Maintaining Data Integrity in EEPROM's

Ed Patnaude, Sr. Applications Engineer
Maxwell Technologies Inc., 9244 Balboa Ave., San Diego, Ca 92123

Abstract

Introduction

Data corruption is a major concern in applications that rely on nonvolatile memory for long-term data storage. Even with the hardware and software protection techniques that are incorporated into memory devices, data corruption is still a possibility.

When analyzing data corruption probabilities in nonvolatile memories, the question should not be if it would occur, but what to do when it occurs. By implementing proper data protection techniques, both in hardware and in software, the chances of data corruption occurring can be greatly reduced. With the addition of error detection, data correction and data recovery circuitry, the risk of system failure due to data corruption in a non-volatile memory device can be minimized.

There are a number of ways that memories can be made nonvolatile. SRAM's can be made nonvolatile with the use of battery back-up circuitry. PROM's, in which a fuse is blown at the time of programming, are nonvolatile, however these devices are only available in low densities. The most accepted nonvolatile memories are the re-writable EEPROM and the block re-writable Flash EEPROM. This paper will address maintaining data integrity in EEPROM's, although many of the design concepts relate to all nonvolatile memories.

A typical EEPROM is implemented in a floating gate technology. A data bit is programmed into the memory cell by charging or discharging a transistor's gate. An insolating material, which encapsulates the transistor's gate, prevents the charge from leaking off. EEPROMs can retain data for over ten years in both the powered and un-powered state.

In today's systems EEPROM's are quite often used to store program code or operational parameters. They are programmed once and expected to retain data for the life of the application, whether the device is powered or not. Loss of data or data corruption can lead to system failure. It is important that designers understand the sources of data corruption and implement software and hardware schemes to protect against it.

Source of Data Corruption

The number one cause of data corruption in nonvolatile memories is software bugs. Errors in the software can lead to unwanted erase/write cycles, violation of timing parameters resulting in wrong data being written or data being written to the wrong location, and interruption in programming cycles.

In EEPROM's, exceeding the devices guaranteed erase/write cycles will eventually burn through the memory cell's gate insulation, causing permanent damage and resulting in the inability of the memory cell to retain programmed data.

Impurities in the semiconductor materials can provide leakage paths from the memory cells resulting in shorter than expected data retention times.

When a power failure occurs while a write cycle is in progress, and it is not allowed to complete, data written to the EEPROM must be considered corrupted.

EEPROM's are most prone to data corruption during power on and off. If hardware protection is not properly implemented,

unintentional writes, due to noise or uncontrolled logic levels on the device's control lines, can result in inadvertent writes.

Protecting EEPROM's from data corruption

EEPROM manufactures can implement testing that will screen out devices containing impurities in the semiconductor structure, which can lead to premature data retention failures.

EEPROM's provide the designer both hardware and software data protection. Proper use of these features will minimize the risk of data corruption occurring.

In addition to hardware and software protection, other steps can be taken to assure data integrity. Careful power supply design, error detection and correction techniques, and power supervisory circuits should all be used to maintain data integrity in the EEPROM's.

Software Data Protection

Software Data Protection (SDP) locks the memory preventing unintentional erase/writes from occurring. Once SDP is enabled a three-byte password is written into memory, temporarily unlocking it, followed by the data that is to be programmed. Once the data is written and the programming cycle completes, SDP is again enabled.

Software Data Protection may not protect stored data when the device falls below the guaranteed operating voltage of the EEPROM. Hardware write protection must be implemented to assure data integrity.

Hardware Data Protection

An EEPROM is most susceptible to data corruption during power on and off. Although these devices can internally operate to below 2 volts, functionality cannot be expected. During power cycling it is imperative that the memory content be protected by the proper implementation of the hardware protection built into the EEPROM.

Many EEPROM's contain noise filters on the /CE and /WE inputs which keep short voltage spikes, that fall below the devices input low threshold, from triggering an inadvertent write.

Maintaining Data Integrity

If a controlled power cycle is required, the EEPROM supply voltage should be taken all the way to zero volts and not let to sit at some ambiguous voltage where it may be vulnerable to an inadvertent write.

The use of error detection and correction circuitry (EDAC) can be used to maintain data integrity.

To improve data retention time, typically greater than ten years, reprogramming the EEPROM periodically will recharge the memory cells which will greatly increase a devices data retention time.

If a write cycle is in progress, and the EEPROM is powered off without letting it complete, data that has been written must be considered invalid. To avoid this from happening the voltage supply should be designed so that the voltage fall slow enough that the write cycle has time completes before the level drops below the lowest specified operating voltage of the EEPROM.

Power supply supervisory circuitry should be used to control the state of the EEPROM during power on and off. When a power loss is sensed, all further writes should be halted.

Summary

EEPROM's are today's choice for non-volatile memories. They are mainly used to store program code and system parameters. Unlike other memory types, which are continuously re-written, EEPROMs are normally programmed once and are expected to retain that data for years to come.

With today's manufacturing and screening processes, having a EEPROM fail prematurely, under normal operating conditions, is very unlikely.

A robust hardware and software design, along with a contingency plan should corruption occur, can greatly minimized the risk of system failure due to data corruption in a EEPROM.