Interfacing the PCM16C00 with Serial EEPROMs: Methodology and Data Security

National Semiconductor
Application Note 970
Jon Fluker
October 1994

Note: This application note uses the following notation convention: hexadecimal numbers are represented with the prefix ''0x''; numbers with no prefix are decimal.

OVERVIEW

The PCMCIA standard requires, for basic compatibility, that each PCMCIA card contain a small Card information Structure (CIS), which starts at offset 0 of the card's Attribute Memory space. At a minimum, this structure contains basic information about the card's capabilities and capacities (size, speed, etc.). Ideally, this CIS data should be stored in non-volatile memory to prevent corruption. Other critical information, for example an Ethernet node ID on a LAN card, might also be stored in non-volatile memory on the card. Security of this sort of data is of highest importance; any corruption of this data may render the card useless. However, field-programmability of the CIS and other configuration data must be considered.

The PCM16C00 interfaces directly to serial EEPROMs of two different sizes: 512k bytes and 2k bytes (4k bits and 16k bits respectively), which conform to the MICROWIRE™ protocol. Examples of these devices are the National Semiconductor NM93C66 and NM93C86 4k bit and 16k bit MICROWIRE serial EEPROMs. The PCM16C00 includes all the necessary pins to interface cleanly to these devices.

Note: The initial version of the PCM16C00 operates in both read and write modes with the 16k bit EEPROM only. The PCM16C00 reads, but cannot write the 4k bit EEPROM. This is due to a subtle difference in the WRITE operation for the two devices. Therefore, it is recommended that the 16k bit EEPROM (NM93C86) be used for card designs which will program the EEPROM after assembly, using the PCM16C00, and the 4k bit EEPROM (NM93C66) be used *only* on cards which will have the EEPROM written prior to assembly. If an EEPROM write sequence is initiated on a card using the 4k bit EEPROM, the RDY/BSY pin on the PCMCIA socket will be held low indefinitely.

PCM16C00 ARCHITECTURE

The PCM16C00 contains 2k bytes of SRAM which ''shadows'' the data stored in the serial EEPROM. At card insertion, or after a system reset, the PCM16C00 will automatically load the contents of the serial EEPROM into its internal SRAM. The use of fast internal SRAM minimizes system latency for attribute memory accesses. The PCM16C00 also has the ability to write the data stored in its internal SRAM and specific registers (in Attribute Memory locations 0x000 through 0xFFE, on even-byte boundaries) back to the EEPROM. This allows card manufacturers to ''burn'' the CIS into their cards after assembly and to accommodate CIS upgrades for the end user.

The Attribute Memory space in the PCM16C00 is broken into five segments: the range from 0x0000 through 0x03E2 is SRAM which is intended for CIS storage. The range from 0x03E4 through 0x03FE is intended for PCM16C00 specific registers (only 0x3E4 through 0x3F6 are implemented in PCM16C00, 0x3F8 through 0x3FE are reserved for future use—''RFU''). These two segments cover 512 bytes. The third segment of Attribute Memory is 1.5k bytes of SRAM from 0x0400 through 0x0FFE. The fourth segment of the Attribute Memory space includes the PCM16C00-specific ID and EEPROM Control Registers and several RFU registers located from 0x1000 through 0x101E. The fifth segment includes all of the PCMCIA standard-compliant Configuration Registers in locations 0x1020 through 0x105E. The PCM16C00 will decode any Attribute Memory accesses above 0x105E, and assert the $\overline{\text{EARD}}$ pin, allowing a card designer to use external Attribute Memory if needed. Refer to Table I for a detailed Attribute Memory map of the PCM16C00, and to the PCM16C00 datasheet for register specifics.

In a card design using a 512 byte EEPROM, only the first two segments of Attribute Memory will be stored in non-volatile memory upon an EEPROM write event. With a 2k byte EEPROM, the first three segments will be stored. The other segments, including EEPROM Control Register and PCMCIA Configuration Registers are dynamically configured by the host after card insertion and interpretation of the CIS data by Card Services.

The PCM16C00's EEPROM control circuitry directly interfaces to 4k bit and 16k bit serial EEPROMs, organized as 8 or 16 bits, which conform to the MICROWIRE protocol. The PCM16C00 EEPROM interface is configured via the EESIZE and EEORG inputs. The EESIZE input is set high for 16k bit EEPROMs, low for 4k bit EEPROMs. The EEORG input is set high for 16-bit-organized EEPROMs, low for 8-bit organized EEPROMs. Both EESIZE and EEORG have internal 100 kΩ pullup resistors, and so may be left floating if the EEPROM used is 16k bit size organized into 16-bit words. Refer to Table II.

MICROWIRE™ is a trademark of National Semiconductor Corporation.

 TL/F/11684 RRD-B30M125/Printed in U. S. A.

TABLE I. PCM16C00 Attribute Memory Map

Register Description	Register Type	Address (Hex)	Stored in EEPROM
Card Information Storage	PCMCIA CIS	0x000–0x03E2	Yes
Pin Polarity Register	PCM16C00 Specific	0x03E4	Yes
PMGR and Clock Register	PCM16C00 Specific	0x03E6	Yes
CTERM 0 Register	PCM16C00 Specific	0x03E8	Yes
CTERM 1 Register	PCM16C00 Specific	0x03EA	Yes
Arbiter Priority Register	PCM16C00 Specific	0x03EC	Yes
Arbiter Latency Register	PCM16C00 Specific	0x03EE	Yes
Miscellaneous Register	PCM16C00 Specific	0x03F0	Yes
Digital Port Direction Register	PCM16C00 Specific	0x03F2	Yes
Digital Port Register	PCM16C00 Specific	0x03F4	Yes
Wait State Timer Register	PCM16C00 Specific	0x03F6	Yes
Reserved for Future Use Registers	PCM16C00 Specific	0x03F8–0x03FE	Yes
Card Information Storage	PCMCIA CIS	0x0400–0x0FFE	Optional
ID Register	PCM16C00 Specific	0x1000	No
EEPROM Control Register	PCM16C00 Specific	0x1002	No
Reserved for Future Use Registers	PCM16C00 Specific	0x1004–0x101E	No
Function 0 Configuration Option Register	PCMCIA	0x1020	No
Function 0 Configuration Status Register	PCMCIA	0x1022	No
Function 0 Pin Replacement Register	PCMCIA	0x1024	No
Unused	PCMCIA	0x1026	No
Function 0 I/O Event Register	PCMCIA	0x1028	No
Function 0 Base A Register	PCMCIA Extension	0x102A	No
Function 0 Base B Register	PCMCIA Extension	0x102C	No
Unused	PCMCIA Extension	0x102E–0x1030	No
Function 0 Limit Register	PCMCIA Extension	0x1032	No
Reserved for Future Use Registers	PCMCIA Extension	0x1034–0x103E	No
Function 1 Configuration Option Register	PCMCIA	0x1040	No
Function 1 Configuration Status Register	PCMCIA	0x1042	No
Function 1 Pin Replacement Register	PCMCIA	0x1044	No
Unused	PCMCIA	0x1046	No
Function 1 I/O Event Register	PCMCIA	0x1048	No
Function 1 Base A Register	PCMCIA Extension	0x104A	No
Function 1 Base B Register	PCMCIA Extension	0x104C	No
Unused	PCMCIA Extension	0x104E–0x1050	No
Function 1 Limit Register	PCMCIA Extension	0x1052	No
Reserved for Future Use Registers	PCMCIA Extension	0x1054–0x105E	No

TABLE II. PCM16C00 and EEPROM Compatibility Matrix

PCM16C00 Configuration: EESIZE	EEORG	EEPROM Device Supported	EEPROM Organization
0	0	NM93C66 or Equiv	512 x 8-bit
0	1	NM93C66 or Equiv	256 x 16-bit
1	0	NM93C86 or Equiv	2048 x 8-bit
1	1	NM93C86 or Equiv	1024 x 8-bit

The PCM16C00's internal SRAM is organized as 8 bits on even byte boundaries only. This conforms to the PCMCIA standard. If the EEPROM is organized as 16 bits, the PCM16C00 stores data in the SRAM in low/high format in consecutive byte locations. For example, if a 16-bit organized EEPROM is used on the card, the low byte at word 0 of the EEPROM will be shadowed in Attribute location 0x0000 and the high byte will be shadowed at location 0x0002. The low byte at word 1 of the EEPROM will be shadowed at Attribute location 0x0004, and the high byte at 0x0006, etc. For 8-bit organized EEPROMs, EEPROM byte 0 is shadowed at Attribute location 0x0000, EEPROM byte 1 is shadowed in Attribute location 0x0002 and so on. The PCM16C00's EEPROM interface circuit handles all of this data steering automatically. The entire EEPROM address space is used. Although the physical SRAM space used is the same size as the EEPROM space, the Attribute Memory space is double the size of the EEPROM. Odd-address accesses to Attribute Memory (HADDR(0) = 1) are invalid.

The PCM16C00 supports the following serial op-code instructions for the 93C series MICROWIRE EEPROM series: READ, WRITE, EWEN (Erase/Write ENable) and EWDS (Erase/Write DiSable). Since the 93C series of EEPROMs do not require a memory location to be erased before being written, the ERASE command is not supported. The ERAL (ERase AL) and WRAL (WRite AL) commands are also not used by the PCM16C00. EEPROM read sequences are initiated by a system reset (i.e., a valid high on the PCM16C00 RESET pin) or setting the Read EEPROM bit in the PCM16C00's EEPROM Control Register located at offset 0x1002. EEPROM write sequences can only be initiated by setting the Write EEPROM and Enable EEPROM bits in the EEPROM Control Register.

EEPROM PROGRAMMING METHODOLOGIES

The most efficient way to program the EEPROM is to use the PCM16C00 to write the EEPROM after the card is assembled. This is done by writing the CIS data to the SRAM and configuring the PCM16C00 Specific Registers (0x03E4 through 0x03F6) and then initiating an EEPROM write by writing the value 0x81 to the EEPROM Control Register (0x1002). This methodology allows the CIS to be written on the card during the normal single-insert card test phase.

An EEPROM write sequence may only be initiated when the PCM16C00 is configured as a memory-only interface, i.e., when neither ConfFunc bit is set in the Configuration Option Registers at offsets 0x1020 and 0x1040. When configured for memory-only interface, the PCMCIA signal IREQ is defined as RDY/BSY. The PCM16C00 will force the RDY/BSY signal low while the EEPROM is being written. The host cannot access the card while RDY/BSY is low. Most serial EEPROMs specify a maximum write cycle time of 1 ms to 10 ms per byte. For the 2k byte serial EEPROM, the total time needed to write the entire EEPROM could theoretically reach 20 seconds. In a lab setting at NSC, write times of 2 to 3 seconds were measured for the NM93C86 16k bit EEPROM in 16-bit organization mode. The EEPROM write sequence should rarely, if ever, be used by the end user.

The EEPROM could also be programmed externally, prior to assembly of the card. This requires standard EEPROM burning hardware, and requires an extra production step as compared to programming the EEPROM on the card.

CIS DATA SECURITY

At power-up, after a system reset, or at the completion of a write sequence, the PCM16C00's EEPROM controller automatically sends an EWDS (Erase/Write Disable) instruction to the EEPROM. This ensures that data stored on the EEPROM will not be destroyed during power transitions due to uncontrolled interface signals or noise on power supply lines. National Semiconductor serial EEPROMs power up in the Program Disable Mode[1]. The PCM16C00 will only generate an EWEN (Erase/Write enable) instruction when the EEPROM Write/Enable EEPROM bits (D7 and D0) in the EEPROM Control Register at offset 0x1002 are set high by host software.

The PCM16C00 EEPROM controller circuit includes another feature which will minimize the jeopardy of corrupting nonvolatile CIS data on a card due to unintentional writes to the EEPROM Write and Enable EEPROM bits in the EEPROM Control Register. The Miscellaneous Register located at offset 0x3F0 contains five bits (D4–D0) which are described as the EEPROM Start Address. They form the upper five bits of the EEPROM address at which the EEPROM controller circuit will begin writing or reading. These five bits essentially form a ''page select''. The size of the page depends on the EEPROM size selected. In order to allow the PCM16C00 registers to be stored in the EEPROM, the start address must be below the lowest PCM16C00 register (Pin Polarity Register at offset 0x3E4), but must also be as high as possible, to protect a maximum amount of CIS data. All data below this start address is write-protected.

In the case of the 2 kB EEPROM, an 11-bit address is required. With the five upper bits programmable (via the Miscellaneous Register), a start address may be formed on 64-bit boundaries anywhere in the 2k byte space. Starting at address 0x3E4, the next lower 64-bit boundary is at 0x380 (remember that attribute memory space is on even-byte boundaries). To achieve this, the value 0x07 must be programmed into the five LSBs of the Miscellaneous Register. This leaves the lower 448 bytes in the EEPROM protected from accidental overwrite. In the case of an ethernet LAN card, the Ethernet node ID (6 bytes) should be located in the lower 448 bytes of the attribute memory space, between the CISTPL__END byte and location 0x380.

In the case of the 512 byte EEPROM, a 9-bit address is required. With the five upper bits programmable (via the Miscellaneous Register), a start address may be formed on 16-bit boundaries anywhere in the 512 byte space. Starting at address 0x3E4, the next lower 16-bit boundary is at 0x3E0. To achieve this, the value 0x1F must be programmed into the five LSBs of the Miscellaneous Register. This leaves the lower 496 bytes in the EEPROM protected from accidental overwrite. In this case, the Ethernet node ID should be located in the lower 496 bytes of the attribute memory space, between the CISTPL__END byte and location 0x3E0.

The multifunction LAN/modem CIS developed at NSC contains approximately 256 bytes of data. The Ethernet ID is placed in locations 0x374 through 0x37E, so that it cannot be overwritten in either scenario.

The sequence for correctly initializing the EEPROM and write-protecting the CIS on a card is very specific. A ''blank'' serial EEPROM will contain 1's in all locations. The method for initializing the EEPROM using the PCM16C00 is to write the CIS and other data (e.g., Ethernet node ID) to the PCM16C00 attribute memory SRAM and the PCM16C00 specific registers (at offsets 0x3E4 through 0x3F6) from the host system, and the kick off an EEPROM write sequence by writing the value 0x81 to the EEPROM Control Register. In order to write the entire EEPROM (starting at address 0), the EEPROM Start Address field in the Miscellaneous Register must be 0x00. This is the value which will be stored in the EEPROM. To implement true write protection, a 2nd EEPROM write must be executed after the Start Address field is modified to its final value.

The EEPROM Control Register is located at offset 0x1002 in attribute space. Typically, the host controller will be configured to open a 4 kB attribute memory window, which must, per the PCMCIA standard, start on a 4k boundary. This means that in order for the Card Services to be able to access the PCM16C00 configuration registers (0x1020 thru 0x1052), a 4k window must be opened from 0x1000 to 0x2000. This window excludes the PCM16C00 specific registers, but does include the EEPROM Control Register, so if this window is left open, rogue software could inadvertently kick off an EEPROM write by writing a certain pattern to the register. The CIS data and Ethernet ID will not be affected by this write if the previously described Start Address technique is implemented.

It should be noted that the EEPROM Start Address field in the Miscellaneous Register also affects EEPROM reads which are initiated by setting the Read EEPROM bit (D6) in the EEPROM Control Register. In this case, the EEPROM Start Address field must be reset to all zeros in order to copy the entire EEPROM contents into the shadow SRAM. This is not an issue for reset-initiated EEPROM reads, since a reset clears the EEPROM Start Address field.

A secondary security feature of the PCM16C00 is the blocking of EEPROM writes when either function is configured. If the ConfFunc bit (D0) of either Configuration Option Register (located at offset 0x1020 for function 0 and offset 0x1040 for function 1) is set (high), then the PCM16C00 will not overwrite the EEPROM.

ALTERNATIVE CIS DATA SECURITY OPTIONS

The card manufacturer can program the EEPROM prior to installation on the card. This solution would allow the card manufacturer to use the 93CS series of serial EEPROMs (e.g., the NM93CS66), which have built-in write protection. The PCM16C00 does not have the capability to activate (or deactivate) this mode, making it is physically impossible for the PCM16C00 to overwrite the CIS. This eliminates the possibility of field upgrading the card's CIS, however.

The card manufacturer can use an external PROM installed in the card's external attribute space (activated by the PCM16C00's EARD# pin) for the Ethernet ID. Small PROMs exist solely for this type of application (e.g., National Semiconductor's DM74S188 32-byte TTL PROM)[2]. Their only control input is a single output enable, which would be tied to $\overline{\text{EARD}}$. The power budget of a card must be carefully considered when using this solution since these PROMs can consume 70 mA or more statically.

REFERENCES

[1] National Semiconductor Memory Databook, Application Brief 15

[2] DM74S 188 Datasheet, National Semiconductor Memory Databook

National Semiconductor Corporation
1111 West Bardin Road
Arlington, TX 76017
Tel: 1(800) 272-9959
Fax: 1(800) 737-7018

National Semiconductor Europe
Fax: (+49) 0-180-530 85 86
Email: cnjwge@tevm2.nsc.com
Deutsch Tel: (+49) 0-180-530 85 85
English Tel: (+49) 0-180-532 78 32
Français Tel: (+49) 0-180-532 93 58
Italiano Tel: (+49) 0-180-534 16 80

National Semiconductor Hong Kong Ltd.
13th Floor, Straight Block,
Ocean Centre, 5 Canton Rd.
Tsimshatsui, Kowloon
Hong Kong
Tel: (852) 2737-1600
Fax: (852) 2736-9960

National Semiconductor Japan Ltd.
Tel: 81-043-299-2309
Fax: 81-043-299-2408