Parallel EEPROM Data Protection

Advantages of EEPROMs

EEPROMs provide the memory solution wherever reprogrammable, nonvolatile memory is required. They are easy to use, requiring little or no support hardware such as refresh clocks or batteries. Each memory location can be selectively changed without impact on any other location; blanket erasure and rewriting of the entire device or a large section of it is not required.

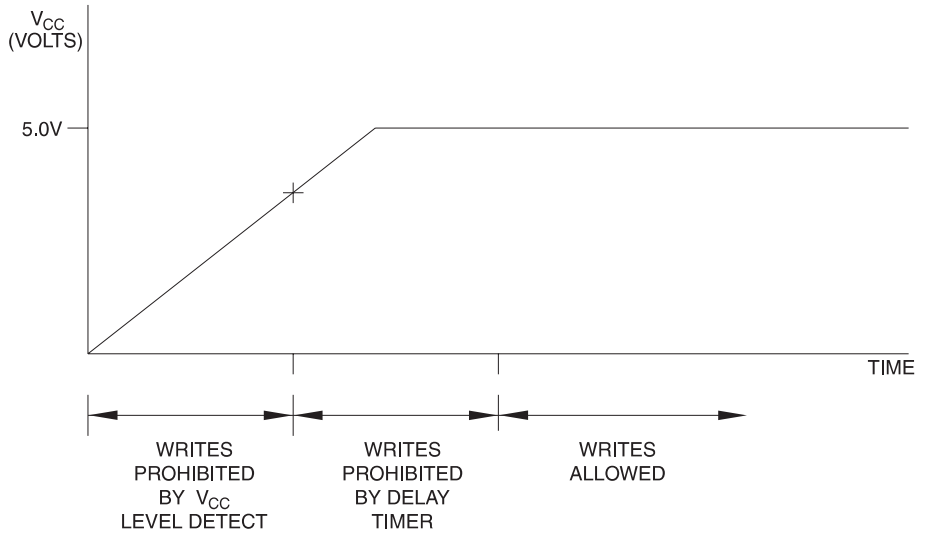
EEPROMs made at Atmel were designed to provide the best features available. Atmel EEPROMs provide high speed read access times so that many applications can use them without inserting costly wait states. The page mode write operation of Atmel EEPROMs allows for the fastest effective write time available in EEPROM memories. Since all of Atmel's devices are made in CMOS, they offer the benefits of low operating and standby power.

In order to take advantage of all of the benefits of Atmel EEPROMs, care must be taken to maintain the integrity of the data. While an EEPROM will retain its data for many years with or without power applied, improper operation of the device could result in data being inadvertently rewritten.

When is Data Susceptible to Corruption

In the use of any memory device, it is expected that the data stored in it is available as it is written. This is especially true of EEPROMs since their code often controls the operation of the system in which they are contained. Unlike most other memory types that are rewritten in systems, EEPROMs are often expected to retain their data for a period of many years, with or without power applied and during power transitions. For these reasons, added attention is given to avoid corrupting data in EEPROMs.

Figure 1. Hardware Data Protection - Power Level Sense Detector and Power On Delay Timer



Parallel EEPROMs

Application Note

Rev. 0543C–10/98

There are a number of situations in which data is particularly prone to corruption. These situations include powering on and off of the devices, noise spikes on the control lines and system glitches. Atmel EEPROMs include features to help protect against each of these potential sources of inadvertent writes. Atmel data protection features are broken down into two different types: hardware data protection features and software data protection features.

Atmel Hardware Data Protection Features

Atmel EEPROMs include four different types of hardware data protection. These features provide protection against most inadvertent writes that might occur in a system. Atmel hardware data protection features include: three line write control, power level sense detector, power on delay timer and noise filters on $\overline{CE}$ and $\overline{WE}$.

THREE-LINE WRITE CONTROL: In order to write a device the $\overline{OE}$ signal must be high with the $\overline{CE}$ and $\overline{WE}$ signals low. Holding any of the three lines in the opposite state will prohibit a write cycle. For example, whenever the $\overline{OE}$ signal is low, a write to the device cannot be started.

POWER LEVEL SENSE DETECTOR: An active circuit in Atmel EEPROMs monitors the level of the supply voltage to the device. If the supply is below 3.8 volts, typical, write cycles to the devices can not be activated.

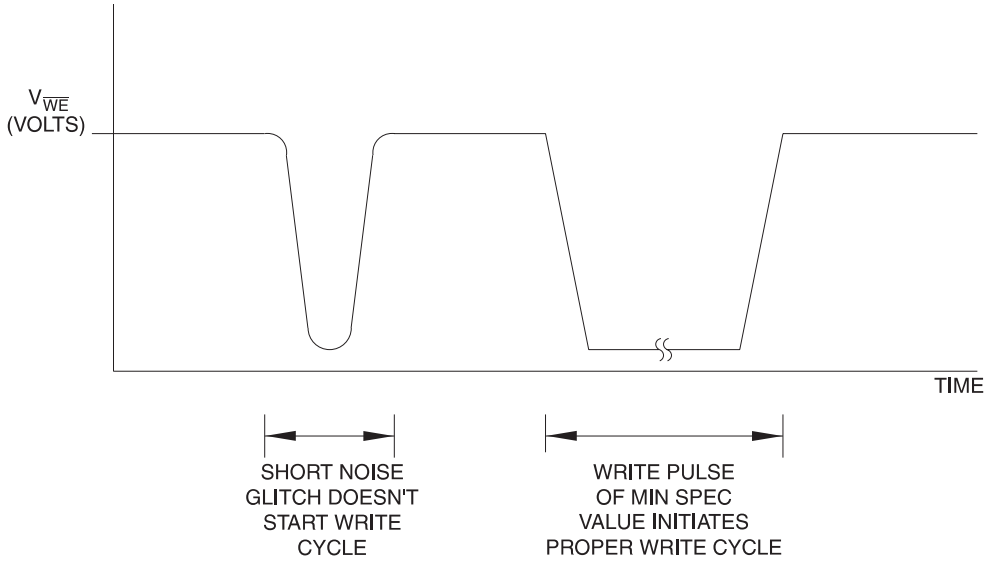
POWER ON DELAY TIMER: As power is applied to Atmel EEPROMs, the power level sense detector will issue an internal signal that indicates that the supply is above the sense level. At this time an internal timer is initiated that times out in typically 5 ms. During this time period, writes to the device cannot be performed. This delay period serves two purposes. First, it allows the supply level additional time to rise to within the standard operating region before writes are permitted. Secondly, it lets the system stabilize and present the correct levels to the control pins of the EEPROM so that the EEPROM doesn't react to its inputs before they are actually valid. Figure 1 shows the combined action of the power supply level detector and the delay timer upon writes to the device.

NOISE FILTERS ON $\overline{WE}$ AND $\overline{CE}$: If brief noise pulses below V_{IH} occur on the $\overline{WE}$ or $\overline{CE}$ inputs to the device, a write cycle will not be initiated. Internal to the EEPROM, a noise filter does not allow the short pulses to activate a write cycle. As shown in Figure 2, write pulses of sufficient length will still initiate writes but short noise spikes on the $\overline{WE}$ or $\overline{CE}$ control lines will not.

Atmel Software Data Protection Feature

Available on some Atmel EEPROMs is a user selectable feature that requires a software sequence at the beginning of each write cycle in order for a write to be performed. To enable the software data protection feature, a series of three-write commands to specific addresses with specific data must be performed. Once set, the same 3-byte code must begin each write request. (A separate write cycle to enable the software feature is not necessary; after any write that is preceded with the 3-byte code, the software data protection function will be enabled, see Figure 3.) The feature may be disabled by issuing a 6-byte code to the device as shown in Figure 4. After being set, the software data protection feature remains active until its disable command is issued. Power transitions will not reset the software data protection feature, but the feature will prevent against inadvertent writes during power transitions.

Figure 2. Hardware Data Protection - Noise Filter



The software data protection feature protects data against various causes of inadvertent writes. Since it is active during power transitions it protects data when powering on or off the device. Noise spikes that occur on the control lines will be ignored since they will not show the correct address and data needed to start a write cycle. Even for system malfunctions, such as when write pulses of adequate length are given to the device, the software feature can prevent the corruption of the data in the EEPROM. The address locations used for the software code are not sacrificed from the usable memory array. The device recognizes the software code and does not alter the data stored at the address locations of the code. Byte locations of code are still usable, and don't have to be rewritten.

System Design Considerations

Designing systems with data integrity in mind can greatly reduce the chance of lost data. The amount of attention needed depends upon the nature of the design. Following are a few areas that might need special attention in certain designs.

External Power On Protection

Many systems will have a PON (power on) signal to control the operation of the system. Such a signal can be gated with the logic creating the $\overline{OE}$ signal to the EEPROM, holding $\overline{OE}$ low when the PON signal is false. Similarly, a PON-type signal could be gated with the $\overline{WE}$ or $\overline{CE}$ logic, forcing $\overline{WE}$ or $\overline{CE}$ high when writes should not be allowed.

If the system does not include a PON-type signal, one can be created from various programmable voltage reference devices. With such a device, the user can select the voltage supply level below which the device cannot be written. It should be noted that in many systems, using Atmel's EEPROMS with their internal power level detection and power delay timer, no additional power on circuitry is required for the device.

Multiple Power Supplies

In systems that utilize more than one power supply, extra care must be taken during power transitions to both the EEPROM and the devices controlling the inputs to the EEPROM. Power on rates of the different supplies are likely to vary. Using programmable voltage reference devices to detect the power level of both supplies and forcing the $\overline{OE}$ pin low when either line is below the desired level may be used in such situations to avoid inadvertent writes.

Memory Cards

Since memory cards are often pushed into and pulled out of systems that are already powered on, they have additional chances of inadvertent writes. If the edge connector is arranged such that power and control lines are not asserted in a prescribed manner, false writes to the device may occasionally occur depending upon how the card is inserted. To provide proper power on sequencing, a card could be designed with its control pins recessed from the edge of the card. Resistors would be placed on the card to connect $\overline{CE}$ and $\overline{WE}$ to V_{CC} and $\overline{OE}$ to ground. This arrangement insures that power is first applied to the device and that the control pins are not in the write state until each pin is being controlled by the host system. Variations of this technique may be used effectively in different systems; the basic idea is to guarantee systematic application of the power and control pins such that a write state is not entered upon insertion or removal of the card from the host.

Figure 3. Software Data Protection - Enable

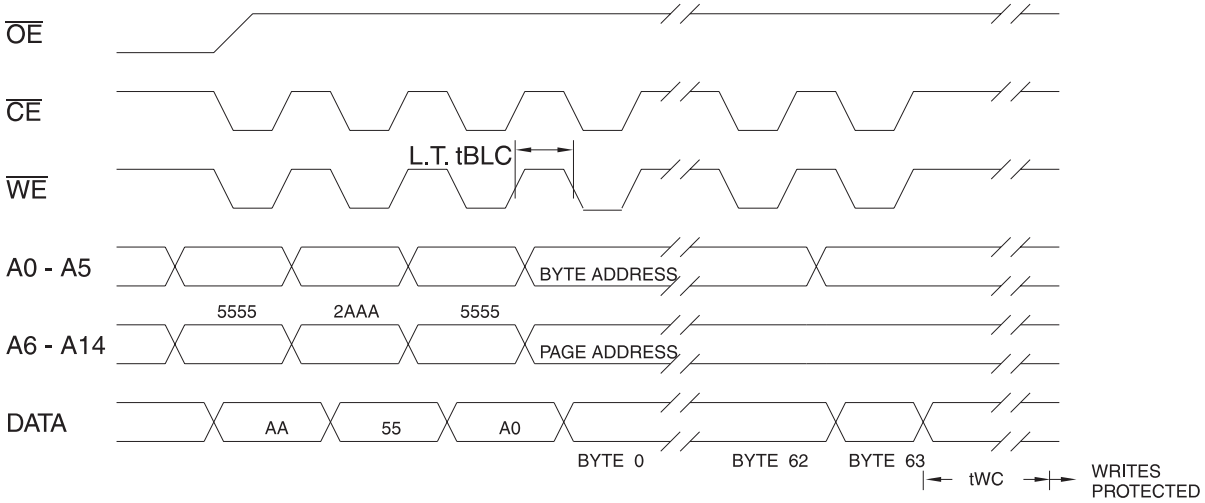
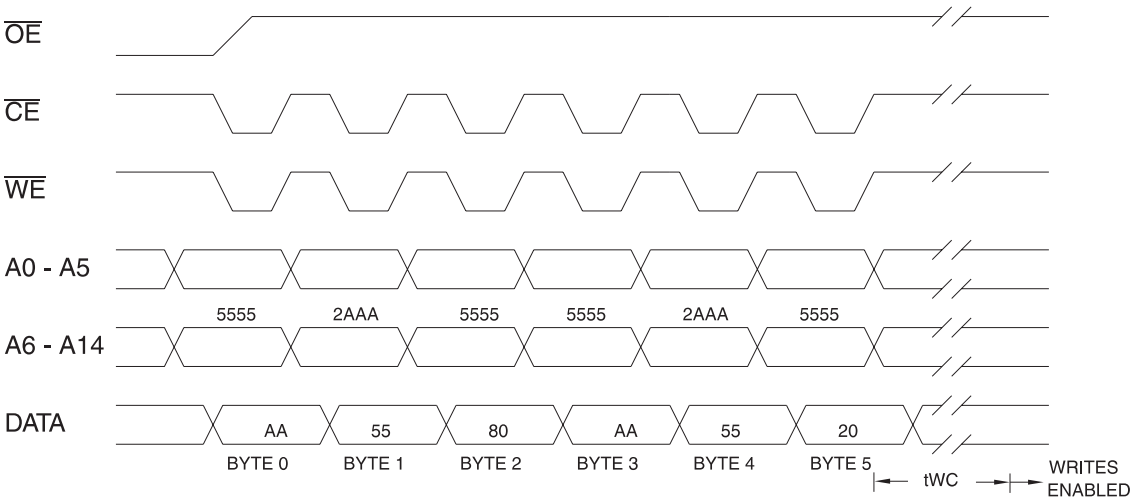


Figure 4. Software Data Protection - Disable



Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel U.K., Ltd.
Coliseum Business Centre
Riverside Way
Camberley, Surrey GU15 3YL
England
TEL (44) 1276-686677
FAX (44) 1276-686697

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road
Tsimshatsui East
Kowloon, Hong Kong
TEL (852) 27219778
FAX (852) 27221369

Japan
Atmel Japan K.K.
Tonetsu Shinkawa Bldg., 9F
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4 42 53 60 00
FAX (33) 4 42 53 60 01

Fax-on-Demand
North America:
1-(800) 292-8635

International:
1-(408) 441-0732

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

BBS
1-(408) 436-4309

0543C–10/98/xM