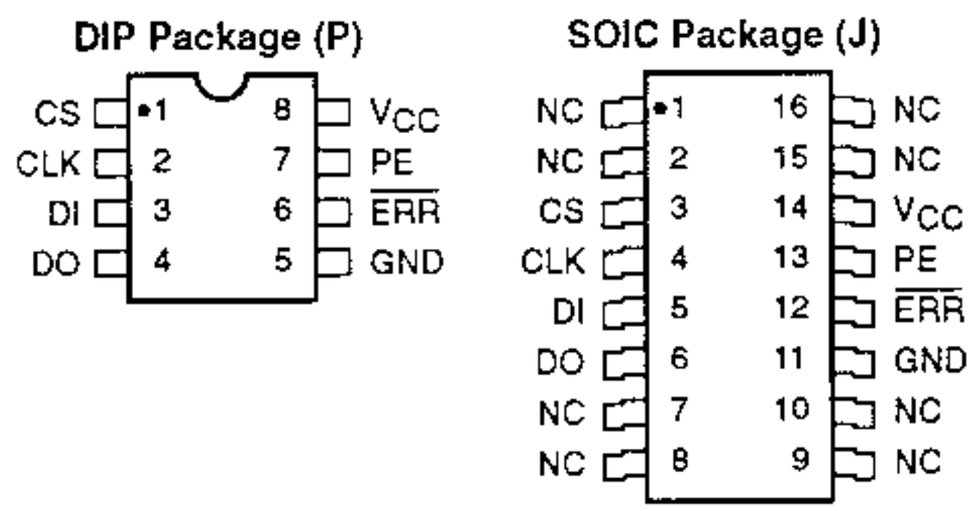
FEATURES

- Single 5V Supply
- Password READ/WRITE Protection: 1 to 8 Bytes
- Memory Pointer WRITE Protection
- Sequential READ Operation
- 256 x16 or 512 x 8 Selectable Serial Memory
- High Speed Synchronous Protocol
- Commercial, Industrial and Automotive Temperature Ranges
- Operating Frequency: DC–3MHz
- Low Power Consumption:
  –Active: 3 mA
  –Standby: 250 µA
- 100,000 Program/Erase Cycles
- 100 Year Data Retention

DESCRIPTION

The CAT35C704 is a 4K-bit Serial E²PROM that safeguards stored data from unauthorized access by use of a user selectable (1 to 8 byte) access code and a movable memory pointer. Two operating modes provide unprotected and password-protected operation allowing the user to configure the device as anything from a ROM to a fully protected no-access memory. The CAT35C704 uses a unique serial-byte synchronous communication protocol and has a Sequential Read feature where data can be sequentially clocked out of the memory array. The device is available in 8-pin DIP or 16-pin SOIC packages.

PIN CONFIGURATION



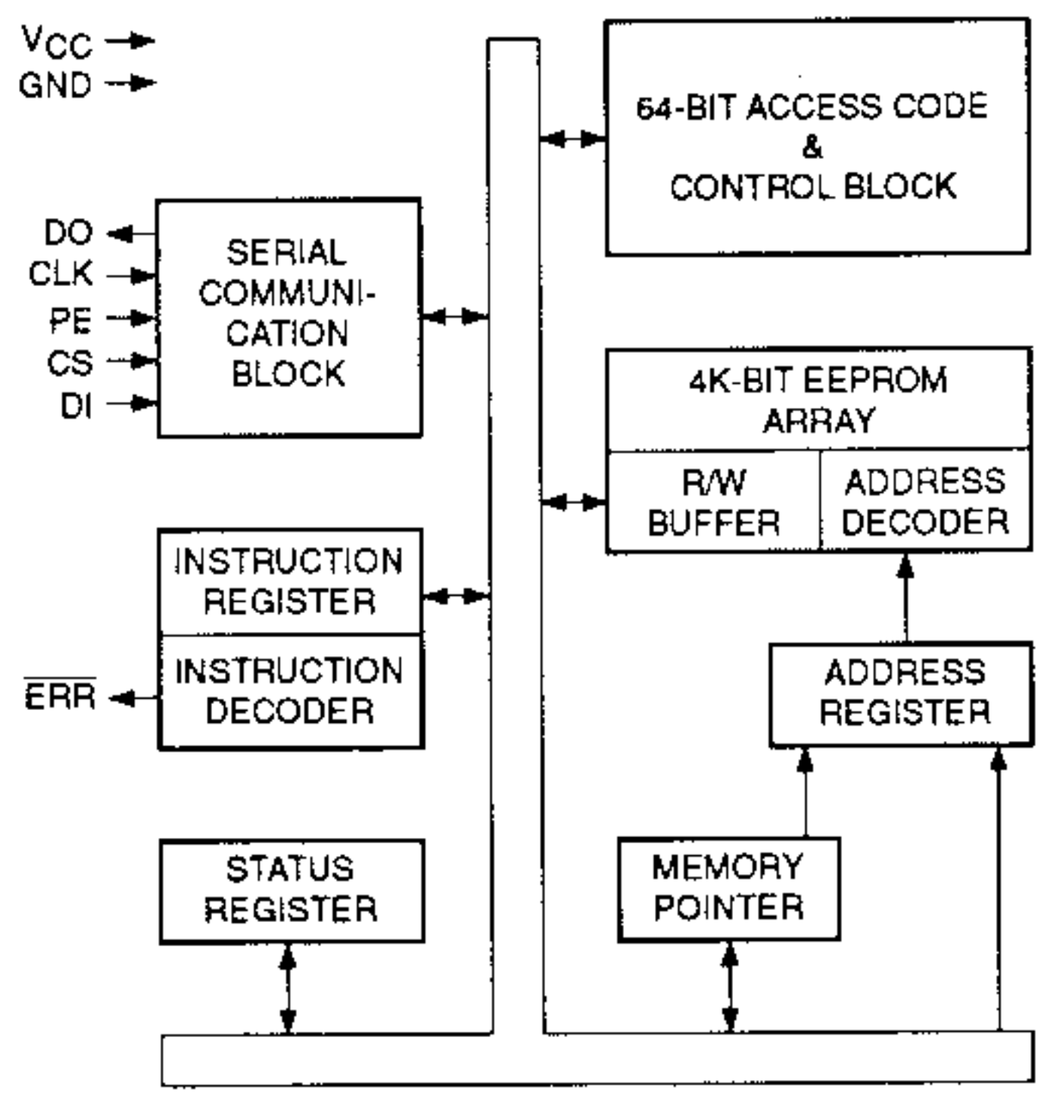
5074 FHD F01

PIN FUNCTIONS

Pin Name	Function
CS	Chip Select
DO(1)	Serial Data Output
CLK	Clock Input
DI(1)	Serial Data Input
PE	Parity Enable
$\overline{ERR}$	Error Indication Pin
Vcc	+5V Power Supply
GND	Ground

Note:
(1) DI, DO may be tied together to form a common I/O.

BLOCK DIAGRAM



35C704 F02

ABSOLUTE MAXIMUM RATINGS*

Temperature Under Bias ..... –55°C to +125°C

Storage Temperature ..... –65°C to +150°C

Voltage on Any Pin with
Respect to Ground[1] ..... –2.0V to +V_{CC} + 2.0V

V_{CC} with Respect to Ground ..... –2.0V to +7.0V

Package Power Dissipation
Capability (T_a = 25°C) 1.0W

Lead Soldering Temperature (10 secs) ..... 300°C

Output Short Circuit Current[2] 100mA

*COMMENT

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

RELIABILITY CHARACTERISTICS

Symbol	Parameter	Min.	Max.	Units	Reference Test Method
N_{END}[3]	Endurance	100,000		Cycles/Byte	MIL-STD-883, Test Method 1033
T_{DR}[3]	Data Retention	100		Years	MIL-STD-883, Test Method 1008
V_{ZAP}[3]	ESD Susceptability	2000		Volts	MIL-STD-883, Test Method 3015
I_{LTH}[3][4]	Latch-up	100		mA	JEDEC Standard 17

D.C. CHARACTERISTICS

V_{CC} = +5V ±10%,unless otherwise specified.

Symbol	Parameter	Limits			Units	Test Conditions
		Min.	Typ.	Max.		
I_{CC}	Power Supply Current (Operating)			3	mA	V_{CC} = 5.5V, CS = V_{CC} DO is Unloaded.
I_{SB}	Power Supply Current (Standby)			250	µA	V_{CC} = 5.5V, CS = 0V DI = 0V, CLK = 0V
V_{IL}	Input Low Voltage	–0.1		0.8	V	
V_{IH}	Input High Voltage	2			V	
V_{OL}	Output Low Voltage			0.4	V	I_{OL} = 2.1mA
V_{OH}	Output High Voltage	2.4			V	I_{OH} = –400µA
I_{LI}[5]	Input Leakage Current			2	µA	V_{IN} = 5.5V
I_{LO}	Output Leakage Current			10	µA	V_{OUT} = 5.5V, CS = 0V

Note:
(1) The minimum DC input voltage is –0.5V. During transitions, inputs may undershoot to –2.0V for periods of less than 20 ns. Maximum DC voltage on output pins is V_{CC} +0.5V, which may overshoot to V_{CC} + 2.0V for periods of less than 20ns.
(2) Output shorted for no more than one second. No more than one output shorted at a time.
(3) This parameter is tested initially and after a design or process change that affects the parameter.
(4) Latch-up protection is provided for stresses up to 100 mA on address and data pins from –1V to V_{CC} +1V.
(5) PE pin test conditions: $V_{IH} < V_{IN} < V_{IL}$

A.C. CHARACTERISTICS

V_{CC} = +5V ±10%,unless otherwise specified.

Symbol	Parameter	Limits			Units	Test Conditions
		Min.	Typ.	Max.		
t_{CSS}	CS Setup Time	150			ns	C_L = 100pF V_{IN} = V_{IH} or V_{IL} V_{OUT} = V_{OH} or V_{OL}
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}(1) (2)	CLK to DO High-Z Delay			50	ns	
t_{EW}	Program/Erase Pulse Width			12	ms	
t_{CSL}	CS Low Pulse Width	200			ns	
t_{CKH}	CLK High Pulse Width	165			ns	
t_{CKL}	CLK Low Pulse Width	100			ns	
t_{SV}	$\overline{ERR}$ Output Delay			150	ns	C_L = 100pF
t_{VCCS}(1)	V_{CC} to CS Setup Time	5			µs	C_L = 100pF
t_{CSZ}(1)	CS to DO High-Z Delay			50	ns	
t_{CSD}	CS to DO Busy Delay			150	ns	
f_{CLK}	Clock Frequency	DC		3	MHz	

Note:
(1) This parameter is tested initially and after a design or process change that affects the parameter.
(2) t_{HZ} is measured from the falling edge of the clock to the time when the output is no longer driven.

PASSWORD PROTECTION

The CAT35C704 is a 4K-bit E²PROM 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 2 illlustrates this partitioning of the memory array.

WRITE PROTECTION

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 3 illustrates this partitioning of the memory array.

Figure 1. A.C. Timing

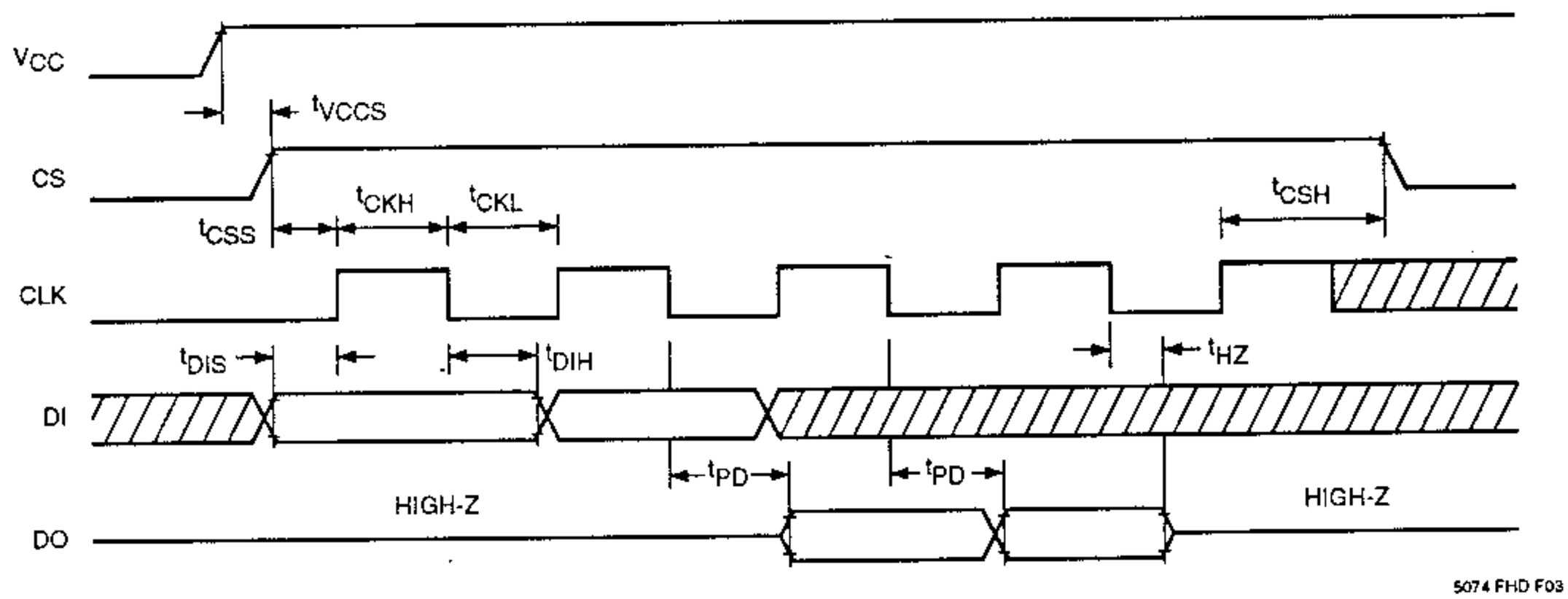
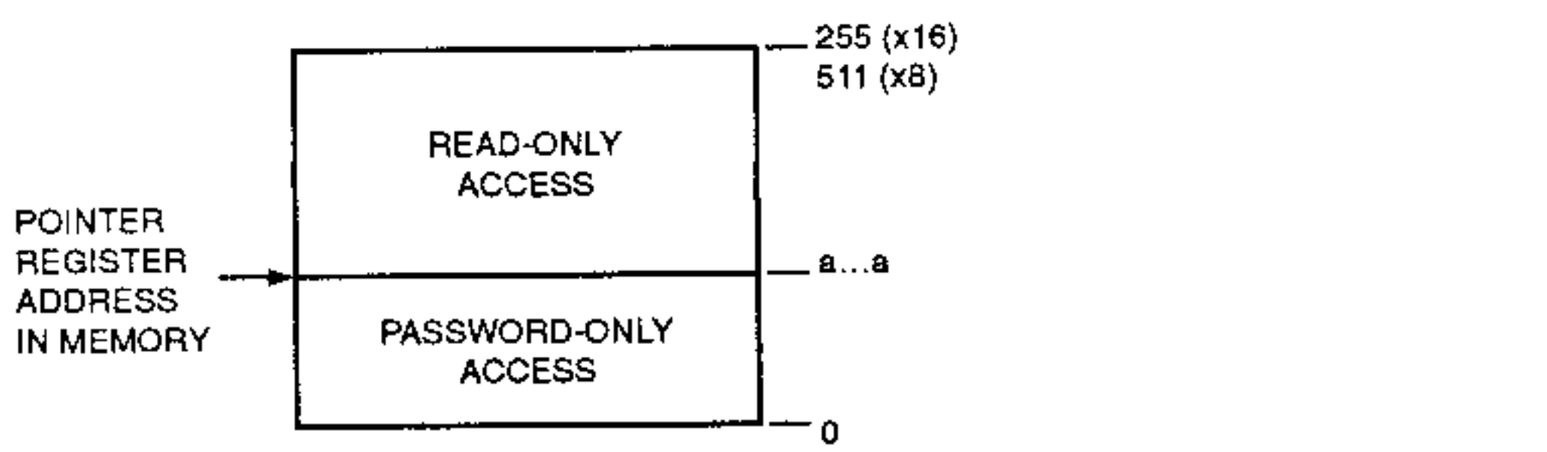


Figure 2. Secure Mode



READ SEQUENTIAL

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.

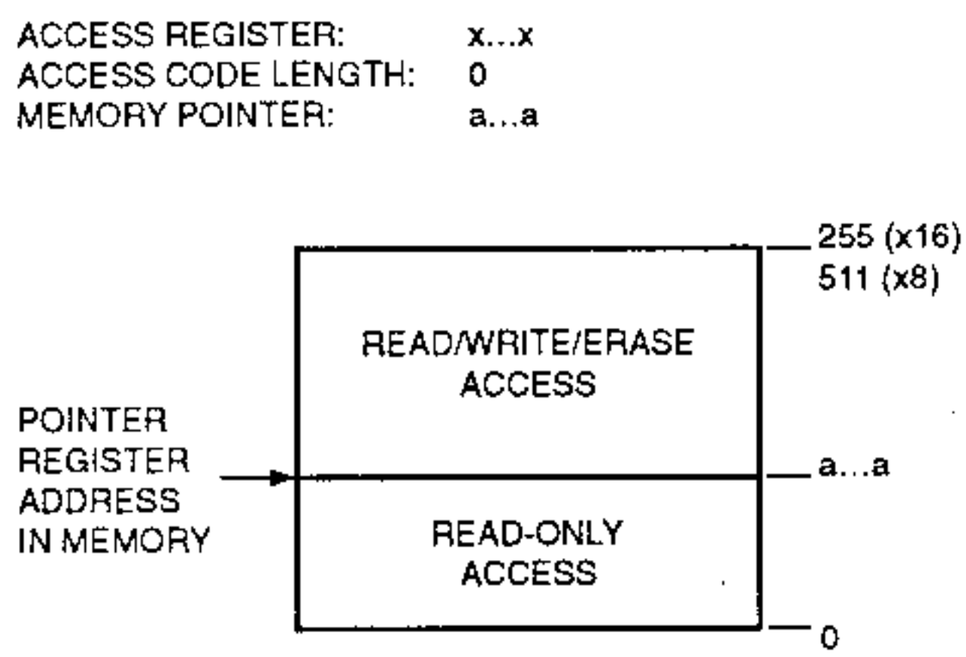
The CAT35C704 communicates with external devices via a synchronous serial communication protocol (SECS) that has a maximum transmission rate of 3 MHz. The data transmission may be a continuous stream of data or it can be packed by pulsing Chip Select LOW in between each packet of information. (Except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

PIN DESCRIPTIONS

CS

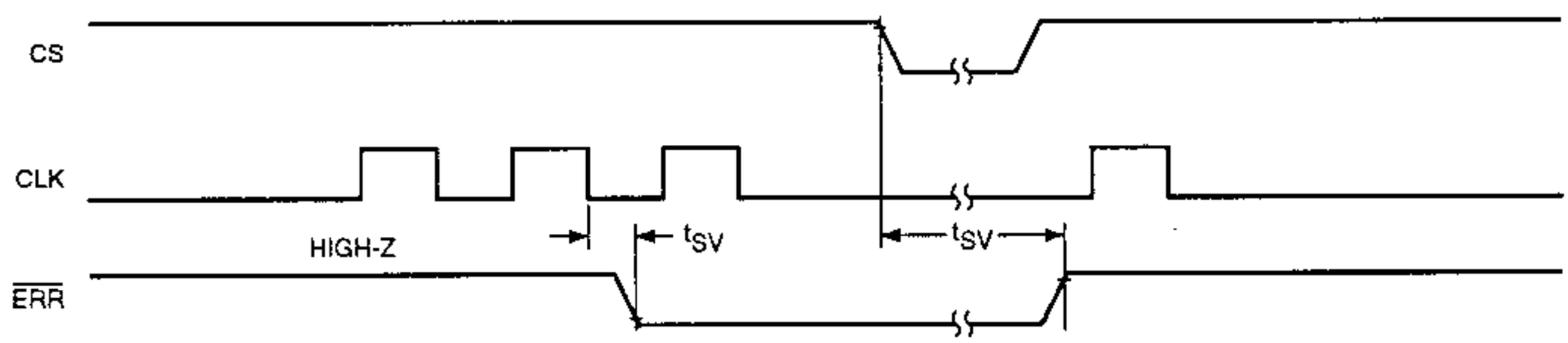
Chip Select is a TTL compatible input which, when set HIGH, allows normal operation of the device. Any time Chip Select is set LOW, it resets the device, terminating all I/O communication, and puts the output in a high impedance state. CS is used to reset the device if an error condition exists or to 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 program/erase or the access-enable status, nor does it terminate a programming cycle once it has started. The program/erase and access-enable operations, once enabled, will remain enabled until specific disabling instructions are sent or until power is removed.

Figure 3. Unprotected Mode(1)



5074 FHD F05

Figure 4. $\overline{ERR}$ Pin Timing



5074 FHD F06

Note:
(1) x = DON'T CARE; a = ADDRESS BIT.

Stock No. 21010-02 2/98

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.

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 program/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 program/erase cycle is completed. DO will stay HIGH until the completion of the next instruction's opcode and, if the next instruction is a READ, DO will output the appropriate data at the end of the instruction. If the ENABLE BUSY instruction has not been previously executed, DO will stay in a high impedance state. DO will

Figure 5. Program/Erase Timing

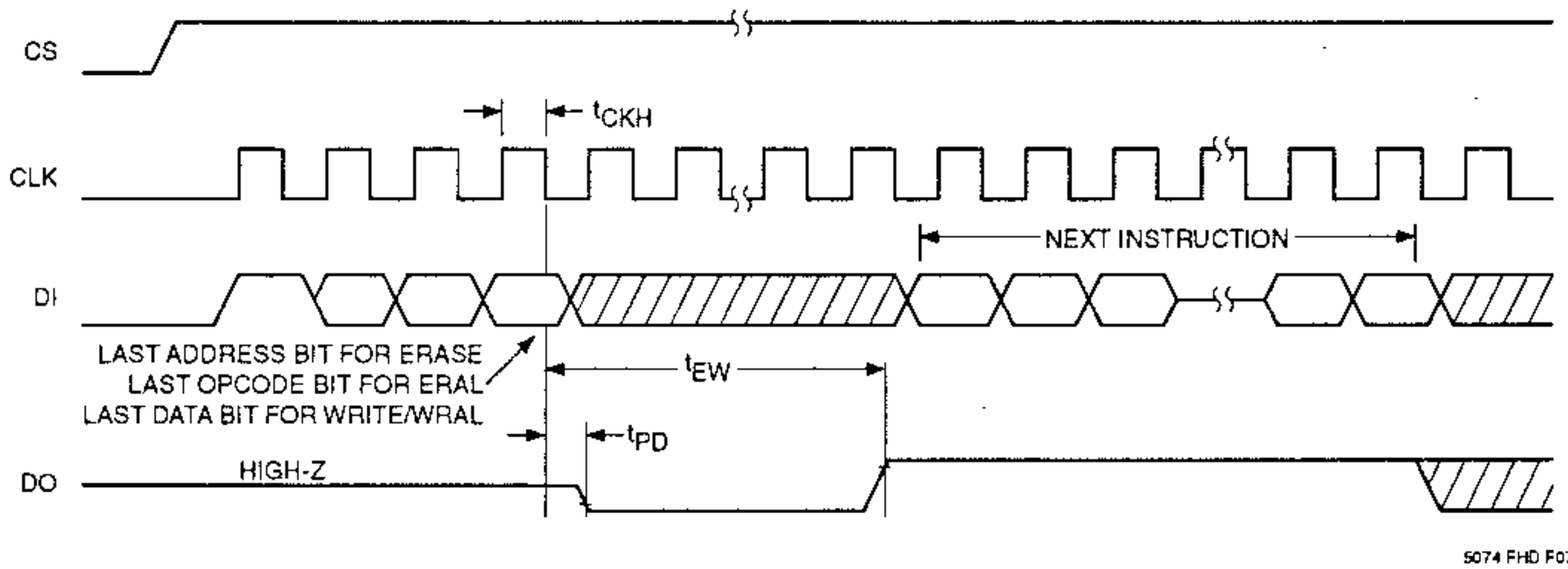
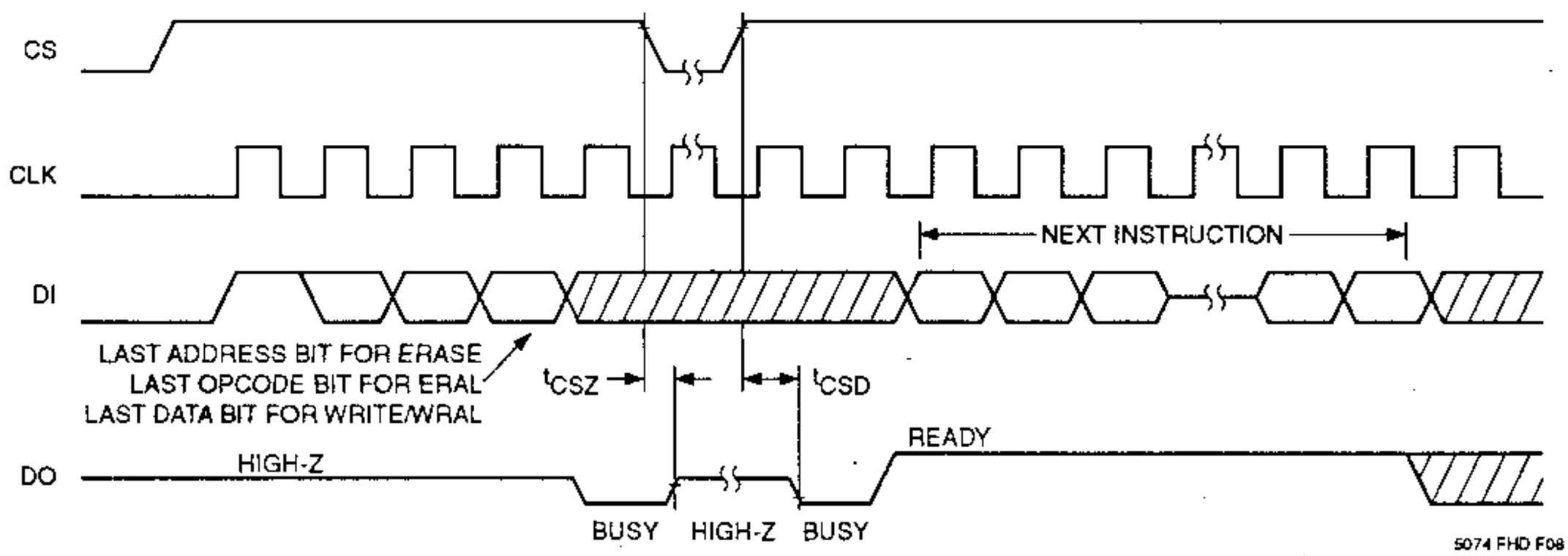


Figure 6. CS to DO Status Timing



also go to the high impedance state if an error condition is detected. If the ENABLE BUSY instruction has not been executed, to determine whether the device is in a program/erase cycle or in an error condition, a READ STATUS instruction may be entered. When the device is in a program/erase cycle it will output an 8-bit status word. If it does not, it is in an error condition.

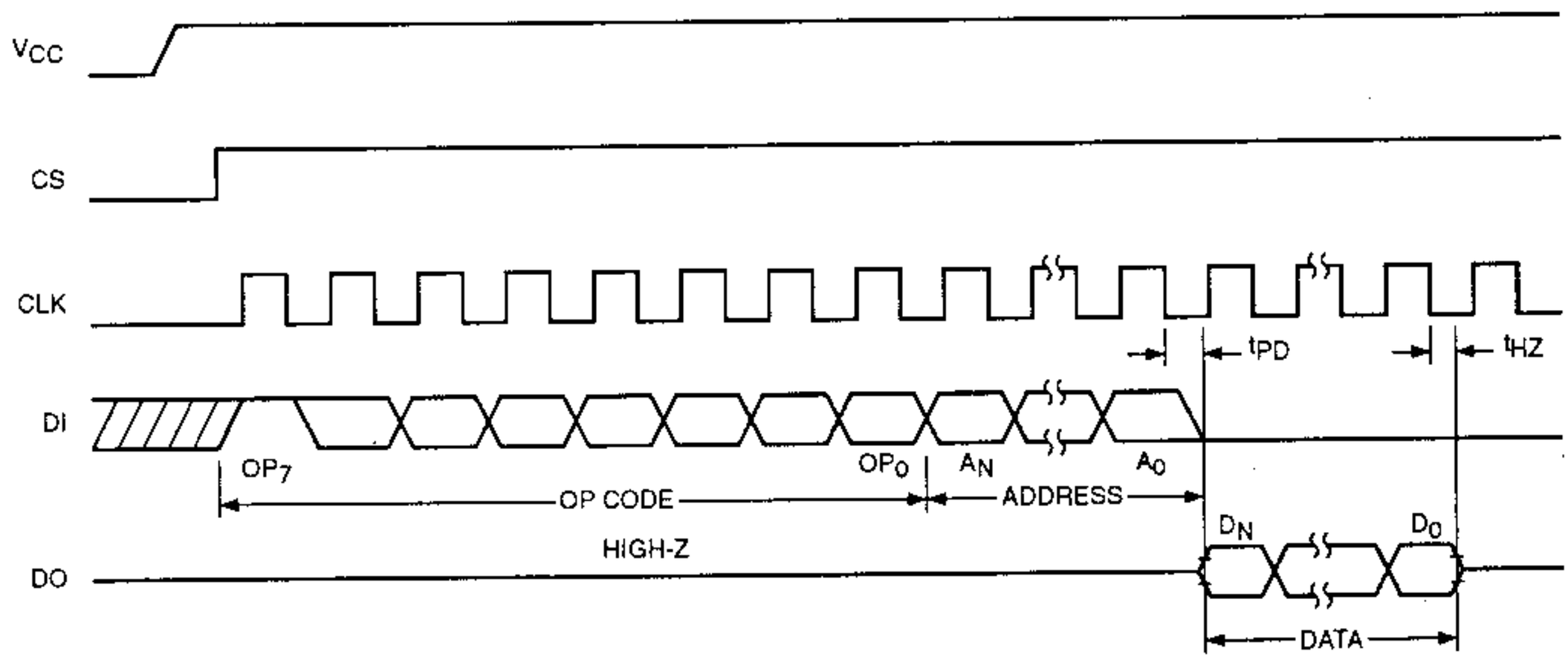
PE

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.

$\overline{ERR}$

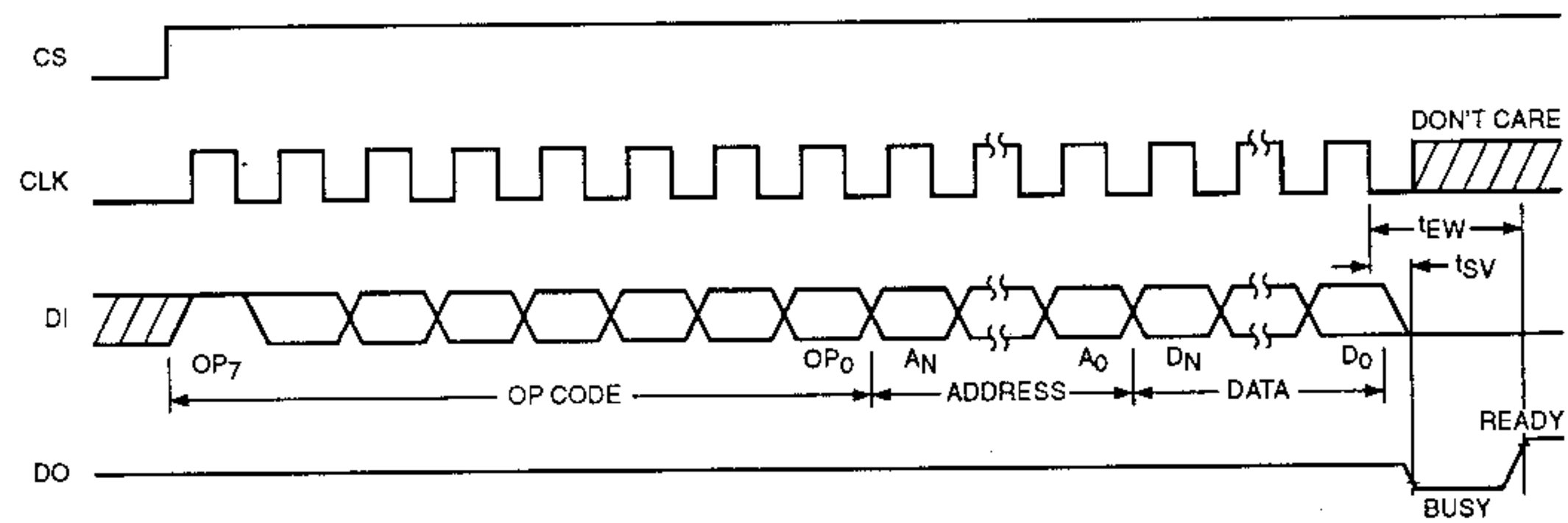
The Error indication pin is an open drain output. If either an instruction or parity error exists, the ERR pin will output a "0" until the device is reset. This can be done by pulsing CS LOW.

Figure 7. Read Timing



5074 FHD F10

Figure 8. Write Timing



5074 FHD F11

Stock No. 21010-02 2/98