DISABLING FLASH WRITE PROTECTION

This document provides information on disabling flash memory write protection so that the Processor-Controlled Test (PCT) Flash Programming interface can be used to erase and re-program the memory. There are many methods used by different manufacturers to write protect flash memory, so this document should be used in conjunction with flash memory datasheets and board schematics.

There are three basic types of write protection:

- Circuitry external to the flash
- Software Write protection (by a controlling device)
- Write protection within the flash

The first step is to identify what mechanism is being used to protect the flash. The flash datasheet will indicate whether there is a Write Protect pin as well as a Write Enable pin. Locate these pins on the board schematics and follow traces back to identify the controlling mechanism. This could be a CPLD, logic gates, link, etc.

If the controlling device is a CPLD, check whether this is on a bus that will allow the processor to control the relevant I/O pins. If not, there may be some external switches or links for manual switching.

EXTERNAL CIRCUITRY

Examples of methods used to write protect flash by external means include:

- Changing the logic level of pins on the flash by writing appropriate values to registers in the flash controller or by switching logic gates. Relevant pins may be Write Protect and/or Write Enable.
- Removable links (jumpers)
- Switching a higher than normal voltage through to specific pins on the flash (e.g. 12 volts).

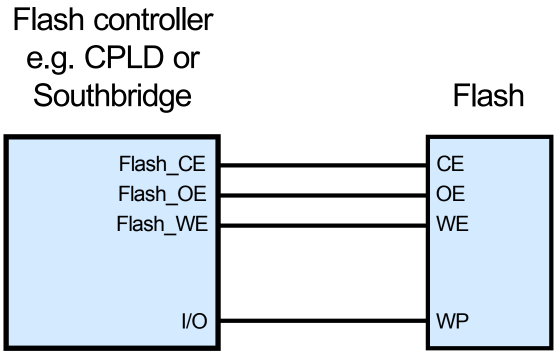

Diagram 1. Write Protect controlled by CPDL

Diagram 1 shows a flash device that has both Write Enable and Write Protect pins. Write protection is handled by an I/O port on the CPLD. The logic level of the Write Protect pin is controlled by writing the appropriate values to the CPLD I/O register.

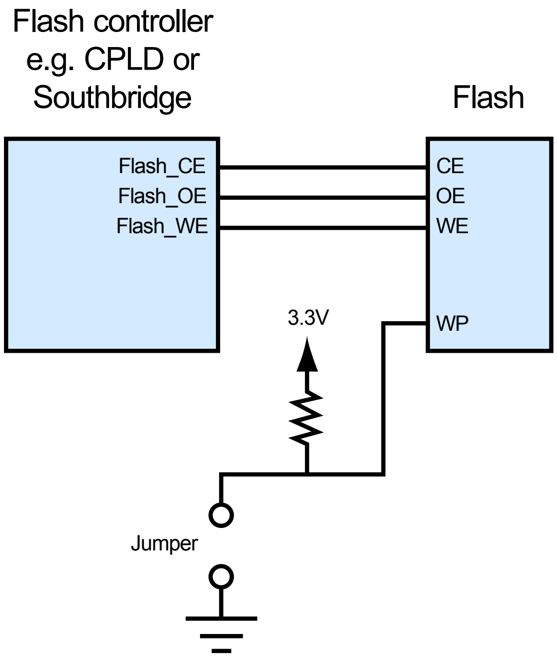

Diagram 2. Write Protect controlled by link

In Diagram 2 a link manually disables the Write Protect line: WP is pulled low to disable it. In the case of active-low WP#, it would be pulled high to disable protection.

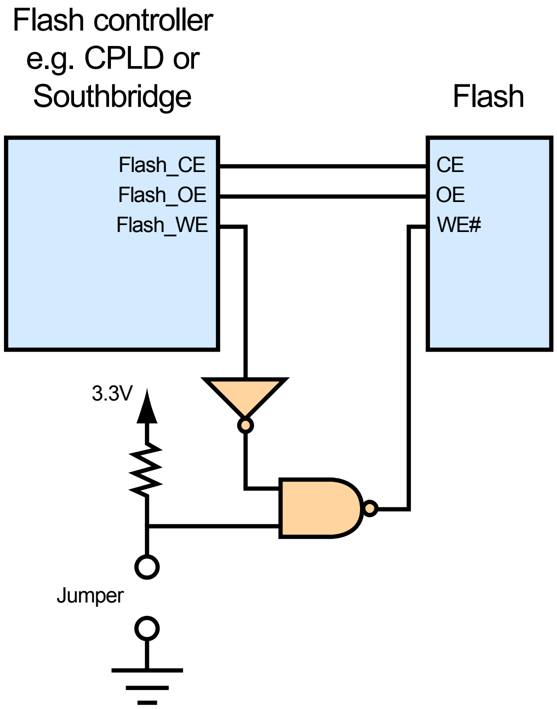

Diagram 3. Write Enable controlled by link

In diagram 3, the flash does not have a Write Protect pin. Logic gates are used to allow write protection by means of a link. When the link is open WE# follows Flash_WE so there is no write protection. When the link is closed, WE# is held high, preventing writes.

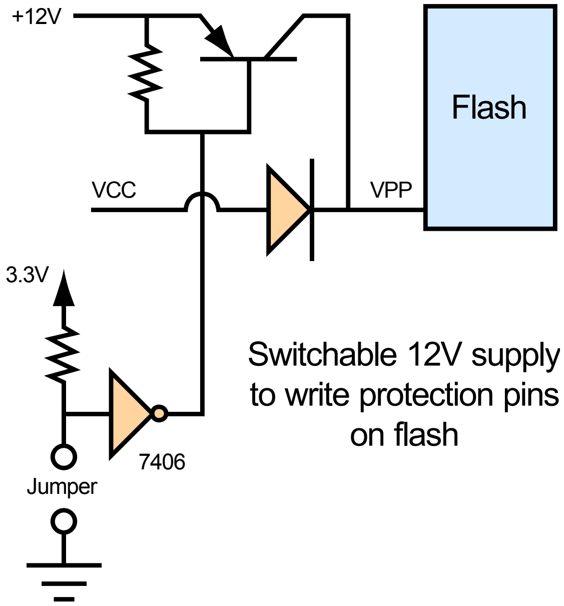

Diagram 4. Increased voltage to specific pins

Some flash devices require an increased voltage to be applied to specific pins in order to disable write protection. Diagram 4 shows circuitry that applies a 12V supply to pins on the flash device when the link is closed.

Internal Write Protection

The various internal methods used to write protect flash memory include:

- Sector locking. This is reversible using the appropriate unlock command sequence. Attempts to program locked sectors will fail. These can be unlocked prior to Flash Programming by writing an appropriate PCT TSL/1 script. Some flash devices provide a command sequence to temporarily unlock sectors. Device datasheets give all the required command sequences.
- Secured silicon sector protection (one write only is possible, either by the device manufacturer or board manufacturer. These sectors can’t be re-written.
- Temporary write protection on all sectors is often automatically applied when voltage levels are not normal, e.g. during board boot. This should not be an issue during PCT Flash Programming

This is only a sample of some of the methods used to write protect flash devices. Datasheets for both the flash and the board are clearly necessary to find out how to disable the protection.

SOFTWARE WRITE PROTECTION

Most Flash devices have a controlling device. In the case of Intel® platforms, the controlling device could be the Platform Controller Hub (PCH). In the case of Freescale® platforms, the controller device can be the processor. As the Flash device is a 'downstream' device of the controller, the designer may implement a software lock mechanism. The various internal methods used to write protect flash include:

- Disable Flash Write Signal. The controller may accept Flash commands from the processor, but may block the actual write signal from appearing on the bus. This has the same effect as the hardware write protect explained previously. This is reversible by using the appropriate register write in the controller to disable the blocking of the write signal.

- Disable Write Signal for a Memory Range. This is a preferred method of BIOS/Firmware engineers to stop accidental programming of a Flash device. The Flash device is mapped to the memory space of the processor it is connected to. This memory range can be locked from write access by changing registers within the controller. Therefore, if a sequence to write to the Flash devices is intercepted, the controller will stop the Write Enable signal again based on the write protect memory range. This is reversible by using the appropriate register write in the controller to enable the memory range for write access.

ASSET CONTACTS:

Please contact your ScanWorks sales representative for more information.

ASSET InterTech, Inc.
2201 N. Central Expy., Ste 105
Richardson, TX 75080
+1 888 694-6250 or +1 972 437-2800
http://www.asset-intertech.com